UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO
FACULTAD DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA, INFORMÁTICA Y MECÁNICA
ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

TESIS

PROPUESTA DE IMPLEMENTACIÓN DE LA NTP-ISO/IEC 27005:2018 APLICANDO LA METODOLOGÍA MAGERIT PARA EL ÁREA FUNCIONAL DE INFORMÁTICA Y TELECOMUNICACIONES DE LA DIRECCIÓN DESCONCENTRADA DE CULTURA DE CUSCO

PRESENTADO POR:

Br. ALEXANDER PAVEL IBARRA HUAMAN
Br. SHAROM MITCHEL NOLAZCO SANDOVAL

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO INFORMÁTICO Y DE SISTEMAS

ASESOR:
Dr. EMILIO PALOMINO OLIVERA

CUSCO – PERÚ
2024

INFORME DE ORIGINALIDAD

(Aprobado por Resolución Nro.CU-303-2020-UNSAAC)

El que suscribe, **Asesor** del trabajo de investigación/tesis titulada: "Propuesta de Implementación de la NTP-ISO/IEC 27005:2018 aplicando la metodología MAGERIT para el Área Funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco

presentado por: Alexander Pavel Ibarra Huaman con DNI Nro.: 70396576 presentado por: Sharon Michel Nolazco Sandoval con DNI Nro.: 72196065 para optar el título profesional/grado académico de Ingeniero Informático y de Sistemas

Informo que el trabajo de investigación ha sido sometido a revisión por 2 veces, mediante el Software Antiplagio, conforme al Art. 6° del ***Reglamento para Uso de Sistema Antiplagio de la UNSAAC*** y de la evaluación de originalidad se tiene un porcentaje de 5 %.

Evaluación y acciones del reporte de coincidencia para trabajos de investigación conducentes a grado académico o título profesional, tesis

Porcentaje	Evaluación y Acciones	Marque con una (X)
Del 1 al 10%	No se considera plagio.	X
Del 11 al 30 %	Devolver al usuario para las correcciones.	
Mayor a 31%	El responsable de la revisión del documento emite un informe al inmediato jerárquico, quien a su vez eleva el informe a la autoridad académica para que tome las acciones correspondientes. Sin perjuicio de las sanciones administrativas que correspondan de acuerdo a Ley.	

Por tanto, en mi condición de asesor, firmo el presente informe en señal de conformidad y **adjunto** la primera página del reporte del Sistema Antiplagio.

Cusco, 01 de Julio de 2024

Firma

Post firma: Emilio Paolino Olivera

Nro. de DNI: 23860669

ORCID del Asesor: 0000-0001-8663-3737

Se adjunta:

1. Reporte generado por el Sistema Antiplagio.
2. Enlace del Reporte Generado por el Sistema Antiplagio: **oid:** 27259:343148738

NOMBRE DEL TRABAJO
tesis final_Pavel y Sharon.docx

AUTOR
Pavel_Sharon Ibarra_Nolasco

RECUENTO DE PALABRAS
52470 Words

RECUENTO DE CARACTERES
296828 Characters

RECUENTO DE PÁGINAS
480 Pages

TAMAÑO DEL ARCHIVO
22.4MB

FECHA DE ENTREGA
Mar 28, 2024 10:20 PM GMT-5

FECHA DEL INFORME
Mar 28, 2024 10:26 PM GMT-5

5% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 0% Base de datos de Internet
- 0% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 5% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 10 palabras)
- Fuentes excluidas manualmente
- Bloques de texto excluidos manualmente

Dedicatorias

Dedico esta tesis a mi papá Reynaldo Ibarra Callañaupa, por su inquebrantable guía y sabiduría, y por ser siempre un ejemplo de fortaleza y dedicación.

A mi mamá María Huaman Gutiérrez, cuyo amor y apoyo incondicionales me han dado la fuerza para seguir adelante, incluso en los momentos más difíciles.

A mi hermano Anatoli Plinio Ibarra Huaman, por ser una fuente constante de alegría y por recordarme siempre la importancia de los sueños y la perseverancia.

A mi enamorada y amigos por su paciencia, y apoyo constante a lo largo de esta etapa de mi vida universitaria.

Bach. Alexander Pavel Ibarra Huaman

Dedico esta tesis a mis padres; Faustina Sandoval Salvador y Carlos Nolazco Manco quienes me enseñaron el valor del conocimiento y el esfuerzo. En especial a mi madre por su apoyo incondicional a lo largo de este camino.

A mis hermanos por estar siempre ahí, por entender mis ausencias y por celebrar cada pequeño avance conmigo.

A mi enamorado y amigos por su paciencia, comprensión y apoyo constante a lo largo de este arduo pero gratificante camino académico.

Bach. Sharom Mitchel Nolazco Sandoval

Agradecimientos

Queremos dedicar un especial agradecimiento a nuestras familias, quienes han sido nuestra roca durante este desafiante proyecto de investigación. A nuestros padres y madres, por su inquebrantable apoyo, por su fe en nuestras capacidades y por ser nuestra guía en los momentos de duda.

Queremos expresar nuestra profunda gratitud a nuestro asesor de tesis Dr. Emilio Palomino Olivera por su orientación experta y paciencia durante todo el proceso de investigación.

Al Ing. Jisbaj Gamarra Salas por sus consejos y sugerencias fueron fundamentales para la realización de este proyecto de investigación.

A nuestra querida alma mater: Universidad Nacional de San Antonio Abad del Cusco, por brindarnos la oportunidad de crecer y desarrollarnos académicamente a lo largo de todos estos años de estudios.

Bach. Alexander Pavel Ibarra Huaman y Bach. Sharom Mitchel Nolazco Sandoval

Resumen

Hoy en día, es muy importante priorizar la información para cualquier organismo u organización. Entre estos actores, los sistemas de información, los procesos y la tecnología de la información son activos muy importantes. Se debe garantizar la confidencialidad, disponibilidad e integridad de la información para mantener el cumplimiento.

La Dirección Desconcentrada de Cultura de Cusco (DDC) actualmente no cuenta con un plan de seguridad informática, ya que dicho plan es de tal importancia para la seguridad de la información y equipos informáticos pertenecientes a la institución antes mencionada.

Para el desarrollo de la propuesta se realizó un análisis de la situación actual de la Dirección Desconcentrada de Cultura de Cusco mediante una entrevista realizada al director y encuestas al personal y trabajadores del Área Funcional de Informática y Telecomunicaciones, lo que nos ayudó a tener una visión de la protección que se les da a los datos de la institución y al manejo y mantenimiento de los equipos informáticos.

Luego del análisis se procedió a elaborar la propuesta de implementación de la NTP-ISO/IEC 27005:2018 aplicando la metodología MAGERIT, para el Área Funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco en las sedes ubicadas en Av. La Cultura 238 Condominio Huáscar y Calle Saphy N° 723, que permitirá reducir el impacto de los riesgos a nivel físico, lógico y organizacional.

Palabras claves: activos, riesgos, MAGERIT, seguridad.

Abstract

Nowadays, it is crucial to prioritize information for any entity or organization. Among these actors, information systems, processes, and information technology are very important assets. Ensuring the confidentiality, availability, and integrity of information is essential to maintain compliance.

The Dirección Desconcentrada de Cultura de Cusco (DDC) currently lacks an information security plan, as such a plan is of paramount importance for the security of information and computer equipment belonging to the aforementioned institution.

For the development of the proposal, an analysis of the current situation of the Dirección Desconcentrada de Cultura de Cusco was conducted through an interview with the director and surveys of the personnel and workers of the Área Funcional de Informática y Telecomunicaciones. This helped us gain insight into the protection given to the institution's data and the management and maintenance of computer equipment.

After the analysis, the proposal for the implementation of NTP-ISO/IEC 27005:2018 was prepared, applying the MAGERIT methodology, for the Área Funcional de Informática y Telecomunicaciones of the Dirección Desconcentrada de Cultura de Cusco at the locations on Av. La Cultura 238 Condominio Huáscar and Calle Saphy No. 723. This will reduce the impact of risks at the physical, logical, and organizational levels.

Keywords: assets, risks, MAGERIT, security.

Introducción

En el dinámico panorama actual, donde la gestión eficaz de la seguridad de la información es esencial, se hace imperativo comprender y abordar los riesgos de manera integral. Este proyecto de tesis se sumerge en un proceso estructurado que sirve como cimiento para la robustez y la resiliencia del entorno organizativo de la Dirección Desconcentrada de Cultura de Cusco.

Se desarrollará una propuesta de implementación de la NTP-ISO/IEC 27005:2018 aplicando la metodología MAGERIT para el Área Funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco, en el cual inicialmente se hará un análisis del Área Funcional de Informática y Telecomunicaciones para poder identificar las debilidades y amenazas en temas de seguridad de la información. Posteriormente se va a elaborar salvaguardas, políticas y proponer planes de acción evaluando los riegos de seguridad informática.

A través de este proyecto de tesis, se busca proporcionar una visión clara de los pasos cruciales en la gestión de riesgos de seguridad de la información, estableciendo un fundamento sólido para la toma de decisiones informadas y la protección continua de los activos organizativos de la Dirección Desconcentrada de Cultura de Cusco

INDICE

INDICE DE IMÁGENES

INDICE DE TABLAS

ANEXOS

Capítulo I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción del problema

El Área Funcional de Informática y Telecomunicaciones desempeña diversas responsabilidades, incluyendo la gestión y soporte de hardware, software, bases de datos y redes para las distintas áreas de la Dirección Desconcentrada de Cultura de Cusco.

Sin embargo, es importante destacar que actualmente, esta área no tiene implementado una norma para una adecuada gestión de riesgos de seguridad de la información, ni políticas para el manejo y cuidado de los sistemas de información, donde tampoco se tienen identificados sus activos por lo tanto no cuentan con medidas de seguridad para proteger sus activos ante cualquier tipo de amenaza.

Es esencial que el área de Informática y Telecomunicaciones satisfaga los requisitos estipulados por el gobierno para la implementación de dicha norma. Esto permitirá la evaluación, mitigación y clasificación de los riesgos, amenazas y vulnerabilidades que puedan surgir en la institución.

1.2. Formulación del problema

En base a la descripción del problema del Área Funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco planteamos la siguiente pregunta:

¿Es posible implementar la NTP-ISO/IEC 27005:2018 aplicando la metodología MAGERIT para proteger los activos de información para el Área Funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco?

1.3. Nombre de la investigación

"Propuesta de implementación de la NTP-ISO/IEC 27005:2018 aplicando la metodología MAGERIT para el Área Funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco"

1.4. Antecedentes de la investigación

Título: "Propuesta de un marco de trabajo para la cláusula de adquisición, desarrollo y mantenimiento de sistemas de la ISO/IEC 27002: 2013 "Código de buenas prácticas para la gestión de seguridad de la información" para la oficina de tecnologías de la información y comunicaciones de la EPS. SEDACUSCO S. A."

Autor: Gonzalez Auccapuri Fanny

Universidad: Universidad Nacional de San Antonio Abad del Cusco

Año: 2016

Resumen:

Este trabajo de tesis propone diseñar un marco de términos de adquisición, desarrollo y mantenimiento del sistema según el enfoque de la norma ISO 27002:2013 también conocida como "Buenas prácticas para la gestión de la seguridad de la información" para EPS. SEDACUSCO S.A. Esta propuesta está destinada a cumplir con los requisitos de la organización para la seguridad de la información. El objetivo del trabajo es analizar la situación actual de la empresa y a través de ello diseñar un marco de condiciones de adquisición, desarrollo y mantenimiento de sistemas según el enfoque de la norma ISO/IEC 27002:2013 también conocida como "Código de buenas prácticas sobre gestión de seguridad de la información para EPS SEDACUSCO S.A. demuestra que a través de su desarrollo mejorará las pautas de seguridad de la información y logrará un alto nivel de seguridad para los activos de información empresarial.

Conclusiones:

a. En esta tesis se han recolectado datos, documentos e información de los procesos informáticos de EPS SEDACUSCO S.A., actividades a través de las cuales se puede determinar información sobre el estado actual de los procesos de adquisición, desarrollo y mantenimiento de sistemas en la oficina de tecnologías de la información y comunicaciones.
b. De acuerdo con las observaciones empíricas y la información proporcionada por la oficina de tecnologías de la información y comunicaciones de la EPS SEDACUSCO, los datos de los procesos de pago han sido identificados como el activo de información más importante de la EPS SEDACUSCO S.A.
c. Se puede plantear una propuesta marco para la adquisición, desarrollo y mantenimiento del sistema ISO/IEC 27002:2013, para esto se desarrollaron secuencias de actividades,

diagramas de procesos del negocio y documentación para cada control de la cláusula objeto de estudio para su utilización en la OTIC. En el desarrollo de la propuesta se siguieron los lineamientos y reglas de la ISO/IEC 27002.

d. Dada la situación actual de OTIC en relación con los términos de adquisición, desarrollo y mantenimiento de los sistemas, el marco propuesto sugiere un cambio del enfoque tradicional hacia un enfoque más seguro de los sistemas de información según ISO/IEC 27002:2013 listas y controles para la adquisición, desarrollo y mantenimiento del sistema.
e. Se realizó la implementación de un sistema de información denominado "El sistema de uso del Código de Buenas Prácticas en la Gestión de la Seguridad de la Información" para la oficina de tecnologías de la información y comunicaciones de la EPS SEDACUSCO S.A., a través del cual se podrá finalizar los documentos establecidos en la propuesta y facilitar el desempeño de la misma organización.

Título: "DISEÑO DEL PLAN DE SEGURIDAD INFORMÁTICA BASADO EN LA NTP ISO/IEC 27001:2014 PARA LA MUNICIPALIDAD DEL CENTRO POBLADO DE SALCEDO - PUNO"

Autor: Camapaza Quispe Abdon Anders

Universidad: Universidad Andina del cusco

Año: 2019

Resumen:

En el Perú, cada organismo público está obligado a implementar planes de seguridad de la información o sistemas de gestión de seguridad de la información que permitan preservar las dimensiones de confidencialidad, integridad y disponibilidad de la información, con base en la norma técnica peruana NTP ISO/IEC 27001:2014,pero por diversas razones y circunstancias esto no sucedió, aduciendo falta de presupuesto, falta de conocimiento, falta de personal capacitado para hacerlo, consultorías de seguridad muy costosas, etc. Razón por la cual los organismos estatales no cumplen con la implementación de sus planes para garantizar la seguridad de la información. Es el caso del municipio en el centro poblado de Salcedo Puno, donde existe un desconocimiento, no se tuvo un plan de corto o mediano plazo al momento de diseñar, salvo la implementación de un plan de seguridad de la información, oportunidad dinámica para impulsar esta investigación. El presente trabajo tuvo como objetivo desarrollar un plan de seguridad de la información basado en la NTP ISO/IEC 27001:2014, en el cual se

realizan diagnósticos situacionales del municipio en el centro poblado de Salcedo Puno para determinar vulnerabilidades y amenazas a la seguridad de la información. Luego se elaborará un plan de seguridad informática con el objetivo de definir los alcances del plan, definir los requisitos legales, desarrollar las políticas de seguridad y proponer el plan a la oficina administrativa y financiera del municipio en el centro poblado de Salcedo Puno. Finalmente, el plan de seguridad informática se complementará con una evaluación de los riesgos de seguridad informática para desarrollar los controles correspondientes para mitigarlos.

Conclusiones:

1. Se ha diseñado un plan de seguridad de la información basado en la NTP ISO/IEC 27001:2014, para que su aplicación minimice o mitigue el impacto de los riesgos que representan los activos de información del centro poblado de Salcedo Puno. Las políticas y controles adecuados para amenazas y riesgos son esenciales en las organizaciones de hoy. Además, en esta conclusión se aborda el compromiso de los administradores municipales del centro poblado de Salcedo Puno en la implementación de la propuesta del PSI.
2. Se analizaron las áreas funcionales del municipio en el centro poblado de Salcedo Puno, para determinar que el área de informática y procesamiento de datos se encuentra dentro del perímetro del plan de seguridad de la información, dependiendo de la oficina administrativa y financiera del municipio en el centro poblado de Salcedo Puno.
3. La evaluación de los riesgos a los que están expuestos los activos de información en el municipio del centro poblado de Salcedo Puno, se ha desarrollado teniendo en cuenta la metodología MAGERIT v.3. Esta evaluación ayuda a identificar la probabilidad de ocurrencia de un riesgo y especialmente las acciones a tomar de acuerdo a los controles mantenidos de la NTP ISO/IEC 27001:2014.
4. Considerando los riesgos identificados, se ha desarrollado un listado de controles de seguridad para mitigar los riesgos altos y medios identificados durante el diseño del Plan de Seguridad de la Información del municipio del centro poblado de Salcedo Puno.

Título: "MODELO DE GESTIÓN DE RIESGOS BASADOS EN LA NORMA ISO/IEC 27005 Y METODOLOGÍA MAGERIT PARA MEJORAR LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL HOSPITAL REGIONAL DE LAMBAYEQUE"

Autores: Puyén Santos Vicente Raúl y Rivas Palacios Betty Guiliana

Universidad: Universidad Nacional Pedro Ruiz Gallo

Año: 2018

Resumen:

Los avances en tecnología hoy en día traen riesgos asociados con la información operada por cualquier organización o agencia, pública o privada; por ello, estas organizaciones centran sus mayores esfuerzos en mantener la confidencialidad, integridad, disponibilidad, trazabilidad y credibilidad de la información que procesan bajo su control, controlan su integridad; por lo tanto, la información se considera su principal activo. Asumiendo que la información es un activo importante de las organizaciones u organizaciones, es necesario gestionar su seguridad, identificando y analizando los activos de información, identificando los activos críticos, identificando las debilidades y amenazas a estos activos críticos y recomendando controles para ayudar a reducir sus riesgos. El uso apropiado de los modelos de gestión de riesgos de seguridad de la información mejora una cultura de seguridad de la información en toda la organización o agencia, genera confianza en el cliente y pone su potencial y capacidades por delante de los competidores. Este estudio propone mejorar la gestión de la seguridad de la información en el hospital regional de Lambayeque, mediante la aplicación de un modelo de gestión de riesgos basado en la norma ISO 27005 y el método MAGERIT.

Conclusiones:

- El análisis realizado como parte de nuestra investigación reveló que el hospital regional de Lambayeque no cuenta con estándares, políticas o estrategias para el manejo de la seguridad de la información en sus instalaciones. El uso de un modelo de gestión de riesgos basado en la norma ISO/IEC 27005 y la metodología MAGERIT recomendada le permite cumplir con seis de los ocho lineamientos especificados en la política de seguridad de la información emitida por el Ministerio de Salud.
- De la evaluación de los expertos en seguridad de la información, se puede concluir que "el modelo de gestión de riesgos basado en la norma ISO/IEC 27005 y la metodología MAGERIT para mejorar la gestión de la seguridad de la información en el hospital regional distrito de Lambayeque", las etapas del modelo presentado son completos y

claros, coherentes y en cierta medida apropiados, por lo que es un modelo válido para realizar la gestión de riesgos y es útil para los hospitales de la región Lambayeque, por lo que este modelo puede ayudar a mejorar la seguridad de la información de la organización.

Título: "Implementación de una Metodología de Gestión de Riesgos alineada a la ISO 27005 y MAGERIT para el proceso "OSE" de una empresa de facturación electrónica en la ciudad de Lima"

Autor: Carmona Torres Leonardo Dante

Universidad: Universidad Tecnológica del Perú

Año: 2021

Resumen:

El siguiente informe examina la implementación de la gestión de riesgos de acuerdo con la norma ISO 27005 para el proceso de entorno de sistema operativo para una empresa de facturación electrónica. El primer capítulo, se presenta un árbol para que podamos identificar el problema principal, sus causas y efectos, y luego definir la meta, el alcance, los límites y la justificación del proyecto para el juicio. El segundo capítulo presenta el contexto nacional e internacional, el marco teórico utilizado en base a la norma ISO 27005 y MAGERIT, nuestro marco conceptual básico y marco metodológico. El tercer capítulo presenta el desarrollo del método según la norma ISO 27005 y MAGERIT. El cuarto capítulo presenta los resultados y la encuesta de satisfacción con la metodología, costos y beneficios.

Conclusiones:

- El resumen de clasificación e inventario de activos desarrollado permite identificar los activos más importantes de la organización, mejorando así la forma en que responde a posibles riesgos inmediatos.
- El resumen de análisis de riesgos se desarrolla para ayudar a identificar los riesgos y su gravedad para evitar su fenómeno.
- Establecer controles y planes de acción para los riesgos identificados que permitan reducirlos o llevarlos a un nivel aceptable para la organización.

1.5. Justificación

El proyecto desarrollará una propuesta de implementación de NTP-ISO/IEC 27005:2018, aplicará la metodología MAGERIT con el propósito de evaluar, mitigar y categorizar los riesgos, amenazas y vulnerabilidades de seguridad que existen en el Área Funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco.

1.6. Objetivos

1.6.1. Objetivo general

- Elaborar una propuesta de implementación de la NTP-ISO/IEC 27005:2018 aplicando la metodología MAGERIT para el Área Funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco.

1.6.2. Objetivos específicos

- Identificar y valorar los activos en el Área Funcional de Informática y Telecomunicaciones.
- Evaluar las amenazas y vulnerabilidades asociadas con los activos identificados
- Identificar los riesgos y valorarlos en función de la probabilidad de incidencia e impacto de cada amenaza.
- Identificar salvaguardas para la protección de los activos de amenazas que puedan materializarse.

1.7. Alcances

En el presente proyecto se toma en cuenta los siguientes alcances:

- En el desarrollo del proyecto se realizará un proceso de investigación cuantitativa el cual será descriptivo abarcando una descripción, registro, análisis e interpretación de la naturaleza actual, así como la comprensión de procesos y fenómenos de la realidad estudiada. Esto implica la recolección y selección de datos (investigación conceptual, observación, encuestas por medio de entrevistas y cuestionario).

- Se realizará en el Área Funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco.
- Se desarrollará la propuesta de implementación de la NTP-ISO/IEC 27005:2018 aplicando la metodología MAGERIT.

1.8. Limitaciones

En el presente proyecto se toma en cuenta las siguientes limitaciones:

- Falta de instituciones u organismos dedicados a la capacitación de la norma ISO/IEC 27005:2018 en el ámbito regional.
- Escasa bibliografía sobre la implementación de dicha norma en las entidades.
- En el ámbito geográfico de estudio se cuenta con muy pocos profesionales especializados en la implementación de dicha norma.

1.9. Metodología

La metodología que se utilizará en el presente proyecto de tesis es el método descriptivo aplicativo el cual describe con detalle un fenómeno o situación específica con el propósito de aplicar los hallazgos de manera práctica en un contexto real. Se utiliza para entender a fondo un problema o situación y luego aplicar ese conocimiento para resolver problemas, tomar decisiones informadas o diseñar intervenciones efectivas. Este método no solo busca comprender el fenómeno, sino también encontrar formas de utilizar esa comprensión para generar impacto o mejorar la situación en la práctica.

1.9.1. Técnicas de recolección de datos

El presente proyecto de tesis utilizará técnicas de recolección de datos que son los siguientes:

- **Observación**

  Nos permite ver lo que sucede en una situación real, organizando y registrando los eventos relevantes según un plan definido y según el problema que se está analizando.

- **Entrevistas**

Se realizaron entrevistas con una serie de preguntas al jefe del Área Funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco, con respecto a la situación actual de la institución y activos.

- **Encuestas**

Se realizaron formularios para el personal del Área Funcional de Informática y Telecomunicaciones y para todo el personal de la Dirección Desconcentrada de Cultura de Cusco, con el propósito de recolectar información en relación al tema a desarrollar. Dicha información servirá como soporte para datos en el desarrollo de la metodología MAGERIT.

Capítulo II. MARCO TEÓRICO

2.1. Información

"La información es un conjunto organizado de datos relevantes para uno o más sujetos que extraen de él un conocimiento, es una serie de conocimientos comunicados, compartidos o transmitidos y que constituyen por lo tanto algún tipo de mensaje. Sin embargo, su definición varía según la disciplina o el enfoque desde el cual se la piense." (Equipo editorial, Etecé, 2020)

"En informática se denomina información al conjunto de datos organizados y procesados que funcionan como mensajes, instrucciones y operaciones o cualquier otro tipo de actividad que tenga lugar en una computadora". (Significados.com, s.f.)

2.2. Seguridad

"La capacidad de las redes o sistemas de información para soportar, con cierto grado de confianza, incidentes o acciones ilegales o maliciosas que amenacen la disponibilidad, la credibilidad o la seguridad y se puede acceder a la seguridad de los datos y servicios almacenados o transmitidos que estas redes y sistemas proporcionan o realizan." (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012, p. 104)

2.3. Seguridad de la información

"Confianza en que el sistema de información está libre de daños o daños inaceptables." (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012, p. 104)

2.3.1. Objetivos de la seguridad de la información

"a) Confidencialidad: Solo está disponible para entidades u operaciones autorizadas, incluidas las medidas de seguridad para la información personal y de propiedad.

b) Disponibilidad: Garantizar el acceso y uso oportuno de la información.

c) Integridad: Asegúrese de que la información no sea rechazada y que sea auténtica, y que evite la modificación o destrucción innecesaria de la información." (El Peruano, 2021, p. 38)

2.4. Activo

"Un activo es cualquier cosa que tiene valor para la organización y necesita protección." (ISO/IEC 2018 & INACAL 2018, 2018, p. 18)

"Un componente o función de un sistema de información que puede verse comprometido de forma intencionada o no intencionada con las consiguientes consecuencias para la organización. El activo puede ser información, datos, servicios, aplicaciones(software), equipos(hardware), comunicaciones, recursos administrativos, físicos y humanos." (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012, p. 97)

2.4.1. Tipos de activos

2.4.1.1. Activos esenciales

"Se clasifica en la información (datos de interés para la administración pública, datos vitales), datos de carácter personal (de nivel alto, nivel medio, nivel bajo) y datos clasificados (nivel confidencial, difusión limitada, sin clasificar, de carácter público)."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 7)

2.4.1.2. Datos / Información

"La información es un activo abstracto que será almacenado en equipos o soportes de información como: ficheros, copias de respaldo, datos de configuración, datos de gestión interna, credenciales (ej. contraseñas), datos de control de acceso, registro de actividad."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,pp. 8-9)

Son los siguientes:

- ficheros

- copias de respaldo
- datos de configuración
- datos de gestión interna
- credenciales (ej. contraseñas)
- datos de validación de credenciales
- datos de control de acceso
- [log] registro de actividad
- código fuente
- código ejecutable
- datos de prueba

2.4.1.3. Claves criptográficas

"La criptografía se emplea para proteger el secreto o autenticar a las partes. Las claves criptográficas, combinando secretos e información pública son esenciales para garantizar el funcionamiento de los mecanismos criptográficos."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 9)

Son los siguientes:

- claves de cifrado
- secreto compartido
- clave pública de cifrado
- clave privada de descifrado
- claves de firma
- certificados de claves públicas

2.4.1.4. Servicios

"Función que satisface una necesidad de los usuarios (del servicio)."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,pp. 10-11)

Son los siguientes:

- anónimo (sin requerir identificación del usuario)
- al público en general (sin relación contractual)
- a usuarios externos (bajo una relación contractual)
- interno (a usuarios de la propia organización)
- world wide web
- acceso remoto a cuenta local
- correo electrónico
- almacenamiento de ficheros
- transferencia de ficheros
- intercambio electrónico de datos
- servicio de directorio
- gestión de identidades
- gestión de privilegios
- PKI - infraestructura de clave pública

2.4.1.5. Software

"Estos son programas de computadora que realizan tareas específicas en una computadora. Por ejemplo, un sistema operativo, una aplicación, un navegador web, un juego o un programa". (GCFGlobal, s.f.)

2.4.1.6. Hardware

"El hardware (frente al hardware) es la parte física de una computadora, es decir, cualquier cosa que se pueda tocar: teclado, mouse, monitor, impresora, cables, tarjetas electrónicas, carcasa, disco duro, memoria de grupo, parlante, micrófono, etc. etc., se consideran materiales". (Vélez Martínez, s.f.)

"Una definición de hardware es un conjunto de circuitos electrónicos, memoria y dispositivos de entrada/salida." (Tanenbaum, 2000, p. 8)

Son los siguientes:

- grandes equipos
- equipos medios

- informática personal
- informática móvil
- agendas electrónicas
- equipo virtual
- equipamiento de respaldo
- periféricos
    - medios de impresión
    - escáneres
    - dispositivos criptográficos
- dispositivo de frontera
- soporte de la red
    - módems
    - concentradores
    - conmutadores
    - encaminadores, pasarelas
    - [firewall] cortafuegos
    - punto de acceso inalámbrico
- centralita telefónica
- teléfono IP

2.4.1.7. Redes de comunicaciones

"Corresponde tanto a las instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro. Por ejemplo: red telefónica, red inalámbrica, telefonía móvil, red local, Internet." (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,pp. 11-12)

2.4.1.8. Soportes de información

"Se consideran a los dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo, como: electrónicos (discos, discos virtuales, almacenamiento en red, disquetes, (CD-ROM), memorias USB, DVD, tarjetas de memoria, tarjetas inteligentes) y los no electrónicos (material impreso, cinta de papel)." (Dirección General de Modernización

Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 12)

Son los siguientes:

- Electrónicos
  - discos
  - discos virtuales
  - almacenamiento en red
  - disquetes
  - cederrón (CD-ROM)
  - memorias USB
  - DVD
  - cinta magnética
  - tarjetas de memoria
  - tarjetas inteligentes
- No electrónicos
  - material impreso
  - cinta de papel
  - microfilm
  - tarjetas perforadas

2.4.1.9. Equipamiento auxiliar

"Se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos. Como: generadores eléctricos, equipos de climatización, cableado, suministros esenciales."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 12)

2.4.1.10. Instalaciones

"Son los lugares donde se hospedan los sistemas de información y comunicaciones. Pueden ser: edificios, cuartos, plataformas móviles (vehículo terrestre, vehículo aéreo, vehículo marítimo), instalaciones de respaldo."(Dirección General de

Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 13)

Son los siguientes:

- recinto
- edificio
- cuarto
- plataformas móviles
    - vehículo terrestre: coche, camión, etc.
    - vehículo aéreo: avión, etc.
    - vehículo marítimo: buque, lancha, etc.
    - contenedores
- canalización
- instalaciones de respaldo

2.4.1.11. Personal

"Son las personas relacionadas con los sistemas de información como: usuarios externos, usuarios internos, administradores (de sistemas, de comunicaciones, de BBDD, de seguridad), desarrolladores / programadores, proveedores."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 13)

2.5. Amenaza

"Las amenazas pueden causar daños a la propiedad, las amenazas pueden ser naturales o provocadas por el hombre, y pueden ser accidentales o intencionales. La amenaza puede provenir de dentro o fuera de la organización." (ISO/IEC 2018 & INACAL 2018, 2018, p. 19)

"Es una causa potencial de falla que puede causar daño a un sistema de información o una organización."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 97)

2.5.1. Tipos de amenazas

2.5.1.1. Desastres Naturales

"Son sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta, son de origen accidental. Se clasifican en:

- **Fuego:** incendios.
- **Daños por agua:** inundaciones.
- **Desastres naturales**: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,pp. 25-26)

2.5.1.2. De origen industrial

"Son sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Pueden ser de origen accidental o deliberada. Se clasifican en:

- **Fuego:** incendios.
- **Daños por agua:** escapes, fugas, inundaciones.
- **Desastres industriales:** explosiones, derrumbe, sobrecarga eléctrica.
- **Contaminación mecánica:** vibraciones, polvo, suciedad.
- **Contaminación electromagnética:** interferencias de radio, campos magnéticos, luz ultravioleta.
- **Avería de origen físico o lógico:** fallos en los equipos y/o fallos en los programas.
- **Corte del suministro eléctrico:** pérdida de suministro de energía.
- **Condiciones inadecuadas de temperatura o humedad:** deficiencias en la aclimatación de los locales.
- **Fallo de servicios de comunicaciones:** pérdida de los medios de telecomunicación.
- **Interrupción de otros servicios y suministros esenciales:** recursos de los que depende la operación de los equipos como papel para las impresoras, tóner.
- **Degradación de los soportes de almacenamiento de la información:** avería del hardware, falla en el funcionamiento del software.

- **Emanaciones electromagnéticas:** intercepción de señales parásitas comprometedoras.”(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,pp. 27-32)

2.5.1.3. Errores y fallos no intencionados

“Son los fallos no intencionales causados por las personas, son de origen humano(accidental). Se clasifican en:

- **Errores de los usuarios:** equivocaciones de las personas cuando usan los servicios, datos.
- **Errores del administrador:** equivocaciones de personas con responsabilidades de instalación y operación.
- **Errores de monitorización (log):** inadecuado registro de actividades.
- **Errores de configuración:** introducción de datos de configuración erróneos.
- **Deficiencias en la organización:** cuando no está claro quién tiene que hacer exactamente qué y cuándo.
- **Difusión de software dañino:** propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas.
- **Errores de [re-]encaminamiento:** envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde no es debido**.**
- **Errores de secuencia:** alteración accidental del orden de los mensajes transmitidos.
- **Escapes de información:** la información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella.
- **Alteración accidental de la información:** sólo se identifica sobre datos en general.
- **Destrucción de información:** pérdida accidental de información.
- **Fugas de información:** revelación por indiscreción.
- **Vulnerabilidades de los programas (software):** defectos en el código.
- **Errores de mantenimiento / actualización de programas (software):** defectos en los procedimientos o controles de actualización del código.

- **Errores de mantenimiento / actualización de equipos (hardware):** defectos en los procedimientos o controles de actualización de los equipos.
- **Caída del sistema por agotamiento de recursos:** carencia de recursos suficientes provoca la caída del sistema.
- **Pérdida de equipos:** provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.
- **Indisponibilidad del personal:** ausencia accidental del puesto de trabajo como enfermedad, guerra." (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012, pp. 33-39)

2.5.1.4. Ataques intencionados

"Son fallos deliberados causados por las personas, son de origen humano(deliberado). Se clasifican en:

- Manipulación de los registros de actividad
- Manipulación de la configuración
- Suplantación de la identidad del usuario
- Abuso de privilegios de acceso
- Uso no previsto
- Difusión de software dañino
- [Re-]encaminamiento de mensajes
- Alteración de secuencia
- Acceso no autorizado
- Análisis de tráfico
- Repudio
- Interceptación de información (escucha)
- Modificación deliberada de la información
- Destrucción de información
- Divulgación de información
- Manipulación de programas
- Manipulación de los equipos
- Denegación de servicio
- Robo

- Ataque destructivo
- Ocupación enemiga
- Indisponibilidad del personal
- Extorsión
- Ingeniería social (picaresca)"(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,pp. 40-47)

2.6. Vulnerabilidad

"La vulnerabilidad no causa daño en sí misma, debe existir una amenaza para explotarla." (ISO/IEC 2018 & INACAL 2018, 2018, p. 22)

"Es una eficiencia o debilidad en el diseño, implementación u operación de un sistema que permite o facilita la percepción de una amenaza." (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012, p. 105)

2.6.1. Ejemplos de vulnerabilidades

"Son los siguientes:

- **Hardware:** almacenamiento no protegido, copiado no controlado, susceptibilidad a humedad, polvo, corrosión, mantenimiento insuficiente / instalación defectuosa de medios de almacenamiento.
- **Software: f**alta o insuficiente prueba de software, fallas bien conocidas en el software, software ampliamente distribuido, falta de documentación, falta de mecanismos de identificación y autenticación como autenticación de usuario.
- **Red:** falta de prueba de envío o recepción de un mensaje, conexiones de red pública sin protección, falta de identificación y autenticación del remitente y el receptor.
- **Personal:** ausencia de personal, uso incorrecto de software y hardware, trabajo no supervisado por personal externo o de limpieza, falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería.

- **Local:** uso inadecuado o descuidado de control de acceso físico a edificios y recintos, ubicación en un área susceptible de inundación, red de energía inestable, falta de protección física del edificio, puertas y ventanas.
- **Organización:** falta de auditorías regulares (supervisión), falta de reportes de fallas registrados en bitácoras del administrador y operador, falta de control de activos fuera de las instalaciones, falta de procedimientos para reportar debilidades de la seguridad."(ISO/IEC 2018 & INACAL 2018, 2018,pp. 71-75)

2.7. Salvaguarda

"Es un proceso o mecanismo tecnológico que reduce el riesgo, varían con el avance tecnológico porque aparecen tecnologías nuevas, porque cambian los activos a considerar, porque evoluciona el catálogo de salvaguardas disponibles."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 103)

2.7.1. Tipos de salvaguardas

"Se clasifican en:

- Protecciones generales u horizontales
- Protección de los datos / información
- Protección de las claves criptográficas
- Protección de los servicios
- Protección de las aplicaciones (software)
- Protección de los equipos (hardware)
- Protección de las comunicaciones
- Protección en los puntos de interconexión con otros sistemas
- Protección de los soportes de información
- Protección de los elementos auxiliares
- Seguridad física – Protección de las instalaciones
- Salvaguardas relativas al personal
- Salvaguardas de tipo organizativo

- Continuidad de operaciones”(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,pp. 53-56)

2.8. Impacto

“Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que éstas tendrían sobre el sistema. La única consideración que queda hacer es relativa a las dependencias entre activos.

Es frecuente que el valor del sistema se centre en la información que maneja y los servicios que presta; pero las amenazas suelen materializarse en los medios. Para enlazarse unos con otros recurriremos al grafo de dependencias. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012, p. 28)”

2.9. Riesgo

“El riesgo es la suma de los posibles resultados de un evento indeseable y la probabilidad de que ocurra.” (ISO/IEC 2018 & INACAL 2018, 2018, p. 16)

“El riesgo es una estimación de la cantidad de riesgo para uno o más activos que causa daños o perjuicios a la organización.” (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012, p. 102)

2.10. Impacto potencial

“Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.” (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,pp. 28-29)

2.11. Riesgo potencial

“Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en

cuenta la probabilidad de ocurrencia." (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,pp. 29-31)

2.12. Impacto residual

"Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de posible impacto que se denomina residual." (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 35)

2.13. Riesgo residual

"Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual." (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 35)

2.14. Gestión de Riesgos

"La Gestión de Riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo.

En su forma general contiene cuatro fases

- **Análisis**: Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.
- **Clasificación**: Determina si los riesgos encontrados y los riesgos restantes son aceptables.
- **Reducción**: Define e implementa las medidas de protección. Además, sensibiliza y capacita los usuarios conforme a las medidas.
- **Control**: Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento.

Todo el proceso está basado en las llamadas políticas de seguridad, normas y reglas institucionales, que forman el marco operativo del proceso, con el propósito de:

- Potenciar las capacidades institucionales, reduciendo la vulnerabilidad y limitando las amenazas con el resultado de reducir el riesgo.
- Orientar el funcionamiento organizativo y funcional.
- Garantizar comportamiento homogéneo.
- Garantizar corrección de conductas o prácticas que nos hacen vulnerables.
- Conducir a la coherencia entre lo que pensamos, decimos y hacemos."(ERB, s.f.)"

2.15. Auditoría de seguridad

"Es el estudio y examen independiente del historial y actividades de un sistema de información, con la finalidad de comprobar la idoneidad de los controles del sistema, asegurar su conformidad con la estructura de seguridad y procedimientos operativos establecidos, a fin de detectar brechas en la seguridad y recomendar cambios en los procedimientos, controles y estructuras de seguridad."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 99)

2.15.1. Beneficios

"Son los siguientes:

- Mejora los controles internos de seguridad de la empresa.
- Detecta debilidades en los sistemas de seguridad como errores, omisiones o fallos.
- Identifica posibles actuaciones fraudulentas (acceso a datos no autorizados o robos a nivel interno).
- Ayuda a eliminar los puntos débiles de la empresa en cuestión de seguridad (webs, correo electrónico o accesos remotos, por ejemplo).
- Permite controlar los accesos, tanto físicos como virtuales (revisión de privilegios de acceso).
- Permite mantener sistemas y herramientas actualizadas." (AMBIT, 2021)

2.15.2. Tipos de auditorías de seguridad

"Se clasifican en:

- **Auditorías internas y externas:** dependiendo de quién realice la auditoría se denominan internas, cuando son realizadas por personal de la propia empresa (aunque pueden tener apoyo o asesoramiento externo) o externas, cuando se realizan por empresas externas que son independientes de la empresa.
- **Auditorías técnicas:** Son aquellas auditorías cuyo objetivo se centra en una parte concreta o acotada de un sistema informático.
- **Auditorías por objetivo:** Se trata de auditorías de seguridad técnicas que se diferencia según el objetivo que persigan. Las más comunes son sitios web, forense, redes, control de acceso, hacking ético." (AMBIT, 2021)

2.16. Ataque

Intento de destruir, exponer, alterar o inhabilitar un sistema de información o la información que el sistema maneja, o violar alguna política de seguridad de alguna otra manera. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 99)

2.17. Proyecto de seguridad

Agrupación de tareas orientadas a tratar el riesgo del sistema. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012, p. 102)

2.18. Plan de seguridad

Conjunto de proyectos de seguridad que permiten materializar las decisiones de gestión de riesgos. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012, p. 102)

2.19. Plan de tratamiento

Documento que evalúa las posibles acciones que se deben tomar para mitigar los riesgos existentes teniendo en cuenta los criterios de aceptación de riesgos definidos por la entidad. (Plan de Tratamiento de Riesgos,2022, p.3)

2.20.NTP-ISO/IEC 27001:2014 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos.

"Esta Norma Técnica Peruana ha sido elaborada por el Comité Técnico de Normalización de Codificación e intercambio electrónico de datos, mediante el Sistema 1 o de Adopción, durante los meses de abril a junio de 2014, utilizando como antecedente a la norma ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems- Requirements y la ISO/IEC 27001:2013/ COR 1 2013 Information technology - Security techniques - Information security management systems- Requirements."(ISO/IEC 2013 & INDECOPI 2014, 2014, iv)

"Esta Norma Técnica Peruana especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. También incluye requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información orientados a las necesidades de la organización."(ISO/IEC 2013 & INDECOPI 2014, 2014, vii)

2.20.1. Secciones de la NTP-ISO/IEC 27001:2014 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos.

Se divide en:

- **Sección 1- Contexto de la organización:**

  "Se definen los requerimientos para comprender la organización y su contexto, comprender las necesidades y expectativas de las partes interesadas y finalmente determinar el alcance del sistema de gestión de seguridad de la información." (ISO/IEC 2013 & INDECOPI 2014, 2014,pp. 2-3)

- **Sección 2- Liderazgo**

  "Se definen las responsabilidades de la dirección, el establecimiento de los roles y responsabilidades y finalmente el contenido de las políticas de seguridad de la información." (ISO/IEC 2013 & INDECOPI 2014, 2014,pp. 3-5)

- **Sección 3- Planificación**

  "Se definen los requerimientos para tratar los riesgos y las oportunidades, valoración del riesgo de seguridad de la información, el tratamiento de riesgos de seguridad de la información, el plan de tratamiento de riesgos y finalmente la determinación de objetivos de seguridad de la información."(ISO/IEC 2013 & INDECOPI 2014, 2014,pp. 5-8)

- **Sección 4- Soporte**

  "Se definen los requerimientos sobre la disponibilidad de recursos, competencia, concientización, comunicación y la información documentada." (ISO/IEC 2013 & INDECOPI 2014, 2014,pp. 9-12)

- **Sección 5- Operación**

  "Se definen los requerimientos de planificación y control operacional, la evaluación de riesgos de seguridad de la información y el tratamiento de riesgos." (ISO/IEC 2013 & INDECOPI 2014, 2014,pp. 12-13)

- **Sección 6- Evaluación del desempeño**

  "Se definen los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y finalmente la revisión por la dirección." (ISO/IEC 2013 & INDECOPI 2014, 2014,pp. 13-15)

- **Sección 7- Mejora**

  "Se definen los requerimientos para el tratamiento de no conformidades y acciones correctivas y finalmente la mejora continua." (ISO/IEC 2013 & INDECOPI 2014, 2014,pp. 16-17)

2.21. NTP-ISO/IEC 27002:2013 Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información.

"ISO/IEC 27002 en su segunda edición publicada como ISO/IEC 27002:2013 Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información - es un documento de guía utilizado como referencia para la selección, implantación y gestión de los controles, tanto para las organizaciones con un sistema de gestión de la seguridad de la información (SGSI) basado en la norma ISO/IEC 27001, proporciona información detallada sobre los controles enumerados en el Anexo A; como para cualquier organización que cuente con las mejores prácticas en materia de seguridad de la información y que desee implantar los controles de seguridad de la información comúnmente aceptados."(OSTEC, 2016 & BSI, s.f.)

"La norma ISO/IEC 27002:2013 Tecnología de la información - técnicas de seguridad - código de prácticas para los controles de seguridad de la información ha sido revisada y se espera que se publique en febrero de este año bajo el nombre de ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad - edición de los controles de seguridad de la información." (OSTEC, 2016 & BSI, s.f.)

"Todas las organizaciones que cuenten con un SGSI o con buenas prácticas de seguridad de la información tendrán que trazar y actualizar sus controles en función de las nuevas directrices de la norma ISO/IEC 27002 actualizada, de acuerdo con las necesidades y el contexto de la organización."(OSTEC, 2016 & BSI, s.f.)

2.21.1. Principales secciones de la NTP-ISO/IEC 27002:2013 Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información

- **Sección 5 – Política de Seguridad de la Información**

  "Se debe crear un documento sobre la política de seguridad de la información de la empresa, que debe contener los conceptos de seguridad de la información, una estructura para establecer los objetivos y las formas de control, el compromiso de la dirección con la política, entre tantos otros factores."(OSTEC, 2016 & BSI, s.f.)

- **Sección 6 – Organización de la Seguridad de la Información**

  "Para implementar la Seguridad de la Información en una empresa, es necesario establecer una estructura para gestionarla de una manera adecuada. Para ello, las actividades de seguridad de la información deben ser coordinadas por representantes de la organización, que deben tener responsabilidades bien definidas y proteger las informaciones de carácter confidencial."(OSTEC, 2016 & BSI, s.f.)

- **Sección 7 – Gestión de activos**

  "Activo, según la norma, es cualquier cosa que tenga valor para la organización y que necesita ser protegido. Pero para ello los activos deben ser identificados y clasificados, de modo que un inventario pueda ser estructurado y posteriormente mantenido. Además, deben seguir reglas documentadas, que definen qué tipo de uso se permite hacer con dichos activos."(OSTEC, 2016 & BSI, s.f.)

- **Sección 8 – Seguridad en recursos humanos**

  "Antes de la contratación de un empleado – o incluso de proveedores – es importante que sea debidamente analizado, principalmente si se trata de información de carácter confidencial. La intención de esta sección es mitigar el riesgo de robo, fraude o mal uso de los recursos. Y cuando el empleado esté trabajando en la empresa, debe ser consciente de las amenazas relativas a la seguridad de la información, así como de sus responsabilidades y obligaciones."(OSTEC, 2016 & BSI, s.f.)

- **Sección 9 – Seguridad física y del medio ambiente**

  "Los equipos e instalaciones de procesamiento de información crítica o sensible deben mantenerse en áreas seguras, con niveles y controles de acceso apropiados, incluyendo protección contra amenazas físicas y ambientales."(OSTEC, 2016 & BSI, s.f.)

- **Sección 10 – Seguridad de las operaciones y comunicaciones**

  "Es importante que estén definidos los procedimientos y responsabilidades por la gestión y operación de todos los recursos de procesamiento de la información. Esto incluye la gestión de servicios tercerizados, la planificación de recursos de los sistemas para minimizar el riesgo de fallas, la creación de procedimientos para la generación de copias de seguridad y su recuperación, así como la administración segura de las redes de comunicaciones".(OSTEC, 2016 & BSI, s.f.)

- **Sección 11 – Control de acceso**

  "El acceso a la información, así como a los recursos de procesamiento de la información y los procesos de negocios, debe ser controlado con base en los requisitos de negocio y en la seguridad de la información. Debe garantizarse el acceso de usuario autorizado y prevenido el acceso no autorizado a los sistemas de información, a fin de evitar daños a documentos y recursos de procesamiento de la información que estén al alcance de cualquiera."(OSTEC, 2016 & BSI, s.f.)

- **Sección 12 – Adquisición, desarrollo y mantenimiento de sistemas**

  "Los requisitos de seguridad de los sistemas de información deben ser identificados y acordados antes de su desarrollo y/o de su implementación, para que así puedan ser protegidos para el mantenimiento de su confidencialidad, autenticidad o integridad por medios criptográficos."(OSTEC, 2016 & BSI, s.f.)

- **Sección 13 – Gestión de incidentes de seguridad de la información**

  "Los procedimientos formales de registro y escalonamiento deben ser establecidos y los empleados, proveedores y terceros deben ser conscientes de los procedimientos para notificar los eventos de seguridad de la información para asegurar que se comuniquen lo más rápido posible y corregidos en tiempo hábil."(OSTEC, 2016 & BSI, s.f.)

- **Sección 14 – Gestión de continuidad del negocio**

  "Los planes de continuidad del negocio deben ser desarrollados e implementados, con el fin de impedir la interrupción de las actividades del negocio y asegurar que las operaciones esenciales sean rápidamente recuperadas."(OSTEC, 2016 & BSI, s.f.)

- **Sección 15 – Conformidad**

  "Es importante evitar la violación de cualquier ley criminal o civil, garantizando estatutos, regulaciones u obligaciones contractuales y de cualesquiera requisitos de seguridad de la información. En caso necesario, la empresa puede contratar una consultoría especializada, para que se verifique su conformidad y adherencia a los requisitos legales y reglamentarios." (OSTEC, 2016 & BSI, s.f.)

2.22. NTP ISO/IEC 27005: Tecnología de la información. Técnicas de seguridad. Gestión de riesgos de la seguridad de la información

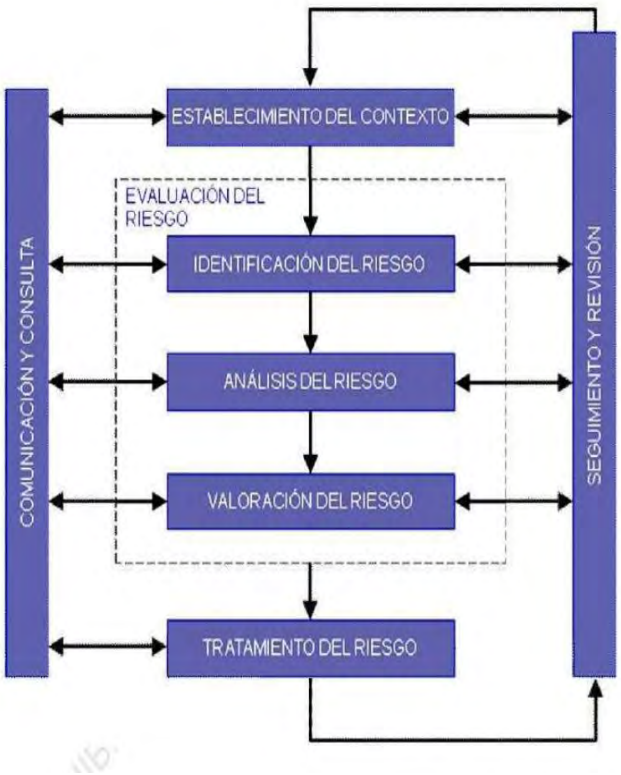
"Esta Norma Técnica Peruana ha sido elaborada por el Comité Técnico de Normalización de Codificación e intercambio electrónico de datos, mediante el Sistema 1 o de Adopción, durante los meses de julio a setiembre de 2018, utilizando como antecedente a la norma ISO/IEC 27005:2018 Information technology - Security techniques - Information security risk management." (ISO/IEC 2018 & INACAL 2018, 2018, iv)

"Esta norma técnica peruana brinda lineamientos para organizar un evento reivindicativo sin miedo dentro de una organización. Sin embargo, esta norma técnica peruana no nos brinda ningún razonamiento específico para superar la audaz verdad del enunciado. Se apoya en la lógica basada en activos, amenazas y vulnerabilidades para identificar riesgos. Está diseñado para respaldar la implementación exitosa de informes de audacia basados en el marco de procesamiento de riesgos. Aplicable a cualquier tipo de organización (es decir, empresa comercial, agencia gubernamental, organización sin fines de lucro). (ISO/IEC 2018 & INACAL 2018, 2018, viii)

2.22.1. Proceso de gestión de riesgos de la seguridad de la información

Imagen 1

Proceso de gestión de riesgos de la seguridad de la información.



Fuente: ISO/IEC 27005:2018(2018).

Son los siguientes:

1. **Establecimiento del contexto**

   El proceso se detalla a continuación:

   Entrada: Información sobre la organización relevante para proporcionar

contexto para la gestión de riesgos de seguridad de la información. (ISO/IEC 2018 & INACAL 2018,2018, p. 10)

Acción: Crear un contexto interno y externo para la gestión de riesgos de seguridad de la información. Esto incluye establecer los estándares básicos necesarios para administrar los riesgos de seguridad de la información, definir el alcance y los límites, y establecer una organización adecuada para administrar los riesgos de seguridad y las actividades de información. (ISO/IEC 2018 & INACAL 2018, 2018, p. 10)

Guía de implementación: Definición de objetivos de gestión de riesgos de seguridad de la información (soporte de SGSI, planificación de respuesta a incidentes, descripción de los requisitos de seguridad de la información del producto). (ISO/IEC 2018 & INACAL 2018, 2018, p. 10)

Salida: Estándares básicos, alcance, especificaciones de límites y organización de los procesos de gestión de riesgos de seguridad de la información. (ISO/IEC 2018 & INACAL 2018, 2018, p. 10)

2. Evaluación del riesgo

El proceso se detalla a continuación:

Entrada: Los criterios básicos, alcance, límites, y la organización para el proceso de gestión del riesgo de seguridad de la información que está siendo establecido. (ISO/IEC 2018 & INACAL 2018, 2018, p. 16)

Acción: Los riesgos deberían ser identificados, cuantificados o descritos cualitativamente, y priorizados contra criterios de valoración del riesgo y objetivos relevantes para la organización. (ISO/IEC 2018 & INACAL 2018, 2018, p. 16)

Guía de implementación: La evaluación del riesgo consiste en las siguientes actividades:

- Identificación del riesgo
- Análisis del riesgo
- Valoración del riesgo

La evaluación de riesgos determina el valor de los activos de información, identifica las amenazas y vulnerabilidades aplicables que existen (o pueden existir), identifica los controles existentes y su impacto en los riesgos

identificados y potenciales, prioriza los riesgos resultantes y los asigna al grupo de riesgo métrica. Contexto establecido. (ISO/IEC 2018 & INACAL 2018, 2018, pp. 16-17)

Salida: Una lista de los riesgos evaluados, priorizados de acuerdo al criterio de valoración de riesgos. (ISO/IEC 2018 & INACAL 2018, 2018, p. 17)

3. Tratamiento del riesgo

El proceso se detalla a continuación:

Entrada: Una lista del riesgo priorizada de acuerdo a los criterios de valoración del riesgo en relación a los posibles escenarios que llevan a tales riesgos. (ISO/IEC 2018 & INACAL 2018, 2018, p. 31)

Acción: Seleccionar controles para reducir, retener, evitar, o transferir los riesgos y definir un plan de tratamiento de riesgos. (ISO/IEC 2018 & INACAL 2018, 2018, p.31)

Guía de implementación: Estas opciones deben ser seleccionadas basándose en el resultado de la evaluación de riesgos, consiste en 4 opciones:

- Modificación del riesgo
- Retención del riesgo
- Evitar el riesgo
- Compartir el riesgo

Estas opciones se consideran teniendo en cuenta la percepción del riesgo por parte de las partes interesadas y los medios de comunicación más apropiados con esas partes interesadas. (ISO/IEC 2018 & INACAL 2018, 2018, pp. 31-34)

Salida: Plan de tratamiento del riesgo y riesgos residuales sujetos a la decisión de aceptación por la alta dirección de la organización. (ISO/IEC 2018 & INACAL 2018, 2018, p. 34)

4. Aceptación del riesgo

El proceso se detalla a continuación:

Entrada: Plan de tratamiento del riesgo y evaluación del riesgo residual sujeto a la aceptación de la decisión de la dirección de la organización. (ISO/IEC 2018 & INACAL 2018, 2018, p. 37)

Acción: La decisión de asumir riesgos y responsabilidades debe tomarse y

registrarse formalmente. (ISO/IEC 2018 & INACAL 2018, 2018, p. 37)

Guía de implementación: El plan de tratamiento de riesgos describe cómo se evalúa el riesgo e intenta cumplir con los criterios de tolerancia al riesgo. Es importante que el director sea responsable de revisar y aprobar el plan de tratamiento de riesgos propuesto y el riesgo residual resultante. (ISO/IEC 2018 & INACAL 2018, 2018, pp. 37-38)

Salida: Una lista de riesgos aceptados y la justificación de los riesgos que no cumplen con los criterios normales de aceptación de riesgos de la organización. (ISO/IEC 2018 & INACAL 2018, 2018, pp. 37-38)

5. Comunicación y consulta del riesgo

El proceso se detalla a continuación:

Entrada: Toda la información de riesgos obtenida como resultado de las actividades de gestión de riesgos. (ISO/IEC 2018 & INACAL 2018, 2018, p. 38)

Acción: La información acerca de los riesgos debería ser intercambiada y/o compartida entre los tomadores de decisiones y otros interesados. (ISO/IEC 2018 & INACAL 2018, 2018, p. 38)

Guía de implementación: La comunicación de riesgos es una actividad que tiene como objetivo llegar a un acuerdo sobre cómo gestionar los riesgos a través del intercambio y/o intercambio de información sobre riesgos entre los responsables de la toma de decisiones y otras partes interesadas. Es importante colaborar con las unidades de comunicación o relaciones públicas apropiadas dentro de la organización para coordinar todas las tareas relacionadas con la comunicación de riesgos. (ISO/IEC 2018 & INACAL 2018, 2018, pp. 39-40)

Salida: Es importante trabajar con los departamentos de comunicaciones o relaciones públicas pertinentes dentro de su organización para coordinar todas las tareas de comunicación de riesgos. (ISO/IEC 2018 & INACAL 2018, 2018, p. 40)

6. Seguimiento y revisión del riesgo

El proceso se detalla a continuación:

Entrada: Toda la información obtenida de las actividades de gestión del riesgo.

(ISO/IEC 2018 & INACAL 2018, 2018, p. 40)

Acción: Supervise y revise los riesgos y sus factores (es decir, activos, impactos, amenazas, vulnerabilidades) para identificar cambios en el contexto de su organización y mantener una visión integral del riesgo. (ISO/IEC 2018 & INACAL 2018, 2018, p. 41)

Guía de implementación: Las amenazas, vulnerabilidades, oportunidades o resultados pueden cambiar repentinamente y requieren un monitoreo continuo para detectar estos cambios. Las actividades de monitoreo de riesgos deben repetirse periódicamente y las opciones de tratamiento de riesgos seleccionadas deben revisarse periódicamente. Las organizaciones deben revisar todos los riesgos periódicamente y en caso de cambios significativos. (ISO/IEC 2018 & INACAL 2018, 2018, pp. 41-42)

Salida: Coordinación continua de la gestión de riesgos con los objetivos comerciales de la organización y los criterios de aceptación de riesgos. (ISO/IEC 2018 & INACAL 2018, 2018, p. 42)

2.23. Metodología MAGERIT

"MAGERIT" es una metodología pública que se puede utilizar libremente y sin autorización previa. Las entidades cubiertas por el Programa Nacional de Seguridad (ENS) se preocupan principalmente por cumplir con el principio de gestión de seguridad basada en riesgos, así como con el requisito de análisis y gestión de riesgos, basados en la dependencia de las tecnologías de la información. cumplir misiones, prestar servicios y alcanzar los objetivos de la organización."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 7)

"En la terminología de la norma ISO 31000, MAGERIT cumple con lo que se denomina un "Proceso de Gestión de Riesgos", apartado. ("Implementación de la Gestión de Riesgos") en el "Marco de Gestión de Riesgos". En otras palabras, MAGERIT implementa un Proceso de Gestión de Riesgos dentro de un marco que permite a los reguladores tomar decisiones que toman en cuenta los riesgos asociados con el uso de la tecnología de la información."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 7)

MAGERIT se tiene desarrollado en 3 libros

Libro 1: Método

"En este libro encontramos pautas para gestionar los riesgos de seguridad de la información en una organización. Sin embargo, este documento no proporciona métodos específicos para gestionar los riesgos de seguridad de la información."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,pp. 12-13)

"En consecuencia, la organización debe definir su enfoque de gestión de riesgos. Por ejemplo, el alcance del sistema de gestión de seguridad de la información (SGSI), el contexto de gestión de riesgos o el sector industrial. Se determinar los activos de la institución, amenaza, impactos que tenían estas amenazas y salvaguardas."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,pp. 12-13)

Libro 2: Catálogo de elementos.

El objetivo de este catálogo de elementos que aparecen en un proyecto de análisis y gestión de riesgos es doble:

- "Por un lado, facilitar el trabajo de los ejecutores de proyectos, en el sentido de proporcionarles elementos estándar que puedan adoptar rápidamente, centrándose en características específicas del sistema que se analiza."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 6)
- Por otro lado, estandarizar los resultados de los análisis, fomentando terminología y criterios para poder comparar o incluso integrar los análisis realizados por diferentes grupos."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 6)

Libro 3: Guía de técnicas.

"Este documento es una guía de la metodología MAGERIT. Se considera posible el conocimiento y comprensión de los conceptos de análisis y gestión de riesgos tal y como se

especifica en el manual de metodología."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 4)

"El propósito de este documento es describir algunas de las técnicas utilizadas en el análisis y gestión de riesgos. Se considera una técnica un conjunto de procedimientos y prácticas que ayudan a lograr los objetivos establecidos."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 4)

"Todas las técnicas de este libro se pueden utilizar sin asistencia automática; pero su aplicación repetitiva o compleja recomienda utilizar las herramientas de la manera más amplia y frecuente posible."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 4)

MAGERIT tiene los siguientes objetivos:
Directos:

1. "Sensibilizar a los responsables de comunicación sobre la existencia de riesgos y la necesidad de gestionarlos.
2. Ofrece un método sistemático para el análisis de riesgos derivados del uso de las tecnologías de la información y la comunicación (TIC).
3. Ayuda a detectar y planificar el tratamiento a tiempo para controlar los riesgos."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 8)

Indirectos:

4. "Preparar a la Organización para los procesos de auditoría, evaluación, certificación o acreditación, según corresponda."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 9)

"MARGERIT divide la gestión de riesgos en dos tareas, ambas actividades, análisis y tratamiento se combinan en el proceso denominado Gestión de Riesgos."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 19)

1) Análisis de riesgos:

"Permite determinar lo que tiene la organización y estimar lo que podría suceder. El análisis de riesgos es un enfoque metódico para la identificación de riesgos en una serie de pasos:"(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 19)

a. "Identificar los activos que son relevantes para la Organización, la relación entre ellos y su valor, en términos del daño (costos) que causará su degradación.
b. Identificar amenazas a estos activos.
c. Identificar las salvaguardas a aplicar y su eficacia frente a los riesgos.
d. Impacto estimado, definido como daño a la propiedad como resultado de la realización de la amenaza.
e. Estimación del riesgo, definido como el efecto ponderado de la ocurrencia (o realización esperada) de la amenaza."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,p. 22)

Imagen 2

Elementos del análisis de riesgos potenciales.

Fuente: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método (2012).

El análisis de los riesgos se lleva a cabo por medio de las siguientes tareas:

MAR.1: Caracterización de los activos

"El objetivo de estas tareas es identificar los activos que componen el sistema, determinar las dependencias entre ellos y determinar la porción del valor del sistema que genera cada activo. Podemos resumirlo en la expresión conócete a ti mismo. El resultado de esta actividad es el informe denominado modelo de valor."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,pp. 37-40)

Sub - tareas:

MAR.1 – Caracterización de los activos

MAR.11 – Identificación de los activos

MAR.12 – Dependencias entre activos

MAR.13 – Valoración de los activos

MAR.2: Caracterización de las amenazas

"El objetivo de estas tareas es describir las características del entorno al que se enfrenta el sistema, lo que podría suceder, las consecuencias que se producirían y lo que es probable que suceda. Se puede resumir en la expresión conoce a tu enemigo. El resultado de esta actividad es el informe denominado mapa de riesgos."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,pp. 40-42)

Sub - tareas:

MAR.2 – Caracterización de las amenazas

MAR.21 – Identificación de las amenazas

MAR.22 – Valoración de las amenazas

MAR.3: Caracterización de las salvaguardas

"El objetivo de estas tareas es doble: saber qué necesitamos para proteger el sistema y saber si tenemos un sistema de protección que cubra nuestras necesidades. El resultado de esta actividad se concreta en varios informes: declaración de aplicabilidad, evaluación de salvaguardas, insuficiencias (o vulnerabilidades del sistema de protección)."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,pp. 42-43)

Sub - tareas:

MAR.3 – Caracterización de las salvaguardas

MAR.31 – Identificación de las salvaguardas

MAR.32 – Valoración de las salvaguardas

MAR.4: Estimación del estado de riesgo

"El objetivo de estas tareas es tener una estimación informada de lo que podría suceder (impacto) y lo que es probable que suceda (riesgo)." (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012,pp. 43-45)

Sub - tareas:

MAR.4 – Estimación del estado de riesgo

MAR.41 – Estimación del impacto

MAR.42 – Estimación del riesgo

2) Tratamiento de riesgos:

"Permite organizar una fuerza de defensa concienzuda y cuidadosa, velando para que nada malo suceda, y al mismo tiempo preparándose para enfrentar emergencias, sobrevivir incidentes y continuar operando en las mejores condiciones; dado que nada es perfecto, se dice que el riesgo se reduce al nivel residual asumido por la dirección."(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012, p. 19)

Capítulo III. DESARROLLO DE LA SOLUCIÓN

En este capítulo desarrollaremos un modelo de implementación basándonos en la NTP-ISO/IEC 27005:2018 (Tecnología de la información. Técnicas de seguridad. Gestión de riesgos de la seguridad de la información) aplicando la metodología MAGERIT (Metodología de análisis y gestión de riesgos de los sistemas de información) en el área funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco.

Se compone de los siguientes pasos:

El primer paso es el "Establecimiento del contexto" en el cual se va a obtener toda la información relevante sobre la organización, es decir, el alcance, límites, estudio de la organización (negocio, misión, visión, valores, estructura y organigrama de la organización).

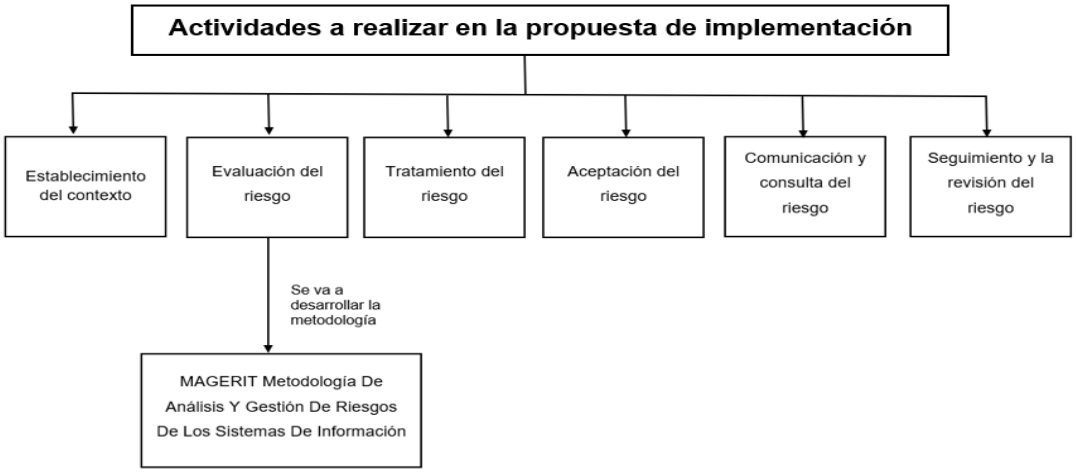
El segundo paso es la "evaluación del riesgo" para lo cual aplicamos la metodología MAGERIT donde se va a identificar y valorar de acuerdo a las dimensiones de seguridad (confidencialidad, integridad y disponibilidad) a los activos, amenazas y vulnerabilidades, salvaguardas y la estimación del estado del riesgo.

El tercer paso denominado "tratamiento del riesgo" consiste en la implementación de un plan de tratamiento de riesgos en función del resultado obtenido en el proceso de evaluación de riesgo.

El cuarto paso es la "aceptación del riesgo" en el cual los riesgos y el plan de tratamiento obtenidos anteriormente deben ser revisados y aprobados por los directores de la organización.

Imagen 3

Actividades a realizar en la propuesta de implementación.



Fuente: Elaboración propia adaptada del libro ISO/IEC 27005:2018(2018).

PASO 1: Establecimiento del contexto

(Capítulo 7, libro ISO/IEC 27005:2018)

- **Nombre de la institución**

  Dirección Desconcentrada de Cultura de Cusco

- **Descripción de la institución**

  La Dirección Desconcentrada de Cultura del Cusco es una institución encargada de proteger, conservar y difundir el patrimonio cultural y natural de la región Cusco, promoviendo el desarrollo sostenible y la valorización de la cultura como un factor clave para el desarrollo integral de la sociedad.

1. Propósito

(7.1. Consideraciones generales, libro ISO/IEC 27005:2018)

La propuesta de implementación se realizará dentro del marco de trabajo para el Área Funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco. Con el propósito de identificar, evaluar y gestionar los riesgos relacionados con la seguridad de la información de manera sistemática y efectiva. Colaborando de esta manera a que la institución comprenda y mitigue eventuales riesgos relacionados con la seguridad de la información, abordando aspectos como amenazas, vulnerabilidades para los activos.

2. Criterios básicos

(7.2. Criterios básicos, libro ISO/IEC 27005:2018)

2.1. Criterio de valoración del riesgo

En este criterio se van a valorar los riesgos (Bajo, Medio y Alto). Para determinar dicha valoración se va a considerar los valores del impacto de la probabilidad de ocurrencia.

Con respecto al impacto se tendrán los siguientes valores:

- 37-45 Catastrófico
- 28-36 Crítico
- 19-27 Medio
- 10-18 Menor

- 1-9 Insignificante

Con respecto a la probabilidad se tendrán los siguientes valores:

- 1 Insignificante
- 2 Moderada
- 3 Dañina
- 4 Extrema

2.2. Criterio de impacto

En este criterio, se medirá el impacto de los riesgos mediante la aplicación de la fórmula descrita en el libro MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas:

valor de un activo x degradación de cada amenaza identificada

2.3. Criterios de aceptación del riesgo

Este criterio describe qué medidas se va a tomar para la aceptación de los riesgos para lo cual se va a considerar el costo, beneficio de la implementación de los planes de tratamiento (salvaguardas).

3. Alcance y límites

(7.3. El alcance y los límites, libro ISO/IEC 27005:2018)

3.1. Los objetivos estratégicos del negocio, las estrategias y las políticas de la organización

- Los objetivos estratégicos del negocio de la organización
  - **Misión**

    La Dirección Desconcentrada de Cultura de Cusco establece, ejecuta y supervisa las políticas nacionales y sectoriales del Estado en materia de cultura, a través de sus áreas programáticas relacionadas con el Patrimonio Cultural de la Nación, la gestión de las industrias culturales y la pluralidad creativa en todo el territorio peruano. También tiene la labor de concertar, articular y coordinar la política estatal de la implementación del derecho a la consulta, correspondiendo a los gobiernos regionales y locales la decisión final sobre la medida.

- **Visión**

  La Dirección Desconcentrada de Cultura de Cusco es una institución reconocida como eje fundamental del desarrollo sostenible del país, que promueve la ciudadanía intercultural, la integración social y la protección del patrimonio cultural de la nación, facilitando un mayor acceso a la población, a los productos culturales y artísticos y afianzando la identidad peruana.

- Las estrategias de la organización: Son los principios rectores (valores morales) de la organización:
  - compromiso
  - equidad
  - responsabilidad
  - honestidad
  - respeto
  - tolerancia

3.2. Los procesos del negocio

Se identificaron los siguientes procesos de negocio que ayudan a lograr los objetivos específicos de la Dirección Desconcentrada de Cultura de Cusco.

- Crear estrategias de preservación y conservación del patrimonio material e inmaterial.
- Orientar, fomentar, promocionar las industrias culturales y las industrias vinculadas a la expresión artística.
- Promover y garantizar la igualdad social y derechos de los pueblos indígenas, generando mecanismos para difundir una práctica intercultural evitando cualquier tipo de exclusión o discriminación de los diferentes pueblos del país, construyendo y fortaleciendo la identidad nacional.
- Brindar orientación, información y venta de tickets al público usuario, atendiendo los trámites, permisos que requieren para la construcción, ampliación de sus inmuebles, entre otros.
- Realizar la supervisión, fiscalización, defensa de los intereses, proyectos especiales, programas de la DDCC, y la sanción.

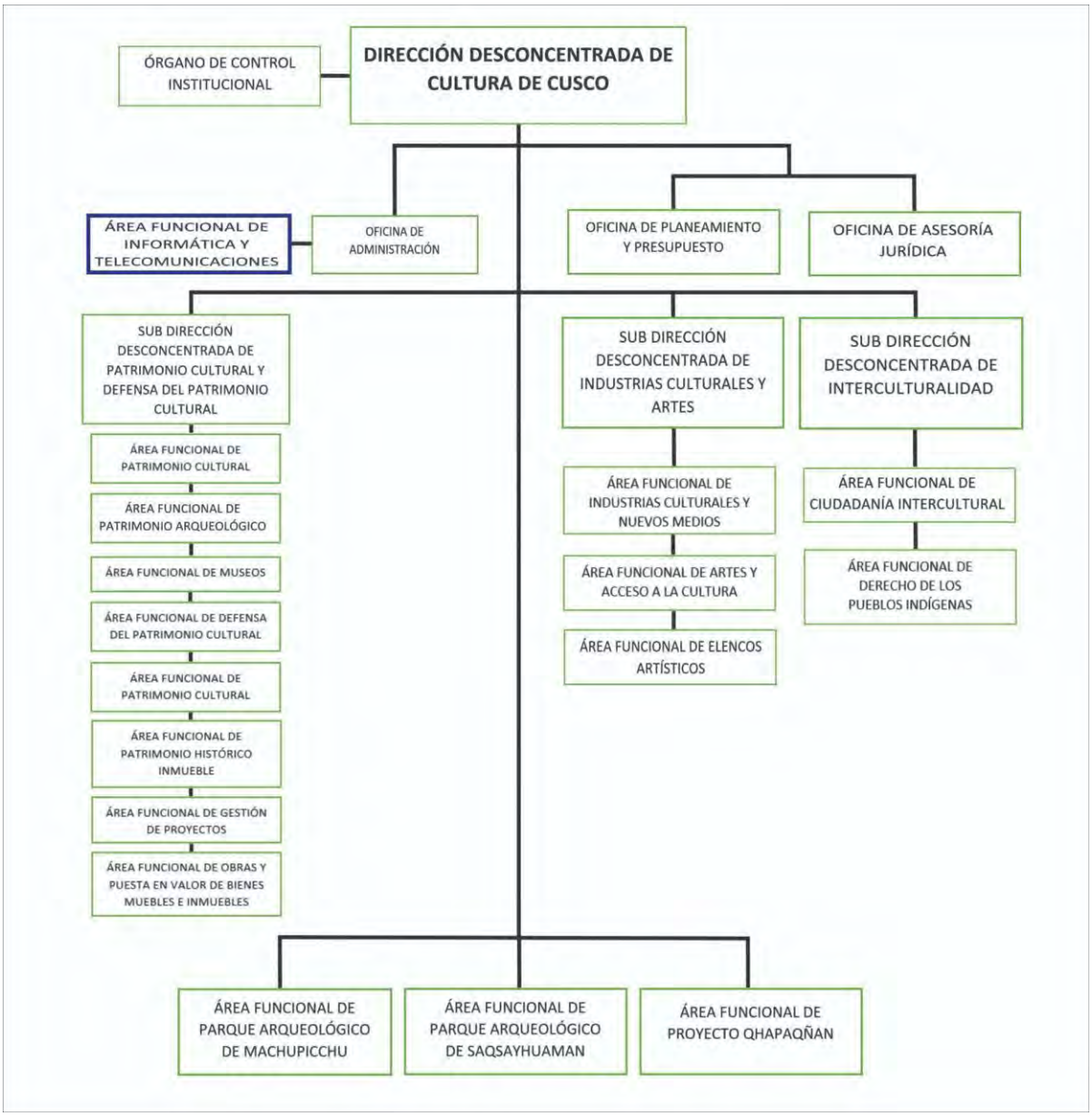
- Concluir procesos de investigación a través de la publicación de resultados no solo en medios impresos, sino también en medios virtuales, como Twitter, blogs, publirreportajes, entre otros.

3.3. Las funciones y estructura de la organización

- Funciones de la organización
    - Normar, conservar, promover, inventariar y difundir el Patrimonio Cultural de su Jurisdicción en armonía con la política trazada por el órgano central.
    - Fomentar, desarrollar y difundir las diversas manifestaciones culturales, así como las expresiones del folklore y del arte popular.
    - Fomentar, mediante acciones de estímulo que incluye el otorgamiento de premios, la libre creación intelectual y artística en todas sus manifestaciones culturales.
    - Establecer en coordinación con los organismos turísticos una política de conocimiento y acercamiento cultural.
    - Apoyar y promover la cooperación técnica y financiera, nacional e internacional orientada a ejecutar proyectos y programas de desarrollo cultural y de puesta en valor del patrimonio.
    - Reconocer oficialmente, previa evaluación como centros culturales a las entidades que lo soliciten.
    - Realizar y promover investigaciones y acciones culturales.
- Estructura de la organización

Imagen 4

Estructura Organizacional de la Dirección Desconcentrada de Cultura de Cusco.



Fuente:

https://www.culturacusco.gob.pe/dmdocuments/transparencia/organigrama/2019%20-%20ORGANIGRAMA%20DDC.pdf

3.4. La política de seguridad de la información de la organización

La Dirección Desconcentrada de Cultura de Cusco no cuenta con política de seguridad de la información de la organización.

3.5. El enfoque global de la organización a la gestión del riesgo

La Dirección Desconcentrada de Cultura de Cusco no cuenta con un enfoque global.

3.6. Los activos de información

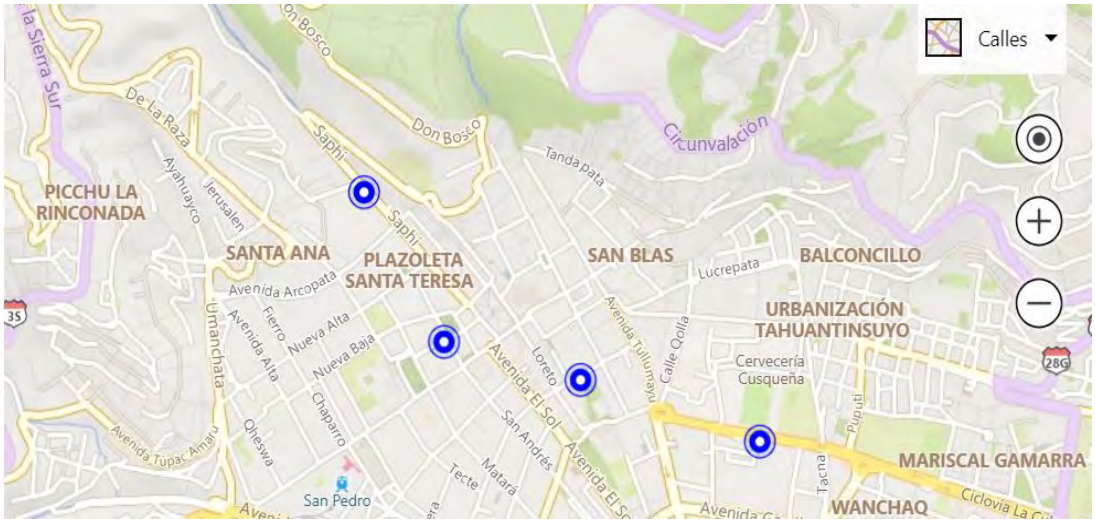
Para la propuesta de implementación se trabajará con los activos brindados por el área funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco.

3.7. Las ubicaciones físicas de la organización y sus características geográficas

- Av. La Cultura 238 Condominio Huáscar -se encuentra la oficina del área funcional de informática y telecomunicaciones
- Calle Saphy N° 723 - se encuentra la oficina del área funcional de informática y telecomunicaciones
- Palacio Inka del Kusikancha, Calle Maruri 340
- Casa Garcilaso, calle Heladeros 165

Imagen 5

Ubicación Geográfica de las sedes de la Dirección Desconcentrada de Cultura de Cusco.



Fuente: https://www.culturacusco.gob.pe/contacto/

3.8. Las restricciones que afectan la organización

Con respecto a nuestra propuesta de implementación no se cuenta con alguna restricción.

3.9. Las expectativas de las partes interesadas (stakeholders)

Que la propuesta de implementación a desarrollar cumpla con los siguientes objetivos:

- Identificar, evaluar y clasificar los riesgos, amenazas y vulnerabilidades que puedan existir en el Área Funcional de Informática y Telecomunicaciones.
- Implementar políticas, técnicas de seguridad y gestión de riesgos.
- Ser capaz de elaborar un informe situacional del Área Funcional de Informática y Telecomunicaciones de la DDCC.

4. Organización para la gestión del riesgo de seguridad de la información

(7.4. Organización para la gestión del riesgo de seguridad de la información, libro ISO/IEC 27005:2018)

El Área Funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco está conformado por:

- Jefe de área
  - ⇒Funciones:
  - Liderar y supervisar el área funcional de Informática y Telecomunicaciones.
- Personal de Desarrolladores / Programadores
  - ⇒Funciones:
  - Desarrollador front end
  - Desarrollador back end
  - Tester de Software
- Personal de Soporte técnico
  - ⇒Funciones:
  - Soporte ofimático
  - Soporte técnico
- Personal de Redes
  - ⇒Funciones:
  - Instalación de redes

- Mantenimiento de redes
- Solución de problemas de red
- Configuración de redes

PASO 2. Evaluación del riesgo

(Capítulo 8, libro ISO/IEC 27005:2018)

Según la norma ISO/IEC 27005:2018 la evaluación del riesgo se desarrolla en 4 actividades, en el cual se va a aplicar la metodología MAGERIT para desarrollar de manera más amplia los riesgos a identificar.

2.1. Descripción general de la evaluación del riesgo de seguridad de la información

(8.1. Descripción general de la evaluación del riesgo de seguridad de la información , libro ISO/IEC 27005:2018)

Los riesgos identificados serán descritos de forma cualitativa, de acuerdo a la norma ISO/IEC 27005:2018 se clasifica en:

2.2. Identificación del riesgo

(8.2. Identificación del riesgo, libro ISO/IEC 27005:2018)

Se va a determinar lo siguiente:

- Identificación de activos (MAR.1. Caracterización de los activos)
- Identificación de las amenazas (MAR.2. Caracterización de las amenazas)
- Identificación de controles existentes: La Dirección Desconcentrada de Cultura de Cusco no cuenta con dichos controles.
- Identificación de vulnerabilidades (MAR.2. Caracterización de las amenazas: MAR.2.1. Identificación de las amenazas)

2.3. Análisis del riesgo

(8.3. Análisis del riesgo, libro ISO/IEC 27005:2018)

Se va a determinar lo siguiente:

- Metodologías de análisis del riesgo: Se realizará un análisis cuantitativo y cualitativo de los riesgos. (8.3.1 Metodologías de análisis del riesgo, libro *ISO/IEC 27005:2018)*
- Determinación del nivel de riesgo (MAR.4. Estimación del estado de riesgo**)**

2.4. Valoración del riesgo

(8.4. Valoración del riesgo, libro ISO/IEC 27005:2018)

Se va a determinar lo siguiente:

- Evaluación de los riesgos priorizados de acuerdo a los criterios de valoración del riesgo (MAR.4. Estimación del estado de riesgo)

Adicionalmente se implementará salvaguardas (MAR.3. Caracterización de las salvaguardas)

Se desarrollará de manera detallada la metodología MAGERIT:

MAR.1. Caracterización de los activos

(3. Método de análisis de riesgos - 3.1.1. Paso 1: Activos, libro MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método, (pp.22-27))

MAR.1.1. Identificación de los activos

(3.2.1. Tarea MAR.1: Caracterización de los activos, libro MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método, (pp.37-38))

De acuerdo a la encuesta realizada al área funcional de informática y telecomunicaciones se identificó y se clasificaron de acuerdo al tipo de activo. Son los siguientes:

1- [D] Datos/Información

Los datos son la materia prima a partir de la cual se obtiene la información. La información es un activo abstracto que se almacena en un dispositivo o medio (generalmente agrupado como un archivo o base de datos) o se transfiere de un lugar a otro a través de la transmisión de datos.

Con respecto a la encuesta realizada se identificó los siguientes activos:

- Datos de configuración
- Base de datos de la página de web de la DDCC
- Log de actividades (registro de actividades)
- Datos de prueba

- Documentos digitales

2- [K] Claves criptográficas

La criptografía se utiliza para proteger secretos o verificar la identidad de las partes. Las claves de cifrado, que combinan información secreta y pública, son esenciales para que funcionen los mecanismos de cifrado.

Con respecto a la encuesta realizada se identificó los siguientes activos:

- Contraseña de acceso a la base de datos de la página web de la DDCC
- Contraseña de acceso al NVR
- Contraseña de acceso al router

3- [S] Servicio

Función que satisface una necesidad de los usuarios (del servicio). Esta sección contempla servicios prestados por el sistema.

Con respecto a la encuesta realizada se identificó los siguientes activos:

- Página Help Desk (mesa de ayuda)
- Páginas web institucionales: se encuentran las siguientes páginas web:
    - Dirección Desconcentrada de Cultura de Cusco
    - Machupicchu - Página Oficial
    - Casa Garcilaso
    - Biblioteca Central Dirección Desconcentrada de Cultura de Cusco

      Se encuentran los siguientes sistemas web:
    - Siga Institucional
    - Siga Mef Web
    - Seguimiento PAS
    - Sistema ERP
    - Correo institucional Zimbra
- Soporte técnico

4- [SW] Software - Aplicaciones informáticas

Se le conoce también al software como programa o aplicaciones. Las aplicaciones gestionan, analizan y transforman datos para que la información pueda utilizarse para prestar servicios.

Con respecto a la encuesta realizada se identificó los siguientes activos:

- Aplicaciones como:
    - Mongo DB
    - SQL server
    - Java
    - Javascript
    - Net beans
    - Typescript
    - Data grips
    - IntelliJ IDIA
    - Laravel
    - Django
    - ExpressJs
    - Angular
    - Jitsi Meet
- Antivirus
- Sistemas Operativos
- Ofimática

5- [HW] Hardware - Equipamiento informático

Se refiere a activos físicos tangibles diseñados para respaldar directa o indirectamente los servicios proporcionados por una organización, por lo que almacenan datos de manera temporal o permanente. Sirven de respaldo en la ejecución de aplicaciones informáticas o son responsables del procesamiento o la transmisión de datos.

Con respecto a la encuesta realizada se identificó los siguientes activos:

- Computadoras desktops (CPU, teclado, estabilizador, mouse, cámara, micrófono)
- Laptops
- Equipos de reprografía
- Firewall
- Router

6- [COM] Redes de comunicaciones

Son un medio de transporte para transferir datos de un lugar a otro.

Con respecto a la encuesta realizada se identificó los siguientes activos:

- Internet
- Internet de respaldo

7- [Media] Soportes de información

Se incluyen los dispositivos físicos que permiten el almacenamiento permanente o al menos a largo plazo de la información.

Dentro de estos dispositivos se clasifican en electrónicos (información digital guardada en un dispositivo de almacenamiento físico) y no electrónicos (información digital guardada en material impreso)

Con respecto a la encuesta realizada se identificó los siguientes activos, en este caso exceptuando el material impreso ya que no hacen uso de ello:

- USB
- Disco duro externo
- Servidores
- Repositorios de código fuente: el cual hacen uso de GitHub, GitLab

8- [AUX] Equipamiento Auxiliar

Se incluyen otros equipos que soportan los sistemas de información pero que no están directamente relacionados con los datos.

Con respecto a la encuesta realizada se identificó los siguientes activos:

- Generador eléctrico
- UPS de alimentación de emergencia
- Equipo de climatización (aire acondicionado)
- Mobiliario
- NVR
- Equipamiento de destrucción de soportes de información, con respecto a este activo no se consideró ya que no cuentan con dicho equipamiento.

9- [L] Instalaciones

Se incluyen los lugares donde se alojan los sistemas de información y comunicación.

Con respecto a la encuesta realizada se identificó los siguientes activos:

- Oficina (local)

10-[P] Personal

Se incluye el personal relacionado con los sistemas de información.

Con respecto a la encuesta realizada se identificó los siguientes activos:

- Jefe de área
- P.Desarrolladores / Programadores
- P.Soporte técnico
- P.Redes

MAR.1.2. Dependencias entre activos

(3.2.1. Tarea MAR.1: Caracterización de los activos*, libro MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método, (p.39))*

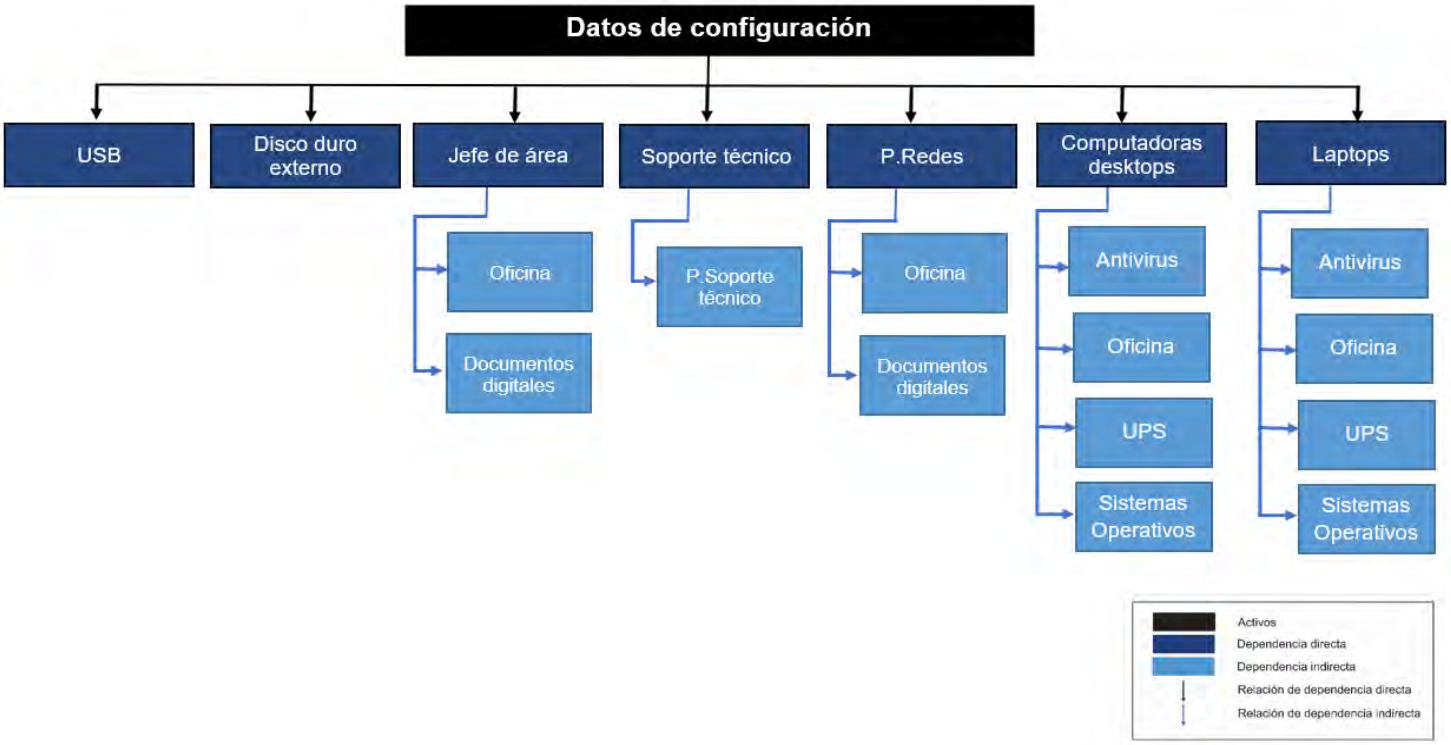
Con respecto a la clasificación de los activos se va a identificar si tienen alguna dependencia directa, indirecta o bidireccional.

Dependencias directas e indirectas

En las siguientes imágenes se muestran mapas conceptuales de los activos, donde se evidencian sus dependencias directas e indirectas de manera descendente.

Imagen 6

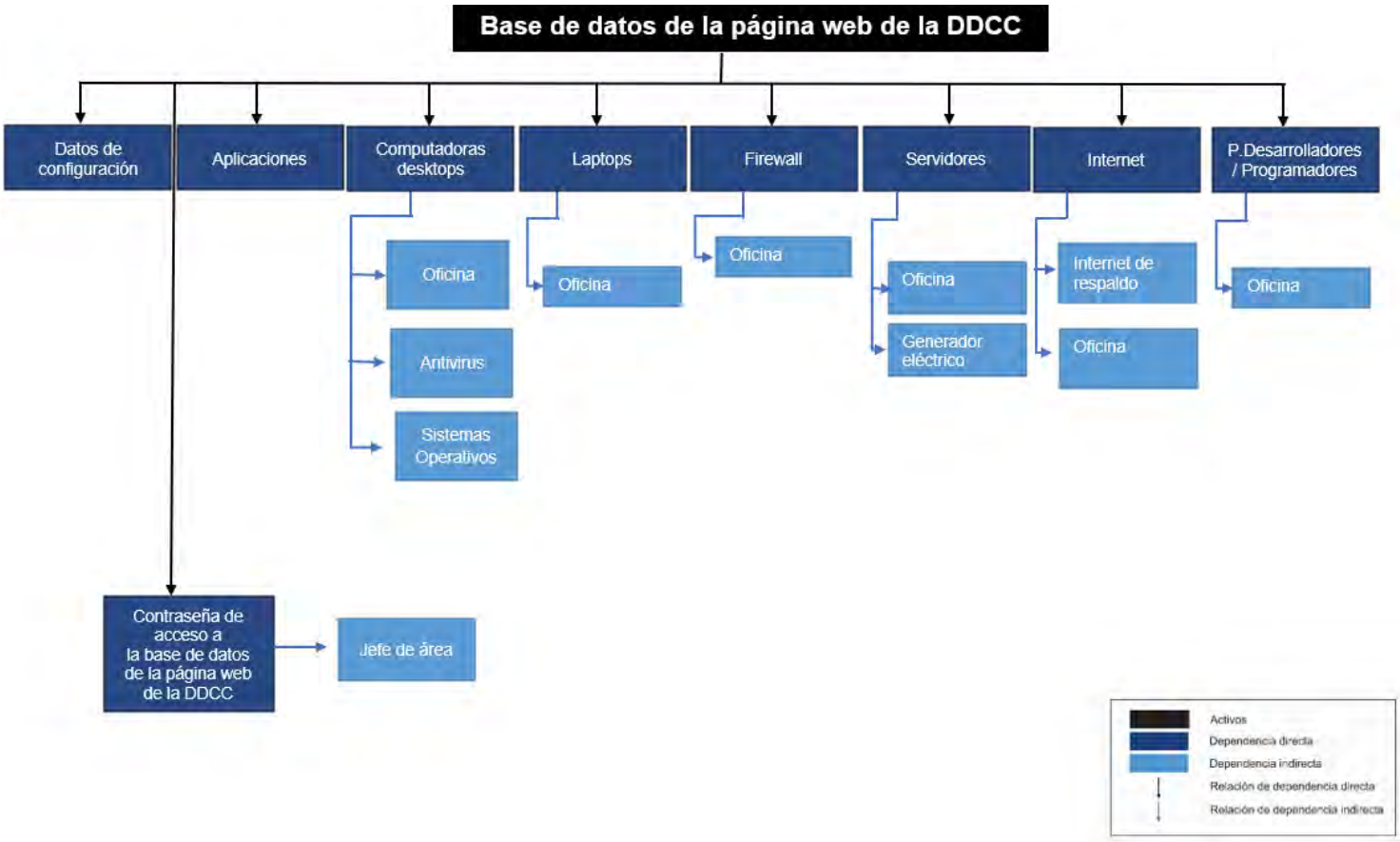
Mapa conceptual de las dependencias directas e indirectas del activo: Datos de configuración.



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1)

Imagen 7

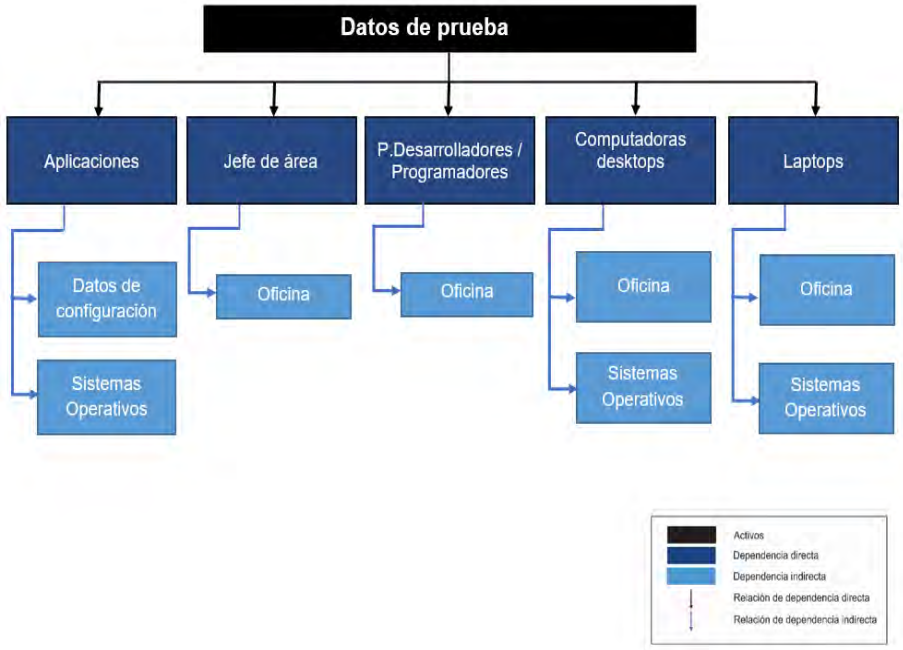
Mapa conceptual de las dependencias directas e indirectas del activo: Base de datos de la página web de la DDCC



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 8

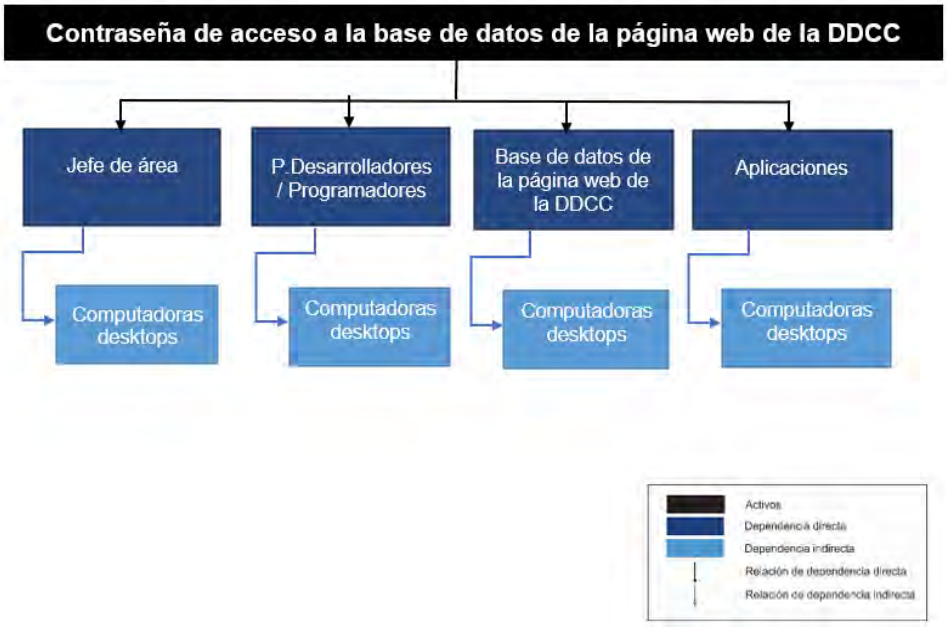
Mapa conceptual de las dependencias directas e indirectas del activo: Datos de prueba



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 9

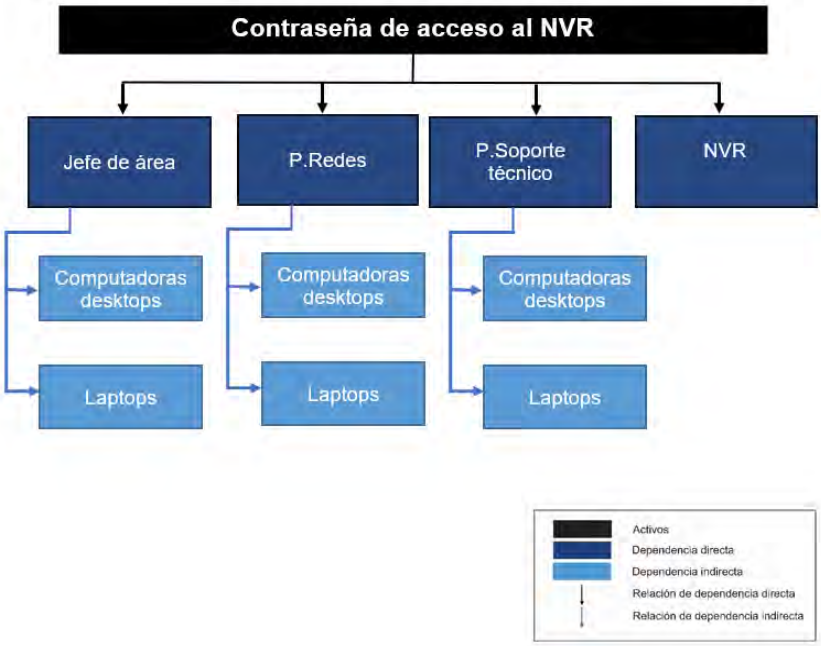
Mapa conceptual de las dependencias directas e indirectas del activo: Contraseña de acceso a la base de datos de la página web de la DDCC



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 10

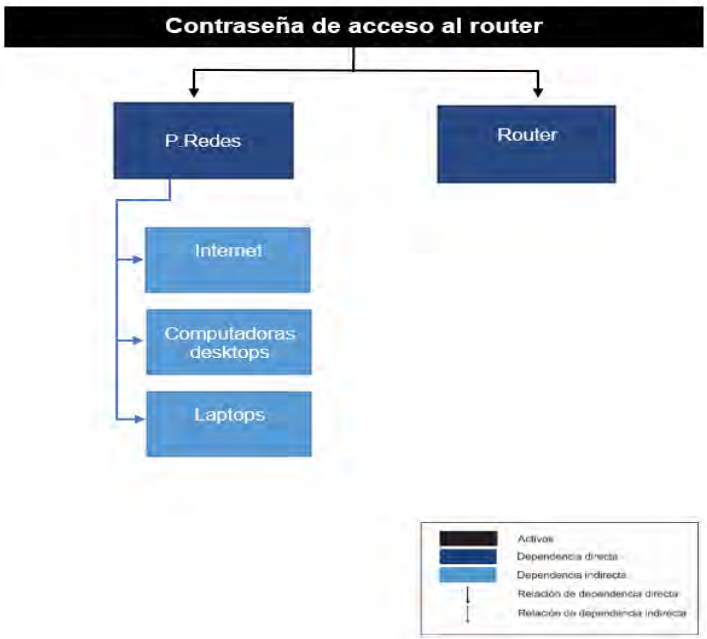
Mapa conceptual de las dependencias directas e indirectas del activo: Contraseña de acceso al NVR



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 11

Mapa conceptual de las dependencias directas e indirectas del activo: Contraseña de acceso al router



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

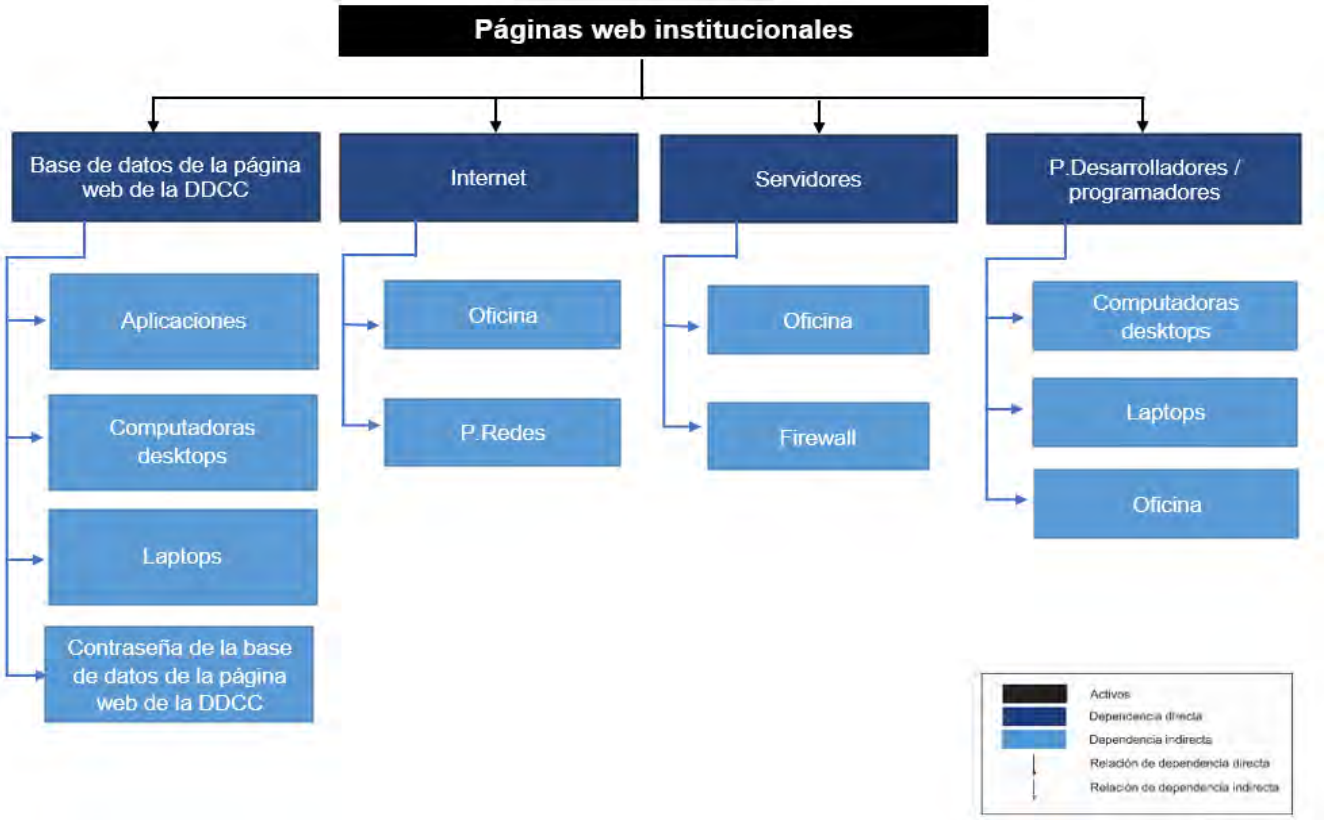
Imagen 12

Mapa conceptual de las dependencias directas e indirectas del activo: Página Help Desk.

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 13

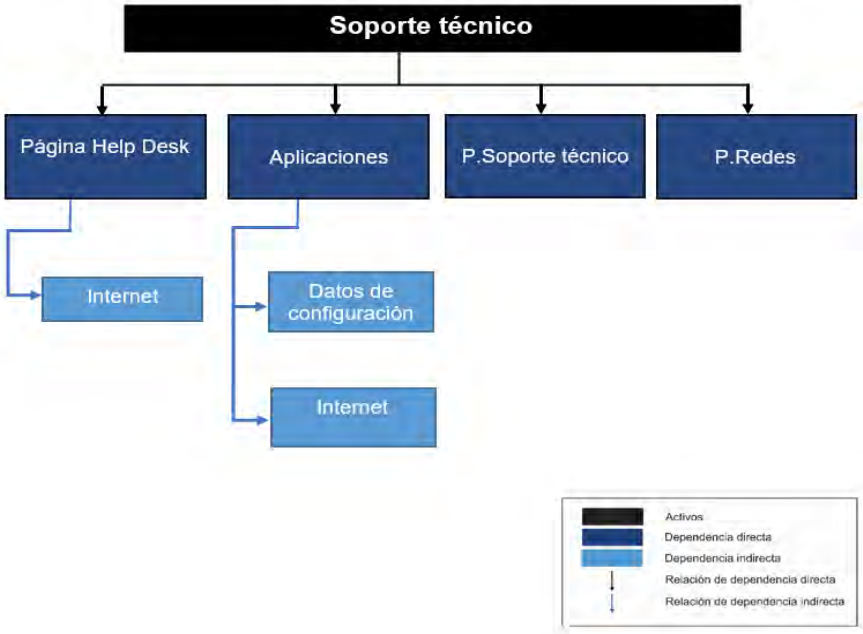
Mapa conceptual de las dependencias directas e indirectas del activo: Páginas web institucionales



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 14

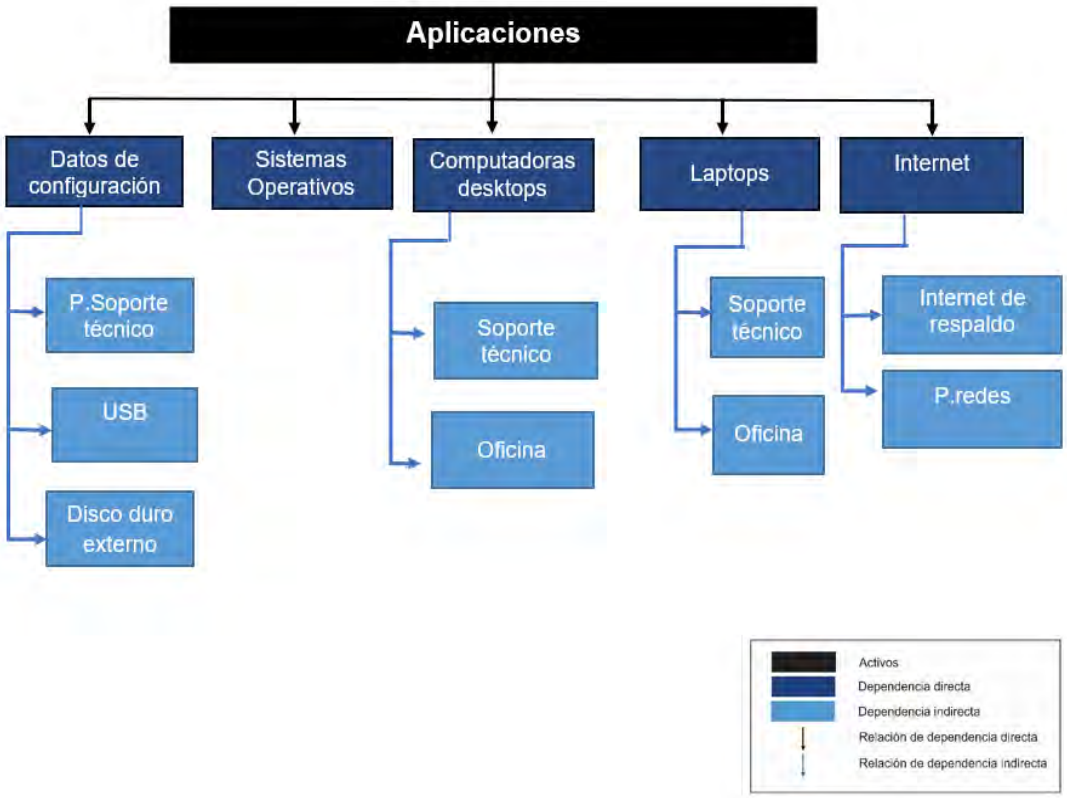
Mapa conceptual de las dependencias directas e indirectas del activo: Soporte técnico



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 15

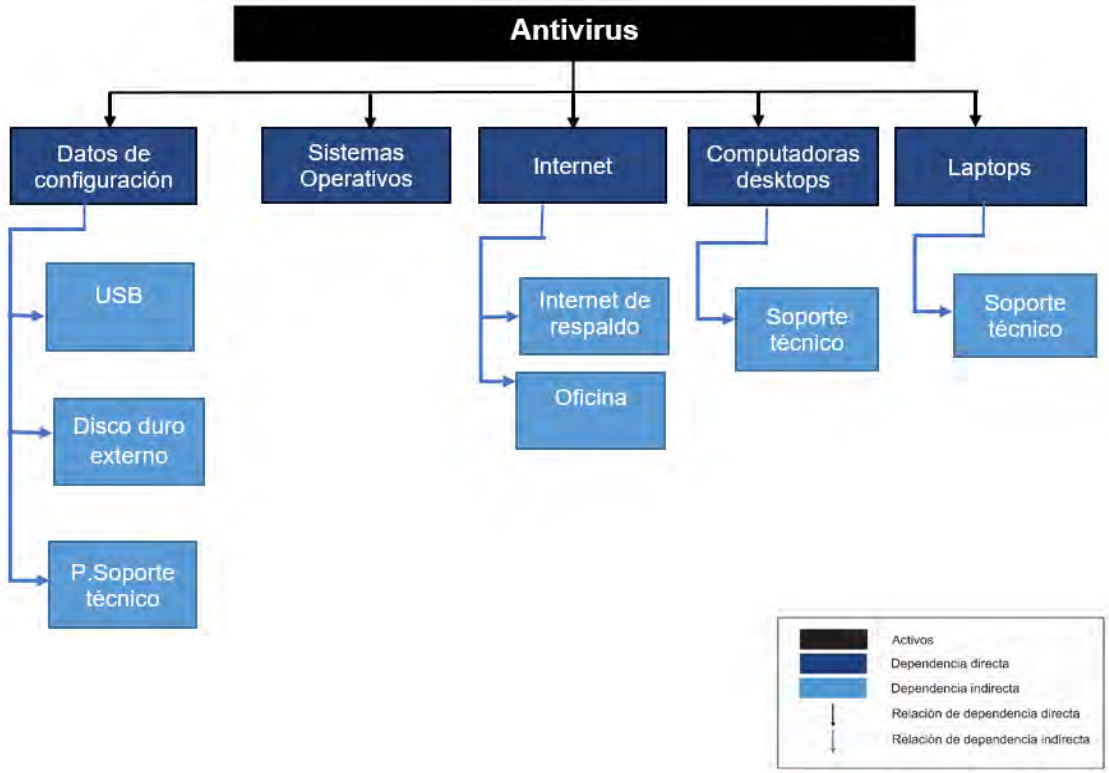
Mapa conceptual de las dependencias directas e indirectas del activo: Aplicaciones



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 16

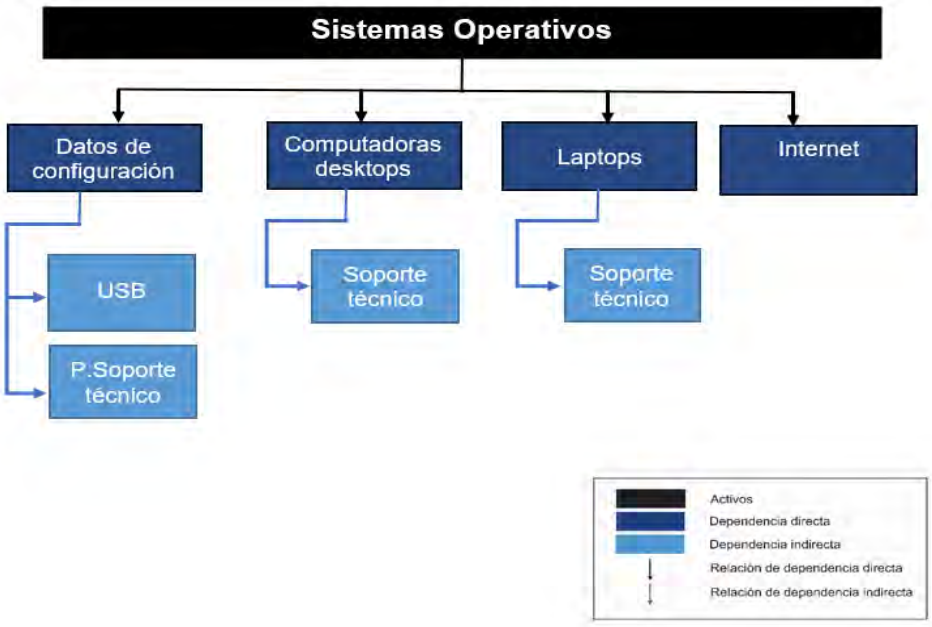
Mapa conceptual de las dependencias directas e indirectas del activo: Antivirus



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 17

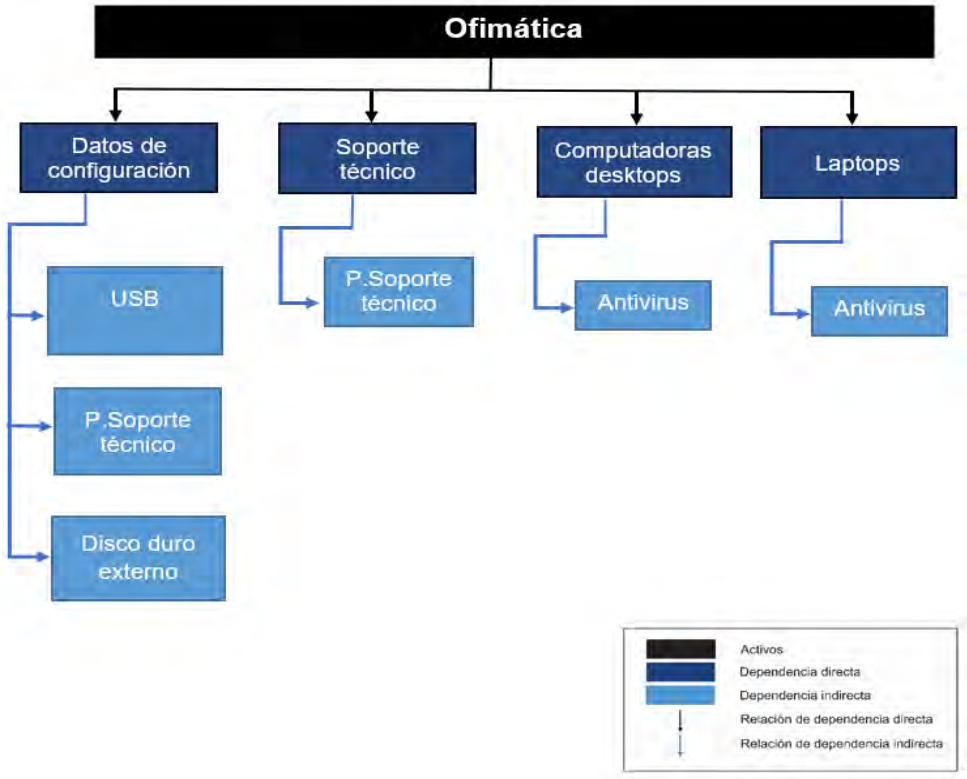
Mapa conceptual de las dependencias directas e indirectas del activo: Sistemas Operativos



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 18

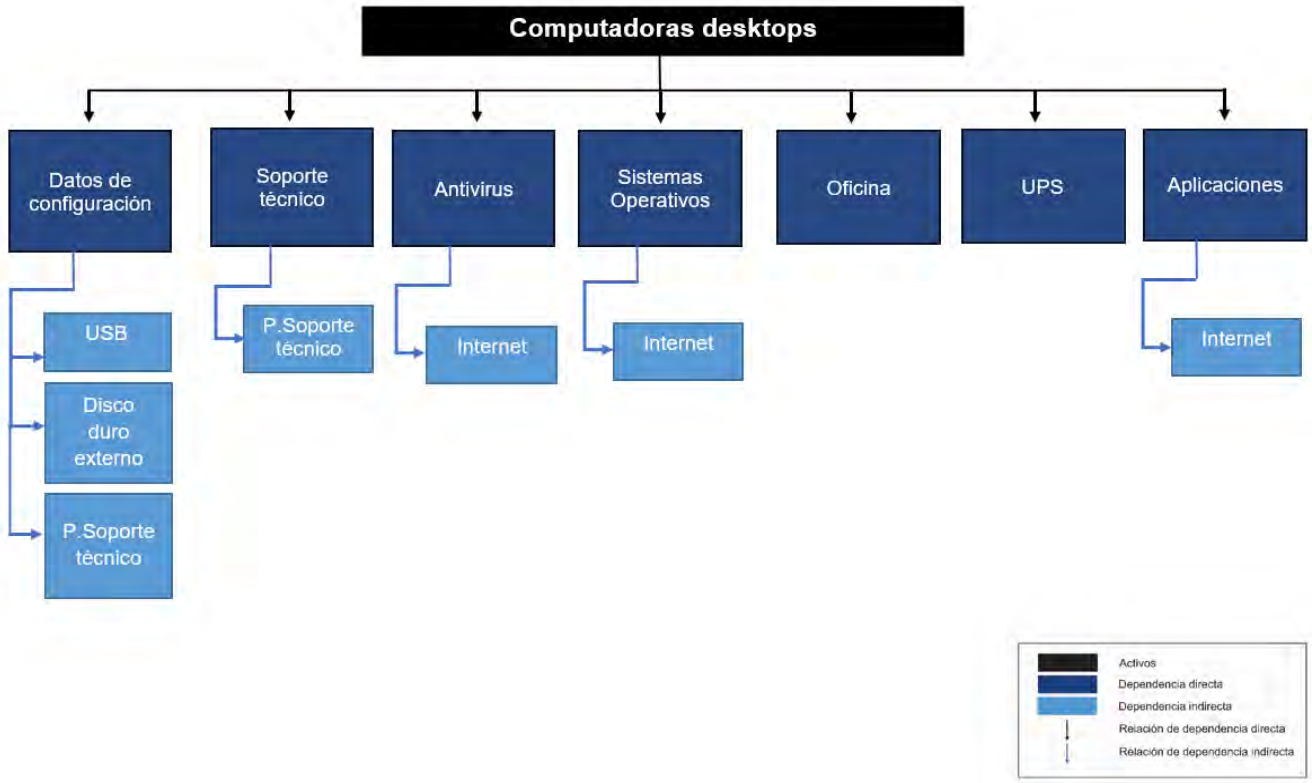
Mapa conceptual de las dependencias directas e indirectas del activo: Ofimática



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 19

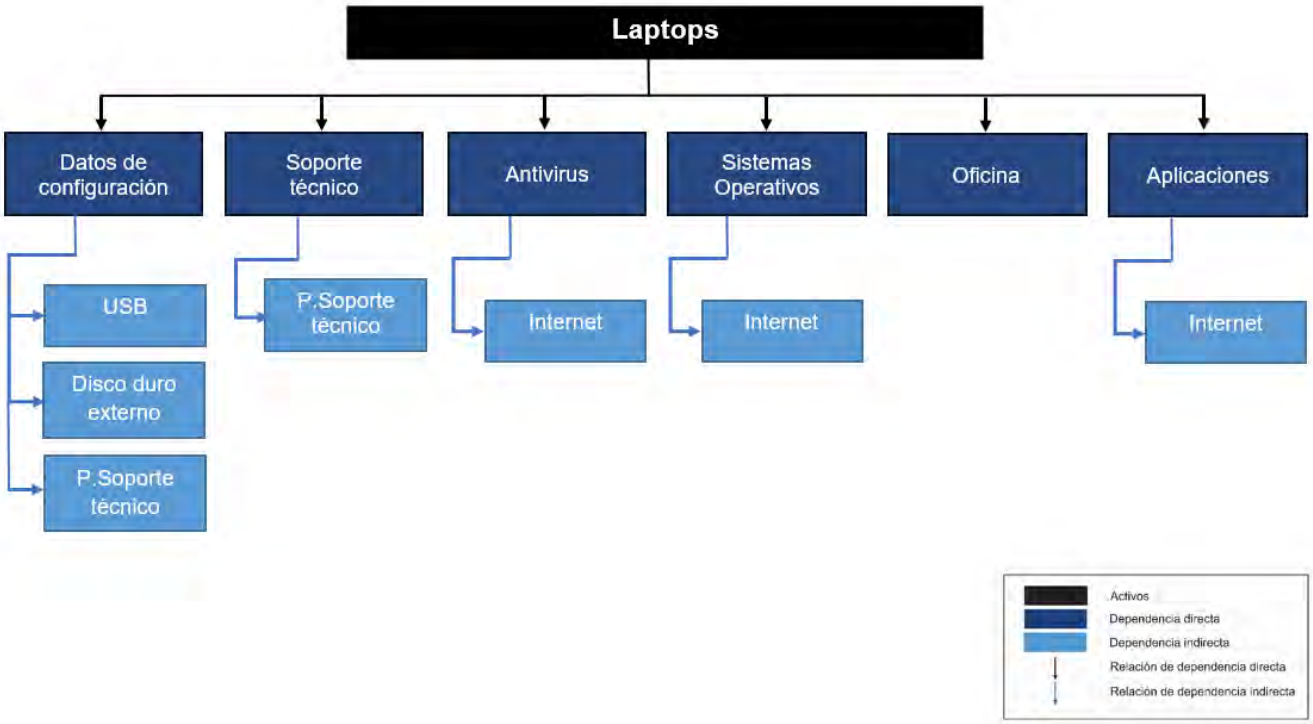
Mapa conceptual de las dependencias directas e indirectas del activo: Computadoras desktops



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 20

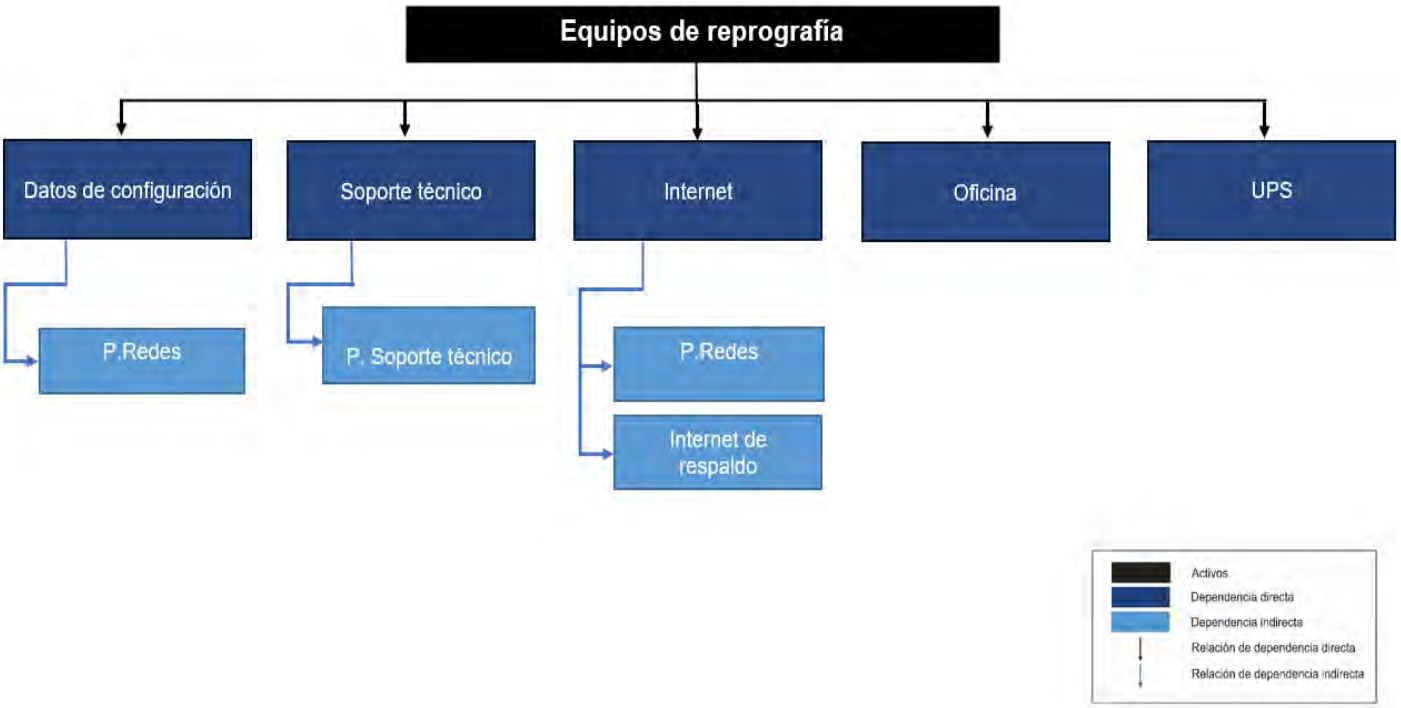
Mapa conceptual de las dependencias directas e indirectas del activo: Laptops



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1)

Imagen 21

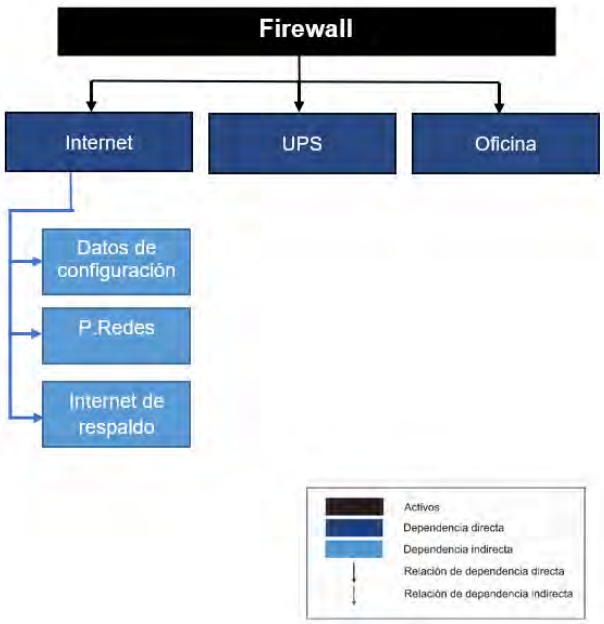
Mapa conceptual de las dependencias directas e indirectas del activo: Equipos de reprografía



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 22

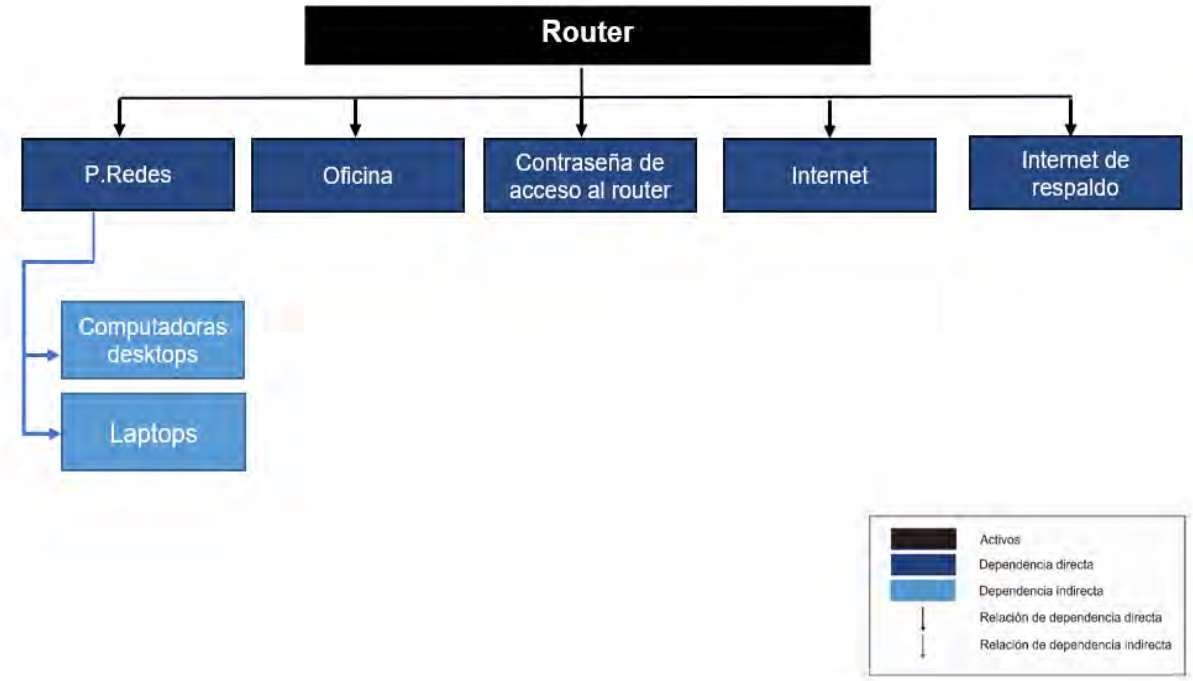
Mapa conceptual de las dependencias directas e indirectas del activo: Firewall



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 23

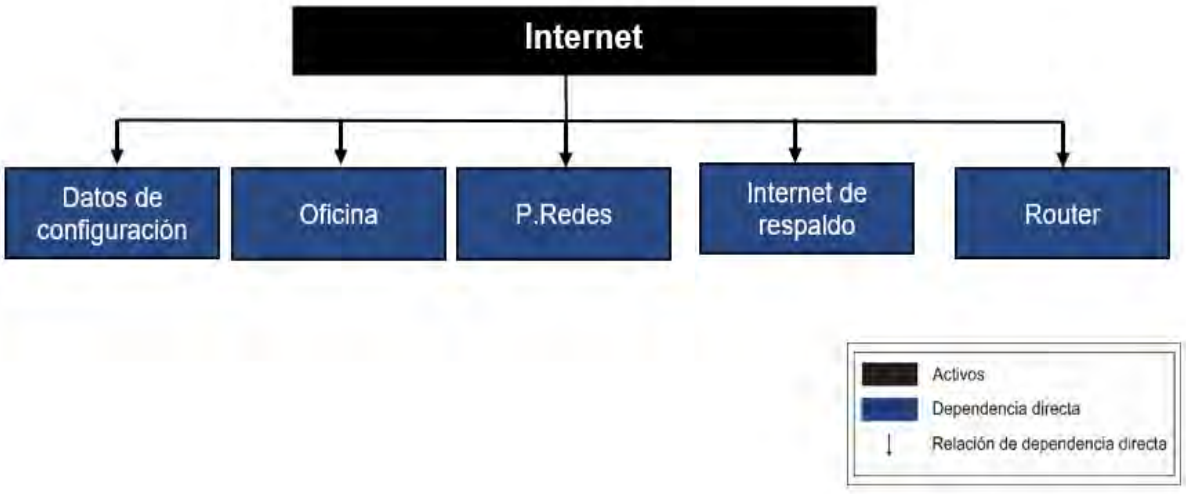
Mapa conceptual de las dependencias directas e indirectas del activo: Router



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 24

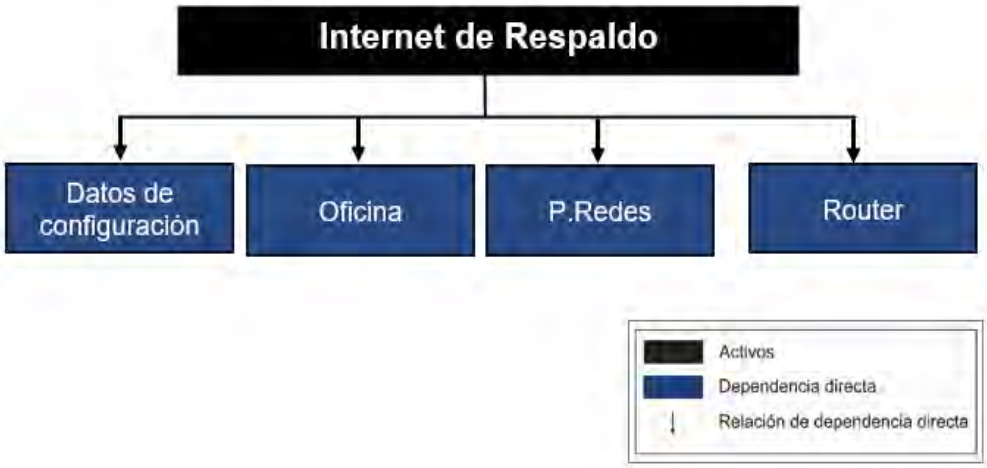
Mapa conceptual de las dependencias directas e indirectas del activo: Internet



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 25

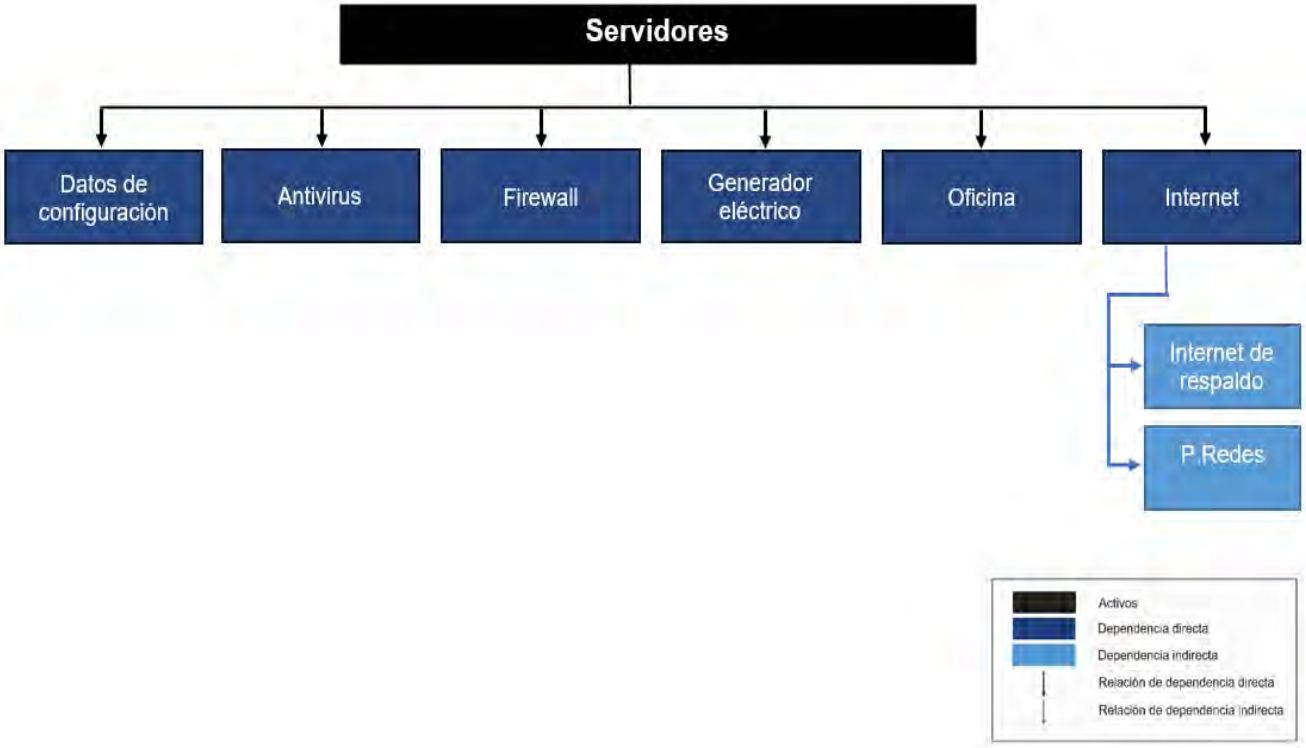
Mapa conceptual de las dependencias directas e indirectas del activo: Internet de respaldo



*Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1)***.**

Imagen 26

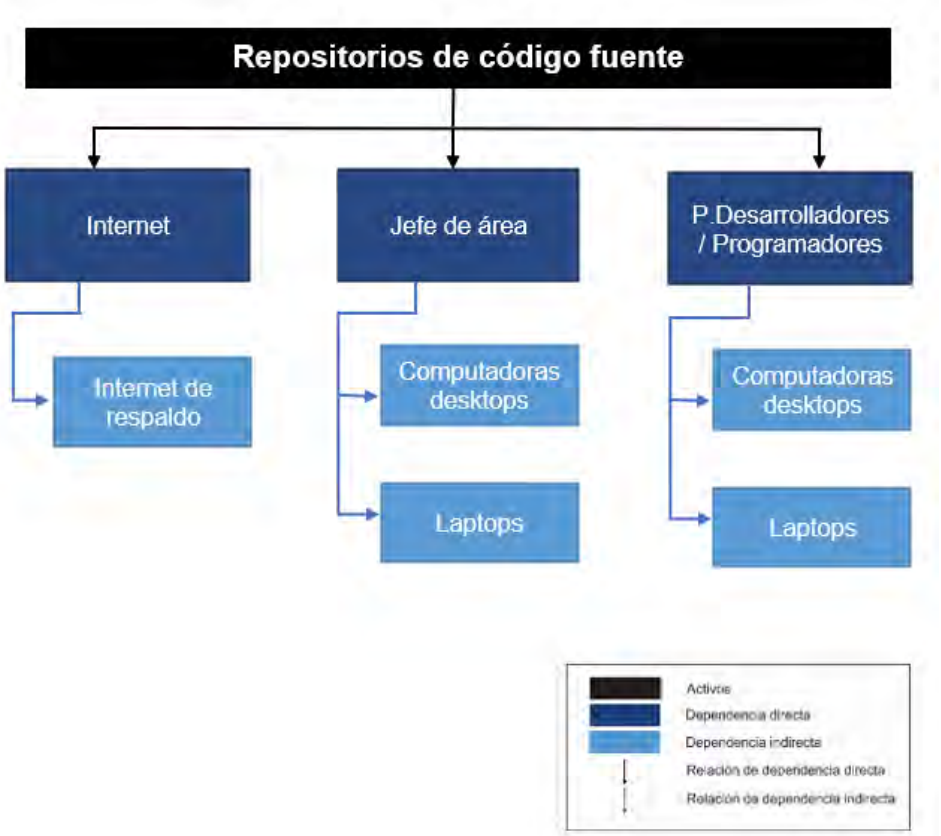
Mapa conceptual de las dependencias directas e indirectas del activo: Servidores



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 27

Mapa conceptual de las dependencias directas e indirectas del activo: Repositorios de código fuente



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 28

Mapa conceptual de las dependencias directas e indirectas del activo: Generador Eléctrico

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 29

Mapa conceptual de las dependencias directas e indirectas del activo: UPS

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 30

Mapa conceptual de las dependencias directas e indirectas del activo: Equipo de climatización

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

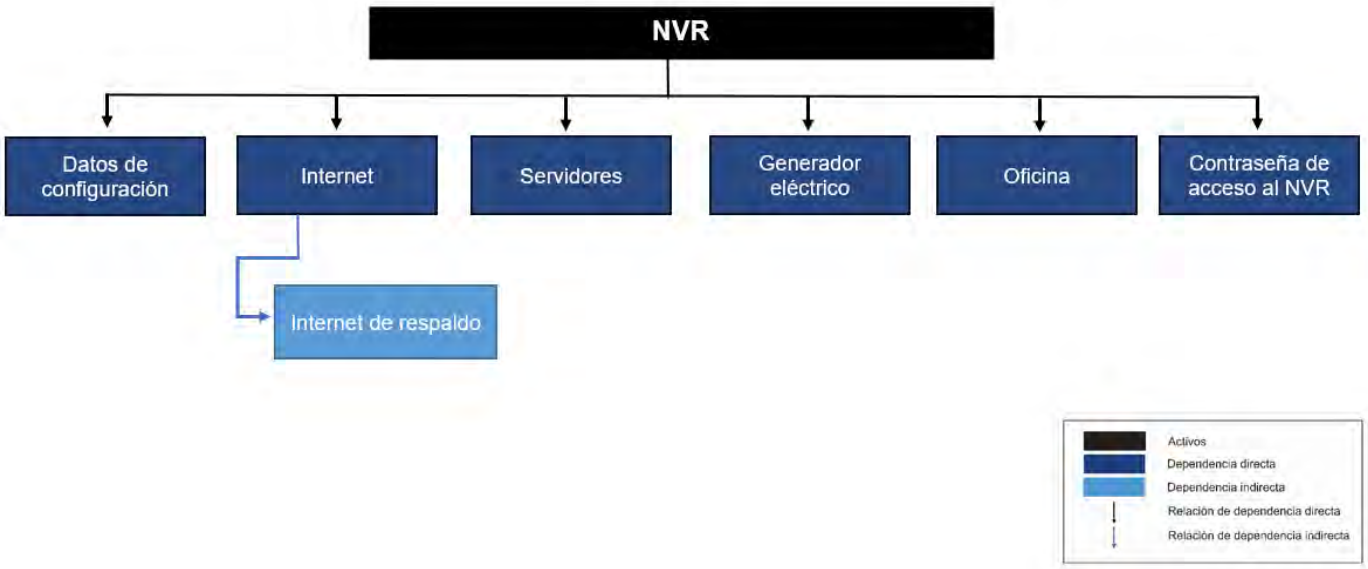
Imagen 31

Mapa conceptual de las dependencias directas e indirectas del activo: Mobiliario

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 32

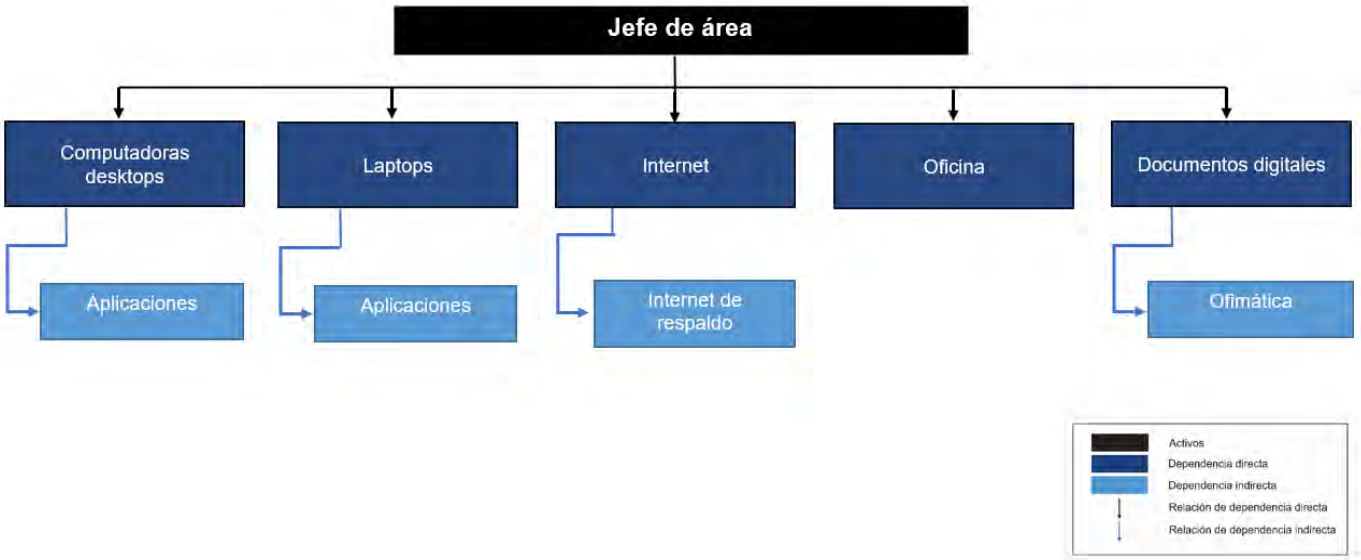
Mapa conceptual de las dependencias directas e indirectas del activo: NVR



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 33

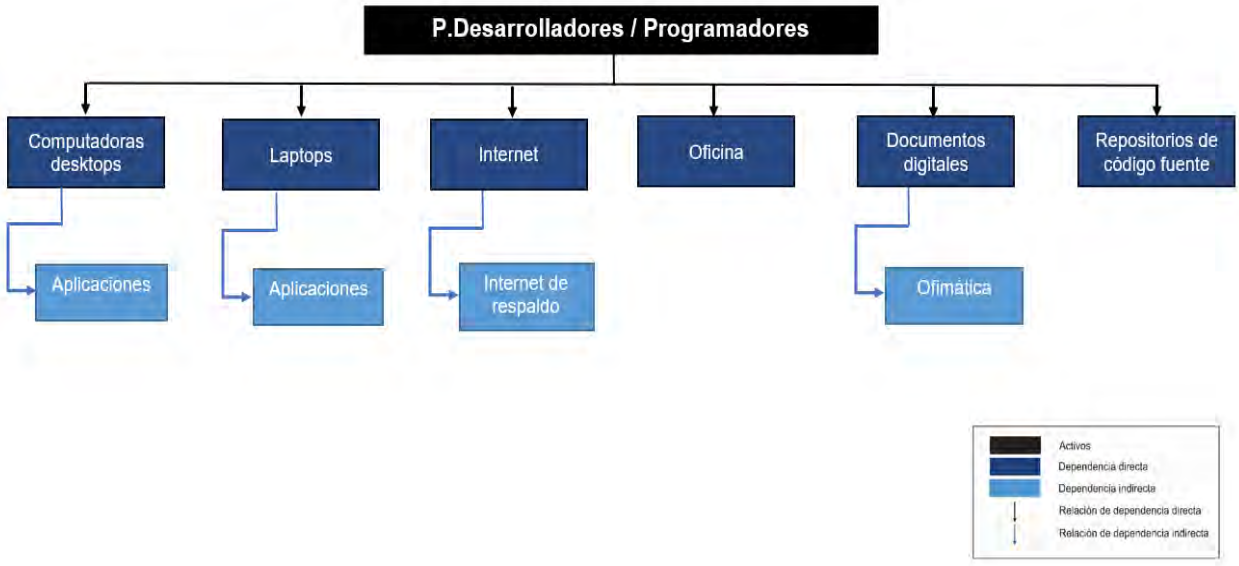
Mapa conceptual de las dependencias directas e indirectas del activo: Jefe de área



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 34

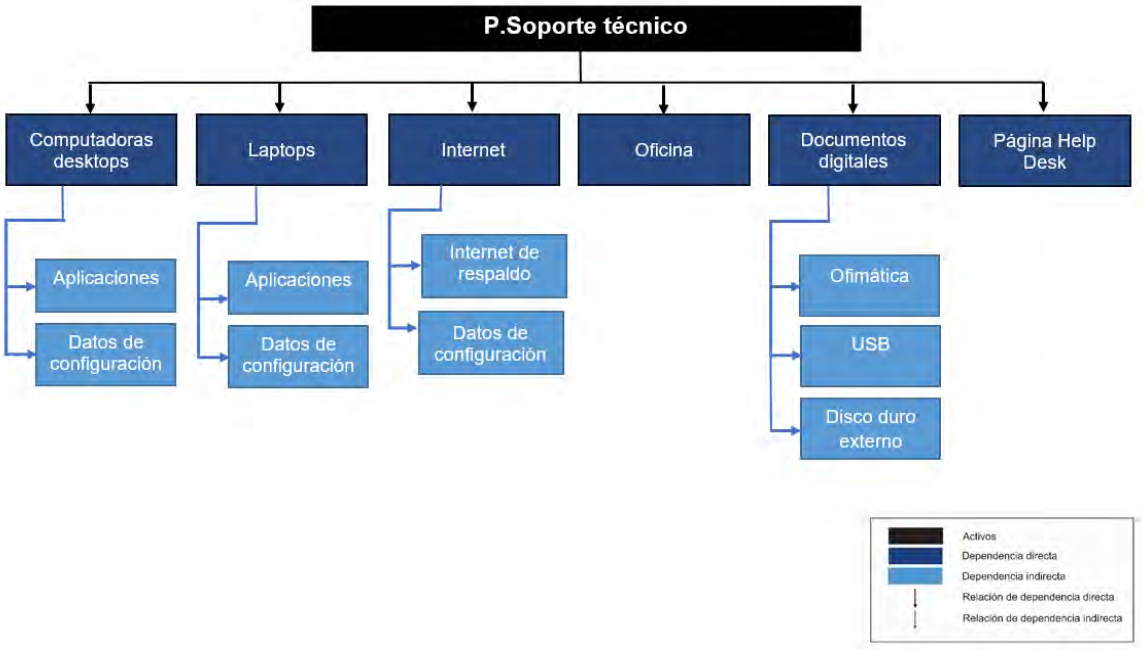
Mapa conceptual de las dependencias directas e indirectas del activo: P. Desarrolladores / Programadores



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 35

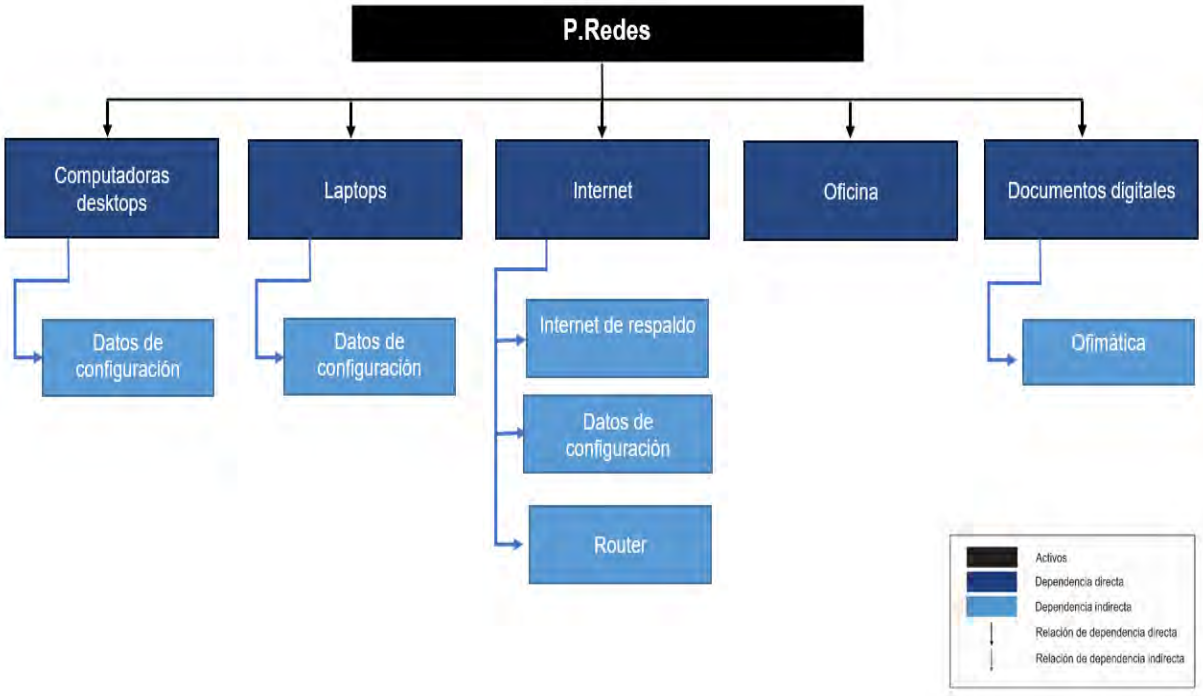
Mapa conceptual de las dependencias directas e indirectas del activo: P. Soporte técnico.



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 36

Mapa conceptual de las dependencias directas e indirectas del activo: P. Redes



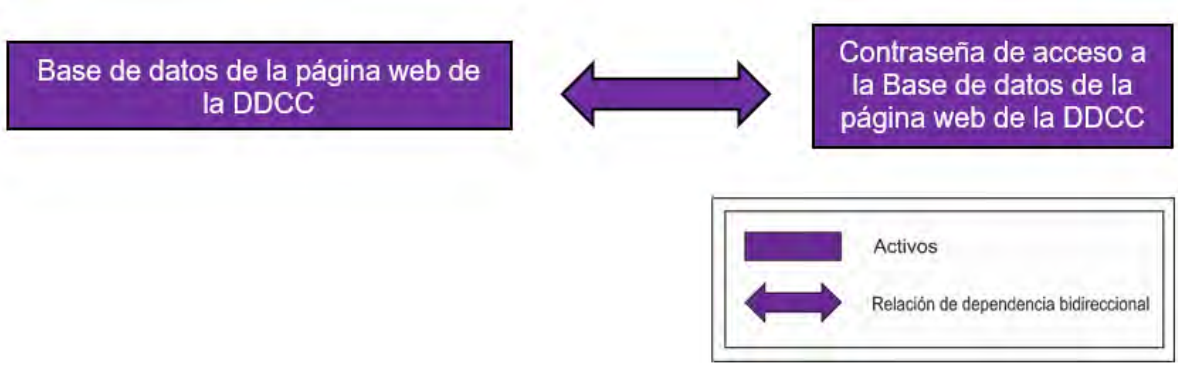
Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Dependencias bidireccionales

En las siguientes imágenes se muestran a los activos que cuentan con dependencias bidireccionales entre ellos.

Imagen 37

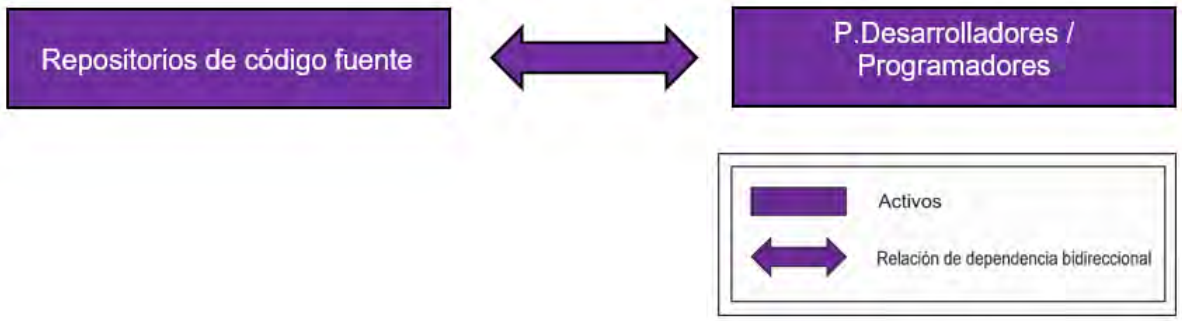
Relación de dependencia bidireccional del activo: Base de datos de la página web de la DDCC



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 38

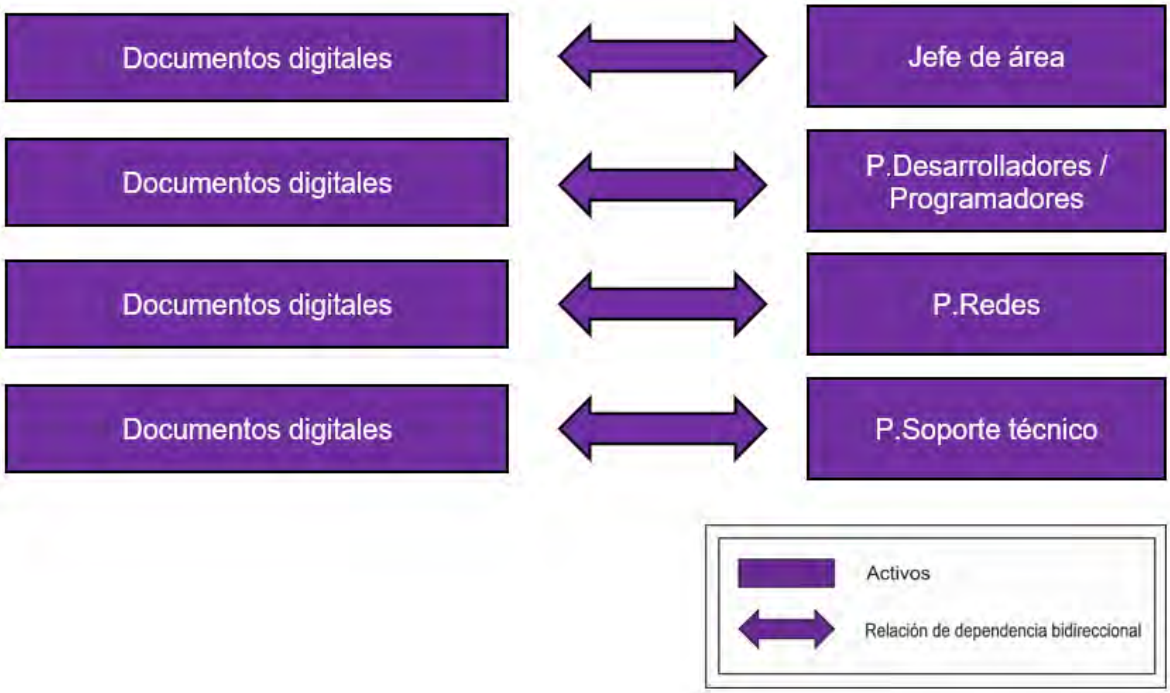
Relación de dependencia bidireccional del activo: Repositorios de código fuente



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 39

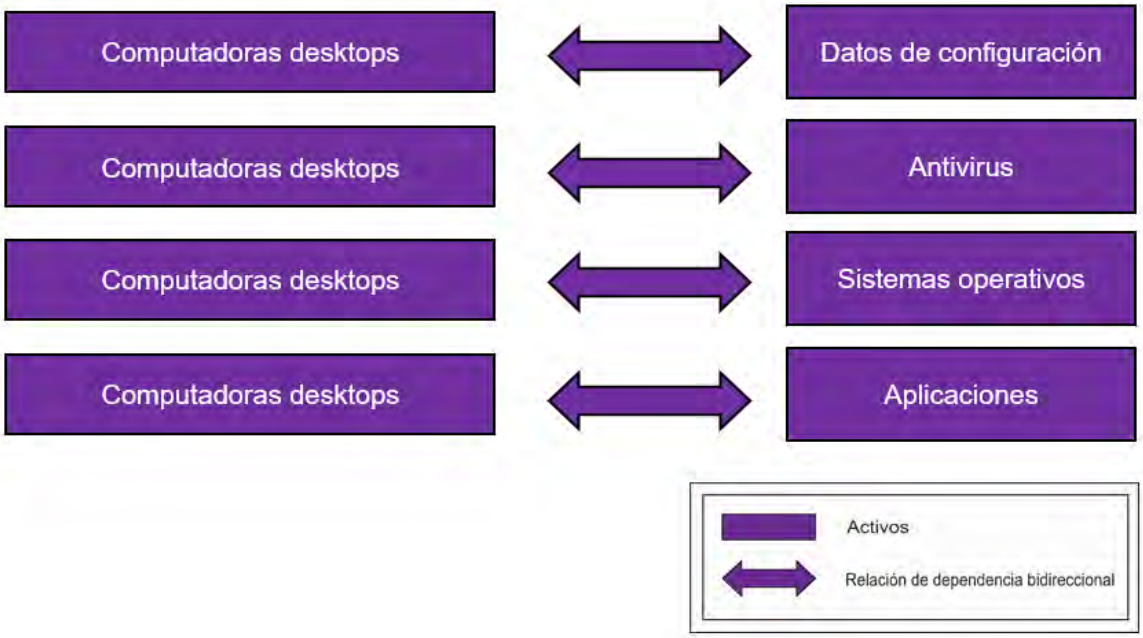
Relación de dependencias bidireccionales del activo: Documentos digitales



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 40

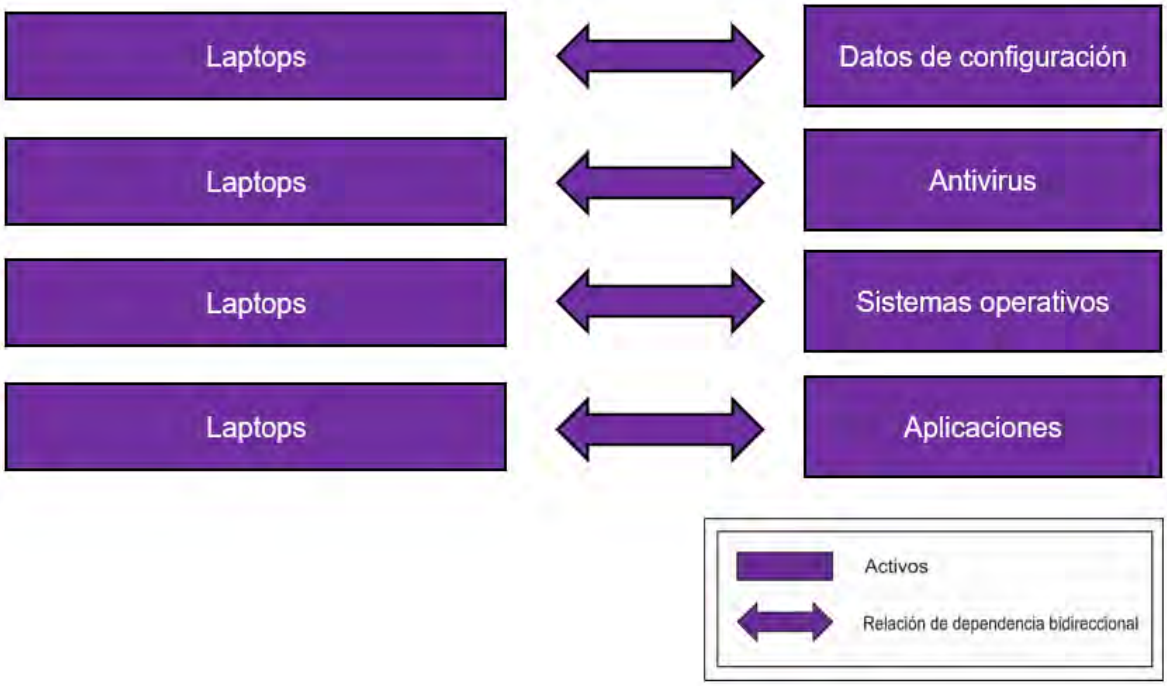
Relación de dependencias bidireccionales del activo: Computadoras desktops



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 41

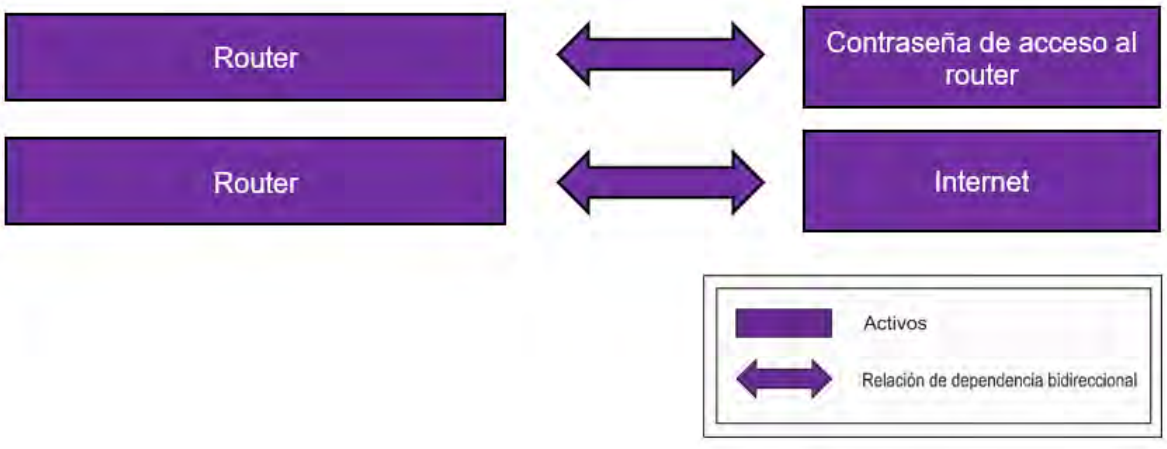
Relación de dependencias bidireccionales del activo: Laptops



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 42

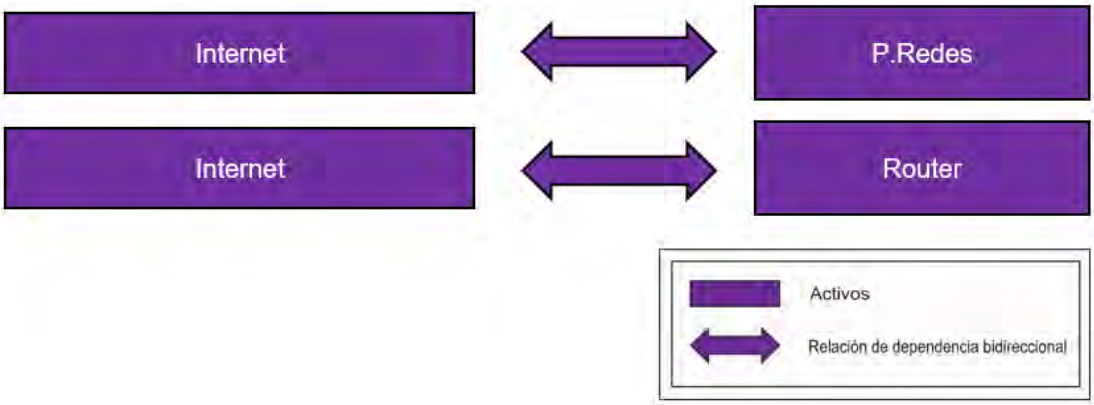
Relación de dependencias bidireccionales del activo: Router



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 43

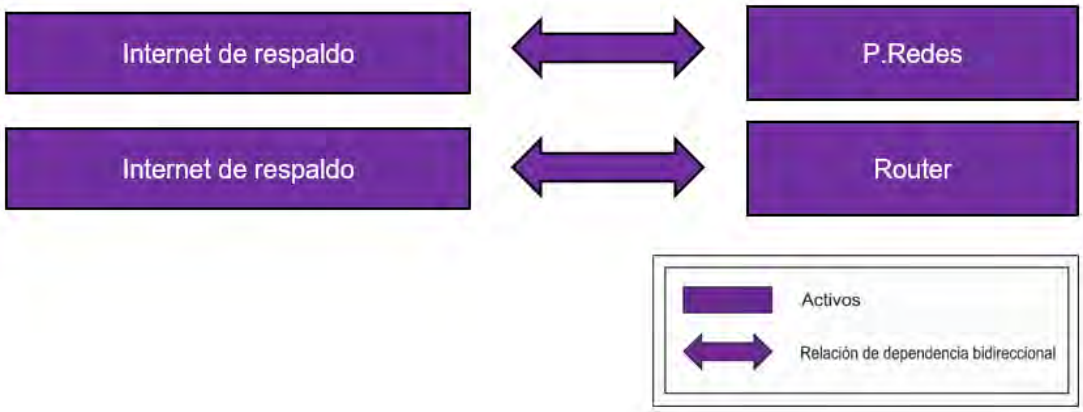
Relación de dependencias bidireccionales del activo: Internet



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 44

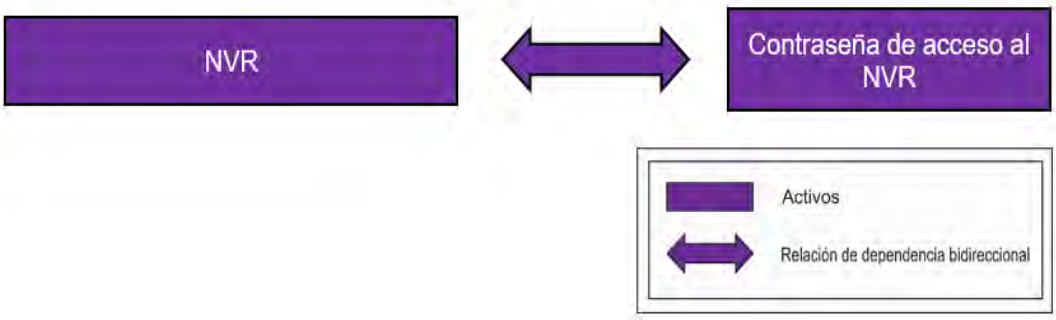
Relación de dependencias bidireccionales del activo: Internet de respaldo



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Imagen 45

Relación de dependencia bidireccional del activo: NVR



Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

Mejor perspectiva de los tipos de activos

Para obtener una mejor perspectiva de los tipos de activos y sus dependencias (directas, indirectas y bidireccionales) se elaboró unos cuadros de doble entrada en el cual se detalla lo siguiente:

El cuadro nos muestra al activo **"Datos de configuración"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta). También se observa en los cuadros resaltados de color morado una relación de dependencia bidireccional con el activo **"Computadoras desktops y Laptops"**.

Activo: Datos de configuración							
Activos		Dependencia indirecta					
		Oficina	Documentos digitales	Antivirus	UPS	Sistemas Operativos	P. Soporte técnico
Dependencia directa	USB						
	Disco duro externo						
	Jefe de área						
	Soporte técnico						
	P.Redes						
	Computadoras desktops						
	Laptops						

Tabla 1: *Resumen de dependencias del activo: Datos de configuración*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"Base de datos de la página web de la DDCC"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta). También se observa en los cuadros resaltados de color morado una relación de dependencia bidireccional con el activo "**Contraseña de acceso a la base de datos de la página web de la DDCC"**.

Activo: Base de datos de la página web de la DDCC							
	Activos	Dependencia indirecta					
		Oficina	Antivirus	Sistemas Operativos	Internet de respaldo	Jefe de área	Generador eléctrico
Dependencia directa	Datos de configuración						
	Aplicaciones						
	Computadoras desktops						
	Laptops						
	Firewall						
	Data center						
	Internet						
	P.Desarrolladores / Programadores						
	Contraseña de acceso a la base de datos de la página web de la DDCC						

Tabla 2: *Resumen de dependencias del activo: Base de datos de la página web de la DDCC*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"Datos de prueba"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta).

Activo: Datos de prueba				
Activos		Dependencia indirecta		
		Datos de configuración	Sistemas Operativos	Oficina
Dependencia directa	Aplicaciones			
	Jefe de área			
	P.Desarrolladores / Programadores			
	Computadoras desktops			
	Laptops			

Tabla 3: *Resumen de dependencias del activo: Datos de prueba*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"Documentos digitales"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta). También se observa en los cuadros resaltados de color morado una relación de dependencia bidireccional con el activo **"Jefe de área, P.Desarrolladores/ Programadores, P.Redes, P.Soporte técnico"**.

Activo: Documentos digitales						
Activos		Dependencia indirecta				
		Datos de configuración	Soporte técnico	Antivirus	Oficina	Sistemas Operativos
Dependencia directa	Ofimática					
	Computadoras desktops					
	Laptops					
	Jefe de área					
	P.Desarrolladores / Programadores					
	P.Redes					
	P.Soporte técnico					

Tabla 4: *Resumen de dependencias del activo: Documentos digitales*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"Contraseña de acceso a la base de datos de la página web de la DDCC"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta). También se observa en los cuadros resaltados de color morado una relación de dependencia bidireccional con el activo **"Base de datos de la página web de la DDCC"**

Activo: Contraseña de acceso a la base de datos de la página web de la DDCC		
Activos		Dependencia indirecta
		Computadoras desktops
Dependencia directa	Jefe de área	
	P.Desarrolladores / Programadores	
	Base de datos de la página web de la DDCC	
	Aplicaciones	

Tabla 5: *Resumen de dependencias del activo: Contraseña de acceso a la base de datos de la página web de la DDCC*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"Contraseña de acceso al NVR"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta). También se observa en los cuadros resaltados de color morado una relación de dependencia bidireccional con el activo **"NVR"**.

Activo: Contraseñas de acceso al NVR			
Activos		Dependencia indirecta	
		Computadoras desktops	Laptops
Dependencia directa	Jefe de área		
	P.Redes		
	P.Soporte técnico		
	NVR		

Tabla 6: *Resumen de dependencias del activo: Contraseña de acceso al NVR*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"Contraseña de acceso al router"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta). También se observa en los cuadros resaltados de color morado una relación de dependencia bidireccional con el activo **"Router"**.

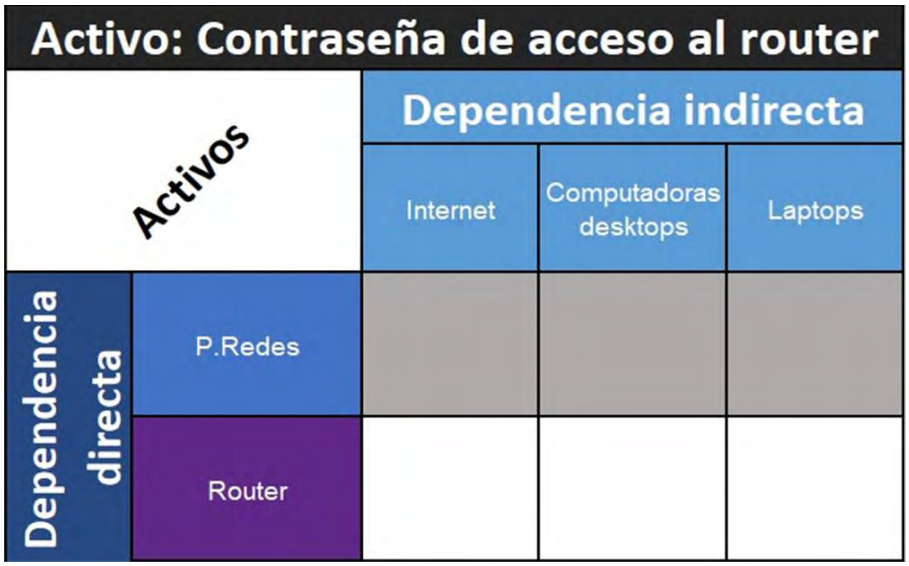


Tabla 7: *Resumen de dependencias del activo: Contraseña de acceso al router*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta).

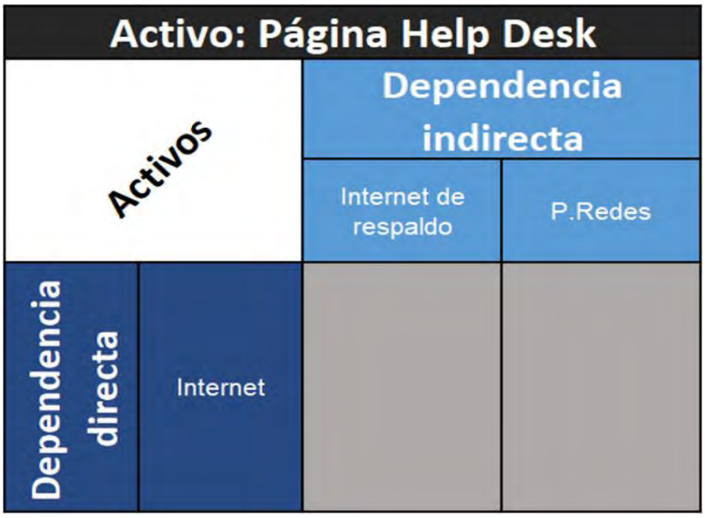


Tabla 8: *Resumen de dependencias del activo: Página Help Desk*
Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"Páginas web institucionales"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta)

Activo: Páginas web institucionales									
Activos		Dependencia indirecta							
		Aplicaciones	Computadoras desktops	Laptops	Contraseña de la base de datos de la página web de la DDCC	Oficina	P. Redes	Firewall	Internet de respaldo
Dependencia directa	Base de datos de la página web de la DDCC								
	Internet								
	Servidores								
	P.Desarolladores / Programadores								

Tabla 9: *Resumen de dependencias del activo: Páginas web institucionales*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"Soporte técnico"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta).

Activo: Soporte técnico			
Activos		Dependencia indirecta	
		Datos de configuración	Internet
Dependencia directa	Página Help Desk		
	Aplicaciones		
	P.Soporte técnico		
	P.Redes		

Tabla 10: *Resumen de dependencias del activo: Soporte técnico*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"Aplicaciones"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta). También se observa en los cuadros resaltados de color morado una relación de dependencia bidireccional con el activo **"Computadoras desktops y Laptops"**.

Activo: Aplicaciones							
Activos		Dependencia indirecta					
		P. Soporte técnico	USB	Disco duro externo	Soporte técnico	Oficina	Internet de respaldo	P. Redes
Dependencia directa	Datos de configuración							
	Sistemas Operativos							
	Computadoras desktops							
	Laptops							
	Internet							

Tabla 11: *Resumen de dependencias del activo: Aplicaciones*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"Antivirus"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta). También se observa en los cuadros resaltados de color morado una relación de dependencia bidireccional con el activo **"Computadoras desktops y Laptops"**.

Activo: Antivirus							
Activos		Dependencia indirecta					
		USB	Disco duro externo	P.Soporte técnico	Internet de respaldo	Oficina	Soporte técnico
Dependencia directa	Datos de configuración						
	Sistemas Operativos						
	Internet						
	Computadoras desktops						
	Laptops						

Tabla 12: *Resumen de dependencias del activo: Antivirus*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"Sistemas operativos"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta). También se observa en los cuadros resaltados de color morado una relación de dependencia bidireccional con el activo **"Computadoras desktops y Laptops"**.

Activo: Sistemas Operativos				
Activos		Dependencia indirecta		
		USB	P.Soporte técnico	Soporte técnico
Dependencia directa	Datos de configuración			
	Computadoras desktops			
	Laptops			
	Internet			

Tabla 13: *Resumen de dependencias del activo: Sistemas Operativos*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"Ofimática"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta).

Activo: Ofimática					
Activos		Dependencia indirecta			
		USB	P.Soporte técnico	Disco duro externo	Antivirus
Dependencia directa	Datos de configuración				
	Soporte técnico				
	Computadoras desktops				
	Laptops				

Tabla 14: *Resumen de dependencias del activo: Ofimática*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"Computadoras desktops"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta). También se observa en los cuadros resaltados de color morado una relación de dependencia bidireccional con el activo **"Datos de configuración, Antivirus, Sistemas operativos, Aplicaciones"**.

Activo: Computadoras desktops					
Activos		Dependencia indirecta			
		USB	Disco duro externo	P.Soporte técnico	Internet
Dependencia directa	Datos de configuración				
	Soporte técnico				
	Antivirus				
	Sistemas Operativos				
	Oficina				
	UPS				
	Aplicaciones				

Tabla 15: *Resumen de dependencias del activo: Computadoras desktops*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"Laptops"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta). También se observa en los cuadros resaltados de color morado una relación de dependencia bidireccional con el activo **"Datos de configuración, Antivirus, Sistemas operativos, Aplicaciones"**.

Activo: Laptops					
Activos		Dependencia indirecta			
		USB	Disco duro externo	P.Soporte técnico	Internet
Dependencia directa	Datos de configuración				
	Soporte técnico				
	Antivirus				
	Sistemas Operativos				
	Oficina				
	Aplicaciones				

Tabla 16: *Resumen de dependencias del activo: Laptops*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"Equipos de reprografía"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta).

Activo: Equipos de reprografía				
Activos		Dependencia indirecta		
		P.Redes	P.Soporte técnico	Internet de respaldo
Dependencia directa	Datos de configuración			
	Soporte técnico			
	Internet			
	Oficina			
	UPS			

Tabla 17: *Resumen de dependencias del activo: Equipos de reprografía*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"Firewall"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta).

Activo: Firewall				
Activos		Dependencia indirecta		
		Datos de configuración	P.Redes	Internet de respaldo
Dependencia directa	Internet			
	UPS			
	Oficina			

Tabla 18: *Resumen de dependencias del activo: Firewall*
Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"Router"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta). También se observa en los cuadros resaltados de color morado una relación de dependencia bidireccional con el activo **"Contraseña de acceso al router, Internet"**.

Activo: Router				
Activos		Dependencia indirecta		
		Computadoras	Laptops	Internet de respaldo
Dependencia directa	P. redes			
	Oficina			
	Contraseña de acceso al router			
	Internet			

Tabla 19: *Resumen de dependencias del activo: Router*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"Servidores"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta).

Activo: Servidores			
Activos		Dependencia indirecta	
		Internet de respaldo	P.Redes
Dependencia directa	Datos de configuración		
	Antivirus		
	Firewall		
	Generador eléctrico		
	Oficina		
	Internet		

Tabla 20: *Resumen de dependencias del activo: Servidores*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"Repositorios de código fuente"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta).

Activo: Repositorios de código fuente				
Activos		Dependencia indirecta		
		Computadoras	Laptops	Internet de respaldo
Dependencia directa	Internet			
	Jefe de Area			
	P.Desarolladores / Programadores			

Tabla 21: *Resumen de dependencias del activo: Repositorios de código fuente*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"NVR"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta). También se observa en los cuadros resaltados de color morado una relación de dependencia bidireccional con el activo **"Contraseña de acceso al NVR"**.

Activo: NVR		
Activos		Dependencia indirecta
		Internet de respaldo
Dependencia directa	Datos de configuración	
	Internet	
	Data Center	
	Generador eléctrico	
	Oficina	
	Contraseña de acceso al NVR	

Tabla 22: *Resumen de dependencias del activo: NVR*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"Jefe de área"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta). También se observa en los cuadros resaltados de color morado una relación de dependencia bidireccional con el activo **"Documentos digitales"**.

Activo: Jefe de área				
Activos		Dependencia indirecta		
		Aplicaciones	Internet de respaldo	Ofimática
Dependencia directa	Computadoras desktops			
	Laptops			
	Internet			
	Oficina			
	Documentos digitales			

Tabla 23: *Resumen de dependencias del activo: Jefe de área*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"P. Desarrolladores / Programadores"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta). También se observa en los cuadros resaltados de color morado una relación de dependencia bidireccional con el activo **"Documentos digitales"**.

Activo: P. Desarrolladores / Programadores				
Activos		Dependencia indirecta		
		Aplicaciones	Internet de respaldo	Ofimática
Dependencia directa	Computadoras desktops			
	Laptops			
	Internet			
	Oficina			
	Documentos digitales			

Tabla 24: *Resumen de dependencias del activo: P. Desarrolladores / Programadores*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"P. Soporte técnico"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta). También se observa en los cuadros resaltados de color morado una relación de dependencia bidireccional con el activo **"Documentos digitales"**.

Activo: P. Soporte técnico							
Activos		Dependencia indirecta					
		Aplicaciones	Datos de configuración	Internet de respaldo	Ofimática	USB	Disco duro externo
Dependencia directa	Computadoras desktops						
	Laptops						
	Internet						
	Oficina						
	Documentos digitales						
	Página Help Desk						

Tabla 25: *Resumen de dependencias del activo: P. Soporte técnico*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

El cuadro nos muestra al activo **"P. Redes"** y a los activos de dependencia directa e indirecta. Además, se evidencian los cuadros resaltados de color plomo la relación de los activos de dependencia directa e indirecta mediante el cual este último obtiene dicha relación (dependencia indirecta). También se observa en los cuadros resaltados de color morado una relación de dependencia bidireccional con los activos **"Internet y Documentos digitales"**.

Activo: P. Redes					
Activos		Dependencia indirecta			
		Datos de configuración	Internet de respaldo	Router	Ofimática
Dependencia directa	Computadoras desktops				
	Laptops				
	Internet				
	Oficina				
	Documentos digitales				

Tabla 26: *Resumen de dependencias del activo: P. redes*

Fuente: Elaboración propia adaptada de MAGERIT – Libro I - Método, (MAR.1.1).

MAR.1.3. Valoración de los activos

(3.2.1. Tarea MAR.1: Caracterización de los activos, libro MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método, (pp.39-40))

Los activos se van a valorar en las siguientes dimensiones:

	Dimensiones de la seguridad		
Valor del activo	**Confidencialidad**	**Integridad**	**Disponibilidad**
3	Información restringida	Alta	Uso frecuente
2	Información interna	Media	Uso medio
1	Información interna y/o pública	Baja	Uso bajo

Tabla 27: *Dimensiones de la seguridad*
Fuente: Elaboración propia adaptada del libro MAGERIT - Libro II - Catálogo de Elementos (p.15).

El valor de los activos se va a determinar de la siguiente forma donde se va a realizar el análisis de riesgos solo a los activos de criticidad alta y media:

Valor del Activo = Confidencialidad + Integridad + Disponibilidad

Valor total del activo	Valoración del activo
7 - 9	Alto
4 - 6	Medio
1 - 3	Bajo

Tabla 28: *Rango de valoración de activos*
Fuente: Elaboración propia adaptada del libro MAGERIT - Libro II - Catálogo de Elementos (p.19).

Clasificación de la Confidencialidad

Valor del activo	Clasificación	Definición
3	Información restringida	Información secreta, de gran relevancia para la DDCC, debido a su extrema confidencialidad, esta información es accesible a un número reducido de individuos: - Director de la DDCC. - Jefe del área funcional de Informática y Telecomunicaciones.

2	Información confidencial	Información de carácter confidencial, manejado por un grupo limitado de personas pertenecientes a la DDCC que hacen uso de ella para poder desempeñar sus responsabilidades: - Personal del área funcional de Informática y Telecomunicaciones.
1	Información interna y/o pública	Información de uso interno (manejado por el personal de las áreas funcionales de la DDCC) y/o público (público en general).

Tabla 29: *Clasificación de la dimensión de la seguridad: Confidencialidad*
Fuente: Elaboración propia adaptada del libro MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Clasificación de la integridad

Valor del activo	Clasificación	Definición
3	Alta	Es la información o recurso que al ser modificado y/o dañado de forma voluntaria o involuntaria provoca un daño alto a la DDCC.
2	Media	Es la información o recurso que al ser modificado y/o dañado de forma voluntaria o involuntaria provoca un daño medio a la DDCC.
1	Baja	Es la información o recurso que al ser modificado y/o dañado de forma voluntaria o involuntaria provoca un daño bajo a la DDCC.

Tabla 30: *Clasificación de la dimensión de la seguridad: Integridad*
Fuente: Elaboración propia adaptada del libro MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Clasificación de la disponibilidad

Valor del activo	Clasificación	Definición
3	Uso frecuente	Activo muy importante para la continuidad del correcto funcionamiento de la DDCC, es un recurso vital y alternativo que no puede estar indisponible por un largo periodo de tiempo.
2	Uso medio	Activo importante para la continuidad del correcto funcionamiento de la DDCC, pero existen alternativas para reducir la indisponibilidad de este activo a un tiempo corto.
1	Uso bajo	Activo de apoyo o secundario para la DDCC, el cual se tiene duplicado y/o se cuenta con un respaldo inmediato; y si en caso se presenta indisponibilidad este no llega a afectar a los procesos y/o actividades más importantes de la DDCC.

Tabla 31: *Clasificación de la dimensión de la seguridad: Disponibilidad*
Fuente: Elaboración propia adaptada del libro MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

A continuación, se detalla la valoración total de los tipos de activos tomando en cuentas las dimensiones de seguridad (confidencialidad, integridad y disponibilidad):

Identificación de los activos				Dimensiones de la seguridad			Valoración del activo	
N° Activo	Tipo de activo	Nombre del activo	Descripción	Confidencialidad	Integridad	Disponibilidad	Valor total del activo	Nivel del activo
D1	Datos / Información	Datos de configuración	Son datos (de direcciones ip válidas, licencias, cuentas de registro de usuarios) que permiten que los equipos o sistemas funcionen correctamente y se integren de manera efectiva en una infraestructura más amplia.	3	1	1	5	Medio
D2	Datos / Información	Base de datos de la página web de la DDCC	Conjunto de datos estructurados, organizados y almacenados de forma digital en el cual se gestiona información relacionada a la Dirección Desconcentrado de Cultura de Cusco.	3	3	3	9	Alto
D3	Datos / Información	Log de actividades	Es un registro de actividades que almacena todos los cambios que hacen los usuarios en sus computadoras del personal de la institución.	1	1	1	3	Bajo
D4	Datos / Información	Datos de prueba	Datos que se van a utilizar para probar un determinado software(aplicación) y direcciones IP de prueba.	1	1	1	3	Bajo
D5	Datos / Información	Documentos digitales	Se refiere a: memorándum,informes mensuales, oficios, configuración de activos(aplicaciones, servidores,base de datos), documentación de código fuente.	2	2	2	6	Medio
K1	Claves criptográficas	Contraseña de acceso a la base de datos de la página web de la DDCC	Es una clave de acceso para autenticar la identidad de un usuario y permitirle el acceso a la base de datos de la página web.	3	3	3	9	Alto

K2	Claves criptográficas	Contraseña de acceso al NVR	Es una clave secreta que se utiliza para autenticar la identidad del usuario y permitirle acceder, gestionar las cámaras de seguridad y grabaciones almacenadas en el NVR.	3	3	1	7	Alto
K3	Claves criptográficas	Contraseña de acceso al router	Es una clave que se utiliza para proteger y limitar el acceso a la configuración y funciones del enrutador con el fin de proteger la integridad y la privacidad de la red doméstica o institucional.	3	3	1	7	Alto
S1	Servicios	Página Help Desk	Es una página web (mesa de ayuda) adquirida para agilizar la atención de incidencias y requerimientos de la Dirección Desconcentrada de Cultura de Cusco y/o usuarios externos(personas ajenas a la institución) manejado por el área funcional de Informática y Telecomunicaciones	1	3	3	7	Alto
S2	Servicios	Páginas web institucionales	Son páginas web y sistemas web desarrollados y manejados por el área funcional de Informática y Telecomunicaciones, con el fin de brindar comunicación y divulgación sobre sus objetivos,actividades,servicios en línea y/o manejo administrativo institucional.	2	3	3	8	Alto
S3	Servicios	Soporte técnico	Es un servicio del área funcional de Informática y Telecomunicaciones, encargado de las siguientes funciones: mantenimiento en software,hardware(equipos informáticos ,equipos de reprografía) y redes.	1	1	2	4	Medio
SW1	Software - Aplicaciones informáticas	Aplicaciones	Son programas de software diseñados para realizar tareas específicas en una computadora u otro dispositivo electrónico.	1	1	3	5	Medio
SW2	Software - Aplicaciones informáticas	Antivirus	Un antivirus es un programa o software diseñado para detectar, prevenir y eliminar o neutralizar software malicioso, como virus, gusanos, troyanos, spyware y otros tipos de malware.	1	2	3	6	Medio

SW3	Software - Aplicaciones informáticas	Sistemas Operativos	Un sistema operativo (SO) es un software que actúa como intermediario entre el hardware de una computadora y las aplicaciones o programas que se ejecutan en ella.	1	2	2	5	Medio
SW4	Software - Aplicaciones informáticas	Ofimática	Son los programas de Microsoft Office(Word,Excel,Power Point,Ms Project,etc) que se enfocan en automatizar y optimizar las tareas y funciones diarias en la oficina.	1	1	2	4	Medio
HW1	Hardware - Equipamiento informático	Computadoras desktops	Son sistemas informáticos diseñados para ser utilizados en un entorno fijo, como una oficina o un hogar. El cual consta de los siguientes componentes: CPU, teclado, estabilizador, mouse,unidad de almacenamiento,cámara, micrófono.	1	2	3	6	Medio
HW2	Hardware - Equipamiento informático	Laptops	Son dispositivos portátiles que combinan la funcionalidad de una computadora personal en un formato compacto y liviano.	1	2	3	6	Medio
HW3	Hardware - Equipamiento informático	Equipos de reprografía	Son dispositivos utilizados para copiar y reproducir documentos, imágenes y otros materiales impresos.	1	1	2	4	Medio
HW4	Hardware - Equipamiento informático	Firewall	Llamados también cortafuegos. Es una medida de seguridad que se utiliza para proteger una red de computadora o un sistema informático de accesos no autorizados y ataques cibernéticos.	2	3	3	8	Alto
HW5	Hardware - Equipamiento informático	Router	Es un dispositivo de red que se utiliza para conectar múltiples dispositivos en una red y dirigir el tráfico de datos entre ellos. Facilitan la conexión entre la red local y la red externa, como Internet.	2	3	3	8	Alto

COM1	Redes de comunicaciones	Internet	Es una red global de computadoras interconectadas que permite la comunicación y el intercambio de información a nivel mundial.	2	3	3	8	Alto
COM2	Redes de comunicaciones	Internet de respaldo	Es un respaldo de red global de computadoras interconectadas que permite la comunicación y el intercambio de información a nivel mundial.	2	3	3	8	Alto
Media1	Soportes de información	USB	Es un dispositivo de almacenamiento por el cual se comparte información a través de diferentes usuarios.	1	1	1	3	Bajo
Media2	Soportes de información	Disco duro externo	Es un dispositivo de almacenamiento portátil por el cual se comparte información a través de un cable de conexión utilizado para ampliar la capacidad de almacenamiento y permitir la transferencia de datos.	1	1	1	3	Bajo
Media3	Soportes de información	Servidores	Es una instalación física que alberga equipos informáticos y sistemas de almacenamiento, procesamiento y gestión de datos.	3	3	3	9	Alto
Media4	Soportes de información	Repositorios de código fuente	Un repositorio de código fuente es un lugar donde se almacena y gestiona el código de un proyecto de software. Los repositorios pueden estar en línea o en un servidor local, y son utilizados por desarrolladores para colaborar en el desarrollo de software, realizar un seguimiento de las versiones y gestionar cambios en el código.	3	2	2	7	Alto
AUX1	Equipamiento Auxiliar	Generador eléctrico	Es un dispositivo que utiliza cuando se necesita generar electricidad en lugares donde no hay suministro de energía de la red eléctrica o como respaldo en caso de cortes de energía.	1	3	3	7	Alto

AUX2	Equipamiento Auxiliar	UPS	Es un dispositivo que protege los equipos electrónicos y sistemas sensibles ante fluctuaciones de voltaje, caídas de energía o apagones, permitiendo que los dispositivos continúen funcionando de manera ininterrumpida.	1	3	3	7	Alto
AUX3	Equipamiento Auxiliar	Equipo de climatización	El aire acondicionado es un sistema de climatización que se utiliza para regular la temperatura, la humedad y la ventilación de un espacio cerrado, ya sea una habitación, una casa, una oficina o un edificio.	1	1	1	3	Bajo
AUX4	Equipamiento Auxiliar	Mobiliario	El mobiliario se refiere a los muebles y elementos utilizados para amueblar y equipar un espacio, ya sea en el hogar, la oficina, un comercio u otros entornos.	1	1	1	3	Bajo
AUX5	Equipamiento Auxiliar	NVR	Es un sistema de videovigilancia en red.	3	3	3	9	Alto
L1	Instalaciones	Oficina	Es un espacio físico donde se hospedan los activos mencionados.	3	3	3	9	Alto
P1	Personal	Jefe de área	Es un profesional encargado de liderar y supervisar el área funcional de Informática y Telecomunicaciones.	3	3	3	9	Alto
P2	Personal	P.Desarrolladores / Programadores	Es el personal que conforma el subárea de software en el área funcional de Informática y Telecomunicaciones.	3	3	2	8	Alto
P3	Personal	P.Soporte técnico	Es el personal que conforma el subárea de soporte técnico en el área funcional de Informática y Telecomunicaciones.	1	2	2	5	Medio
P4	Personal	P.Redes	Es el personal que conforma el subárea de redes en el área funcional de Informática y Telecomunicaciones.	2	2	2	6	Medio

Tabla 32: *Cuadro de valoración de los tipos de activos*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Identificación de activos: MAR.1.1: Identificación de los activos del libro MAGERIT – Libro I – Métodos

Dimensiones de la seguridad: 3. Dimensiones de valoración del libro MAGERIT – Libro II - Catálogo de Elementos
Valoración del activo: MAR.1.3: Valoración de los activos del libro MAGERIT – Libro I - Métodos

MAR.2. Caracterización de las amenazas

(3. Método de análisis de riesgos - 3.1.2. Paso 2: Amenazas, libro MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método, (pp.27-31))

MAR.2.1. Identificación de las amenazas

(3.2.2. Tarea MAR.2: Caracterización de las amenazas, libro MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método, (pp.40-41))

En esta fase se van a identificar las amenazas que presenten cada activo y como resultado se tendrá una relación de las amenazas

A. Desastres naturales

Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

Origen: Natural (accidental).

DESASTRES NATURALES	
Tipos de amenazas	**Descripción**
Fuego	Incendio: posibilidad de que el fuego acabe con los recursos del sistema.
Daños por agua	Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
Desastres Naturales	Incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalanchas, corrimiento de tierras. Se excluyen desastres específicos tales como incendios e inundaciones.

Tabla 33: *Amenazas de tipo: Desastres naturales*

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos (5. Amenazas).

B. De origen industrial

Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.

DE ORIGEN INDUSTRIAL	
Tipos de amenazas	**Descripción**
Fuego	Incendio: posibilidad de que el fuego acabe con los recursos del sistema.
Daños por agua	Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
Desastres industriales	Desastres debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico. Se excluyen amenazas específicas como incendio e inundación.
Contaminación mecánica	Vibraciones, polvo, suciedad.
Contaminación electromagnética	Interferencias de radio, campos magnéticos, luz ultravioleta.
Avería de origen físico o lógico	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
Corte del suministro eléctrico	Cese de la alimentación de potencia.
Condiciones inadecuadas de temperatura o humedad	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad.
Fallo de servicios de comunicaciones	Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.

Interrupción de otros servicios y suministros esenciales	Otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner, refrigerante.
Degradación de los soportes de almacenamiento de la información	Como consecuencia del paso del tiempo.
Emanaciones electromagnéticas	Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información.

Tabla 34: *Amenazas de tipo: De origen industrial*

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos (5. Amenazas).

C. Errores y fallos no intencionados

Fallos no intencionales causados por las personas. La numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.
Origen: Humano (accidental)

ERRORES Y FALLOS NO INTENCIONADOS	
Tipos de amenazas	**Descripción**
Errores de los usuarios	Equivocaciones de las personas cuando usan los servicios, datos, etc.
Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación.
Errores de monitorización (log)	Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos.
Errores de configuración	Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.
Deficiencias en la organización	Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc.
Difusión de software dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
Errores de [re-]encaminamiento	Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.

Errores de secuencia	Alteración accidental del orden de los mensajes transmitidos.
Escapes de información	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.
Alteración accidental de la información	Alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
Destrucción de información	Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
Fugas de información	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.
Vulnerabilidades de los programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.
Errores de mantenimiento / actualización de programas (software)	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.
Errores de mantenimiento / actualización de equipos (hardware)	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.
Caída del sistema por agotamiento de recursos	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

Pérdida de equipos	La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales.
Indisponibilidad del personal	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica.

Tabla 35: *Clasificación de la dimensión de la seguridad: Errores y fallos no intencionados*

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos (5. Amenazas).

D. Ataques intencionados

Fallos deliberados causados por las personas.

La numeración no es consecutiva para coordinar con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.

Origen: Humano (deliberado)

ATAQUES INTENCIONADOS	
Tipos de amenazas	**Descripción**
Manipulación de los registros de actividad (log)	Amenaza que implica la alteración intencionada de los registros que registran las actividades.
Manipulación de la configuración	Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.
Suplantación de la identidad del usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.
Abuso de privilegios de acceso	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.
Uso no previsto	Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.
Difusión de software dañino	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.

Re-encaminamiento de mensajes	Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.
Alteración de secuencia	Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.
Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.
Análisis de tráfico	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina “monitorización de tráfico”.
Repudio	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.

Interceptación de información	El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.
Modificación deliberada de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.
Destrucción de información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.
Divulgación de información	Revelación de información.
Manipulación de programas	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
Manipulación de los equipos	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
Denegación de servicios	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
Robo	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias.

Ataque destructivo	Vandalismo, terrorismo, acción militar. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.
Ocupación enemiga	Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.
Indisponibilidad del personal	Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos.
Extorsión	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.
Ingeniería social (picaresca)	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.

Tabla 36: *Clasificación de la dimensión de la seguridad: Ataques intencionados*

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos (5. Amenazas).

Con respecto a las amenazas mencionadas anteriormente, se identificó las amenazas para cada activo

Tipos de activos	Amenazas
DATOS / INFORMACIÓN	Errores de configuración
	Errores de los usuarios
	Errores de monitorización
	Errores del administrador
	Escapes de información
	Alteración accidental de la información
	Fugas de información
	Modificación deliberada de la información
	Divulgación de información
	Destrucción de información
	Manipulación de los registros de actividad (log)
	Manipulación de la configuración
	Repudio
	Suplantación de la identidad del usuario
	Abuso de privilegios de acceso
	Errores del administrador
	Fugas de información
	Escapes de información
	Errores de los usuarios

	Alteración accidental de la información
CLAVES CRIPTOGRÁFICAS	Destrucción de información
	Suplantación de la identidad del usuario
	Abuso de privilegios de acceso
	Acceso no autorizado
	Modificación deliberada de la información
	Divulgación de información
	Destrucción de información
	Errores del administrador
	Errores de [re-]encaminamiento
	Errores de secuencia
	Escapes de información
	Alteración accidental de la información
	Fugas de información
	Errores de mantenimiento / actualización de programas (software)
SERVICIOS	Caída del sistema por agotamiento de recursos
	Errores de los usuarios
	Abuso de privilegios de acceso
	Alteración de secuencia
	Acceso no autorizado
	Modificación deliberada de la información
	Divulgación de información
	Uso no previsto
	[Re-]encaminamiento de mensajes

	Repudio
	Denegación de servicio
	Suplantación de la identidad del usuario
	Avería de origen físico o lógico
	Errores del administrador
	Difusión de software dañino
	Alteración accidental de la información
	Destrucción de información
SOFTWARE	Vulnerabilidades de los programas (software)
	Errores de mantenimiento / actualización de programas (software)
	Errores de los usuarios
	Uso no previsto
	Divulgación de información
	Abuso de privilegios de acceso
	Acceso no autorizado
	Manipulación de programas
	Modificación deliberada de la información
	Fuego
	Daños por agua
	Desastres naturales
	Desastres industriales
HARDWARE	Contaminación mecánica
	Contaminación electromagnética
	Avería de origen físico o lógico

	Corte del suministro eléctrico
	Condiciones inadecuadas de temperatura o humedad
	Emanaciones electromagnéticas
	Errores del administrador
	Errores de mantenimiento / actualización de equipos (hardware)
	Caída del sistema por agotamiento de recursos
	Pérdida de equipos
HARDWARE	Abuso de privilegios de acceso
	Uso no previsto
	Acceso no autorizado
	Manipulación de los equipos
	Denegación de servicio
	Robo
	Ataque destructivo
	Fallo de servicios de comunicaciones
	Errores del administrador
	Errores de [re-]encaminamiento
	Errores de secuencia
	Escapes de información
	Fugas de información
	Errores de mantenimiento / actualización de equipos (hardware)
REDES DE	Caída del sistema por agotamiento de recursos
COMUNICACIONES	Suplantación de la identidad del usuario
	Abuso de privilegios de acceso

	Uso no previsto
	[Re-]encaminamiento de mensajes
	Alteración de secuencia
	Acceso no autorizado
	Análisis de tráfico
	Interceptación de información (escucha)
	Modificación deliberada de la información
	Denegación de servicio
	Fuego
	Desastres naturales
	Daños por agua
	Contaminación electromagnética
	Desastres industriales
	Contaminación mecánica
	Avería de origen físico o lógico
	Condiciones inadecuadas de temperatura o humedad
SOPORTES DE	Degradación de los soportes de almacenamiento
INFORMACIÓN	de información
	Emanaciones electromagnéticas
	Fallo de servicios de comunicaciones
	Alteración accidental de la información
	Errores de los usuarios
	Errores del administrador
	Errores de mantenimiento / actualización de equipos (hardware)

	Pérdida de equipos
	Indisponibilidad del personal
	Uso no previsto
	Manipulación de los equipos
	Ataque destructivo
SOPORTES DE	Acceso no autorizado
INFORMACIÓN	Destrucción de información
	Divulgación de información
	Robo
	Modificación deliberada de la información
	Fuego
	Daños por agua
	Desastres naturales
EQUIPAMIENTO	Desastres industriales
AUXILIAR	Contaminación mecánica
	Contaminación electromagnética
	Avería de origen físico o lógico
	Condiciones inadecuadas de temperatura humedad
	Interrupción de otros servicios y suministros esenciales
	Emanaciones electromagnéticas
	Corte de suministro eléctrico
	Fallo de servicios de comunicaciones
	Degradación de los soportes de almacenamiento de información
	Errores del administrador

	Errores de mantenimiento / actualización de equipos (hardware)
	Pérdida de equipos
	Errores de los usuarios
	Errores de administrador
	Uso no previsto
EQUIPAMIENTO	Acceso no autorizado
AUXILIAR	Manipulación de los equipos
	Robo
	Ataque destructivo
	Ocupación enemiga
	Manipulación de la configuración
	Divulgación de información
	Desastres naturales
	Fuego
	Daños por agua
	Desastres industriales
	Contaminación mecánica
	Corte de suministro eléctrico
	Errores de los usuarios
	Errores del administrador
	Uso no previsto
INSTALACIONES	Acceso no autorizado
	Ataque destructivo
	Ocupación enemiga
	Indisponibilidad del personal

	Fuego
	Desastres naturales
	Deficiencias en la organización
	Escapes de información
PERSONAL	Fugas de información
	Indisponibilidad del personal
	Suplantación de la identidad del usuario
	Repudio
	Extorsión
	Ingeniería social (picaresca)

Se identificó las vulnerabilidades:

(ANEXO D (INFORMATIVO) Vulnerabilidades y métodos para evaluación de vulnerabilidades, libro NTP-ISO/IEC 27005:2018, (pp.71-77))

	Falta de esquemas periódicos de reemplazo
HARDWARE	Mantenimiento insuficiente / instalación defectuosa de medios de almacenamiento
	Falta de copias de respaldo
	Falta de políticas con respecto a la incorrecta asignación de derechos de acceso
SOFTWARE	Descarga y uso no controlado de software
	Falla en producir reportes de gestión
	Malware y software malicioso
	Falta o insuficiente análisis de la configuración, actualización del antivirus

RED	Pobre conjunto de cableado estructurado e infraestructura antigua
	Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería
PERSONAL	Susceptibilidad de la ingeniería social
	Falta de conciencia de seguridad
	Uso incorrecto de software y hardware
	Descuido en la gestión de contraseñas
	Ausencia de personal
	Falta de procedimientos de identificación y evaluación de riesgos
	Falta de pruebas de verificación del mantenimiento de servicio
	Falta o insuficiente Acuerdo de Nivel de Servicio
	Falta de asignación apropiada de responsabilidades por la seguridad de la información
	Falta de planes de continuidad
ORGANIZACIÓN	Falta de procedimientos para manejo de información clasificada
	Falta de proceso disciplinario definido en caso de incidente de seguridad de la información
	Falta de política formal sobre uso de computadoras móviles
	Falta de mecanismos de seguimiento establecidos para brechas de seguridad
	Falta de procedimientos para reportar debilidades de la seguridad
	Falta de procedimientos de estipulación de cumplimiento con derechos de propiedad intelectual
	Falta de proceso disciplinario definido en caso de incidente de cuidado de activos

MAR.2.2. Valoración de las amenazas

(3.2.2. Tarea MAR.2: Caracterización de las amenazas, libro MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método, (pp.41-42))

En los siguientes cuadros se muestran a los activos que cuentan con tipos de amenazas, en el cual se evalúa la probabilidad de incidencia y la degradación. (Degradación: Muy baja=1, Baja=2,Media=3,Alta=4.Muy alta=5)

Amenazas para el tipo de activo Datos / Información

AMENAZAS SEGÚN MAGERIT PARA EL TIPO DE ACTIVO DATOS / INFORMACIÓN [D]			
Activos [D]	**Errores y fallos no intencionados**	**Probabilidad de incidencia**	**Degradación**
Datos de configuración	Errores de los usuarios	3	3
	Errores del administrador	3	3
	Errores de configuración	3	3
	Escapes de información	2	4
	Alteración accidental de la información	2	3

	Destrucción de información	2	5
	Fugas de información	2	4
Base de datos de la página web de la DDCC	Errores de los usuarios	3	4
	Errores del administrador	2	4
	Escapes de información	2	4
	Alteración accidental de la información	2	4
	Destrucción de información	2	5
	Fugas de información	2	4
Log de actividades	Errores de los usuarios	3	1
	Errores del administrador	3	1
	Errores de monitorización	2	1
	Escapes de información	3	2
	Alteración accidental de la información	3	1

	Destrucción de información	3	2
	Fugas de información	3	2
Datos de prueba	Errores de los usuarios	3	1
	Errores del administrador	3	1
	Escapes de información	2	1
	Alteración accidental de la información	3	2
	Destrucción de información	2	2
	Fugas de información	2	1
Documentos digitales	Errores de los usuarios	3	3
	Errores del administrador	3	3
	Escapes de información	4	3
	Alteración accidental de la información	3	3
	Destrucción de información	4	3

	Fugas de información	4	3

Tabla 37: *Valoración de las amenazas de errores y fallos no intencionados para los activos de tipo Datos / Información*
Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

AMENAZAS SEGÚN MAGERIT PARA EL TIPO DE ACTIVO DATOS / INFORMACIÓN [D]			
Activos [D]	**Ataques intencionados**	**Probabilidad de incidencia**	**Degradación**
Datos de configuración	Suplantación de la identidad del usuario	2	3
	Abuso de privilegios de acceso	2	4
	Modificación deliberada de la información	2	4
	Destrucción de información	2	4
Base de datos de la página web de la DDCC	Suplantación de la identidad del usuario	1	3
	Abuso de privilegios de acceso	3	5
	Modificación deliberada de la información	3	5
	Destrucción de información	3	5

	Divulgación de información	3	4
Log de actividades	Manipulación de los registros de actividad (log)	2	1
	Manipulación de la configuración	2	1
	Suplantación de la identidad del usuario	2	1
	Abuso de privilegios de acceso	2	1
	Repudio	2	1
	Modificación deliberada de la información	2	1
	Destrucción de información	2	1
Datos de prueba	Suplantación de la identidad del usuario	2	1
	Abuso de privilegios de acceso	2	1
	Modificación deliberada de la información	2	3
	Destrucción de información	2	4
	Suplantación de la identidad del usuario	3	3

Documentos digitales	Abuso de privilegios de acceso	3	3
	Modificación deliberada de la información	3	4
	Destrucción de información	3	4

Tabla 38: *Valoración de las amenazas de ataques intencionados para los activos de tipo Datos / Información*
Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

Amenazas para el tipo de activo Claves criptográficas

AMENAZAS SEGÚN MAGERIT PARA EL TIPO DE ACTIVO CLAVES CRIPTOGRÁFICAS [K]			
Activos [K]	**Errores y fallos no intencionados**	**Probabilidad de incidencia**	**Degradación**
Contraseña de acceso a la base de datos de la página web de la DDCC	Errores de los usuarios	3	5
	Errores del administrador	3	5
	Escapes de información	2	3
	Alteración accidental de la información	2	4

	Destrucción de información	2	4
	Fugas de información	2	3
Contraseña de acceso al NVR	Errores del administrador	3	4
	Escapes de información	2	3
	Alteración accidental de la información	2	2
	Destrucción de información	2	2
	Fugas de información	2	3
Contraseña de acceso al router	Errores de los usuarios	3	4
	Errores del administrador	3	4
	Escapes de información	2	4
	Alteración accidental de la información	3	3
	Destrucción de información	2	4

	Fugas de información	2	4

Tabla 39: *Valoración de las amenazas de errores y fallos no intencionados para los activos de tipo Claves criptográficas*
Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

AMENAZAS SEGÚN MAGERIT PARA EL TIPO DE ACTIVO CLAVES CRIPTOGRÁFICAS [K]			
Activos [K]	**Ataques intencionados**	**Probabilidad de incidencia**	**Degradación**
Contraseña de acceso a la base de datos de la página web de la DDCC	Suplantación de la identidad del usuario	2	3
	Abuso de privilegios de acceso	2	3
	Acceso no autorizado	3	4
	Modificación deliberada de la información	2	4
	Destrucción de información	2	4
	Suplantación de la identidad del usuario	2	3
	Acceso no autorizado	3	3

Contraseña de acceso al NVR	Modificación deliberada de la información	2	2
	Destrucción de información	2	2
Contraseña de acceso al router	Suplantación de la identidad del usuario	2	3
	Abuso de privilegios de acceso	2	3
	Acceso no autorizado	3	3
	Modificación deliberada de la información	3	5
	Destrucción de información	3	5

Tabla 40: *Valoración de las amenazas de ataques intencionados para los activos de tipo Claves criptográficas*
Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

Amenazas para el tipo de activo Servicios

AMENAZAS SEGÚN MAGERIT PARA EL TIPO DE ACTIVO SERVICIOS [S]			
Activos [S]	**Errores y fallos no intencionados**	**Probabilidad de incidencia**	**Degradación**
	Errores de los usuarios	2	1

Página Help Desk	Errores del administrador	2	3
	Errores de [re-]encaminamiento	2	1
	Escapes de información	2	1
	Alteración accidental de la información	2	2
	Destrucción de información	2	4
	Fugas de información	2	1
	Caída del sistema por agotamiento de recursos	3	2
Páginas web institucionales	Errores del administrador	3	4
	Errores de [re-]encaminamiento	2	4
	Errores de secuencia	2	4
	Escapes de información	2	4
	Alteración accidental de la información	2	4
	Destrucción de información	2	5

	Fugas de información	2	4
	Errores de mantenimiento / actualización de programas (software)	3	2
	Caída del sistema por agotamiento de recursos	3	2
Soporte técnico	Errores de los usuarios	2	1
	Errores del administrador	3	3

Tabla 41: *Valoración de las amenazas de errores y fallos no intencionados para los activos de tipo Servicios*
Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

AMENAZAS SEGÚN MAGERIT PARA EL TIPO DE ACTIVO SERVICIOS [S]			
Activos [S]	**Ataques intencionados**	**Probabilidad de incidencia**	**Degradación**
Página Help Desk	Suplantación de la identidad del usuario	2	2
	Alteración de secuencia	2	2
	Acceso no autorizado	2	3
	Modificación deliberada de la información	2	2

	Destrucción de información	2	4
	Divulgación de información	2	2
Páginas web institucionales	Suplantación de la identidad del usuario	2	2
	Uso no previsto	2	2
	Acceso no autorizado	2	2
	Modificación deliberada de la información	3	4
	Destrucción de información	3	4
	Denegación de servicio	3	3
Soporte técnico	Suplantación de la identidad del usuario	3	3
	Abuso de privilegios de acceso	3	3
	Uso no previsto	2	3
	Alteración de secuencia	3	2
	Repudio	3	2

	Denegación de servicio	2	4

Tabla 42: *Valoración de las amenazas de ataques intencionados para los activos de tipo Servicios*
Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

Amenazas para el tipo de activo Software

AMENAZAS SEGÚN MAGERIT PARA EL TIPO DE ACTIVO SOFTWARE [SW]			
Activos [SW]	**De origen industrial**	**Probabilidad de incidencia**	**Degradación**
Aplicaciones	Avería de origen físico o lógico	3	2
Antivirus	Avería de origen físico o lógico	3	2
Sistemas Operativos	Avería de origen físico o lógico	4	3
Ofimática	Avería de origen físico o lógico	4	2

Tabla 43: *Valoración de las amenazas de ataques de origen industrial para los activos de tipo Software*
Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

AMENAZAS SEGÚN MAGERIT PARA EL TIPO DE ACTIVO SOFTWARE [SW]			
Activos [SW]	**Errores y fallos no intencionados**	**Probabilidad de incidencia**	**Degradación**
Aplicaciones	Errores de los usuarios	3	2
	Errores del administrador	3	2
	Difusión de software dañino	2	3
	Alteración accidental de la información	3	2
	Vulnerabilidades de los programas (software)	2	3
	Errores de mantenimiento / actualización de programas (software)	3	3
Antivirus	Errores de los usuarios	3	3
	Errores del administrador	3	3
	Difusión de software dañino	2	2
	Alteración accidental de la información	3	3
	Destrucción de información	2	4

	Errores de mantenimiento / actualización de programas (software)	3	3
Sistemas Operativos	Errores de los usuarios	2	5
	Errores del administrador	2	3
	Difusión de software dañino	2	4
	Alteración accidental de la información	1	5
	Vulnerabilidades de los programas (software)	3	2
	Errores de mantenimiento / actualización de programas (software)	3	3
Ofimática	Errores de los usuarios	3	3
	Difusión de software dañino	3	3
	Alteración accidental de la información	2	3
	Destrucción de información	2	4
	Errores de mantenimiento / actualización de programas (software)	2	2

Tabla 44: *Valoración de las amenazas de errores y fallos no intencionados para los activos de tipo Software*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

AMENAZAS SEGÚN MAGERIT PARA EL TIPO DE ACTIVO SOFTWARE [SW]			
Activos [SW]	**Ataques intencionados**	**Probabilidad de incidencia**	**Degradación**
Aplicaciones	Uso no previsto	3	2
	Difusión de software dañino	3	3
	Manipulación de programas	3	2
Antivirus	Abuso de privilegios de acceso	3	3
	Uso no previsto	3	1
	Difuso de software dañino	3	3
	Acceso no autorizado	3	3
	Modificación deliberada de la información	3	3
	Destrucción de información	3	5
	Manipulación de programas	3	4
	Difuso de software dañino	3	4

Sistemas Operativos	Modificación deliberada de la información	2	4
	Destrucción de información	2	4
	Manipulación de programas	3	3
Ofimática	Uso no previsto	2	2
	Difuso de software dañino	2	4
	Destrucción de información	3	4
	Manipulación de programas	3	3

Tabla 45: *Valoración de las amenazas de ataques intencionados para los activos de tipo Software*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

Amenazas para el tipo de activo Hardware

AMENAZAS SEGÚN MAGERIT PARA EL TIPO DE ACTIVO HARDWARE [HW]			
Activos [HW]	**Desastres naturales**	**Probabilidad de incidencia**	**Degradación**
	Fuego	2	5

Computadoras desktops	Daños por agua	2	5
	Desastres naturales	2	5
Laptops	Fuego	2	5
	Daños por agua	2	5
	Desastres naturales	2	5
Equipos de reprografía	Fuego	2	5
	Daños por agua	2	5
	Desastres naturales	2	5
Firewall	Fuego	2	5
	Daños por agua	2	5
	Desastres naturales	2	5
Router	Fuego	2	5
	Daños por agua	2	5

	Desastres naturales	2	5

Tabla 46: *Valoración de las amenazas de desastres naturales para los activos de tipo Hardware*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

AMENAZAS SEGÚN MAGERIT PARA EL TIPO DE ACTIVO HARDWARE [HW]			
Activos [HW]	**De origen industrial**	**Probabilidad de incidencia**	**Degradación**
Computadoras desktops	Fuego	2	5
	Daños por agua	3	5
	Desastres industriales	2	5
	Contaminación mecánica	4	4
	Contaminación electromagnética	3	3
	Avería de origen físico o lógico	4	4
	Corte del suministro eléctrico	2	3

	Condiciones inadecuadas de temperatura o humedad	2	3
	Emanaciones electromagnéticas	2	2
Laptops	Fuego	2	5
	Daños por agua	3	5
	Desastres industriales	2	5
	Contaminación mecánica	4	4
	Contaminación electromagnética	2	3
	Avería de origen físico o lógico	3	4
	Corte del suministro eléctrico	2	2
	Condiciones inadecuadas de temperatura o humedad	2	3
	Emanaciones electromagnéticas	2	2
	Fuego	2	5
	Daños por agua	3	5

Equipos de reprografía	Desastres industriales	2	5
	Contaminación mecánica	3	4
	Contaminación electromagnética	2	3
	Avería de origen físico o lógico	3	4
	Corte del suministro eléctrico	3	4
	Condiciones inadecuadas de temperatura o humedad	2	3
	Emanaciones electromagnéticas	2	2
Firewall	Fuego	2	5
	Daños por agua	2	5
	Desastres industriales	2	5
	Contaminación mecánica	3	3
	Contaminación electromagnética	2	2
	Avería de origen físico o lógico	3	4

	Corte del suministro eléctrico	2	2
	Condiciones inadecuadas de temperatura o humedad	1	3
	Emanaciones electromagnéticas	2	2
Router	Fuego	2	5
	Daños por agua	2	5
	Desastres industriales	2	5
	Contaminación mecánica	3	4
	Contaminación electromagnética	2	2
	Avería de origen físico o lógico	3	4
	Corte del suministro eléctrico	2	2
	Condiciones inadecuadas de temperatura o humedad	2	2
	Emanaciones electromagnéticas	2	2

Tabla 47: *Valoración de las amenazas de origen industrial para los activos de tipo Hardware*
Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

AMENAZAS SEGÚN MAGERIT PARA EL TIPO DE ACTIVO HARDWARE [HW]			
Activos [HW]	**Errores y fallos no intencionados**	**Probabilidad de incidencia**	**Degradación**
Computadoras desktops	Errores del administrador	3	3
	Errores de mantenimiento / actualización de equipos (hardware)	3	4
	Caída del sistema por agotamiento de recursos	3	4
	Pérdida de equipos	2	5
Laptops	Errores del administrador	3	3
	Errores de mantenimiento / actualización de equipos (hardware)	3	4
	Caída del sistema por agotamiento de recursos	3	4
	Pérdida de equipos	3	5
Equipos de reprografía	Errores del administrador	3	3
	Errores de mantenimiento / actualización de equipos (hardware)	3	4
	Caída del sistema por agotamiento de recursos	4	4

	Pérdida de equipos	2	5
Firewall	Errores del administrador	3	3
	Errores de mantenimiento / actualización de equipos (hardware)	3	4
	Caída del sistema por agotamiento de recursos	2	3
	Pérdida de equipos	2	5
Router	Errores del administrador	3	3
	Errores de mantenimiento / actualización de equipos (hardware)	3	4
	Caída del sistema por agotamiento de recursos	3	3
	Pérdida de equipos	2	5

Tabla 48: *Valoración de las amenazas de errores y fallos no intencionados para los activos de tipo Hardware*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

AMENAZAS SEGÚN MAGERIT PARA EL TIPO DE ACTIVO HARDWARE [HW]			
Activos [HW]	**Ataques intencionados**	**Probabilidad de incidencia**	**Degradación**
Computadoras desktops	Abuso de privilegios de acceso	2	2
	Uso no previsto	3	1
	Acceso no autorizado	2	2
	Manipulación de los equipos	2	2
	Denegación de servicio	2	3
	Robo	3	5
	Ataque destructivo	2	5
Laptops	Abuso de privilegios de acceso	2	2
	Uso no previsto	3	1
	Acceso no autorizado	2	3
	Manipulación de los equipos	2	2

	Denegación de servicio	2	3
	Robo	3	5
	Ataque destructivo	2	5
Equipos de reprografía	Abuso de privilegios de acceso	3	2
	Uso no previsto	3	1
	Acceso no autorizado	2	3
	Manipulación de los equipos	2	4
	Denegación de servicio	2	3
	Robo	3	5
	Ataque destructivo	2	5
Firewall	Acceso no autorizado	2	2
	Manipulación de los equipos	2	2
	Denegación de servicio	2	3

	Robo	2	5
	Ataque destructivo	2	5
Router	Uso no previsto	2	2
	Acceso no autorizado	2	3
	Manipulación de los equipos	1	3
	Denegación de servicio	2	3
	Robo	2	5
	Ataque destructivo	2	5

Tabla 49: *Valoración de las amenazas de ataques intencionados para los activos de tipo Hardware*
Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

Amenazas para el tipo de activo Redes de comunicaciones

AMENAZAS SEGÚN MAGERIT PARA EL TIPO REDES DE COMUNICACIONES [COM]			
Activos [COM]	**De Origen Industrial**	**Probabilidad de incidencia**	**Degradación**
Internet	Fallo de servicios de comunicaciones	4	3
Internet de respaldo	Fallo de servicios de comunicaciones	3	3

Tabla 50: *Valoración de las amenazas de origen industrial para los activos de tipo Redes de comunicaciones*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

AMENAZAS SEGÚN MAGERIT PARA EL TIPO REDES DE COMUNICACIONES [COM]			
Activos [COM]	**De errores y fallos no intencionados**	**Probabilidad de incidencia**	**Degradación**
	Errores del administrador	3	4
	Errores de [re-]encaminamiento	3	4

Internet	Errores de secuencia	3	3
	Escapes de información	2	2
	Fugas de información	2	2
	Errores de mantenimiento / actualización de equipos (hardware)	3	3
	Caída del sistema por agotamiento de recursos	3	3
Internet de respaldo	Errores del administrador	3	4
	Errores de [re-]encaminamiento	4	4
	Errores de secuencia	3	3
	Escapes de información	2	2
	Fugas de información	2	2
	Errores de mantenimiento / actualización de equipos (hardware)	3	3
	Caída del sistema por agotamiento de recursos	3	3

Tabla 51: *Valoración de las amenazas de errores y fallos no intencionados para los activos de tipo Redes de comunicaciones*
Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

AMENAZAS SEGÚN MAGERIT PARA EL TIPO REDES DE COMUNICACIONES [COM]			
Activos [COM]	**Ataques intencionados**	**Probabilidad de incidencia**	**Degradación**
Internet	Abuso de privilegios de acceso	3	1
	Uso no previsto	3	2
	[Re-]encaminamiento de mensajes	3	4
	Alteración de secuencia	3	3
	Acceso no autorizado	3	3
	Análisis de tráfico	2	4
	Interceptación de información (escucha)	2	4
	Modificación deliberada de la información	2	4
	Denegación de servicio	2	4
	Abuso de privilegios de acceso	3	1
	Uso no previsto	4	3

Internet de respaldo	[Re-]encaminamiento de mensajes	3	4
	Alteración de secuencia	3	3
	Acceso no autorizado	3	3
	Análisis de tráfico	2	4
	Interceptación de información (escucha)	2	4
	Modificación deliberada de la información	2	4
	Denegación de servicio	2	4

Tabla 52: *Valoración de las amenazas de ataques intencionados para los activos de tipo Redes de comunicaciones*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

Amenazas para el tipo de activo Soportes de información

AMENAZAS SEGÚN MAGERIT PARA EL TIPO SOPORTES DE INFORMACIÓN [Media]			
Activos [Media]	**Desastres naturales**	**Probabilidad de incidencia**	**Degradación**
USB	Fuego	2	5
	Daños por agua	2	5
	Desastres naturales	2	5
Disco duro externo	Fuego	2	5
	Daños por agua	2	5
	Desastres naturales	2	5
Servidores	Fuego	2	5
	Daños por agua	2	5
	Desastres naturales	2	5

Tabla 53: *Valoración de las amenazas de desastres naturales para los activos de tipo Soportes de información*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

AMENAZAS SEGÚN MAGERIT PARA EL TIPO SOPORTES DE INFORMACIÓN [Media]			
Activos [Media]	**De Origen Industrial**	**Probabilidad de incidencia**	**Degradación**
USB	Fuego	2	5
	Daños por agua	3	5
	Desastres industriales	2	5
	Contaminación mecánica	3	3
	Contaminación electromagnética	3	3
	Avería de origen físico o lógico	3	4
	Condiciones inadecuadas de temperatura o humedad	2	3
	Degradación de los soportes de almacenamiento de información	2	3
	Emanaciones electromagnéticas	3	3
	Fuego	2	5
	Daños por agua	3	5

Disco duro externo	Desastres industriales	2	5
	Contaminación mecánica	4	3
	Contaminación electromagnética	3	3
	Avería de origen físico o lógico	4	4
	Condiciones inadecuadas de temperatura o humedad	2	2
	Degradación de los soportes de almacenamiento de información	2	3
	Emanaciones electromagnéticas	3	3
Servidores	Fuego	2	5
	Daños por agua	3	5
	Desastres industriales	2	5
	Contaminación mecánica	3	3
	Contaminación electromagnética	3	3
	Avería de origen físico o lógico	4	4

	Condiciones inadecuadas de temperatura o humedad	2	3
	Degradación de los soportes de almacenamiento de información	2	3
	Emanaciones electromagnéticas	3	3
Repositorios de código fuente	Fallo de servicios de comunicaciones	3	2

Tabla 54: *Valoración de las amenazas de ataques de origen industrial para los activos de tipo Soportes de información*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

AMENAZAS SEGÚN MAGERIT PARA EL TIPO SOPORTES DE INFORMACIÓN [Media]			
Activos [Media]	**De errores y fallos no intencionados**	**Probabilidad de incidencia**	**Degradación**
USB	Errores de los usuarios	3	3
	Alteración accidental de la información	3	3
	Destrucción de información	3	5
	Errores de mantenimiento / actualización de equipos (hardware)	3	3

	Pérdida de equipos	3	5
Disco duro externo	Errores de los usuarios	3	3
	Alteración accidental de la información	3	3
	Destrucción de información	3	5
	Errores de mantenimiento / actualización de equipos (hardware)	2	3
	Pérdida de equipos	3	5
Servidores	Errores de los usuarios	3	3
	Errores del administrador	3	3
	Errores de mantenimiento / actualización de equipos (hardware)	2	3
	Pérdida de equipos	2	5
	Indisponibilidad del personal	2	2
Repositorios de código fuente	Errores del administrador	2	3

Tabla 55: *Valoración de las amenazas de errores y fallos no intencionados para los activos de tipo Soportes de información*
Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

AMENAZAS SEGÚN MAGERIT PARA EL TIPO SOPORTES DE INFORMACIÓN [Media]			
Activos [Media]	**Ataques intencionados**	**Probabilidad de incidencia**	**Degradación**
USB	Uso no previsto	3	1
	Acceso no autorizado	3	2
	Manipulación de los equipos	3	2
	Robo	3	5
	Ataque destructivo	3	5
Disco duro externo	Uso no previsto	4	1
	Acceso no autorizado	3	2
	Manipulación de los equipos	3	2
	Robo	3	5
	Ataque destructivo	3	5

Servidores	Uso no previsto	2	2
	Acceso no autorizado	2	2
	Modificación deliberada de la información	2	4
	Destrucción de información	2	4
	Divulgación de información	2	2
	Manipulación de los equipos	2	2
	Robo	2	5
	Ataque destructivo	2	5
Repositorios de código fuente	Uso no previsto	2	2
	Acceso no autorizado	2	4
	Modificación deliberada de la información	2	3
	Destrucción de información	2	5
	Divulgación de información	2	4

	Robo	2	4

Tabla 56: *Valoración de las amenazas de ataques intencionados para los activos de tipo Soportes de información*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

Amenazas para el tipo de activo Equipamiento auxiliar

AMENAZAS SEGÚN MAGERIT PARA EL TIPO EQUIPAMIENTO AUXILIAR [AUX]			
Activos [AUX]	**Desastres naturales**	**Probabilidad de incidencia**	**Degradación**
Generador eléctrico	Fuego	2	5
	Daños por agua	2	5
	Desastres naturales	2	5
UPS	Fuego	2	5
	Daños por agua	2	5
	Desastres naturales	2	5

Equipo de climatización	Fuego	2	5
	Daños por agua	2	5
	Desastres naturales	2	5
Mobiliario	Fuego	2	5
	Daños por agua	2	5
	Desastres naturales	2	5
NVR	Fuego	2	5
	Daños por agua	2	5
	Desastres naturales	2	5

Tabla 57: *Valoración de las amenazas de desastres naturales para los activos de tipo Equipamiento auxiliar*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

AMENAZAS SEGÚN MAGERIT PARA EL TIPO EQUIPAMIENTO AUXILIAR [AUX]			
Activos [AUX]	**De Origen Industrial**	**Probabilidad de incidencia**	**Degradación**
Generador eléctrico	Fuego	3	5
	Daños por agua	2	5
	Desastres industriales	3	5
	Contaminación mecánica	3	3
	Contaminación electromagnética	3	1
	Avería de origen físico o lógico	2	4
	Condiciones inadecuadas de temperatura o humedad	2	2
	Interrupción de otros servicios y suministros esenciales	3	2
	Emanaciones electromagnéticas	3	1
	Fuego	2	5
	Daños por agua	3	5

UPS	Desastres industriales	3	5
	Contaminación mecánica	3	3
	Contaminación electromagnética	2	2
	Avería de origen físico o lógico	3	3
	Condiciones inadecuadas de temperatura o humedad	2	2
	Corte de suministro eléctrico	3	2
	Emanaciones electromagnéticas	4	1
Equipo de climatización	Fuego	2	5
	Daños por agua	2	5
	Desastres industriales	3	5
	Contaminación mecánica	3	3
	Contaminación electromagnética	3	1
	Avería de origen físico o lógico	2	3

	Corte de suministro eléctrico	3	3
	Interrupción de otros servicios y suministros esenciales	3	3
	Emanaciones electromagnéticas	3	1
Mobiliario	Fuego	2	5
	Daños por agua	2	5
	Desastres industriales	2	5
	Contaminación mecánica	3	2
	Avería de origen físico o lógico	3	3
NVR	Fuego	2	5
	Daños por agua	2	5
	Desastres industriales	2	5
	Contaminación mecánica	3	3
	Contaminación electromagnética	3	1

	Avería de origen físico o lógico	2	4
	Corte de suministro eléctrico	3	2
	Condiciones inadecuadas de temperatura o humedad	2	1
	Fallo de servicios de comunicaciones	3	2
	Interrupción de otros servicios y suministros esenciales	3	2
	Degradación de los soportes de almacenamiento de información	2	2
	Emanaciones electromagnéticas	4	1

Tabla 58: *Valoración de las amenazas de origen industrial para los activos de tipo Equipamiento auxiliar*
Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

AMENAZAS SEGÚN MAGERIT PARA EL TIPO EQUIPAMIENTO AUXILIAR [AUX]			
Activos [AUX]	**De errores y fallos no intencionados**	**Probabilidad de incidencia**	**Degradación**
	Errores de los usuarios	3	2

Generador eléctrico	Errores del administrador	3	2
	Errores de mantenimiento / actualización de equipos (hardware)	3	3
	Pérdida de equipos	2	5
UPS	Errores de los usuarios	2	3
	Errores de administrador	2	4
	Errores de mantenimiento / actualización de equipos (hardware)	3	3
	Pérdida de equipos	2	5
Equipo de climatización	Errores de los usuarios	2	3
	Errores del administrador	2	3
	Errores de mantenimiento / actualización de equipos (hardware)	3	3
	Pérdida de equipos	2	5
Mobiliario	Errores de mantenimiento / actualización de equipos (hardware)	2	3
	Pérdida de equipos	2	5

NVR	Errores de administrador	2	2
	Errores de mantenimiento / actualización de equipos (hardware)	3	3
	Pérdida de equipos	2	5

Tabla 59: *Valoración de las amenazas de errores y fallos no intencionados para los activos de tipo Equipamiento auxiliar*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

AMENAZAS SEGÚN MAGERIT PARA EL TIPO EQUIPAMIENTO AUXILIAR [AUX]			
Activos [AUX]	**Ataques intencionados**	**Probabilidad de incidencia**	**Degradación**
Generador eléctrico	Uso no previsto	2	2
	Acceso no autorizado	2	2
	Manipulación de los equipos	2	2
	Robo	2	5
	Ataque destructivo	2	5

UPS	Uso no previsto	2	2
	Acceso no autorizado	2	2
	Manipulación de los equipos	1	4
	Robo	2	5
	Ataque destructivo	2	5
Equipo de climatización	Manipulación de los equipos	2	2
	Robo	2	5
	Ataque destructivo	2	5
Mobiliario	Uso no previsto	2	1
	Acceso no autorizado	2	1
	Manipulación de los equipos	2	1
	Robo	2	5
	Ataque destructivo	2	5

	Ocupación enemiga	2	2
NVR	Manipulación de la configuración	2	4
	Uso no previsto	2	1
	Acceso no autorizado	2	1
	Divulgación de información	2	1
	Manipulación de los equipos	2	2
	Robo	2	5
	Ataque destructivo	2	5

Tabla 60: *Valoración de las amenazas de ataques intencionados para los activos de tipo Equipamiento auxiliar*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

Amenazas para el tipo de activo Instalaciones

AMENAZAS SEGÚN MAGERIT PARA EL TIPO INSTALACIONES [L]			
Activos [L]	**Desastres naturales**	**Probabilidad de incidencia**	**Degradación**
Oficina	Fuego	2	5
	Daños por agua	2	5
	Desastres naturales	2	5

Tabla 61: *Valoración de las amenazas de desastres naturales para los activos de tipo Instalaciones*
Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

AMENAZAS SEGÚN MAGERIT PARA EL TIPO INSTALACIONES [L]			
Activos [L]	**De Origen Industrial**	**Probabilidad de incidencia**	**Degradación**
	Fuego	2	5
	Daños por agua	2	2

Oficina	Desastres industriales	2	5
	Contaminación mecánica	2	1
	Corte de suministro eléctrico	2	2

Tabla 62: *Valoración de las amenazas de ataques de origen industrial para los activos de tipo Instalaciones*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

AMENAZAS SEGÚN MAGERIT PARA EL TIPO INSTALACIONES [L]			
Activos [L]	**De errores y fallos no intencionados**	**Probabilidad de incidencia**	**Degradación**
Oficina	Errores de los usuarios	2	2
	Errores del administrador	2	2

Tabla 63: *Valoración de las amenazas de errores y fallos no intencionados para los activos de tipo Instalaciones*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

AMENAZAS SEGÚN MAGERIT PARA EL TIPO INSTALACIONES [L]			
Activos [L]	**Ataques intencionados**	**Probabilidad de incidencia**	**Degradación**
Oficina	Uso no previsto	3	1
	Acceso no autorizado	2	2
	Ataque destructivo	2	5
	Ocupación enemiga	2	5
	Indisponibilidad del personal	2	2

Tabla 64: *Valoración de las amenazas de ataques intencionados para los activos de tipo Instalaciones*
Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

Amenazas para el tipo de activo Personal

AMENAZAS SEGÚN MAGERIT PARA EL TIPO PERSONAL [P]			
Activos [P]	**Desastres naturales**	**Probabilidad de incidencia**	**Degradación**
Jefe de área	Fuego	2	3
	Desastres naturales	2	3
P.Desarrolladores / Programadores	Fuego	2	3
	Desastres naturales	2	3
P.Soporte técnico	Fuego	2	3
	Desastres naturales	2	3
P.Redes	Fuego	2	3
	Desastres naturales	2	3

Tabla 65: *Valoración de las amenazas de desastres naturales para los activos de tipo Personal*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

AMENAZAS SEGÚN MAGERIT PARA EL TIPO PERSONAL [P]			
Activos [P]	**De Origen Industrial**	**Probabilidad de incidencia**	**Degradación**
Jefe de área	Fuego	2	3
P.Desarrolladores / Programadores	Fuego	2	3
P.Soporte técnico	Fuego	2	3
P.Redes	Fuego	2	3

Tabla 66: *Valoración de las amenazas de origen industrial para los activos de tipo Personal*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

AMENAZAS SEGÚN MAGERIT PARA EL TIPO PERSONAL [P]			
Activos [P]	**De errores y fallos no intencionados**	**Probabilidad de incidencia**	**Degradación**
	Deficiencias en la organización	3	3

Jefe de área	Escapes de información	2	3
	Fugas de información	2	3
	Indisponibilidad del personal	3	4
P.Desarrolladores / Programadores	Deficiencias en la organización	3	3
	Escapes de información	2	3
	Fugas de información	2	3
	Indisponibilidad del personal	3	4
P.Soporte técnico	Deficiencias en la organización	3	3
	Indisponibilidad del personal	3	4
P.Redes	Deficiencias en la organización	3	3
	Indisponibilidad del personal	3	4

Tabla 67: *Valoración de las amenazas de errores y fallos no intencionados para los activos de tipo Personal*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

AMENAZAS SEGÚN MAGERIT PARA EL TIPO PERSONAL [P]			
Activos [P]	**Ataques intencionados**	**Probabilidad de incidencia**	**Degradación**
Jefe de área	Repudio	2	1
	Indisponibilidad del personal	2	4
	Extorsión	1	3
	Ingeniería social (picaresca)	1	3
P.Desarrolladores / Programadores	Suplantación de la identidad del usuario	2	4
	Repudio	2	1
	Indisponibilidad del personal	2	4
	Extorsión	1	3
	Ingeniería social (picaresca)	1	3
	Repudio	2	1
	Indisponibilidad del personal	2	4

P.Soporte técnico	Extorsión	1	3
	Ingeniería social (picaresca)	2	4
P.Redes	Repudio	2	1
	Indisponibilidad del personal	2	4
	Extorsión	1	3
	Ingeniería social (picaresca)	2	3

Tabla 68: *Valoración de las amenazas de ataques intencionados para los activos de tipo Personal*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, (MAR.2.2).

MAR.3. Caracterización de las salvaguardas

(3. Método de análisis de riesgos - 3.1.5. Paso 3: Salvaguardas, libro MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método, (pp.31-35))

MAR.3.1. Identificación de las salvaguardas pertinentes

(3.2.3. Tarea MAR.3: Caracterización de las salvaguardas, libro MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método, (pp.42-43))

En esta fase se van a identificar las salvaguardas que presenten cada amenaza

1. Protecciones generales u horizontales

H	Protecciones Generales
H.IA	Identificación y autenticación
H.AC	Control de acceso lógico
H.ST	Segregación de tareas
H.IR	Gestión de incidencias
H.tools	Herramientas de seguridad
H.tools.AV	Herramienta contra código dañino
H.tools.IDS	IDS/IPS: Herramienta de detección / prevención de intrusión
H.tools.CC	Herramienta de chequeo de configuración
H.tools.VA	Herramienta de análisis de vulnerabilidades
H.tools.TM	Herramienta de monitorización de tráfico
H.tools.DLP	DLP: Herramienta de monitorización de contenidos
H.tools.LA	Herramienta para análisis de logs
H.tools.HP	Honey net / honey pot
H.tools.SFV	Verificación de las funciones de seguridad
H.VM	Gestión de vulnerabilidades
H.AU	Registro y auditoría

2. Protección de los datos / información

D	Protección de la Información
D.A	Copias de seguridad de los datos (backup)
D.I	Aseguramiento de la integridad

D.C	Cifrado de la información
D.DS	Uso de firmas electrónicas
D.TS	Uso de servicios de fechado electrónico (time stamping)
3. Protección de las claves criptográficas	
K	Gestión de claves criptográficas
K.IC	Gestión de claves de cifra de información
K.DS	Gestión de claves de firma de información
K.disk	Gestión de claves para contenedores criptográficos
K.comms	Gestión de claves de comunicaciones
K.509	Gestión de certificados
4. Protección de los servicios	
S	Protección de los Servicios
S.A	Aseguramiento de la disponibilidad
S.start	Aceptación y puesta en operación
S.SC	Se aplican perfiles de seguridad
S.op	Explotación
S.CM	Gestión de cambios (mejoras y sustituciones)
S.end	Terminación
S.www	Protección de servicios y aplicaciones web
S.email	Protección del correo electrónico
S.dir	Protección del directorio
S.dns	Protección del servidor de nombres de dominio (DNS)
S.TW	Teletrabajo
S.voip	Voz sobre IP
5. Protección de las aplicaciones (software)	
SW	Protección de las Aplicaciones Informáticas
SW.A	Copias de seguridad (backup)
SW.start	Puesta en producción
SW.SC	Se aplican perfiles de seguridad
SW.op	Explotación / Producción
SW.CM	Cambios (actualizaciones y mantenimiento)
SW.end	Terminación
6. Protección de los equipos (hardware)	
HW	Protección de los Equipos Informáticos

HW.start	Puesta en producción
HW.SC	Se aplican perfiles de seguridad
HW.A	Aseguramiento de la disponibilidad
HW.op	Operación
HW.CM	Cambios (actualizaciones y mantenimiento)
HW.end	Terminación
HW.PCD	Informática móvil
HW.print	Reproducción de documentos
HW.pabx	Protección de la centralita telefónica (PABX)
7. Protección de las comunicaciones	
COM	Protección de las Comunicaciones
COM.start	Entrada en servicio
COM.SC	Se aplican perfiles de seguridad
COM.A	Aseguramiento de la disponibilidad
COM.aut	Autenticación del canal
COM.I	Protección de la integridad de los datos intercambiados
COM.C	Protección criptográfica de la confidencialidad de los datos intercambiados
COM.op	Operación
COM.CM	Cambios (actualizaciones y mantenimiento)
COM.end	Terminación
COM.internet	Internet: uso de ? acceso a
COM.wifi	Seguridad Wireless (WiFi)
COM.mobile	Telefonía móvil
COM.DS	Segregación de las redes en dominios
8. Protección en los puntos de interconexión con otros sistemas	
IP	Puntos de interconexión: conexiones entre zonas de confianza
IP.SPP	Sistema de protección perimetral
IP.BS	Protección de los equipos de frontera
9. Protección de los soportes de información	
MP	Protección de los Soportes de Información
MP.A	Aseguramiento de la disponibilidad
MP.IC	Protección criptográfica del contenido

MP.clean	Limpieza de contenidos
MP.end	Destrucción de soportes
10. Protección de los elementos auxiliares	
AUX	Elementos Auxiliares
AUX.A	Aseguramiento de la disponibilidad
AUX.start	Instalación
AUX.power	Suministro eléctrico
AUX.AC	Climatización
AUX.wires	Protección del cableado
11. Seguridad física – Protección de las instalaciones	
L	Protección de las Instalaciones
L.design	Diseño
L.depth	Defensa en profundidad
L.AC	Control de los accesos físicos
L.A	Aseguramiento de la disponibilidad
L.end	Terminación
12. Salvaguardas relativas al personal	
PS	Gestión del Personal
PS.AT	Formación y concienciación
PS.A	Aseguramiento de la disponibilidad
13. Salvaguardas de tipo organizativo	
G	Organización
G.RM	Gestión de riesgos
G.plan	Planificación de la seguridad
G.exam	Inspecciones de seguridad
14. Continuidad de operaciones	
BC	Continuidad del negocio
BC.BIA	Análisis de impacto (BIA)
BC.DRP	Plan de Recuperación de Desastres (DRP)

MAR.3.2. Valoración de las salvaguardas

(3.2.3. Tarea MAR.3: Caracterización de las salvaguardas, libro MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método, (p.43))

Al analizar cada salvaguarda se identificará los tipos de protección según MAGERIT (Metodología de análisis y gestión de riesgos de los sistemas de información):

1. **[PR] prevención**

   Diremos que una salvaguarda es preventiva cuando reduce las oportunidades de que un incidente ocurra. Si la salvaguarda falla y el incidente llega a ocurrir, los daños son los mismos.

2. **DR] disuasión**

   Diremos que una salvaguarda es disuasoria cuando tiene un efecto tal sobre los atacantes que estos no se atreven o se lo piensan dos veces antes de atacar. Son salvaguardas que actúan antes del incidente, reduciendo las probabilidades de que ocurra; pero que no tienen influencia sobre los daños causados caso de que el atacante realmente se atreva.

3. **[EL] eliminación**

   Diremos que una salvaguarda elimina un incidente cuando impide que éste tenga lugar. Son salvaguardas que actúan antes de que el incidente se haya producido. No reducen los daños caso de que la salvaguarda no sea perfecta y el incidente llegue a ocurrir.

4. **[IM] minimización del impacto / limitación del impacto**

   Se dice que una salvaguarda minimiza o limita el impacto cuando acota las consecuencias de un incidente.

5. **[CR] corrección**

   Diremos que una salvaguarda es correctiva cuando, habiéndose producido un daño, lo repara. Son salvaguardas que actúan después de que el incidente se haya producido y por tanto reducen los daños.

6. **[RC] recuperación**

   Diremos que una salvaguarda ofrece recuperación cuando permite regresar al estado anterior al incidente. Son salvaguardas que no reducen las probabilidades del incidente, pero acotan los daños a un periodo de tiempo.

7. **[MN] monitorización**

Son las salvaguardas que trabajan monitorizando lo que está ocurriendo o lo que ha ocurrido. Si se detectan cosas en tiempo real, podemos reaccionar atajando el incidente para limitar el impacto; si se detectan cosas a posteriori, podemos aprender del incidente y mejorar el sistema de salvaguardas de cara al futuro.

8. **[DC] detección**

Diremos que una salvaguarda funciona detectando un ataque cuando informa de que el ataque está ocurriendo. Aunque no impide el ataque, sí permite que entren en operación otras medidas que atajen la progresión del ataque, minimizando daños.

9. **[AW] concienciación**

Son las actividades de formación de las personas anexas al sistema que pueden tener una influencia sobre él. La formación reduce los errores de los usuarios, lo cual tiene un efecto preventivo. También mejora las salvaguardas de todo tipo pues los que las operan lo hacen con eficacia y rapidez, potenciando su efecto o, al menos, no menoscabándolo por una mala operación.

10. **[AD] administración**

Se refiere a las salvaguardas relacionadas con los componentes de seguridad del sistema. Una buena administración evita el desconocimiento de lo que hay y por tanto impide que hayan puertas desconocidas por las que pudiera tener éxito un ataque. En general pueden considerarse medidas de tipo preventivo.

En el siguiente cuadro se mostrará las salvaguardas identificadas para cada tipo de activo, especificando la descripción de las salvaguardas y el tipo de protección.

Salvaguardas para el tipo de activo Datos/información

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Datos /información	Datos de configuración	Medio	Protección de la Información	Mantener capacitado y concientizado al personal encargado de los datos de configuración (archivo digital de direcciones ip, licencias, cuentas de registro de usuarios) sobre los riesgos asociados al compartir información y las consecuencias para la institución y como para el individuo.	Concienciación
			Copias de seguridad de los datos (backup)	Mantener capacitado al personal encargado de los datos de configuración (archivo digital de direcciones ip, licencias, cuentas de registro de usuarios) sobre los riesgos asociados al eliminar,perder y no contar con copias de respaldo.	Concienciación
			Protección de la Información	Establecer revisiones periódicas de los privilegios de acceso a los datos de configuración para tener asegurado el correcto uso de dichos datos.	Prevención
			Aseguramiento de la integridad	Tener control de acceso basado en roles que aseguren que solo personas autorizadas tengan permiso para modificar dichos archivos.	Prevención
			Copias de seguridad de los datos (backup)	Tener implementado un sistema de copias de seguridad regulares de los archivos críticos, almacenar estas copias en un lugar seguro fuera del alcance directo de los usuarios con acceso a los archivos originales	Recuperación
			Protección de la Información	Proporcionar formación al personal sobre la importancia de la seguridad de la información y mejores prácticas.	Concienciación

Tabla 69: *Salvaguardas para el activo Datos de configuración*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Datos /información	Base de datos de la página web de la DDCC	Alto	Protección de la Información	Mantener entornos de desarrollo, pruebas y producción separados donde los gestores de BDs deberán realizar cambios y pruebas en un entorno controlado antes de aplicarlos a la base de datos de producción.	Prevención
			Protección de la Información	Establecer entornos de desarrollo, pruebas y producción separados donde los gestores de BDs deberán realizar cambios y pruebas en un entorno controlado, realizando supervisiones constantes sobre dichos entornos de desarrollo.	Prevención
			Protección de la Información	Asegurarse de que el personal encargado de la base de datos de la página web de la DDCC reciba capacitación continua y esté consciente de los riesgos vinculados al compartir información parcial o completa.	Concienciación
			Protección de la Información	Tener configurada la base de datos para solicitar confirmación antes de realizar cambios significativos. Agregar pasos adicionales como solicitar una contraseña o confirmación explícita, para evitar modificaciones accidentales.	Disuasión
			Protección de la Información	Establecer en la configuración de la base de datos de manera que sea necesario confirmar antes de eliminar registros significativos. Introduce medidas adicionales, como solicitar una contraseña o una confirmación adicional, con el objetivo de disminuir la probabilidad de eliminaciones involuntarias.	Disuasión
			Protección de la Información	Asegurarse de que el personal encargado de la base de datos de la página web de la DDCC reciba capacitación continua y esté consciente de los riesgos vinculados al comentar información parcial o completa.	Concienciación
			Protección de la Información	Implementar un sistema de acceso basado en roles para garantizar que los usuarios tengan solo los privilegios necesarios para realizar sus tareas y así limitar el acceso a funciones de modificación solo a personal autorizado.	Prevención
			Protección de la Información	Tener configurada la base de datos para solicitar confirmación antes de realizar cambios, agregando pasos adicionales como solicitar una contraseña o confirmación explícita para evitar modificaciones no autorizadas.	Disuasión
			Protección de la Información	Establecer en la configuración de la base de datos de manera que sea necesario confirmar antes de eliminar registros significativos, introduciendo medidas adicionales como solicitar una contraseña o una confirmación adicional, con el objetivo de mitigar la destrucción de la información.	Disuasión
			Protección de la Información	Implementar un sistema de acceso basado en roles para garantizar que los usuarios tengan solo los privilegios necesarios para realizar sus tareas y así limitar el acceso a funciones de modificación solo a personal autorizado.	Prevención

Tabla 70: *Salvaguardas para el activo Base de datos de la página web de la DDCC*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Datos /información	Documentos digitales	Medio	Protección de la Información	Mantener concientizado al personal que maneja los documentos digitales sobre los riesgos asociados al compartir información de manera imprudente.	Concienciación
			Copias de seguridad de los datos (backup)	Fomentar al personal que maneja los documentos digitales a crear copias de seguridad de los archivos más importantes para evitar la eliminación del activo.	Recuperación
			Protección de la Información	Proporcionar formación al personal sobre la importancia de la seguridad de la información y mejores prácticas.	Concienciación
			Aseguramiento de la integridad	Establecer controles de acceso adecuados a los medios de almacenamiento donde se encuentran dichos documentos	Disuasión
			Copias de seguridad de los datos (backup) Aseguramiento de la integridad	Motivar al personal encargado de documentos digitales a realizar copias de respaldo de los archivos críticos como medida preventiva contra la pérdida del activo, al mismo tiempo que se implementan controles de acceso efectivos en los dispositivos de almacenamiento que resguardan dichos documentos.	Recuperación

Tabla 71: *Salvaguardas para el activo Documentos digitales*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Salvaguardas para el tipo de activo Claves criptográficas

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Claves criptográficas	Contraseña de acceso a la base de datos de la página web de la DDCC	Alto	Gestión de claves criptográficas	Implementar filtros antiphishing en el servidor de correo electrónico para detectar y bloquear mensajes de phishing antes de llegar a las bandejas de entrada del personal, así mismo fomentar el uso de gestores de contraseñas seguras y confiables.	Prevención
			Gestión de claves criptográficas	Crear contraseñas seguras que incluyan combinaciones de letras, números y carácteres especiales, así como la importancia de cambiarlas regularmente.	Prevención
			Gestión de claves criptográficas	Tener control de acceso basado en roles que aseguren que solo personas autorizadas tengan potestad sobre dichas contraseñas	Prevención
			Gestión de claves criptográficas	Fomentar el uso de gestores de contraseñas seguras y confiables para controlar cambios	Prevención
			Gestión de claves criptográficas	Fomentar el uso de gestores de contraseñas seguras y confiables para controlar cambios	Prevención
			Gestión de claves criptográficas	Proporcionar formación al personal sobre la importancia de la seguridad de la información y mejores prácticas en contraseñas.	Concienciación
			Gestión de claves criptográficas	Establecer revisiones periódicas de los privilegios de acceso a las contraseñas para tener asegurado el correcto uso de dichos datos.	Prevención
			Gestión de claves criptográficas	Tener control de acceso basado en roles que aseguren que solo personas autorizadas tengan potestad sobre dichas contraseñas	Prevención
			Gestión de claves criptográficas	Fomentar el uso de gestores de contraseñas seguras y confiables para controlar cambios y tener control de acceso basado en roles que aseguren que solo personas autorizadas tengan potestad sobre dichas contraseñas.	Prevención
			Gestión de claves criptográficas	Fomentar el uso de gestores de contraseñas seguras y confiables para controlar cambios y tener control de acceso basado en roles que aseguren que solo personas autorizadas tengan potestad sobre dichas contraseñas.	Prevención

Tabla 72: *Salvaguardas para el activo Contraseña de acceso a la base de datos de la página web de la DDCC*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Claves criptográficas	Contraseña de acceso al NVR	Alto	Gestión de claves criptográficas	Crear contraseñas seguras que incluyan combinaciones de letras, números y carácteres especiales, así como la importancia de cambiarlas regularmente.	Prevención
			Gestión de claves criptográficas	Limitar el acceso a la contraseña del NVR a un solo personal bajo responsabilidad del activo	Prevención
			Gestión de claves criptográficas	Mantener total discreción al momento de usar la contraseña	Prevención
			Gestión de claves criptográficas	Limitar el acceso a la contraseña del NVR a un solo personal	Prevención

Tabla 73: *Salvaguardas para el activo Contraseñas de acceso al NVR*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Claves criptográficas	Contraseña de acceso al router	Alto	Gestión de claves criptográficas	Implementar filtros antiphishing en el servidor de correo electrónico para detectar y bloquear mensajes de phishing antes de llegar a las bandejas de entrada del personal, así mismo fomentar el uso de gestores de contraseñas seguras y confiables.	Prevención
			Gestión de claves criptográficas	Crear contraseñas seguras que incluyan combinaciones de letras, números y carácteres especiales, así como la importancia de cambiarlas regularmente.	Prevención
			Gestión de claves criptográficas	Tener control de acceso basado en roles que aseguren que solo personas autorizadas tengan potestad sobre dichas contraseñas	Prevención
			Gestión de claves criptográficas	Fomentar el uso de gestores de contraseñas seguras y confiables para controlar cambios	Prevención
			Gestión de claves criptográficas	Fomentar el uso de gestores de contraseñas seguras y confiables para controlar cambios	Prevención
			Gestión de claves criptográficas	Proporcionar formación al personal sobre la importancia de la seguridad de la información y mejores prácticas en contraseñas.	Concienciación
			Gestión de claves criptográficas	Establecer revisiones periódicas de los privilegios de acceso a las contraseñas para tener asegurado el correcto uso de dichos datos.	Prevención
			Gestión de claves criptográficas	Tener control de acceso basado en roles que aseguren que solo personas autorizadas tengan potestad sobre dichas contraseñas	Prevención
			Gestión de claves criptográficas	Fomentar el uso de gestores de contraseñas seguras y confiables para controlar cambios y tener control de acceso basado en roles que aseguren que solo personas autorizadas tengan potestad sobre dichas contraseñas.	Prevención
			Gestión de claves criptográficas	Fomentar el uso de gestores de contraseñas seguras y confiables para controlar cambios y tener control de acceso basado en roles que aseguren que solo personas autorizadas tengan potestad sobre dichas contraseñas.	Prevención

Tabla 74: *Salvaguardas para el activo Contraseña de acceso al router*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Salvaguardas para el tipo de activo Servicios

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Servicios	Página Help Desk	Alto	Gestión de cambios (mejoras y sustituciones)	Solicitar actualizaciones a la empresa desarrolladora para mitigar fallas en el activo.	Corrección
			Protección de los Servicios	Realizar revisiones periodicas de la información generada en la página Help Desk y limitar el acceso total de la página a un solo personal bajo responsabilidad del activo	Prevención
			Protección de los Servicios	Limitar el acceso total de la página Help Desk a un solo personal bajo responsabilidad del activo	Prevención

Tabla 75: *Salvaguardas para el activo Página Help Desk*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Servicios	Páginas web institucionales	Alto	Gestión de cambios (mejoras y sustituciones)	Tener procedimientos formales para la realización de pruebas rigurosas antes y después de implementar cambios en la página web.	Prevención
			Gestión de cambios (mejoras y sustituciones)	Tener procedimientos formales para la realización de pruebas rigurosas antes y después de implementar cambios en la página web.	Prevención
			Gestión de cambios (mejoras y sustituciones)	Tener procedimientos formales para la realización de pruebas rigurosas antes y después de implementar cambios en la página web.	Prevención
			Protección de los Servicios	Mantener concientizado al personal que maneja información generada por las páginas sobre los riesgos asociados al compartir información y las consecuencias para la institución y como para el individuo.	Concienciación
			Gestión de cambios (mejoras y sustituciones)	Tener procedimientos formales para la realización de pruebas rigurosas antes y después de implementar cambios en la página web.	Prevención
			Protección de servicios y aplicaciones web	Tener una copia de seguridad del proyecto en desarrrollo.	Prevención
			Protección de los Servicios	Proporcionar formación al personal sobre la importancia de la seguridad de la información y mejores prácticas en páginas web institucionales.	Concienciación
			Gestión de cambios (mejoras y sustituciones)	Utiliza sistemas de control de versiones, como Git, para rastrear y controlar cambios en el código fuente de la página web Implementa un registro de cambios accesible y monitorizable para documentar cualquier alteración en el contenido o funcionalidades de la página web. Restringe el acceso al código y a la infraestructura de la página web solo a personal autorizado y asegúrate de mantener políticas de acceso basadas en roles.	Corrección / Monitorización
			Gestión de cambios (mejoras y sustituciones)	Utiliza sistemas de control de versiones, como Git, para rastrear y controlar cambios en el código fuente de la página web Implementa un registro de cambios accesible y monitorizable para documentar cualquier alteración en el contenido o funcionalidades de la página web. Restringe el acceso al código y a la infraestructura de la página web solo a personal autorizado y asegúrate de mantener políticas de acceso basadas en roles.	Corrección / Monitorización
			Protección de servicios y aplicaciones web	Configurar reglas dentro del firewall y filtros para identificar y bloquear tráfico malicioso durante un ataque.	Detección

Tabla 76: *Salvaguardas para el activo Páginas web institucionales*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Salvaguardas para el tipo de activo Software

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Software	Antivirus	Medio	Copias de seguridad (backup)	Tener copia de seguridad del instalador debidamente resguardada	Recuperación
			Copias de seguridad (backup)	Tener copia de seguridad del instalador debidamente resguardada	Recuperación
			Se aplican perfiles de seguridad	Establecer un control de acceso estricto para los ajustes y funciones del antivirus, permitiendo que solo el personal autorizado pueda realizar cambios en la configuración.	Prevención

Tabla 77: *Salvaguardas para el activo Antivirus*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Software	Sistemas Operativos	Medio	Cambios (actualizaciones y mantenimiento)	Realizar un mantenimiento al sistema operativo	Corrección
			Protección de las Aplicaciones Informáticas	Capacitar a los trabajadores sobre las mejores prácticas al realizar actualizaciones, enfatizando la necesidad de permitir que el proceso se complete antes de apagar la máquina.	Concienciación
			Protección de las Aplicaciones Informáticas	Instalar y mantener actualizado un software antivirus y antimalware confiable en todos los sistemas operativos.	Detección
			Protección de las Aplicaciones Informáticas	Instalar y mantener actualizado un software antivirus y antimalware confiable en todos los sistemas operativos.	Detección
			Protección de las Aplicaciones Informáticas	Implementar firmas digitales o checksums para los archivos del sistema, permitiendo la detección de cualquier modificación no autorizada.	Detección
			Copias de seguridad (backup)	Contar con un plan de recuperación del sistema que incluya procedimientos claros para restaurar el sistema operativo y los datos desde las copias de seguridad.	Recuperación

Tabla 78: *Salvaguardas para el activo Sistemas operativos*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Software	Ofimática	Medio	Cambios (actualizaciones y mantenimiento)	Realizar un mantenimiento, actualización del paquete de ofimática	Corrección

Tabla 79: *Salvaguardas para el activo Ofimática*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos

Salvaguardas para el tipo de activo Hardware

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Hardware	Computadoras desktops	Medio	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Cambios (actualizaciones y mantenimiento)	Realizar un mantenimiento al activo dañado.	Corrección
			Cambios (actualizaciones y mantenimiento)	Realizar un mantenimiento al activo dañado.	Corrección
			Aseguramiento de la disponibilidad	Realizar una evaluación periódica de los recursos del sistema, incluyendo la memoria RAM, el procesador y el almacenamiento para así prever la caida por agotamiento de recursos.	Monitorización

Tabla 80: *Salvaguardas para el activo Computadoras desktops*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Hardware	Laptops	Medio	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Cambios (actualizaciones y mantenimiento)	Realizar un mantenimiento al activo dañado.	Corrección
			Cambios (actualizaciones y mantenimiento)	Realizar un mantenimiento al activo dañado.	Corrección
			Aseguramiento de la disponibilidad	Realizar una evaluación periódica de los recursos del sistema, incluyendo la memoria RAM, el procesador y el almacenamiento para así prever la caida por agotamiento de recursos.	Monitorización
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración

Tabla 81: *Salvaguardas para el activo Laptops*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Hardware	Equipos de reprografía	Medio	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Realizar una evaluación periódica de los recursos como tóner , rodillos para así prever la caida por agotamiento de recursos.	Monitorización

Tabla 82: *Salvaguardas para el activo Equipos de reprografía*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Hardware	Firewall	Alto	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Cambios (actualizaciones y mantenimiento)	Realizar un mantenimiento al activo dañado.	Corrección
			Protección de los Equipos Informáticos	Establece procesos formales de revisión periódica de las reglas y configuraciones del firewall.	Monitorización
			Aseguramiento de la disponibilidad	Realizar una evaluación periódica de los recursos del sistema, incluyendo la memoria RAM, el procesador para así prever la caida por agotamiento de recursos.	Monitorización
			Se aplican perfiles de seguridad	Configurar reglas de filtrado y límites de tasa en el firewall para detectar y bloquear patrones de tráfico malicioso asociados con ataques de saturación.	Corrección

Tabla 83: *Salvaguardas para el activo Firewall*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Hardware	Router	Alto	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Configurar límites de tasa para el tráfico de entrada ysalida en el router para evitar sobrecargas repentinas.	Corrección
			Aseguramiento de la disponibilidad	Configurar límites de tasa para el tráfico de entrada ysalida en el router para evitar sobrecargas repentinas.	Corrección

Tabla 84: *Salvaguardas para el activo Router*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Salvaguardas para el tipo de activo Redes de comunicaciones

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Redes de comunicaciones	Internet	Alto	Cambios (actualizaciones y mantenimiento)	Mantenimiento periodico del sistema del cableado estructurado	Corrección
			Aseguramiento de la disponibilidad	Implementar sistemas de gestión de ancho de banda para distribuir y asignar recursos equitativamente entre los usuarios.	Corrección

Tabla 85: *Salvaguardas para el activo Internet*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Redes de comunicaciones	Internet de respaldo	Alto	Cambios (actualizaciones y mantenimiento)	Mantenimiento periodico del sistema del cableado estructurado	Corrección
			Aseguramiento de la disponibilidad	Implementar sistemas de gestión de ancho de banda para distribuir y asignar recursos equitativamente entre los usuarios.	Corrección

Tabla 86: *Salvaguardas para el activo Internet de respaldo*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Salvaguardas para el tipo de activo Soportes de información

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Soportes de información	Servidores	Alto	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Protección de los Soportes de Información	Realizar inspecciones regulares para identificar y corregir posibles fuentes de contaminación electromagnética.	Prevención

Tabla 87: *Salvaguardas para el activo Servidores*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Soportes de información	Repositorios de código fuente		Protección de los Soportes de Información	Gestionar niveles de privilegios de acceso del personal deacuerdo a sus funciones.	Prevención
			Protección de los Soportes de Información	Gestionar niveles de privilegios de acceso del personal deacuerdo a sus funciones.	Prevención
			Protección de los Soportes de Información	Gestionar niveles de privilegios de acceso del personal deacuerdo a sus funciones.	Prevención
			Protección de los Soportes de Información	Tener configurado el repositorio con procesos de autorización y confirmación de los stakeholders o personas responsables sobre cambios a realizar.	Disuasión
			Protección de los Soportes de Información	Limitar el acceso a una persona encargada de ser el administrador de la cuenta de acceso al repositorio.	Prevención
			Protección de los Soportes de Información	Limitar el acceso a una persona encargada de ser el administrador de la cuenta de acceso al repositorio.	Prevención

Tabla 88: *Salvaguardas para el activo Repositorios de código fuente*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Salvaguardas para el tipo de activo Equipamiento auxiliar

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Equipamiento auxiliar	Generador eléctrico	Alto	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración

Tabla 89: *Salvaguardas para el activo Generador eléctrico*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Equipamiento auxiliar	UPS	Alto	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Instalación	Implementar un sistema de supervisión remota que permita monitorear el estado del UPS y recibir alertas en tiempo real sobre eventos críticos como la baja batería. Esto ayuda a identificar problemas antes de que se conviertan en situaciones de emergencia.	Monitorización
			Instalación	Implementar un sistema de supervisión remota que permita monitorear el estado del UPS y recibir alertas en tiempo real sobre eventos críticos como la baja batería. Esto ayuda a identificar problemas antes de que se conviertan en situaciones de emergencia.	Monitorización

Tabla 90: *Salvaguardas para el activo UPS*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Equipamiento auxiliar	NVR	Alto	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración
			Aseguramiento de la disponibilidad	Limitar el acceso a una persona encargada de ser el administrador de la cuenta de acceso del NVR.	Prevención

Tabla 91: *Salvaguardas para el activo NVR*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Salvaguardas para el tipo de activo Instalaciones

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Instalaciones	Oficina	Alto	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral que implique el trabajo remoto.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral que implique el trabajo remoto.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral que implique el trabajo remoto.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral que implique el trabajo remoto.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral que implique el trabajo remoto.	Administración

Tabla 92: *Salvaguardas para el Oficina*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Salvaguardas para el tipo de activo Personal

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Personal	Jefe de área	Alto	Aseguramiento de la disponibilidad	Tener métodos de continuidad para el reemplazo temporal del personal afectado.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad para el reemplazo temporal del personal afectado.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad para el reemplazo temporal del personal afectado.	Administración
			Formación y concienciación	Mantener capacitado y concientizado al personal designado como jefe de área sobre los riesgos asociados al compartir información de su alcance y las consecuencias para la institución y como para el individuo.	Concienciación

Tabla 93: *Salvaguardas para el activo Jefe de área*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Personal	P.Desarrolladores / Programadores	Alto	Aseguramiento de la disponibilidad	Tener métodos de continuidad para el reemplazo temporal del personal afectado.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad para el reemplazo temporal del personal afectado.	Administración
			Aseguramiento de la disponibilidad	Tener métodos de continuidad para el reemplazo temporal del personal afectado.	Administración
			Formación y concienciación	Mantener capacitado y concientizado al personal designado como jefe de área sobre los riesgos asociados al compartir información de su alcance y las consecuencias para la institución y como para el individuo.	Concienciación

Tabla 94: *Salvaguardas para el activo P. Desarrolladores / Programadores*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Personal	P.Soporte técnico	Medio	Aseguramiento de la disponibilidad	Tener métodos de continuidad para el reemplazo temporal del personal afectado.	Administración
			Formación y concienciación	Mantener capacitado al personal sobre la ingeniería social en la institución.	Concienciación

Tabla 95: *Salvaguardas para el activo P. Soporte técnico*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

Tipo de activos	Activos	Nivel del activo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda
Personal	P.Redes	Medio	Aseguramiento de la disponibilidad	Tener métodos de continuidad para el reemplazo temporal del personal afectado.	Administración

Tabla 96: *Salvaguardas para el activo P. Redes*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos, Libro II - Catálogo de Elementos.

MAR.4. Estimación del estado de riesgo

MAR.4.1. Estimación del impacto y MAR.4.2. Estimación del riesgo

(3.2.4. Tarea MAR.4: Estimación del estado de riesgo, libro MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método, (pp.44-45))

En la siguiente tabla se muestra cómo se va a calcular el riesgo en base al impacto y la probabilidad:

Tabla para calcular el riesgo de los activos

Matriz de valoración de riesgos			Probabilidad			
			Insignificante	Moderada	Dañina	Extrema
			1	2	3	4
Impacto	37-45	Catastrófico	Medio	Alto	Alto	Alto
	28-36	Crítico	Medio	Medio	Alto	Alto
	19-27	Medio	Bajo	Medio	Medio	Alto
	10-18	Menor	Bajo	Bajo	Bajo	Medio
	1-9	Insignificante	Bajo	Bajo	Bajo	Medio

Tabla 97: *Matriz de valoración de riesgos*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro III - Guía de Técnicas (p.7).

Descripción de cada color:

ROJO-ALTO:

Tiene un impacto catastrófico y una probabilidad moderada.

Tiene un impacto catastrófico y una probabilidad dañina.

Tiene un impacto catastrófico y una probabilidad extrema.

Tiene un impacto crítico y una probabilidad dañina.

Tiene un impacto crítico y una probabilidad extrema.

Tiene un medio crítico y una probabilidad extrema.

AMARILLO-MEDIO:

Tiene un impacto catastrófico y una probabilidad insignificante.

Tiene un impacto crítico y una probabilidad insignificante.

Tiene un impacto crítico y una probabilidad moderada.

Tiene un impacto medio y una probabilidad moderada.

Tiene un impacto medio y una probabilidad dañina.

Tiene un impacto menor y una probabilidad extrema.

Tiene un impacto insignificante y una probabilidad extrema.

VERDE-BAJO:

Tiene un impacto medio y una probabilidad insignificante.

Tiene un impacto menor y una probabilidad insignificante.

Tiene un impacto menor y una probabilidad moderada.

Tiene un impacto menor y una probabilidad dañina.

Tiene un impacto insignificante y una probabilidad insignificante.

Tiene un impacto insignificante y una probabilidad moderada.

Tiene un impacto insignificante y una probabilidad dañina.

En la siguiente tabla se muestra la evaluación del riesgo de cada amenaza que pueda tener un activo, en el cual se analiza el impacto potencial y la estimación del estado del riesgo potencial.

Evaluación del riesgo para el tipo de activo Datos/información

ACTIVO: Datos/información					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
Datos de configuración (valor del activo=5)	Errores de los usuarios	3	15	Menor	Bajo
	Errores del administrador	3	15	Menor	Bajo
	Errores de configuración	3	15	Menor	Bajo
	Escapes de información	2	20	Medio	Medio
	Alteración accidental de la información	2	15	Menor	Bajo
	Destrucción de información (Errores y fallos no intencionados	2	25	Medio	Medio
	Fugas de información	2	20	Medio	Medio
	Suplantación de la identidad del usuario	2	15	Menor	Bajo
	Abuso de privilegios de acceso	2	20	Medio	Medio
	Modificación deliberada de la información	2	20	Medio	Medio

	Destrucción de información (Ataques intencionados)	2	20	Medio	Medio

Tabla 98: *Cuadro de evaluación de riesgos para el activo Datos de configuración*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Datos/información					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
Base de datos de la página web de la DDCC (valor del activo=9)	Errores de los usuarios	3	36	Crítico	Alto
	Errores del administrador	2	36	Crítico	Medio
	Escapes de información	2	36	Crítico	Medio
	Alteración accidental de la información	2	36	Crítico	Medio
	Destrucción de información (Errores y fallos no intencionados)	2	45	Catastrófico	Alto
	Fugas de información	2	36	Crítico	Medio
	Suplantación de la identidad del usuario	1	27	Medio	Bajo

	Abuso de privilegios de acceso	3	45	Catastrófico	Alto
	Modificación deliberada de la información	3	45	Catastrófico	Alto
	Destrucción de información (Ataques intencionados)	3	45	Catastrófico	Alto
	Divulgación de información	3	36	Crítico	Alto

Tabla 99: *Cuadro de evaluación de riesgos para el activo Base de datos de la página web de la DDCC*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Datos/información					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
	Errores de los usuarios	3	3	Insignificante	Bajo
	Errores del administrador	3	3	Insignificante	Bajo
	Errores de monitorización	2	3	Insignificante	Bajo
	Escapes de información	3	6	Insignificante	Bajo
	Alteración accidental de la información	3	3	Insignificante	Bajo

Log de actividades (valor del activo=3)	Destrucción de información (Errores y fallos no intencionados)	3	6	Insignificante	Bajo
	Fugas de información	3	6	Insignificante	Bajo
	Manipulación de los registros de actividad (log)	2	3	Insignificante	Bajo
	Manipulación de la configuración	2	3	Insignificante	Bajo
	Suplantación de la identidad del usuario	2	3	Insignificante	Bajo
	Abuso de privilegios de acceso	2	3	Insignificante	Bajo
	Repudio	2	3	Insignificante	Bajo
	Modificación deliberada de la información	2	3	Insignificante	Bajo
	Destrucción de información (Ataques intencionados)	2	3	Insignificante	Bajo

Tabla 100: *Cuadro de evaluación de riesgos para el activo Log de actividades*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Datos/información					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
Datos de prueba (valor del activo=3)	Errores de los usuarios	3	3	Insignificante	Bajo
	Errores del administrador	3	3	Insignificante	Bajo
	Escapes de información	2	3	Insignificante	Bajo
	Alteración accidental de la información	3	6	Insignificante	Bajo
	Destrucción de información (Errores y fallos no intencionados)	2	6	Insignificante	Bajo
	Fugas de información	2	3	Insignificante	Bajo
	Suplantación de la identidad del usuario	2	3	Insignificante	Bajo
	Abuso de privilegios de acceso	2	3	Insignificante	Bajo
	Modificación deliberada de la información	2	9	Insignificante	Bajo
	Destrucción de información (Ataques intencionados)	2	12	Menor	Bajo

Tabla 101: *Cuadro de evaluación de riesgos para el activo Datos de prueba*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Datos/información					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
Documentos digitales (valor del activo=6)	Errores de los usuarios	3	18	Menor	Bajo
	Errores del administrador	3	18	Menor	Bajo
	Escapes de información	4	18	Menor	Medio
	Alteración accidental de la información	3	18	Menor	Medio
	Destrucción de información (Errores y fallos no intencionados)	4	18	Menor	Medio
	Fugas de información	4	18	Menor	Medio
	Suplantación de la identidad del usuario	3	18	Menor	Bajo
	Abuso de privilegios de acceso	3	18	Menor	Bajo
	Modificación deliberada de la información	3	24	Medio	Medio
	Destrucción de información (Ataques intencionados)	3	24	Medio	Medio

Tabla 102: *Cuadro de evaluación de riesgos para el activo Documentos digitales*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

Evaluación del riesgo para el tipo de activo Claves criptográficas

ACTIVO: Claves criptográficas					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
Contraseña de acceso a la base de datos de la página web de la DDCC (valor del activo=9)	Errores de los usuarios	3	45	Catastrófico	Alto
	Errores del administrador	3	45	Catastrófico	Alto
	Escapes de información	2	27	Medio	Medio
	Alteración accidental de la información	2	36	Crítico	Medio
	Destrucción de información (Errores y fallos no intencionados)	2	36	Crítico	Medio
	Fugas de información	2	27	Medio	Medio
	Suplantación de la identidad del usuario	2	27	Medio	Medio
	Abuso de privilegios de acceso	2	27	Medio	Medio
	Acceso no autorizado	3	36	Crítico	Alto
	Modificación deliberada de la información	2	36	Crítico	Medio

	Destrucción de información (Ataques intencionados)	2	36	Crítico	Medio

Tabla 103: *Cuadro de evaluación de riesgos para el activo Contraseña de acceso a la base de datos de la página web de la DDCC*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Claves criptográficas					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
Contraseña de acceso al NVR (valor del activo=7)	Errores del administrador	3	28	Crítico	Alto
	Escapes de información	2	21	Medio	Medio
	Alteración accidental de la información	2	14	Menor	Bajo
	Destrucción de información (Errores y fallos no intencionados)	2	14	Menor	Bajo
	Fugas de información	2	21	Medio	Medio
	Suplantación de la identidad del usuario	2	21	Medio	Medio

	Acceso no autorizado	3	21	Medio	Medio
	Modificación deliberada de la información	2	14	Menor	Bajo
	Destrucción de información (Ataques intencionados)	2	14	Menor	Bajo

Tabla 104: *Cuadro de evaluación de riesgos para el activo Contraseña de acceso al NVR*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Claves criptográficas					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
Contraseña de acceso al router (valor del activo=7)	Errores de los usuarios	3	28	Crítico	Alto
	Errores del administrador	3	28	Crítico	Alto
	Escapes de información	2	28	Crítico	Medio
	Alteración accidental de la información	3	21	Medio	Medio
	Destrucción de información (Errores y fallos no intencionados)	2	28	Crítico	Medio
	Fugas de información	2	28	Crítico	Medio
	Suplantación de la identidad del usuario	2	21	Medio	Medio
	Abuso de privilegios de acceso	2	21	Medio	Medio
	Acceso no autorizado	3	21	Medio	Medio

	Modificación deliberada de la información	3	35	Crítico	Alto
	Destrucción de información (Ataques intencionados)	3	35	Crítico	Alto

Tabla 105: *Cuadro de evaluación de riesgos para el activo Contraseña de acceso al router*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

Evaluación del riesgo para el tipo de activo Servicios

ACTIVO: Servicios					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
	Errores de los usuarios	2	7	Insignificante	Bajo
	Errores del administrador	2	21	Medio	Medio
	Errores de [re-]encaminamiento	2	7	Insignificante	Bajo
	Escapes de información	2	7	Insignificante	Bajo
	Alteración accidental de la información	2	14	Menor	Bajo

Página Help Desk (valor del activo=7)	Destrucción de información (Errores y fallos no intencionados)	2	28	Crítico	Medio
	Fugas de información	2	7	Insignificante	Bajo
	Caída del sistema por agotamiento de recursos	3	14	Menor	Bajo
	Suplantación de la identidad del usuario	2	14	Menor	Bajo
	Alteración de secuencia	2	14	Menor	Bajo
	Acceso no autorizado	2	21	Medio	Medio
	Modificación deliberada de la información	2	14	Menor	Bajo
	Destrucción de información (Ataques intencionados)	2	28	Crítico	Medio
	Divulgación de información	2	14	Menor	Bajo

Tabla 106: *Cuadro de evaluación de riesgos para el activo Página Help Desk*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Servicios					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
Páginas web institucionales (valor del activo=8)	Errores del administrador	3	32	Crítico	Alto
	Errores de [re-]encaminamiento	2	32	Crítico	Medio
	Errores de secuencia	2	32	Crítico	Medio
	Escapes de información	2	32	Crítico	Medio
	Alteración accidental de la información	2	32	Crítico	Medio
	Destrucción de información (Errores y fallos no intencionados)	2	40	Catastrófico	Alto
	Fugas de información	2	32	Crítico	Medio
	Errores de mantenimiento / actualización de programas (software)	3	16	Menor	Bajo
	Caída del sistema por agotamiento de recursos	3	16	Menor	Bajo
	Suplantación de la identidad del usuario	2	14	Menor	Bajo
	Uso no previsto	2	16	Menor	Bajo
	Acceso no autorizado	2	16	Menor	Bajo
	Modificación deliberada de la información	3	32	Crítico	Alto

	Destrucción de información (Ataques intencionados)	3	32	Crítico	Alto
	Denegación de servicio	3	24	Medio	Medio

Tabla 107: *Cuadro de evaluación de riesgos para el activo Páginas web institucionales*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Servicios					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
Soporte técnico (valor del activo=4)	Errores de los usuarios	2	4	Insignificante	Bajo
	Errores del administrador	3	12	Menor	Bajo
	Suplantación de la identidad del usuario	3	12	Menor	Bajo
	Abuso de privilegios de acceso	3	12	Menor	Bajo
	Uso no previsto	2	12	Menor	Bajo
	Alteración de secuencia	3	8	Insignificante	Bajo
	Repudio	3	8	Insignificante	Bajo

Tabla 108: *Cuadro de evaluación de riesgos para el activo Soporte técnico*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

Evaluación del riesgo para el tipo de activo Software

ACTIVO: Software					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
Aplicaciones (valor del activo=5)	Avería de origen físico o lógico	3	10	Menor	Bajo
	Errores de los usuarios	3	10	Menor	Bajo
	Errores del administrador	3	10	Menor	Bajo
	Difusión de software dañino (Errores y fallos no intencionados)	2	15	Menor	Bajo
	Alteración accidental de la información	3	10	Menor	Bajo
	Vulnerabilidades de los programas (software)	2	15	Menor	Bajo
	Errores de mantenimiento / actualización de programas (software)	3	15	Menor	Bajo
	Uso no previsto	3	10	Menor	Bajo

	Difusión de software dañino (Ataques intencionados)	3	15	Menor	Bajo
	Manipulación de programas	3	10	Menor	Bajo

Tabla 109: *Cuadro de evaluación de riesgos para el activo Aplicaciones*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Software					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
	Avería de origen físico o lógico	3	12	Menor	Bajo
	Errores de los usuarios	3	18	Menor	Bajo
	Errores del administrador	3	18	Menor	Bajo
	Difusión de software dañino (Errores y fallos no intencionados)	2	12	Menor	Bajo
	Alteración accidental de la información	3	18	Menor	Bajo

Antivirus (valor del activo=6)	Destrucción de información (Errores y fallos no intencionados)	2	24	Medio	Medio
	Errores de mantenimiento / actualización de programas (software)	3	18	Menor	Bajo
	Abuso de privilegios de acceso	3	18	Menor	Bajo
	Difusión de software dañino (Ataques intencionados)	3	18	Menor	Bajo
	Modificación deliberada de la información	3	18	Menor	Bajo
	Destrucción de información (Ataques intencionados)	3	30	Crítico	Alto
	Manipulación de programas	3	24	Medio	Medio

Tabla 110: *Cuadro de evaluación de riesgos para el activo Antivirus*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Software					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
Sistemas Operativos (valor del activo=5)	Avería de origen físico o lógico	4	15	Menor	Medio
	Errores de los usuarios	2	25	Medio	Medio
	Errores del administrador	2	15	Menor	Bajo
	Difusión de software dañino (Errores y fallos no intencionados)	1	20	Medio	Medio
	Alteración accidental de la información	1	25	Medio	Bajo
	Vulnerabilidades de los programas (software)	3	10	Menor	Bajo
	Errores de mantenimiento / actualización de programas (software)	3	15	Menor	Bajo
	Difusión de software dañino (Ataques intencionados)	3	20	Medio	Medio
	Modificación deliberada de la información	2	20	Medio	Medio
	Destrucción de información (Ataques intencionados)	2	20	Medio	Medio
	Manipulación de programas	3	15	Menor	Bajo

Tabla 111: *Cuadro de evaluación de riesgos para el activo Sistemas operativos*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Software					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
Ofimática (valor del activo=4)	Avería de origen físico o lógico	*4*	8	Insignificante	Medio
	Errores de los usuarios	3	12	Menor	Bajo
	Difusión de software dañino (Errores y fallos no intencionados)	3	12	Menor	Bajo
	Alteración accidental de la información	2	12	Menor	Bajo
	Destrucción de información (Errores y fallos no intencionados)	2	16	Menor	Bajo
	Errores de mantenimiento / actualización de programas (software)	2	8	Insignificante	Bajo
	Uso no previsto	2	8	Insignificante	Bajo
	Difusión de software dañino (Ataques intencionados)	2	16	Menor	Bajo
	Destrucción de información (Ataques intencionados)	3	16	Menor	Bajo

	Manipulación de programas	3	12	Menor	Bajo

Tabla 112: *Cuadro de evaluación de riesgos para el activo Ofimática*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

Evaluación del riesgo para el tipo de activo Hardware

ACTIVO: Hardware					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
Computadoras desktops (valor del activo=6)	Fuego (Desastres naturales)	2	30	Crítico	Medio
	Daños por agua (Desastres naturales)	2	30	Crítico	Medio
	Desastres naturales	2	30	Crítico	Medio
	Fuego (De origen industrial)	2	30	Crítico	Medio
	Daños por agua (De origen industrial)	3	30	Crítico	Alto
	Desastres industriales	2	30	Crítico	Medio
	Contaminación mecánica	4	24	Medio	Alto
	Contaminación electromagnética	3	18	Menor	Bajo

	Avería de origen físico o lógico	4	24	Medio	Alto
	Corte del suministro eléctrico	2	18	Menor	Bajo
	Condiciones inadecuadas de temperatura o humedad	2	18	Menor	Bajo
	Emanaciones electromagnéticas	2	12	Menor	Bajo
	Errores del administrador	3	18	Menor	Bajo
	Errores de mantenimiento / actualización de equipos (hardware)	3	24	Medio	Medio
	Caída del sistema por agotamiento de recursos	3	24	Medio	Medio
	Pérdida de equipos	2	30	Crítico	Medio
	Abuso de privilegios de acceso	2	12	Menor	Bajo
	Uso no previsto	3	6	Insignificante	Bajo
	Acceso no autorizado	2	18	Menor	Bajo
	Manipulación de los equipos	2	12	Menor	Bajo
	Denegación de servicio	2	18	Menor	Bajo
	Robo	3	30	Crítico	Alto
	Ataque destructivo	2	30	Crítico	Medio

Tabla 113: *Cuadro de evaluación de riesgos para el activo Computadoras desktops*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Hardware					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
Laptops (valor del activo=6)	Fuego (Desastres naturales)	2	30	Crítico	Medio
	Daños por agua (Desastres naturales)	2	30	Crítico	Medio
	Desastres naturales	2	30	Crítico	Medio
	Fuego (De origen industrial)	2	30	Crítico	Medio
	Daños por agua (De origen industrial)	3	30	Crítico	Alto
	Desastres industriales	2	30	Crítico	Medio
	Contaminación mecánica	4	24	Medio	Alto
	Contaminación electromagnética	2	18	Menor	Bajo
	Avería de origen físico o lógico	3	24	Medio	Medio
	Corte del suministro eléctrico	2	12	Menor	Bajo
	Condiciones inadecuadas de temperatura o humedad	2	18	Menor	Bajo
	Emanaciones electromagnéticas	2	12	Menor	Bajo
	Errores del administrador	3	18	Menor	Bajo

	Errores de mantenimiento / actualización de equipos (hardware)	3	24	Medio	Medio
	Caída del sistema por agotamiento de recursos	3	24	Medio	Medio
	Pérdida de equipos	3	30	Crítico	Alto
	Abuso de privilegios de acceso	2	12	Menor	Bajo
	Uso no previsto	3	6	Insignificante	Bajo
	Acceso no autorizado	2	18	Menor	Bajo
	Manipulación de los equipos	2	12	Menor	Bajo
	Denegación de servicio	2	18	Menor	Bajo
	Robo	3	30	Crítico	Alto
	Ataque destructivo	2	30	Crítico	Medio

Tabla 114: *Cuadro de evaluación de riesgos para el activo Laptops*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Hardware					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
Equipos de reprografía (valor del activo=4)	Fuego (Desastres naturales)	2	20	Medio	Medio
	Daños por agua (Desastres naturales)	2	20	Medio	Medio
	Desastres naturales	2	20	Medio	Medio
	Fuego (De origen industrial)	2	20	Medio	Medio
	Daños por agua (De origen industrial)	3	20	Medio	Medio
	Desastres industriales	2	20	Medio	Medio
	Contaminación mecánica	3	16	Menor	Bajo
	Contaminación electromagnética	2	12	Menor	Bajo
	Avería de origen físico o lógico	3	16	Menor	Bajo
	Corte del suministro eléctrico	3	16	Menor	Bajo
	Condiciones inadecuadas de temperatura o humedad	2	12	Menor	Bajo
	Emanaciones electromagnéticas	2	8	Insignificante	Bajo
	Errores del administrador	3	12	Menor	Bajo

	Errores de mantenimiento / actualización de equipos (hardware)	3	16	Menor	Bajo
	Caída del sistema por agotamiento de recursos	4	16	Menor	Medio
	Pérdida de equipos	2	20	Medio	Medio
	Abuso de privilegios de acceso	3	8	Insignificante	Bajo
	Uso no previsto	3	4	Insignificante	Bajo
	Acceso no autorizado	2	12	Menor	Bajo
	Manipulación de los equipos	2	16	Menor	Bajo
	Denegación de servicio	2	12	Menor	Bajo
	Robo	3	20	Medio	Medio
	Ataque destructivo	2	20	Medio	Medio

Tabla 115: *Cuadro de evaluación de riesgos para el activo Equipos de reprografía*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Hardware					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
Firewall (valor del activo=8)	Fuego (Desastres naturales)	2	40	Catastrófico	Alto
	Daños por agua (Desastres naturales)	2	40	Catastrófico	Alto
	Desastres naturales	2	40	Catastrófico	Alto
	Fuego (De origen industrial)	2	40	Catastrófico	Alto
	Daños por agua (De origen industrial)	2	40	Catastrófico	Alto
	Desastres industriales	2	40	Catastrófico	Alto
	Contaminación mecánica	3	24	Medio	Medio
	Contaminación electromagnética	2	16	Menor	Bajo
	Avería de origen físico o lógico	3	32	Crítico	Alto
	Corte del suministro eléctrico	2	16	Menor	Bajo
	Condiciones inadecuadas de temperatura o humedad	1	24	Medio	Bajo
	Emanaciones electromagnéticas	2	16	Menor	Bajo

	Errores del administrador	3	24	Medio	Medio
	Errores de mantenimiento / actualización de equipos (hardware)	3	32	Crítico	Alto
	Caída del sistema por agotamiento de recursos	2	24	Medio	Medio
	Pérdida de equipos	2	40	Catastrófico	Alto
	Acceso no autorizado	2	16	Menor	Bajo
	Manipulación de los equipos	2	16	Menor	Bajo
	Denegación de servicio	2	24	Medio	Medio
	Robo	2	40	Catastrófico	Alto
	Ataque destructivo	2	40	Catastrófico	Alto

Tabla 116: Cuadro de evaluación de riesgos para el activo Firewall

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Hardware					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor el activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
Router (valor del activo=8)	Fuego (Desastres naturales)	2	40	Catastrófico	Alto
	Daños por agua (Desastres naturales)	2	40	Catastrófico	Alto
	Desastres naturales	2	40	Catastrófico	Alto
	Fuego (De origen industrial)	2	40	Catastrófico	Alto
	Daños por agua (De origen industrial)	2	40	Catastrófico	Alto
	Desastres industriales	2	40	Catastrófico	Alto
	Contaminación mecánica	3	32	Crítico	Alto
	Contaminación electromagnética	2	*16*	Menor	Bajo
	Avería de origen físico o lógico	3	32	Crítico	Alto
	Corte del suministro eléctrico	2	16	Menor	Bajo
	Condiciones inadecuadas de temperatura o humedad	2	16	Menor	Bajo
	Emanaciones electromagnéticas	2	*16*	Menor	Bajo

	Errores del administrador	3	24	Medio	Medio
	Errores de mantenimiento / actualización de equipos (hardware)	3	32	Crítico	Alto
	Caída del sistema por agotamiento de recursos	3	24	Medio	Medio
	Pérdida de equipos	2	40	Catastrófico	Alto
	Uso no previsto	2	16	Menor	Bajo
	Acceso no autorizado	2	24	Medio	Medio
	Manipulación de los equipos	1	24	Medio	Bajo
	Denegación de servicio	2	24	Medio	Medio
	Robo	2	40	Catastrófico	Alto
	Ataque destructivo	2	40	Catastrófico	Alto

Tabla 117: *Cuadro de evaluación de riesgos para el activo Router*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

Evaluación del riesgo para el tipo de activo Redes de comunicaciones

ACTIVO: Redes de comunicaciones					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
Internet (valor del activo = 8)	Fallo de servicios de comunicaciones	4	24	Medio	Alto
	Errores del administrador	3	32	Crítico	Alto
	Errores de [re-]encaminamiento	3	32	Crítico	Alto
	Errores de secuencia	3	24	Medio	Medio
	Escapes de información	2	16	Menor	Bajo
	Fugas de información	2	16	Menor	Bajo
	Errores de mantenimiento / actualización de equipos (hardware)	3	24	Medio	Medio
	Caída del sistema por agotamiento de recursos	3	24	Medio	Medio
	Abuso de privilegios de acceso	3	8	Insignificante	Bajo
	Uso no previsto	3	16	Menor	Bajo

	[Re-]encaminamiento de mensajes	3	32	Crítico	Alto
	Alteración de secuencia	3	24	Medio	Medio
	Acceso no autorizado	3	24	Medio	Medio
	Análisis de tráfico	2	32	Crítico	Medio
	Interceptación de información (escucha)	2	32	Crítico	Medio
	Modificación deliberada de la información	2	32	Crítico	Medio
	Denegación de servicio	2	32	Crítico	Medio

Tabla 118: *Cuadro de evaluación de riesgos para el activo Internet*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Redes de comunicaciones					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación**	**Impacto potencial**	**Estimación del riesgo potencial**
	Fallo de servicios de comunicaciones	3	24	Medio	Medio
	Errores del administrador	3	32	Crítico	Alto
	Errores de [re-]encaminamiento	4	32	Crítico	Alto

Internet de respaldo (valor del activo = 8)	Errores de secuencia	3	24	Medio	Medio
	Escapes de información	2	16	Menor	Bajo
	Fugas de información	2	16	Menor	Bajo
	Errores de mantenimiento / actualización de equipos (hardware)	3	24	Medio	Medio
	Caída del sistema por agotamiento de recursos	3	24	Medio	Medio
	Abuso de privilegios de acceso	3	8	Insignificante	Bajo
	Uso no previsto	4	24	Medio	Alto
	[Re-]encaminamiento de mensajes	3	32	Crítico	Alto
	Alteración de secuencia	3	24	Medio	Medio
	Acceso no autorizado	3	24	Medio	Medio
	Análisis de tráfico	2	32	Crítico	Medio
	Interceptación de información (escucha)	2	32	Crítico	Medio
	Modificación deliberada de la información	2	32	Crítico	Medio
	Denegación de servicio	2	32	Crítico	Medio

Tabla 119: Cuadro de evaluación de riesgos para el activo Internet de respaldo

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

Evaluación del riesgo para el tipo de activo Soportes de información

ACTIVO: Soportes de información					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación**	**Impacto potencial**	**Estimación del riesgo potencial**
USB (valor del activo = 3)	Fuego (Desastres naturales)	2	15	Menor	Bajo
	Daños por agua (Desastres naturales)	2	15	Menor	Bajo
	Desastres naturales	2	15	Menor	Bajo
	Fuego (De origen industrial)	2	15	Menor	Bajo
	Daños por agua (De origen industrial)	3	15	Menor	Bajo
	Desastres industriales	2	15	Menor	Bajo
	Contaminación mecánica	3	9	Insignificante	Bajo
	Contaminación electromagnética	3	9	Insignificante	Bajo
	Avería de origen físico o lógico	3	12	Menor	Bajo
	Condiciones inadecuadas de temperatura o humedad	2	9	Insignificante	Bajo
	Degradación de los soportes de almacenamiento de información	2	9	Insignificante	Bajo

	Emanaciones electromagnéticas	3	9	Insignificante	Bajo
	Errores de los usuarios	3	9	Insignificante	Bajo
	Alteración accidental de la información	3	9	Insignificante	Bajo
	Destrucción de información	3	15	Menor	Bajo
	Errores de mantenimiento / actualización de equipos (hardware)	3	9	Insignificante	Bajo
	Pérdida de equipos	3	15	Menor	Bajo
	Uso no previsto	3	3	Insignificante	Bajo
	Acceso no autorizado	3	6	Insignificante	Bajo
	Manipulación de los equipos	3	6	Insignificante	Bajo
	Robo	3	15	Menor	Bajo
	Ataque destructivo	3	15	Menor	Bajo

Tabla 120: *Cuadro de evaluación de riesgos para el activo USB*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Soportes de información					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
	Fuego (Desastres naturales)	2	15	Menor	Bajo
	Daños por agua (Desastres naturales)	2	15	Menor	Bajo
	Desastres naturales	2	15	Menor	Bajo
	Fuego (De origen industrial)	2	15	Menor	Bajo
	Daños por agua (De origen industrial)	3	15	Menor	Bajo
	Desastres industriales	2	15	Menor	Bajo
	Contaminación mecánica	3	9	Insignificante	Bajo
	Contaminación electromagnética	3	9	Insignificante	Bajo
	Avería de origen físico o lógico	3	12	Menor	Bajo
	Condiciones inadecuadas de temperatura o humedad	2	9	Insignificante	Bajo
	Degradación de los soportes de almacenamiento de información	2	9	Insignificante	Bajo

Disco duro externo (valor del activo = 3)	Emanaciones electromagnéticas	3	9	Insignificante	Bajo
	Errores de los usuarios	3	9	Insignificante	Bajo
	Alteración accidental de la información	3	9	Insignificante	Bajo
	Destrucción de información	3	15	Menor	Bajo
	Errores de mantenimiento / actualización de equipos (hardware)	2	9	Insignificante	Bajo
	Pérdida de equipos	3	15	Menor	Bajo
	Uso no previsto	3	3	Insignificante	Bajo
	Acceso no autorizado	3	6	Insignificante	Bajo
	Manipulación de los equipos	3	6	Insignificante	Bajo
	Robo	3	15	Menor	Bajo
	Ataque destructivo	3	15	Menor	Bajo

Tabla 121: *Cuadro de evaluación de riesgos para el activo Disco duro externo*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Soportes de información					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
Servidores (valor del activo = 9)	Fuego (Desastres Naturales)	2	45	Catastrófico	Alto
	Daños por agua (Desastres Naturales)	2	45	Catastrófico	Alto
	Desastres naturales	2	45	Catastrófico	Alto
	Fuego (De Origen Industrial)	2	45	Catastrófico	Alto
	Daños por agua (De Origen Industrial)	3	45	Catastrófico	Alto
	Desastres industriales	2	45	Catastrófico	Alto
	Contaminación mecánica	3	27	Medio	Medio
	Contaminación electromagnética	3	27	Medio	Medio
	Avería de origen físico o lógico	4	36	Crítico	Alto
	Condiciones inadecuadas de temperatura o humedad	2	18	Menor	Bajo
	Degradación de los soportes de almacenamiento de información	2	27	Medio	Medio

	Emanaciones electromagnéticas	3	27	Medio	Medio
	Errores de los usuarios	3	27	Medio	Medio
	Errores del administrador	3	27	Medio	Medio
	Errores de mantenimiento / actualización de equipos (hardware)	2	27	Medio	Medio
	Pérdida de equipos	2	45	Catastrófico	Alto
	Indisponibilidad del personal	2	18	Menor	Bajo
	Uso no previsto	2	18	Menor	Bajo
	Acceso no autorizado	2	18	Menor	Bajo
	Modificación deliberada de la información	2	36	Crítico	Medio
	Destrucción de información	2	36	Crítico	Medio
	Divulgación de información	2	18	Menor	Bajo
	Manipulación de los equipos	2	18	Menor	Bajo
	Robo	2	45	Catastrófico	Alto
	Ataque destructivo	2	45	Catastrófico	Alto

Tabla 122: *Cuadro de evaluación de riesgos para el activo Servidores*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Soportes de información					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación**	**Impacto potencial**	**Estimación del riesgo potencial**
Repositorios de código fuente (valor del activo = 7)	Fallo de servicios de comunicaciones	3	14	Menor	Bajo
	Errores del administrador	2	21	Medio	Medio
	Uso no previsto	2	14	Menor	Bajo
	Acceso no autorizado	2	28	Crítico	Medio
	Modificación deliberada de la información	2	21	Medio	Medio
	Destrucción de información	2	35	Crítico	Medio
	Divulgación de información	2	28	Crítico	Medio
	Robo	2	28	Crítico	Medio

Tabla 123: *Cuadro de evaluación de riesgos para el activo Repositorios de código fuente*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

Evaluación del riesgo para el tipo de activo Equipamiento auxiliar

ACTIVO: Equipamiento auxiliar					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
Generador eléctrico (valor del activo = 7)	Fuego (Desastres naturales)	2	35	Crítico	Medio
	Daños por agua (Desastres naturales)	2	35	Crítico	Medio
	Desastres naturales	2	35	Crítico	Medio
	Fuego (De origen industrial)	3	35	Crítico	Alto
	Daños por agua (De origen industrial)	2	35	Crítico	Medio
	Desastres industriales	3	35	Crítico	Alto
	Contaminación mecánica	3	14	Medio	Medio
	Contaminación electromagnética	3	7	Insignificante	Bajo
	Avería de origen físico o lógico	2	28	Crítico	Medio
	Condiciones inadecuadas de temperatura o humedad	2	14	Menor	Bajo

	Interrupción de otros servicios y suministros esenciales	3	14	Menor	Bajo
	Emanaciones electromagnéticas	4	7	Insignificante	Medio
	Errores de los usuarios	3	14	Menor	Bajo
	Errores del administrador	3	14	Menor	Bajo
	Errores de mantenimiento / actualización de equipos (hardware)	3	21	Medio	Medio
	Pérdida de equipos	2	35	Crítico	Medio
	Uso no previsto	2	14	Menor	Bajo
	Acceso no autorizado	2	14	Menor	Bajo
	Manipulación de los equipos	2	14	Menor	Bajo
	Robo	2	35	Crítico	Medio
	Ataque destructivo	2	35	Crítico	Medio

Tabla 124: *Cuadro de evaluación de riesgos para el activo Generador eléctrico*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Equipamiento auxiliar					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
UPS (valor del activo = 7)	Fuego (Desastres naturales)	2	35	Crítico	Medio
	Daños por agua (Desastres naturales)	2	35	Crítico	Medio
	Desastres naturales	2	35	Crítico	Medio
	Fuego (De origen industrial)	2	35	Crítico	Medio
	Daños por agua (De origen industrial)	3	35	Crítico	Alto
	Desastres industriales	3	35	Crítico	Alto
	Contaminación mecánica	3	21	Medio	Medio
	Contaminación electromagnética	2	14	Menor	Bajo
	Avería de origen físico o lógico	3	21	Medio	Medio
	Condiciones inadecuadas de temperatura o humedad	2	14	Menor	Bajo
	Corte de suministro eléctrico	3	14	Menor	Bajo
	Emanaciones electromagnéticas	4	7	Insignificante	Medio

	Errores de los usuarios	2	21	Medio	Medio
	Errores de administrador	2	28	Crítico	Medio
	Errores de mantenimiento / actualización de equipos (hardware)	3	21	Medio	Medio
	Pérdida de equipos	2	35	Crítico	Medio
	Uso no previsto	2	14	Menor	Bajo
	Acceso no autorizado	2	14	Menor	Bajo
	Manipulación de los equipos	1	28	Crítico	Bajo
	Robo	2	35	Crítico	Medio
	Ataque destructivo	2	35	Crítico	Medio

Tabla 125: *Cuadro de evaluación de riesgos para el activo UPS*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Equipamiento auxiliar					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
Equipo de climatización (valor del activo = 3)	Fuego (Desastres naturales)	2	15	Menor	Bajo
	Daños por agua (Desastres naturales)	2	15	Menor	Bajo
	Desastres naturales	2	15	Menor	Bajo
	Fuego (De origen industrial)	2	15	Menor	Bajo
	Daños por agua (De origen industrial)	2	15	Menor	Bajo
	Desastres industriales	3	15	Menor	Bajo
	Contaminación mecánica	3	9	Insignificante	Bajo
	Contaminación electromagnética	3	3	Insignificante	Bajo
	Avería de origen físico o lógico	2	9	Insignificante	Bajo
	Corte de suministro eléctrico	3	9	Insignificante	Bajo
	Interrupción de otros servicios y suministros esenciales	3	9	Insignificante	Bajo
	Emanaciones electromagnéticas	3	3	Insignificante	Bajo

	Errores de los usuarios	2	9	Insignificante	Bajo
	Errores del administrador	2	9	Insignificante	Bajo
	Errores de mantenimiento / actualización de equipos (hardware)	3	9	Insignificante	Bajo
	Pérdida de equipos	2	15	Menor	Bajo
	Manipulación de los equipos	2	6	Insignificante	Bajo
	Robo	2	15	Menor	Bajo
	Ataque destructivo	2	15	Menor	Bajo

Tabla 126: *Cuadro de evaluación de riesgos para el activo Equipo de climatización*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Equipamiento auxiliar					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
	Fuego (Desastres naturales)	2	15	Menor	Bajo
	Daños por agua (Desastres naturales)	2	15	Menor	Bajo

Mobiliario (valor del activo = 3)	Desastres naturales	2	15	Menor	Bajo
	Fuego (De origen industrial)	2	15	Menor	Bajo
	Daños por agua (De origen industrial)	2	15	Menor	Bajo
	Desastres industriales	2	15	Menor	Bajo
	Contaminación mecánica	3	6	Insignificante	Bajo
	Avería de origen físico o lógico	3	9	Insignificante	Bajo
	Errores de mantenimiento / actualización de equipos (hardware)	2	9	Insignificante	Bajo
	Pérdida de equipos	2	15	Menor	Bajo
	Uso no previsto	2	3	Insignificante	Bajo
	Acceso no autorizado	2	3	Insignificante	Bajo
	Manipulación de los equipos	2	3	Insignificante	Bajo
	Robo	2	15	Menor	Bajo
	Ataque destructivo	2	15	Menor	Bajo
	Ocupación enemiga	2	6	Insignificante	Bajo

Tabla 127: *Cuadro de evaluación de riesgos para el activo Mobiliario*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Equipamiento auxiliar					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
NVR (valor del activo = 9)	Fuego (Desastres naturales)	2	45	Catastrófico	Alto
	Daños por agua (Desastres naturales)	2	45	Catastrófico	Alto
	Desastres naturales	2	45	Catastrófico	Alto
	Fuego (De origen industrial)	2	45	Catastrófico	Alto
	Daños por agua (De origen industrial)	2	45	Catastrófico	Alto
	Desastres industriales	2	45	Catastrófico	Alto
	Contaminación mecánica	3	27	Medio	Medio
	Contaminación electromagnética	3	9	Insignificante	Bajo
	Avería de origen físico o lógico	2	36	Crítico	Medio
	Corte de suministro eléctrico	3	15	Menor	Bajo
	Condiciones inadecuadas de temperatura o humedad	2	9	Insignificante	Bajo
	Fallo de servicios de comunicaciones	3	18	Menor	Bajo

	Interrupción de otros servicios y suministros esenciales	3	18	Menor	Bajo
	Degradación de los soportes de almacenamiento de información	2	18	Menor	Bajo
	Emanaciones electromagnéticas	4	9	Insignificante	Medio
	Errores de administrador	2	18	Menor	Bajo
	Errores de mantenimiento / actualización de equipos (hardware)	3	27	Medio	Medio
	Pérdida de equipos	2	45	Catastrófico	Alto
	Manipulación de la configuración	2	36	Crítico	Medio
	Uso no previsto	2	9	Insignificante	Bajo
	Acceso no autorizado	2	9	Insignificante	Bajo
	Divulgación de información	2	9	Insignificante	Bajo
	Manipulación de los equipos	2	18	Menor	Bajo
	Robo	2	45	Catastrófico	Alto
	Ataque destructivo	2	45	Catastrófico	Alto

Tabla 128: *Cuadro de evaluación de riesgos para el activo NVR*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

Evaluación del riesgo para el tipo de activo Instalaciones

ACTIVO: Instalaciones					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
Oficina (valor del activo = 9)	Fuego (Desastres naturales)	2	45	Catastrófico	Alto
	Daños por agua (Desastres naturales)	2	45	Catastrófico	Alto
	Desastres naturales	2	45	Catastrófico	Alto
	Fuego (De origen industrial)	2	45	Catastrófico	Alto
	Daños por agua (De origen industrial)	2	18	Menor	Bajo
	Desastres industriales	2	45	Catastrófico	Alto
	Contaminación mecánica	2	9	Insignificante	Bajo
	Corte de suministro eléctrico	2	18	Menor	Bajo
	Errores de los usuarios	2	18	Menor	Bajo
	Errores del administrador	2	18	Menor	Bajo
	Uso no previsto	3	9	Insignificante	Bajo
	Acceso no autorizado	2	18	Menor	Bajo
	Ataque destructivo	2	45	Catastrófico	Alto

	Ocupación enemiga	2	45	Catastrófico	Alto
	Indisponibilidad del personal	2	18	Menor	Bajo

Tabla 129: *Cuadro de evaluación de riesgos para el activo Oficina*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

Evaluación del riesgo para el tipo de activo Personal

ACTIVO: Personal					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
	Fuego (Desastres naturales)	2	27	Medio	Medio
	Desastres naturales	2	27	Medio	Medio
	Fuego (De origen industrial)	2	27	Medio	Medio
	Deficiencias en la organización	3	27	Medio	Medio
	Escapes de información	2	27	Medio	Medio

Jefe de área (valor del activo = 9)	Indisponibilidad del personal (Errores y fallos no intencionados)	3	36	Crítico	Alto
	Repudio	2	9	Insignificante	Bajo
	Indisponibilidad del personal (Ataques intencionados)	2	36	Crítico	Medio
	Extorsión	1	27	Medio	Bajo
	Ingeniería social (picaresca)	1	27	Medio	Bajo

Tabla 130: *Cuadro de evaluación de riesgos para el activo Jefe de área*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Personal					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
	Fuego (Desastres naturales)	2	24	Medio	Medio
	Desastres naturales	2	24	Medio	Medio
	Fuego (De origen industrial)	2	24	Medio	Medio

P.Desarrolladores / Programadores (valor del activo = 8)	Deficiencias en la organización	3	24	Medio	Medio
	Escapes de información	2	24	Medio	Medio
	Indisponibilidad del personal (Errores y fallos no intencionados)	3	32	Crítico	Alto
	Repudio	2	8	Insignificante	Bajo
	Indisponibilidad del personal (Ataques intencionados)	2	32	Crítico	Medio
	Extorsión	1	24	Medio	Bajo
	Ingeniería social (picaresca)	1	24	Medio	Bajo

Tabla 131: *Cuadro de evaluación de riesgos para el activo P. Desarrolladores / Programadores*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Personal					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
P.Soporte técnico (valor del activo = 5)	Fuego (Desastres naturales)	2	15	Menor	Bajo
	Desastres naturales	2	15	Menor	Bajo
	Fuego (De origen industrial)	2	15	Menor	Bajo
	Deficiencias en la organización	3	15	Menor	Bajo
	Indisponibilidad del personal (Errores y fallos no intencionados)	3	20	Medio	Medio
	Repudio	2	5	Insignificante	Bajo
	Indisponibilidad del personal (Ataques intencionados)	2	20	Medio	Medio
	Extorsión	1	15	Menor	Bajo
	Ingeniería social (picaresca)	2	20	Medio	Medio

Tabla 132: *Cuadro de evaluación de riesgos para el activo P.Soporte técnico*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

ACTIVO: Personal					
Activos	**Amenazas**	**Probabilidad**	**Valor total del impacto (valor del activo x degradación)**	**Impacto potencial**	**Estimación del riesgo potencial**
P.Redes (valor del activo = 6)	Fuego (Desastres naturales)	2	18	Menor	Bajo
	Desastres naturales	2	18	Menor	Bajo
	Fuego (De origen industrial)	2	18	Menor	Bajo
	Deficiencias en la organización	3	18	Menor	Bajo
	Indisponibilidad del personal	3	24	Medio	Medio
	Repudio	2	6	Insignificante	Bajo
	Indisponibilidad del personal (Ataques intencionados)	2	24	Medio	Medio
	Extorsión	1	18	Menor	Bajo
	Ingeniería social (picaresca)	2	18	Menor	Bajo

Tabla 133: *Cuadro de evaluación de riesgos para el activo P.Redes*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

Para la obtención de los riesgos residuales se mostrará en el Paso 3. Tratamiento del riesgo de seguridad de la información

PASO 3. Tratamiento del riesgo de seguridad de la información

(Capítulo 9, libro ISO/IEC 27005:2018)

En este paso se seleccionará unas de las 4 opciones para definir el plan de tratamiento del riesgo que son los siguientes:

1. **Modificación del riesgo**

   Llamada también mitigación del riesgo que implementa controles que buscan reducir los riesgos a un nivel aceptable por la organización. Los controles pueden proveer uno o más de los siguientes tipos de protección: corrección, eliminación, prevención, minimización del impacto, disuasión, detección, recuperación, seguimiento (monitoring) y concientización.

2. **Retención del riesgo**

   Para la retención del riesgo se tomará en cuenta el nivel del riesgo. Si el nivel del riesgo satisface el criterio de aceptación de riesgos no hay necesidad de implementar controles adicionales y el riesgo puede ser retenido.

3. **Evitar el riesgo**

   Cuando los riesgos identificados son considerados muy altos, o los costos de implementar otras opciones de tratamiento del riesgo exceden los beneficios, se puede tomar la decisión de evitar el riesgo completamente, retirándose de una actividad planeada o existente o de un conjunto de actividades, o cambiando las condiciones sobre las cuales la actividad es operada.

4. **Compartir el riesgo**

   El riesgo compartido exige una decisión de compartir ciertos riesgos con las partes externas. Compartir un riesgo puede crear nuevos riesgos o modificar los riesgos existentes identificados. Por lo tanto, puede ser necesario el tratamiento adicional de riesgos.

El siguiente cuadro nos muestra los tipos de activo con sus amenazas y vulnerabilidades en específico, implementando salvaguardias para cada tipo de amenaza teniendo como resultado riesgos residuales. También se implementó planes de acción que cubren dichas vulnerabilidades teniendo como resultado riesgos residuales después de la ejecución de dichos planes de acción.

Tipo de activos	Activos	Nivel del activo	Amenaza	Vulnerabilidad	Estimación del riesgo potencial	Tratamiento del riesgo	Salvaguarda	Descripción del salvaguarda	Tipo de protección del salvaguarda	Estimación del riesgo residual con el salvaguarda	Plan de acción	Estimación del riesgo residual esperado después de la ejecución del plan de acción
Datos /información	Base de datos de la página web de la DDCC	Alto	Errores de los usuarios	Falta de política de uso de aplicaciones de mensajería instantánea Falta de procedimientos para manejo de información clasificada. Falta de proceso disciplinario definido en caso de incidente de seguridad de la información.	Alto	Modificación del riesgo	Protección de la Información	Mantener entornos de desarrollo, pruebas y producción separados donde los gestores de BDs deberán realizar cambios y pruebas en un entorno controlado antes de aplicarlos a la base de datos de producción.	Prevención	Medio	Crear políticas de uso de aplicaciones de mensajería instantánea. Crear políticas para el manejo seguro de información clasificada. Crear políticas disciplinarias para incidentes de seguridad de la información.	Bajo
			Errores del administrador		Medio	Modificación del riesgo	Protección de la Información	Establecer entornos de desarrollo, pruebas y producción separados donde los gestores de BDs deberán realizar cambios y pruebas en un entorno controlado, realizando supervisiones constantes sobre dichos entornos de desarrollo.	Prevención	Bajo		Bajo
			Escapes de información		Medio	Modificación del riesgo	Protección de la Información	Asegurarse de que el personal encargado de la base de datos de la página web de la DDCC reciba capacitación continua y esté consciente de los riesgos vinculados al compartir información parcial o completa.	Concienciación	Bajo		Bajo
			Alteración accidental de la información		Medio	Modificación del riesgo	Protección de la Información	Tener configurada la base de datos para solicitar confirmación antes de realizar cambios significativos. Agregar pasos adicionales como solicitar una contraseña o confirmación explícita, para evitar modificaciónes accidentales.	Disuasión	Bajo		Bajo
			Destrucción de información (Errores y fallos no intencionados)		Alto	Modificación del riesgo	Protección de la Información	Establecer en la configuración de la base de datos de manera que sea necesario confirmar antes de eliminar registros significativos. Introduce medidas adicionales, como solicitar una contraseña o una confirmación adicional, con el objetivo de disminuir la probabilidad de eliminaciones involuntarias.	Disuasión	Medio		Bajo
			Fugas de información		Medio	Modificación del riesgo	Protección de la Información	Asegurarse de que el personal encargado de la base de datos de la página web de la DDCC reciba capacitación continua y esté consciente de los riesgos vinculados al compartir información parcial o completa.	Concienciación	Bajo		Bajo
			Abuso de privilegios de acceso		Alto	Modificación del riesgo	Protección de la Información	Implementar un sistema de acceso basado en roles para garantizar que los usuarios tengan solo los privilegios necesarios para realizar sus tareas y así limitar el acceso a funciones de modificación solo a personal autorizado.	Prevención	Medio		Bajo
			Modificación deliberada de la información		Alto	Modificación del riesgo	Protección de la Información	Tener configurada la base de datos para solicitar confirmación antes de realizar cambios, agregando pasos adicionales como solicitar una contraseña o confirmación explícita para evitar modificaciónes no autorizadas.	Disuasión	Medio		Bajo
			Destrucción de información (Ataques intencionados)		Alto	Modificación del riesgo	Protección de la Información	Establecer en la configuración de la base de datos de manera que sea necesario confirmar antes de eliminar registros significativos, introduciendo medidas adicionales como solicitar una contraseña o una confirmación adicional, con el objetivo de mitigar la destrucción de la información.	Disuasión	Medio		Bajo
			Divulgación de información		Alto	Modificación del riesgo	Protección de la Información	Implementar un sistema de acceso basado en roles para garantizar que los usuarios tengan solo los privilegios necesarios para realizar sus tareas y así limitar el acceso a funciones de modificación solo a personal autorizado.	Prevención	Medio		Bajo
Datos /información	Documentos digitales	Medio	Escapes de información	Falta de política de uso de aplicaciones de mensajería instantánea Falta de procedimientos para manejo de información clasificada. Falta de proceso disciplinario definido en caso de incidente de seguridad de la información.	Medio	Modificación del riesgo	Protección de la Información	Mantener concientizado al personal que maneja los documentos digitales sobre los riesgos asociados al compartir información de manera imprudente.	Concienciación	Bajo	Crear políticas de uso de aplicaciones de mensajería instantánea. Crear políticas para el manejo seguro de información clasificada. Crear políticas disciplinarias para incidentes de seguridad de la información.	Bajo
			Destrucción de información (Errores y fallos no intencionados)	Falta de procedimientos para manejo de información clasificada Falta de proceso disciplinario definido en caso de incidente de seguridad de la información	Medio	Modificación del riesgo	Copias de seguridad de los datos (backup)	Fomentar al personal que maneja los documentos digitales a crear copias de respaldo de los archivos más importantes para evitar la eliminación del activo.	Recuperación	Bajo	Crear políticas para el manejo seguro de información clasificada. Crear políticas disciplinarias para incidentes de seguridad de la información.	Bajo
			Fugas de información	Falta de política de uso de aplicaciones de mensajería instantánea Falta de procedimientos para manejo de información clasificada. Falta de proceso disciplinario definido en caso de incidente de seguridad de la información.	Medio	Modificación del riesgo	Protección de la Información	Proporcionar formación al personal sobre la importancia de la seguridad de la información y mejores prácticas.	Concienciación	Bajo	Crear políticas de uso de aplicaciones de mensajería instantánea. Crear políticas para el manejo seguro de información clasificada. Crear políticas disciplinarias para incidentes de seguridad de la información.	Bajo
			Modificación deliberada de la información	Falta de procedimientos para manejo de información clasificada Falta de proceso disciplinario definido en caso de incidente de seguridad de la información	Medio	Modificación del riesgo	Asegurarniento de la integridad	Establecer controles de acceso adecuados a los medios de almacenamiento donde se encuentran dichos documentos	Disuasión	Bajo	Crear políticas para el manejo seguro de información clasificada. Crear políticas disciplinarias para incidentes de seguridad de la información.	Bajo
			Destrucción de información (Ataques intencionados)		Medio	Modificación del riesgo	Copias de seguridad de los datos (backup) Asegurarniento de la integridad	Motivar al personal encargado de documentos digitales a realizar copias de respaldo de los archivos críticos como medida preventiva contra la pérdida del activo, al mismo tiempo que se implementan controles de acceso efectivos en los dispositivos de almacenamiento que resguardan dichos documentos.	Recuperación	Bajo		Bajo
Claves criptográficas	Contraseña de acceso a la base de datos de la página web de la DDCC	Alto	Errores de los usuarios	Descuido en la gestión de contraseñas Falta de proceso disciplinario definido en caso de incidente de seguridad de la información	Alto	Modificación del riesgo	Gestión de claves criptográficas	Implementar filtros antiphishing en el servidor de correo electrónico para detectar y bloquear mensajes de phishing antes de llegar a las bandejas de entrada del personal, así mismo fomentar el uso de gestores de contraseñas seguras y confiables.	Prevención	Medio	Creación de políticas para una adecuada gestión de contraseñas. Crear políticas disciplinarias para incidentes de seguridad de la información.	Bajo
			Errores del administrador		Alto	Modificación del riesgo	Gestión de claves criptográficas	Crear contraseñas seguras que incluyan combinaciones de letras, números y carácteres especiales, así como la importancia de cambiarlas regularmente.	Prevención	Medio		Bajo
			Escapes de información		Medio	Modificación del riesgo	Gestión de claves criptográficas	Tener control de acceso basado en roles que aseguren que solo personas autorizadas tengan potestad sobre dichas contraseñas	Prevención	Bajo		Bajo
			Alteración accidental de la información		Medio	Modificación del riesgo	Gestión de claves criptográficas	Fomentar el uso de gestores de contraseñas seguras y confiables para controlar cambios	Prevención	Bajo		Bajo
			Destrucción de información (Errores y fallos no intencionados)		Medio	Modificación del riesgo	Gestión de claves criptográficas	Fomentar el uso de gestores de contraseñas seguras y confiables para controlar cambios	Prevención	Bajo		Bajo
			Fugas de información		Medio	Modificación del riesgo	Gestión de claves criptográficas	Proporcionar formación al personal sobre la importancia de la seguridad de la información y mejores prácticas en contraseñas.	Concienciación	Bajo		Bajo
			Abuso de privilegios de acceso		Medio	Modificación del riesgo	Gestión de claves criptográficas	Establecer revisiones periódicas de los privilegios de acceso a las contraseñas para tener asegurado el correcto uso de dichos datos.	Prevención	Bajo		Bajo
			Acceso no autorizado	Descuido en la gestión de contraseñas	Alto	Modificación del riesgo	Gestión de claves criptográficas	Tener control de acceso basado en roles que aseguren que solo personas autorizadas tengan potestad sobre dichas contraseñas	Prevención	Medio	Creación de políticas para una adecuada gestión de contraseñas.	Bajo
			Modificación deliberada de la información	Descuido en la gestión de contraseñas Falta de proceso disciplinario definido en caso de incidente de seguridad de la información	Medio	Modificación del riesgo	Gestión de claves criptográficas	Fomentar el uso de gestores de contraseñas seguras y confiables para controlar cambios y tener control de acceso basado en roles que aseguren que solo personas autorizadas tengan potestad sobre dichas contraseñas.	Prevención	Bajo	Creación de políticas para una adecuada gestión de contraseñas. Crear políticas disciplinarias para incidentes de seguridad de la información.	Bajo
			Destrucción de información (Ataques intencionados)		Medio	Modificación del riesgo	Gestión de claves criptográficas	Fomentar el uso de gestores de contraseñas seguras y confiables para controlar cambios y tener control de acceso basado en roles que aseguren que solo personas autorizadas tengan potestad sobre dichas contraseñas.	Prevención	Bajo		Bajo
Claves criptográficas	Contraseña de acceso al NVR	Alto	Errores del administrador	Descuido en la gestión de contraseñas Falta de proceso disciplinario definido en caso de incidente de seguridad de la información	Alto	Modificación del riesgo	Gestión de claves criptográficas	Crear contraseñas seguras que incluyan combinaciones de letras, números y carácteres especiales, así como la importancia de cambiarlas regularmente.	Prevención	Medio	Creación de políticas para una adecuada gestión de contraseñas. Crear políticas disciplinarias para incidentes de seguridad de la información.	Bajo
			Escapes de información		Medio	Modificación del riesgo	Gestión de claves criptográficas	Limitar el acceso a la contraseña del NVR a un solo personal bajo responsabilidad del activo	Prevención	Bajo		Bajo
			Fugas de información		Medio	Modificación del riesgo	Gestión de claves criptográficas	Mantener total discreción al momento de usar la contraseña	Prevención	Bajo		Bajo
			Acceso no autorizado	Descuido en la gestión de contraseñas	Medio	Modificación del riesgo	Gestión de claves criptográficas	Limitar el acceso a la contraseña del NVR a un solo personal	Prevención	Bajo	Creación de políticas para una adecuada gestión de contraseñas.	Bajo
			Errores de los usuarios		Alto	Modificación del riesgo	Gestión de claves criptográficas	Implementar filtros antiphishing en el servidor de correo electrónico para detectar y bloquear mensajes de phishing antes de llegar a las bandejas de entrada del personal, así mismo fomentar el uso de gestores de contraseñas seguras y confiables.	Prevención	Medio		Bajo

Claves criptográficas	Contraseña de acceso al router	Alto	Errores del administrador	Descuido en la gestión de contraseñas Falta de proceso disciplinario definido en caso de incidente de seguridad de la información	Alto	Modificación del riesgo	Gestión de claves criptográficas	Crear contraseñas seguras que incluyan combinaciones de letras, números y carácteres especiales, así como la importancia de cambiarlas regularmente.	Prevención	Medio	Creación de políticas para una adecuada gestión de contraseñas. Crear políticas disciplinarias para incidentes de seguridad de la información.	Bajo
			Escapes de información		Medio	Modificación del riesgo	Gestión de claves criptográficas	Tener control de acceso basado en roles que aseguren que solo personas autorizadas tengan potestad sobre dichas contraseñas	Prevención	Bajo		Bajo
			Alteración accidental de la información		Medio	Modificación del riesgo	Gestión de claves criptográficas	Fomentar el uso de gestores de contraseñas seguras y confiables para controlar cambios	Prevención	Bajo		Bajo
			Destrucción de información (Errores y fallos no intencionados)		Medio	Modificación del riesgo	Gestión de claves criptográficas	Fomentar el uso de gestores de contraseñas seguras y confiables para controlar cambios	Prevención	Bajo		Bajo
			Fugas de información		Medio	Modificación del riesgo	Gestión de claves criptográficas	Proporcionar formación al personal sobre la importancia de la seguridad de la información y mejores prácticas en contraseñas.	Concienciación	Bajo		Bajo
			Abuso de privilegios de acceso		Medio	Modificación del riesgo	Gestión de claves criptográficas	Establecer revisiones periódicas de los privilegios de acceso a las contraseñas para tener asegurado el correcto uso de dichos datos.	Prevención	Bajo		Bajo
			Acceso no autorizado	Descuido en la gestión de contraseñas	Medio	Modificación del riesgo	Gestión de claves criptográficas	Tener control de acceso basado en roles que aseguren que solo personas autorizadas tengan potestad sobre dichas contraseñas	Prevención	Bajo	Creación de políticas para una adecuada gestión de contraseñas.	Bajo
			Modificación deliberada de la información	Descuido en la gestión de contraseñas Falta de proceso disciplinario definido en caso de incidente de seguridad de la información	Alto	Modificación del riesgo	Gestión de claves criptográficas	Fomentar el uso de gestores de contraseñas seguras y confiables para controlar cambios y tener control de acceso basado en roles que aseguren que solo personas autorizadas tengan potestad sobre dichas contraseñas.	Prevención	Medio	Creación de políticas para una adecuada gestión de contraseñas. Crear políticas disciplinarias para incidentes de seguridad de la información.	Bajo
			Destrucción de información (Ataques intencionados)		Alto	Modificación del riesgo	Gestión de claves criptográficas	Fomentar el uso de gestores de contraseñas seguras y confiables para controlar cambios y tener control de acceso basado en roles que aseguren que solo personas autorizadas tengan potestad sobre dichas contraseñas.	Prevención	Medio		Bajo
Servicios	Página Help Desk	Alto	Errores del administrador	Falta o insuficiente Acuerdo de Nivel de Servicio. Falta de actualizaciones de software	Medio	Modificación del riesgo	Gestión de cambios (mejoras y sustituciones)	Solicitar actualizaciones a la empresa desarrolladora para mitigar fallas en el activo.	Corrección	Bajo	Crear políticas sobre la contratación de software a terceros.	Bajo
			Destrucción de información (Errores y fallos no intencionados)	Falta de proceso disciplinario definido en caso de incidente de seguridad de la información	Medio	Modificación del riesgo	Protección de los Servicios	Realizar revisiones periodicas de la información generada en la página Help Desk y limitar el acceso total de la página a un solo personal bajo responsabilidad del activo	Prevención	Bajo	Crear políticas disciplinarias para incidentes de seguridad de la información.	Bajo
			Destrucción de información (Ataques intencionados)		Medio	Modificación del riesgo	Protección de los Servicios	Limitar el acceso total de la página Help Desk a un solo personal bajo responsabilidad del activo	Prevención	Bajo		Bajo
Servicios	Páginas web institucionales	Alto	Errores del administrador	Falta o insuficiente Acuerdo de Nivel de Servicio. Falta de actualizaciones de software Falta en producir reportes de gestión.	Alto	Modificación del riesgo	Gestión de cambios (mejoras y sustituciones)	Tener procedimientos formales para la realización de pruebas rigurosas antes y después de implementar cambios en la página web.	Prevención	Medio	Crear políticas de desarrollo, mantenimiento de software Realizar un constante reportes de gestión detallados sobre el funcionamiento de las paginas	Bajo
			Errores de [re-]encaminamiento	Falta o insuficiente Acuerdo de Nivel de Servicio. Falta de actualizaciones de software	Medio	Modificación del riesgo	Gestión de cambios (mejoras y sustituciones)	Tener procedimientos formales para la realización de pruebas rigurosas antes y después de implementar cambios en la página web.	Prevención	Bajo	Crear políticas de desarrollo, mantenimiento de software	Bajo
			Errores de secuencia		Medio	Modificación del riesgo	Gestión de cambios (mejoras y sustituciones)	Tener procedimientos formales para la realización de pruebas rigurosas antes y después de implementar cambios en la página web.	Prevención	Bajo	Crear políticas de desarrollo, mantenimiento de software	Bajo
			Escapes de información	Falta de política de uso de aplicaciones de mensajería instantánea	Medio	Modificación del riesgo	Protección de los Servicios	Mantener concientizado al personal que maneja información generada por las páginas sobre los riesgos asociados al compartir información y las consecuencias para la institución y como para el individuo.	Concienciación	Bajo	Crear políticas de uso de aplicaciones de mensajería instantánea.	Bajo
			Alteración accidental de la información	Falta de proceso disciplinario definido en caso de incidente de seguridad de la información	Medio	Modificación del riesgo	Gestión de cambios (mejoras y sustituciones)	Tener procedimientos formales para la realización de pruebas rigurosas antes y después de implementar cambios en la página web.	Prevención	Bajo	Crear políticas disciplinarias para incidentes de seguridad de la información.	Bajo
			Destrucción de información (Errores y fallos no intencionados)		Alto	Modificación del riesgo	Protección de servicios y aplicaciones web	Tener una copia de seguridad del proyecto en desarrollo.	Prevención	Medio		Bajo
			Fugas de información	Falta de política de uso de aplicaciones de mensajería instantánea	Medio	Modificación del riesgo	Protección de los Servicios	Proporcionar formación al personal sobre la importancia de la seguridad de la información y mejores prácticas en páginas web institucionales.	Concienciación	Bajo	Crear políticas de uso de aplicaciones de mensajería instantánea.	Bajo
			Modificación deliberada de la información	Falta de proceso disciplinario definido en caso de incidente de seguridad de la información	Alto	Modificación del riesgo	Gestión de cambios (mejoras y sustituciones)	Utiliza sistemas de control de versiones, como Git, para rastrear y controlar cambios en el código fuente de la página web Implementa un registro de cambios accesible y monitorizable para documentar cualquier alteración en el contenido o funcionalidades de la página web. Restringe el acceso al código y a la infraestructura de la página web solo a personal autorizado y asegúrate de mantener políticas de acceso basadas en roles.	Corrección / Monitorización	Medio	Crear políticas disciplinarias para incidentes de seguridad de la información.	Bajo
			Destrucción de información (Ataques intencionados)		Alto	Modificación del riesgo	Gestión de cambios (mejoras y sustituciones)	Utiliza sistemas de control de versiones, como Git, para rastrear y controlar cambios en el código fuente de la página web Implementa un registro de cambios accesible y monitorizable para documentar cualquier alteración en el contenido o funcionalidades de la página web. Restringe el acceso al código y a la infraestructura de la página web solo a personal autorizado y asegúrate de mantener políticas de acceso basadas en roles.	Corrección / Monitorización	Medio		Bajo
			Denegación de servicio	Malware y software malicioso Falta de mecanismos de seguimiento establecidos para brechas de seguridad (firewall de mayor capacidad)	Medio	Modificación del riesgo	Protección de servicios y aplicaciones web	Configurar reglas dentro del firewall y filtros para identificar y bloquear tráfico malicioso durante un ataque.	Detección	Bajo	Asegurarse de que todos los sistemas cuenten con soluciones antivirus actualizadas y configuradas para realizar análisis periódicos. Adquirir e implementar un firewall de mayor capacidad para gestionar el tráfico de red y garantizar una protección efectiva contra amenazas externas.	Bajo
Software	Antivirus	Medio	Destrucción de información (Errores y fallos no intencionados)	Falta de copias de respaldo	Medio	Modificación del riesgo	Copias de seguridad (backup)	Tener copia de seguridad del instalador debidamente resguardada	Recuperación	Bajo	Realizar copias de respaldo de los activadores e instaladores adquiridos.	Bajo
			Destrucción de información (Ataques intencionados)		Alto	Modificación del riesgo	Copias de seguridad (backup)	Tener copia de seguridad del instalador debidamente resguardada	Recuperación	Medio		Bajo
			Manipulación de programas	Falta o insuficiente analisis de la configuración, actualización del antivirus	Medio	Modificación del riesgo	Se aplican perfiles de seguridad	Establecer un control de acceso estricto para los ajustes y funciones del antivirus, permitiendo que solo el personal autorizado pueda realizar cambios en la configuración.	Prevención	Bajo	Evaluar la configuración predeterminada de las funciones del antivirus para asegurarse de que esté optimizada para proporcionar una protección efectiva y minimizar las vulnerabilidades.	Bajo
Software	Sistemas Operativos	Medio	Avería de origen físico o lógico	Malware y software malicioso	Medio	Modificación del riesgo	Cambios (actualizaciones y mantenimiento)	Realizar un mantenimiento al sistema operativo	Corrección	Bajo	Asegurarse de que todos los sistemas cuenten con soluciones antivirus actualizadas y configuradas para realizar análisis periódicos.	Bajo
			Errores de los usuarios	Falta de conciencia de seguridad	Medio	Modificación del riesgo	Protección de las Aplicaciones Informáticas	Capacitar a los trabajadores sobre las mejores prácticas al realizar actualizaciones, enfatizando la necesidad de permitir que el proceso se complete antes de apagar la máquina.	Concienciación	Bajo	Crear políticas sobre el manejo seguro de equipos informáticos (hardware, software)	Bajo
			Difusión de software dañino (Errores y fallos no intencionados)	Malware y software malicioso Descarga y uso no controlado de software	Medio	Modificación del riesgo	Protección de las Aplicaciones Informáticas	Instalar y mantener actualizado un software antivirus y antimalware confiable en todos los sistemas operativos.	Detección	Bajo	Asegurarse de que todos los sistemas cuenten con soluciones antivirus actualizadas y configuradas para realizar análisis periódicos. Crear políticas sobre la descarga no controlada de software.	Bajo
			Difusión de software dañino (Ataques intencionados)		Medio	Modificación del riesgo	Protección de las Aplicaciones Informáticas	Instalar y mantener actualizado un software antivirus y antimalware confiable en todos los sistemas operativos.	Detección	Bajo		Bajo
			Modificación deliberada de la información		Medio	Modificación del riesgo	Protección de las Aplicaciones Informáticas	Implementar firmas digitales o checksums para los archivos del sistema, permitiendo la detección de cualquier modificación no autorizada.	Detección	Bajo		Bajo
			Destrucción de información (Ataques intencionados)		Medio	Modificación del riesgo	Copias de seguridad (backup)	Contar con un plan de recuperación del sistema que incluya procedimientos claros para restaurar el sistema operativo y los datos desde las copias de seguridad.	Recuperación	Bajo		Bajo
Software	Ofimática	Medio	Avería de origen físico o lógico	Malware y software malicioso Descarga y uso no controlado de software	Medio	Modificación del riesgo	Cambios (actualizaciones y mantenimiento)	Realizar un mantenimiento, actualización del paquete de ofimática	Corrección	Bajo	Asegurarse de que todos los sistemas cuenten con soluciones antivirus actualizadas y configuradas para realizar análisis periódicos. Crear políticas sobre la descarga no controlada de software.	Bajo
			Fuego (Desastres naturales)	Falta de planes de continuidad Falta de procedimientos de identificación y	Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo	Creación de planes de continuidad basados en sustitucion inmediata de equipos. Realizar procesos de	Bajo
			Daños por agua (Desastres naturales)		Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo		Bajo
			Desastres naturales		Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo		Bajo

				Falta de procedimientos de identificación y evaluación de riesgos								Realizar procesos de identificación y evaluación de riesgos potenciales que puedan afectar al activo.	
			Fuego (De origen industrial)		Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo			Bajo
			Daños por agua (De origen industrial)		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio			Bajo
Hardware	Computadoras desktops	Medio	Desastres industriales		Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo			Bajo
			Avería de origen físico o lógico	Uso incorrecto de software y hardware	Medio	Modificación del riesgo	Cambios (actualizaciones y mantenimiento)	Realizar un mantenimiento al activo dañado.	Corrección	Bajo	Crear políticas sobre el manejo seguro de equipos informáticos (hardware, software)		Bajo
			Errores de mantenimiento / actualización de equipos (hardware)	Falta de esquemas periódicos de reemplazo Mantenimiento insuficiente / instalación defectuosa de medios de almacenamiento	Medio	Modificación del riesgo	Cambios (actualizaciones y mantenimiento)	Realizar un mantenimiento al activo dañado.	Corrección	Bajo	Creación de planes de mantenimiento, actualización periodica de equipos.		Bajo
			Caída del sistema por agotamiento de recursos	Falta de esquemas periódicos de reemplazo	Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Realizar una evaluación periódica de los recursos del sistema, incluyendo la memoria RAM, el procesador y el almacenamiento para así prever la caida por agotamiento de recursos.	Monitorización	Bajo	Creación de planes de mantenimiento, actualización periodica de equipos.		Bajo
			Fuego (Desastres naturales)		Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo			Bajo
			Daños por agua (Desastres naturales)		Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo			Bajo
			Desastres naturales	Falta de planes de continuidad Falta de procedimientos de identificación y evaluación de riesgos	Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo	Creación de planes de continuidad basados en sustitucion inmediata de equipos. Realizar procesos de identificación y evaluación de riesgos potenciales que puedan afectar al activo.		Bajo
			Fuego (De origen industrial)		Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo			Bajo
			Daños por agua (De origen industrial)		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio			Bajo
Hardware	Laptops	Medio	Desastres industriales		Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo			Bajo
			Avería de origen físico o lógico	Uso incorrecto de software y hardware	Medio	Modificación del riesgo	Cambios (actualizaciones y mantenimiento)	Realizar un mantenimiento al activo dañado.	Corrección	Bajo	Crear políticas sobre el manejo seguro de equipos informáticos (hardware, software)		Bajo
			Errores de mantenimiento / actualización de equipos (hardware)		Medio	Modificación del riesgo	Cambios (actualizaciones y mantenimiento)	Realizar un mantenimiento al activo dañado.	Corrección	Bajo			Bajo
			Caída del sistema por agotamiento de recursos	Falta de esquemas periódicos de reemplazo	Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Realizar una evaluación periódica de los recursos del sistema, incluyendo la memoria RAM, el procesador y el almacenamiento para así prever la caida por agotamiento de recursos.	Monitorización	Bajo	Creación de planes de mantenimiento, actualización periodica de equipos.		Bajo
			Pérdida de equipos		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio			Bajo
			Robo	Falta de política formal sobre uso de computadoras móviles	Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio	Crear políticas sobre el manejo seguro de equipos informáticos (hardware, software)		Bajo
			Fuego (Desastres naturales)		Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo			Bajo
			Daños por agua (Desastres naturales)		Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo			Bajo
			Desastres naturales	Falta de planes de continuidad Falta de procedimientos de identificación y evaluación de riesgos	Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo	Creación de planes de continuidad basados en sustitucion inmediata de equipos. Realizar procesos de identificación y evaluación de riesgos potenciales que puedan afectar al activo.		Bajo
			Fuego (De origen industrial)		Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo			Bajo
			Daños por agua (De origen industrial)		Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo			Bajo
Hardware	Equipos de reprografía	Medio	Desastres industriales		Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo			Bajo
			Caída del sistema por agotamiento de recursos	Falta de esquemas periódicos de reemplazo	Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Realizar una evaluación periódica de los recursos como tóner , rodillos para así prever la caida por agotamiento de recursos.	Monitorización	Bajo	Creación de planes de mantenimiento, actualización periodica de equipos.		Bajo
			Fuego (Desastres naturales)		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio			Bajo
			Daños por agua (Desastres naturales)		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio			Bajo
			Desastres naturales	Falta de planes de continuidad Falta de procedimientos de identificación y evaluación de riesgos	Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio	Creación de planes de continuidad basados en sustitucion inmediata de equipos. Realizar procesos de identificación y evaluación de riesgos potenciales que puedan afectar al activo.		Bajo
			Fuego (De origen industrial)		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio			Bajo
			Daños por agua (De origen industrial)		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio			Bajo
Hardware	Firewall	Alto	Desastres industriales		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio			Bajo
			Contaminación mecánica	Mantenimiento insuficiente / instalación defectuosa de medios de almacenamiento	Medio	Modificación del riesgo	Cambios (actualizaciones y mantenimiento)	Realizar un mantenimiento al activo dañado.	Corrección	Bajo	Crear políticas sobre el manejo seguro de equipos informáticos (hardware, software)		Bajo
			Errores del administrador	Uso incorrecto de software y hardware	Medio	Modificación del riesgo	Protección de los Equipos Informáticos	Establece procesos formales de revisión periódica de las reglas y configuraciones del firewall.	Monitorización	Bajo	Crear políticas sobre el manejo seguro de equipos informáticos (hardware, software)		Bajo
			Caída del sistema por agotamiento de recursos	Falta de esquemas periódicos de reemplazo	Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Realizar una evaluación periódica de los recursos del sistema, incluyendo la memoria RAM, el procesador para así prever la caida por agotamiento de recursos.	Monitorización	Bajo	Creación de planes de mantenimiento, actualización periodica de equipos.		Bajo
			Denegación de servicio	Malware y software malicioso	Medio	Modificación del riesgo	Se aplican perfiles de seguridad	Configurar reglas de filtrado y límites de tasa en el firewall para detectar y bloquear patrones de tráfico malicioso asociados con ataques de saturación.	Corrección	Bajo	Creación de planes de continuidad basados en sustitucion inmediata de equipos.		Bajo
			Fuego (Desastres naturales)		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio			Bajo
			Daños por agua (Desastres naturales)		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio			Bajo
			Desastres naturales	Falta de planes de continuidad Falta de procedimientos de identificación y evaluación de riesgos	Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio	Creación de planes de continuidad basados en sustitucion inmediata de equipos. Realizar procesos de identificación y evaluación de riesgos potenciales que puedan afectar al activo.		Bajo
			Fuego (De origen industrial)		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio			Bajo
			Daños por agua (De origen industrial)		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio			Bajo
Hardware	Router	Alto	Desastres industriales		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio			Bajo
			Caída del sistema por agotamiento de recursos	Falta de esquemas periódicos de reemplazo	Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Configurar límites de tasa para el tráfico de entrada y salida en el router para evitar sobrecargas repentinas.	Corrección	Bajo	Creación de planes de mantenimiento, actualización periodica de equipos.		Bajo
			Denegación de servicio	Malware y software malicioso	Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Configurar límites de tasa para el tráfico de entrada y salida en el router para evitar sobrecargas repentinas.	Corrección	Bajo	Creación de planes de continuidad basados en sustitucion inmediata de equipos.		Bajo
			Errores de mantenimiento / actualización de equipos (hardware)		Medio	Modificación del riesgo	Cambios (actualizaciones y mantenimiento)	Mantenimiento periodico del sistema del cableado estructurado	Corrección	Bajo			Bajo
Redes de comunicaciones	Internet	Alto	Caída del sistema por agotamiento de recursos	Falta de esquemas periódicos de reemplazo Pobre conjunto de cableado	Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Implementar sistemas de gestión de ancho de banda para distribuir y asignar recursos equitativamente entre los usuarios.	Corrección	Bajo	Creación de planes de mantenimiento, actualización periodica de equipos.		Bajo
			Errores de mantenimiento / actualización de equipos (hardware)		Medio	Modificación del riesgo	Cambios (actualizaciones y mantenimiento)	Mantenimiento periodico del sistema del cableado estructurado	Corrección	Bajo			Bajo
Redes de comunicaciones	Internet de respaldo	Alto	Caída del sistema por agotamiento de recursos	Falta de esquemas periódicos de reemplazo Pobre conjunto de cableado	Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Implementar sistemas de gestión de ancho de banda para distribuir y asignar recursos equitativamente entre los usuarios.	Corrección	Bajo	Creación de planes de mantenimiento, actualización periodica de equipos.		Bajo
			Fuego (Desastres Naturales)		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio			Bajo

Soportes de información	Servidores	Alto	Daños por agua (Desastres Naturales)	Falta de planes de continuidad Falta de procedimientos de identificación y evaluación de riesgos	Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio	Creación de planes de continuidad basados en sustitucion inmediata de equipos. Realizar procesos de identificación y evaluación de riesgos potenciales que puedan afectar al activo.	Bajo
			Desastres naturales		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio		Bajo
			Fuego (De Origen Industrial)		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio		Bajo
			Daños por agua (De Origen Industrial)		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio		Bajo
			Desastres industriales		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio		Bajo
			Contaminación electromagnética	Falta de procedimiento de seguimiento de instalaciones de procesamiento de la información	Medio	Modificación del riesgo	Protección de los Soportes de Información	Realizar inspecciones regulares para identificar y corregir posibles fuentes de contaminación electromagnética.	Prevención	Bajo	Crear políticas sobre el manejo seguro de equipos informaticos (hardware, software).	Bajo
Soportes de información	Repositorios de código fuente		Errores del administrador	Falta de políticas con respecto a la incorrecta asignación de derechos de acceso	Medio	Modificación del riesgo	Protección de los Soportes de Información	Gestionar niveles de privilegios de acceso del personal deacuerdo a sus funciones.	Prevención	Bajo	Creación de políticas para la asignación de derechos de acceso, limitación y uso de cuentas en plataformas.	Bajo
			Acceso no autorizado		Medio	Modificación del riesgo	Protección de los Soportes de Información	Gestionar niveles de privilegios de acceso del personal deacuerdo a sus funciones.	Prevención	Bajo		Bajo
			Modificación deliberada de la información	Falta de proceso disciplinario definido en caso de incidente de seguridad de la información	Medio	Modificación del riesgo	Protección de los Soportes de Información	Gestionar niveles de privilegios de acceso del personal deacuerdo a sus funciones.	Prevención	Bajo	Crear políticas disciplinarias para incidentes de seguridad de la información.	Bajo
			Destrucción de información	Falta de políticas con respecto a la incorrecta asignación de derechos de acceso	Medio	Modificación del riesgo	Protección de los Soportes de Información	Tener configurado el repositorio con procesos de autorización y confirmación de los stakeholders o personas responsables sobre cambios a realizar.	Disuasión	Bajo	Creación de políticas para la asignación de derechos de acceso, limitación y uso de cuentas en plataformas.	Bajo
			Divulgación de información	Falta de proceso disciplinario definido en caso de incidente de seguridad de la información	Medio	Modificación del riesgo	Protección de los Soportes de Información	Limitar el acceso a una persona encargada de ser el administrador de la cuenta de acceso al repositorio.	Prevención	Bajo	Crear políticas disciplinarias para incidentes de seguridad de la información.	Bajo
			Robo	Falta de políticas con respecto a la incorrecta asignación de derechos de acceso	Medio	Modificación del riesgo	Protección de los Soportes de Información	Limitar el acceso a una persona encargada de ser el administrador de la cuenta de acceso al repositorio.	Prevención	Bajo	Creación de políticas para la asignación de derechos de acceso, limitación y uso de cuentas en plataformas.	Bajo
Equipamiento auxiliar	Generador eléctrico	Alto	Fuego (Desastres naturales)	Falta de planes de continuidad Falta de procedimientos de identificación y evaluación de riesgos	Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo	Creación de planes de continuidad basados en sustitucion inmediata de equipos. Realizar procesos de identificación y evaluación de riesgos potenciales que puedan afectar al activo.	Bajo
			Daños por agua (Desastres naturales)		Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo		Bajo
			Desastres naturales		Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo		Bajo
			Fuego (De origen industrial)		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio		Bajo
			Daños por agua (De origen industrial)		Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo		Bajo
			Desastres industriales		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio		Bajo
Equipamiento auxiliar	UPS	Alto	Fuego (Desastres naturales)	Falta de planes de continuidad Falta de procedimientos de identificación y evaluación de riesgos	Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo	Creación de planes de continuidad basados en sustitucion inmediata de equipos. Realizar procesos de identificación y evaluación de riesgos potenciales que puedan afectar al activo.	Bajo
			Daños por agua (Desastres naturales)		Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo		Bajo
			Desastres naturales		Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo		Bajo
			Fuego (De origen industrial)		Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Bajo		Bajo
			Daños por agua (De origen industrial)		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio		Bajo
			Desastres industriales		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio		Bajo
			Errores de los usuarios	Falta de proceso disciplinario definido en caso de incidente de cuidado de activos	Medio	Modificación del riesgo	Instalación	Implementar un sistema de supervisión periódica que permita monitorear el estado del UPS y recibir alertas en tiempo real sobre eventos críticos como la baja batería. Esto ayuda a identificar problemas antes de que se conviertan en situaciones de emergencia.	Monitorización	Bajo	Crear políticas disciplinarias para incidentes con el cuidado de activos .	Bajo
			Errores de administrador		Medio	Modificación del riesgo	Instalación	Implementar un sistema de supervisión periódica que permita monitorear el estado del UPS y recibir alertas en tiempo real sobre eventos críticos como la baja batería. Esto ayuda a identificar problemas antes de que se conviertan en situaciones de emergencia.	Monitorización	Bajo		Bajo
Equipamiento auxiliar	NVR	Alto	Fuego (Desastres naturales)	Falta de planes de continuidad Falta de procedimientos de identificación y evaluación de riesgos	Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio	Creación de planes de continuidad basados en sustitucion inmediata de equipos. Realizar procesos de identificación y evaluación de riesgos potenciales que puedan afectar al activo.	Bajo
			Daños por agua (Desastres naturales)		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio		Bajo
			Desastres naturales		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio		Bajo
			Fuego (De origen industrial)		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio		Bajo
			Daños por agua (De origen industrial)		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio		Bajo
			Desastres industriales		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral ante la pérdida del activo.	Administración	Medio		Bajo
			Manipulación de la configuración	Falta de políticas con respecto a la incorrecta asignación de derechos de acceso	Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Limitar el acceso a una persona encargada de ser el administrador de la cuenta de acceso del NVR.	Prevención	Bajo	Creación de políticas para la asignación de derechos de acceso, limitación y uso de cuentas en plataformas.	Bajo
Instalaciones	Oficina	Alto	Fuego (Desastres naturales)	Falta de planes de continuidad Falta de procedimientos de identificación y evaluación de riesgos	Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral que implique el trabajo remoto.	Administración	Medio	Creación de planes de continuidad basados en sustitucion inmediata de equipos. Realizar procesos de identificación y evaluación de riesgos potenciales que puedan afectar al activo.	Bajo
			Daños por agua (Desastres naturales)		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral que implique el trabajo remoto.	Administración	Medio		Bajo
			Desastres naturales		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral que implique el trabajo remoto.	Administración	Medio		Bajo
			Fuego (De origen industrial)		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral que implique el trabajo remoto.	Administración	Medio		Bajo
			Desastres industriales		Alto	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad laboral que implique el trabajo remoto.	Administración	Medio		Bajo
Personal	Jefe de área	Alto	Fuego (Desastres naturales)	Falta de planes de continuidad Falta de procedimientos de identificación y evaluación de riesgos	Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad para el reemplazo temporal del personal afectado.	Administración	Bajo	Creación de planes de continuidad basados en sustitucion inmediata de equipos. Realizar procesos de identificación y evaluación de riesgos potenciales que puedan afectar al activo.	Bajo
			Desastres naturales		Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad para el reemplazo temporal del personal afectado.	Administración	Bajo		Bajo
			Fuego (De origen industrial)		Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad para el reemplazo temporal del personal afectado.	Administración	Bajo		Bajo
			Escapes de información	Falta de proceso disciplinario definido en caso de incidente de seguridad de la información	Medio	Modificación del riesgo	Formación y concienciación	Mantener capacitado y concientizado al personal designado como jefe de área sobre los riesgos asociados al compartir información de su alcance y las consecuencias para la institución y como para el individuo.	Concienciación	Bajo	Crear políticas disciplinarias para incidentes de seguridad de la información.	Bajo
Personal	P.Desarrolladores / Programadores	Alto	Fuego (Desastres naturales)	Falta de planes de continuidad Falta de procedimientos de identificación y evaluación de riesgos	Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad para el reemplazo temporal del personal afectado.	Administración	Bajo	Creación de planes de continuidad basados en sustitucion inmediata de equipos. Realizar procesos de identificación y evaluación de riesgos potenciales que puedan afectar al activo.	Bajo
			Desastres naturales		Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad para el reemplazo temporal del personal afectado.	Administración	Bajo		Bajo
			Fuego (De origen industrial)		Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad para el reemplazo temporal del personal afectado.	Administración	Bajo		Bajo
			Escapes de información	Falta de proceso disciplinario definido en caso de incidente de seguridad de la información.	Medio	Modificación del riesgo	Formación y concienciación	Mantener capacitado y concientizado al personal designado como jefe de área sobre los riesgos asociados al compartir información de su alcance y las consecuencias para la institución y como para el individuo.	Concienciación	Bajo	Crear políticas disciplinarias para incidentes de seguridad de la información.	Bajo
Personal	P.Soporte técnico	Medio	Indisponibilidad del personal (Errores y fallos no intencionados)	Ausencia de personal	Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad para el reemplazo temporal del personal afectado.	Administración	Bajo	Creación de planes de continuidad basados en el remplazo temporal inmediato del personal.	Bajo
			Ingeniería social (picaresca)	Susceptibilidad de la Ingeniería social	Medio	Modificación del riesgo	Formación y concienciación	Mantener capacitado al personal sobre la ingeniería social en la institución.	Concienciación	Bajo	Crear políticas en contra de la ingeniería social	Bajo
	P.Redes	Medio	Indisponibilidad del personal (Errores y fallos no intencionados)	Ausencia de personal	Medio	Modificación del riesgo	Aseguramiento de la disponibilidad	Tener métodos de continuidad para el reemplazo temporal del personal afectado.	Administración	Bajo	Creación de planes de continuidad basados en el remplazo temporal inmediato del personal.	Bajo

PASO 4. Aceptación del Riesgo de seguridad de la información

En este paso se va a proponer una lista de riesgos, los cuales serán estudiados por la institución para filtrar aquellos riesgos que serán aceptados.

Tipo de activos	Activos	Amenaza	Vulnerabilidad	Estimación del riesgo potencial	Salvaguarda
Software	Sistemas Operativos	Difusión de software dañino (Errores y fallos no intencionados)	Malware y software malicioso Descarga y uso no controlado de software	Medio	Protección de las Aplicaciones Informáticas
		Difusión de software dañino (Ataques intencionados)		Medio	Protección de las Aplicaciones Informáticas
Hardware	Computadoras desktops	Fuego (Desastres naturales)	Falta de planes de continuidad Falta de procedimientos de identificación y evaluación de riesgos	Medio	Aseguramiento de la disponibilidad
		Daños por agua (Desastres naturales)		Medio	Aseguramiento de la disponibilidad
		Desastres naturales		Medio	Aseguramiento de la disponibilidad
		Fuego (De origen industrial)		Medio	Aseguramiento de la disponibilidad
		Daños por agua (De origen industrial)		Alto	Aseguramiento de la disponibilidad
		Desastres industriales		Medio	Aseguramiento de la disponibilidad
Hardware	Laptops	Fuego (Desastres naturales)	Falta de planes de continuidad Falta de procedimientos de identificación y evaluación de riesgos	Medio	Aseguramiento de la disponibilidad
		Daños por agua (Desastres naturales)		Medio	Aseguramiento de la disponibilidad
		Desastres naturales		Medio	Aseguramiento de la disponibilidad
		Fuego (De origen industrial)		Medio	Aseguramiento de la disponibilidad
		Daños por agua (De origen industrial)		Alto	Aseguramiento de la disponibilidad
		Desastres industriales		Medio	Aseguramiento de la disponibilidad
		Pérdida de equipos	Falta de política formal sobre uso de computadoras móviles	Alto	Aseguramiento de la disponibilidad
		Robo		Alto	Aseguramiento de la disponibilidad
Hardware	Equipos de reprografía	Fuego (Desastres naturales)	Falta de planes de continuidad Falta de procedimientos de identificación y evaluación de riesgos	Medio	Aseguramiento de la disponibilidad
		Daños por agua (Desastres naturales)		Medio	Aseguramiento de la disponibilidad
		Desastres naturales		Medio	Aseguramiento de la disponibilidad
		Fuego (De origen industrial)		Medio	Aseguramiento de la disponibilidad
		Daños por agua (De origen industrial)		Medio	Aseguramiento de la disponibilidad
		Desastres industriales		Medio	Aseguramiento de la disponibilidad
Hardware	Firewall	Fuego (Desastres naturales)	Falta de planes de continuidad Falta de procedimientos de identificación y evaluación de riesgos	Alto	Aseguramiento de la disponibilidad
		Daños por agua (Desastres naturales)		Alto	Aseguramiento de la disponibilidad
		Desastres naturales		Alto	Aseguramiento de la disponibilidad
		Fuego (De origen industrial)		Alto	Aseguramiento de la disponibilidad
		Daños por agua (De origen industrial)		Alto	Aseguramiento de la disponibilidad
		Desastres industriales		Alto	Aseguramiento de la disponibilidad
Redes de comunicaciones	Internet	Errores de mantenimiento / actualización de equipos (hardware)	Falta de esquemas periódicos de reemplazo Pobre conjunto de cableado estructurado	Medio	Cambios (actualizaciones y mantenimiento)
		Caída del sistema por agotamiento de recursos		Medio	Aseguramiento de la disponibilidad

Redes de comunicaciones	Internet de respaldo	Errores de mantenimiento / actualización de equipos (hardware)	Falta de esquemas periódicos de reemplazo Pobre conjunto de cableado	Medio	Cambios (actualizaciones y mantenimiento)
		Caída del sistema por agotamiento de recursos		Medio	Aseguramiento de la disponibilidad
Equipamiento auxiliar	Generador eléctrico	Fuego (Desastres naturales)	Falta de planes de continuidad Falta de procedimientos de identificación y evaluación de riesgos	Medio	Aseguramiento de la disponibilidad
		Daños por agua (Desastres naturales)		Medio	Aseguramiento de la disponibilidad
		Desastres naturales		Medio	Aseguramiento de la disponibilidad
		Fuego (De origen industrial)		Alto	Aseguramiento de la disponibilidad
		Daños por agua (De origen industrial)		Medio	Aseguramiento de la disponibilidad
		Desastres industriales		Alto	Aseguramiento de la disponibilidad
Equipamiento auxiliar	UPS	Fuego (Desastres naturales)	Falta de planes de continuidad Falta de procedimientos de identificación y evaluación de riesgos	Medio	Aseguramiento de la disponibilidad
		Daños por agua (Desastres naturales)		Medio	Aseguramiento de la disponibilidad
		Desastres naturales		Medio	Aseguramiento de la disponibilidad
		Fuego (De origen industrial)		Medio	Aseguramiento de la disponibilidad
		Daños por agua (De origen industrial)		Alto	Aseguramiento de la disponibilidad
		Desastres industriales		Alto	Aseguramiento de la disponibilidad
Equipamiento auxiliar	NVR	Fuego (Desastres naturales)	Falta de planes de continuidad Falta de procedimientos de identificación y evaluación de riesgos	Alto	Aseguramiento de la disponibilidad
		Daños por agua (Desastres naturales)		Alto	Aseguramiento de la disponibilidad
		Desastres naturales		Alto	Aseguramiento de la disponibilidad
		Fuego (De origen industrial)		Alto	Aseguramiento de la disponibilidad
		Daños por agua (De origen industrial)		Alto	Aseguramiento de la disponibilidad
		Desastres industriales		Alto	Aseguramiento de la disponibilidad
Instalaciones	Oficina	Fuego (Desastres naturales)	Falta de planes de continuidad Falta de procedimientos de identificación y evaluación de riesgos	Alto	Aseguramiento de la disponibilidad
		Daños por agua (Desastres naturales)		Alto	Aseguramiento de la disponibilidad
		Desastres naturales		Alto	Aseguramiento de la disponibilidad
		Fuego (De origen industrial)		Alto	Aseguramiento de la disponibilidad
		Desastres industriales		Alto	Aseguramiento de la disponibilidad

Tabla 135: *Posibles riesgos a aceptar*

Fuente: Elaboración propia adaptada del libro MAGERIT – Libro I - Métodos (MAR.4).

PASO 5. Comunicación y consulta del riesgo de seguridad de la información y PASO 6. Seguimiento y revisión del riesgo de seguridad de la información

Con respecto a los pasos 5 y 6 no se desarrollaron ya que nuestro proyecto de tesis es una propuesta de implementación más no la ejecución de la misma.

Capítulo IV. RESULTADOS

- Se diseñó una propuesta de implementación de la NTP-ISO/IEC 27005:2018 aplicando la metodología MAGERIT, para que con su aplicación se pueda mitigar o disminuir el impacto de los riesgos a los que están expuestos los activos de información para el Área Funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco. (pp. 43-275)
- Se han propuesto políticas (Anexo 3: Políticas) (pp.336-359) claras y planes de acción (pp.270-273) adecuados para las amenazas, vulnerabilidades y riesgos es fundamental hoy en día en las instituciones.
- Un paso crucial fue la clasificación de los activos pertenecientes al Área Funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco, de acuerdo con las directrices de MAGERIT. (pp. 51-111)
- La identificación de amenazas representa otro proceso fundamental, ya que estos datos permitieron calcular la probabilidad de incidencia y degradación (pp. 131-186), impacto (pp.216-268) obteniendo así el riesgo correspondiente.
- Se elaboró una lista de salvaguardas para así poder reducir los riesgos de los activos (pp. 193-213).
- Se obtuvo una lista de riesgos para que sean evaluados por la institución (pp. 274-275).

- Se sacó el porcentaje de los riesgos valorados en bajo, medio y alto para cada tipo de activos:

    1. Datos/ Información:
       Amenazas de riesgo bajo ➔ 60.71 %
       Amenazas de riesgo medio ➔ 28.58 %
       Amenazas de riesgo alto ➔ 10.71 %
    2. Claves criptográficas:
       Amenazas de riesgo bajo ➔ 12.90 %
       Amenazas de riesgo medio ➔ 61.30%
       Amenazas de riesgo alto ➔ 25.80%
    3. Servicios:
       Amenazas de riesgo bajo ➔ 61.11 %
       Amenazas de riesgo medio ➔ 27.77 %

Amenazas de riesgo alto ➔ 11.12 %

4. Software:

   Amenazas de riesgo bajo ➔ 76.74 %

   Amenazas de riesgo medio ➔ 20.93 %

   Amenazas de riesgo alto ➔ 2.33 %

5. Hardware:

   Amenazas de riesgo bajo ➔ 44.64 %

   Amenazas de riesgo medio ➔ 28.58 %

   Amenazas de riesgo alto ➔ 26.78 %

6. Redes de comunicaciones:

   Amenazas de riesgo bajo ➔ 20.58 %

   Amenazas de riesgo medio ➔ 55.90 %

   Amenazas de riesgo alto ➔ 23.52 %

7. Soportes de Información:

   Amenazas de riesgo bajo ➔ 67.53 %

   Amenazas de riesgo medio ➔ 19.49 %

   Amenazas de riesgo alto ➔ 12.98 %

8. Equipamiento auxiliar:

   Amenazas de riesgo bajo ➔ 58.82 %

   Amenazas de riesgo medio ➔ 28.43 %

   Amenazas de riesgo alto ➔ 12.75 %

9. Instalaciones:

   Amenazas de riesgo bajo ➔ 53.33 %

   Amenazas de riesgo medio ➔ 0 %

   Amenazas de riesgo alto ➔ 46.67 %

10. Personal:

    Amenazas de riesgo bajo ➔ 50.00 %

    Amenazas de riesgo medio ➔ 44.74 %

    Amenazas de riesgo alto ➔ 5.26 %

Conclusiones

- La identificación y valoración de los activos en el Área Funcional de Informática y Telecomunicaciones nos permitió obtener una visión clara de los activos que la Dirección Desconcentrada de Cultura de Cusco debe proteger, puesto que al reconocer los activos se logró priorizar los de importancia alta y media cuya protección es esencial para garantizar la operatividad de la institución.
- La evaluación de las amenazas y vulnerabilidades reveló diversas debilidades en los sistemas de seguridad actuales, lo que demostró la necesidad de mejorar las medidas de protección. Se identificaron riesgos tanto internos (errores humanos, fallos técnicos) como externos (acceso no autorizado).
- La identificación y valoración de los riesgos en función de la probabilidad de incidencia e impacto permitió una mejor comprensión de las prioridades de gestión de riesgos. Aquellas amenazas con mayor probabilidad y alto impacto representan los riesgos más catastróficos para la institución, por lo que deben recibir una atención inmediata para evitar daños significativos en la infraestructura tecnológica y en la operatividad institucional.
- Las salvaguardas consideradas para mitigar los riesgos se han planteado en función de prioridades coordinadas con el personal de la institución, indicando el tipo de protección que ofrece cada una de ellas.

Recomendaciones

- Se sugiere que, tras la implementación de la presente propuesta en la Dirección Desconcentrada de Cultura de Cusco, esta pueda ser replicada como modelo en las demás Direcciones Desconcentradas de Cultura. De este modo, la propuesta no solo ofrecería una guía práctica para su adaptación y ejecución en otras regiones, sino que también contribuiría a estandarizar procedimientos y optimizar la gestión cultural a nivel nacional.
- Se sugiere que, una vez recopilada toda la información de la institución, esta sea integrada en un software de automatización de gestión de riesgos. Esto facilitará al personal encargado de la seguridad de la información una evaluación continua y eficiente de los riesgos, garantizando así una mayor protección de los datos sensibles y asegurando el cumplimiento de los controles de seguridad establecidos.

Bibliografía

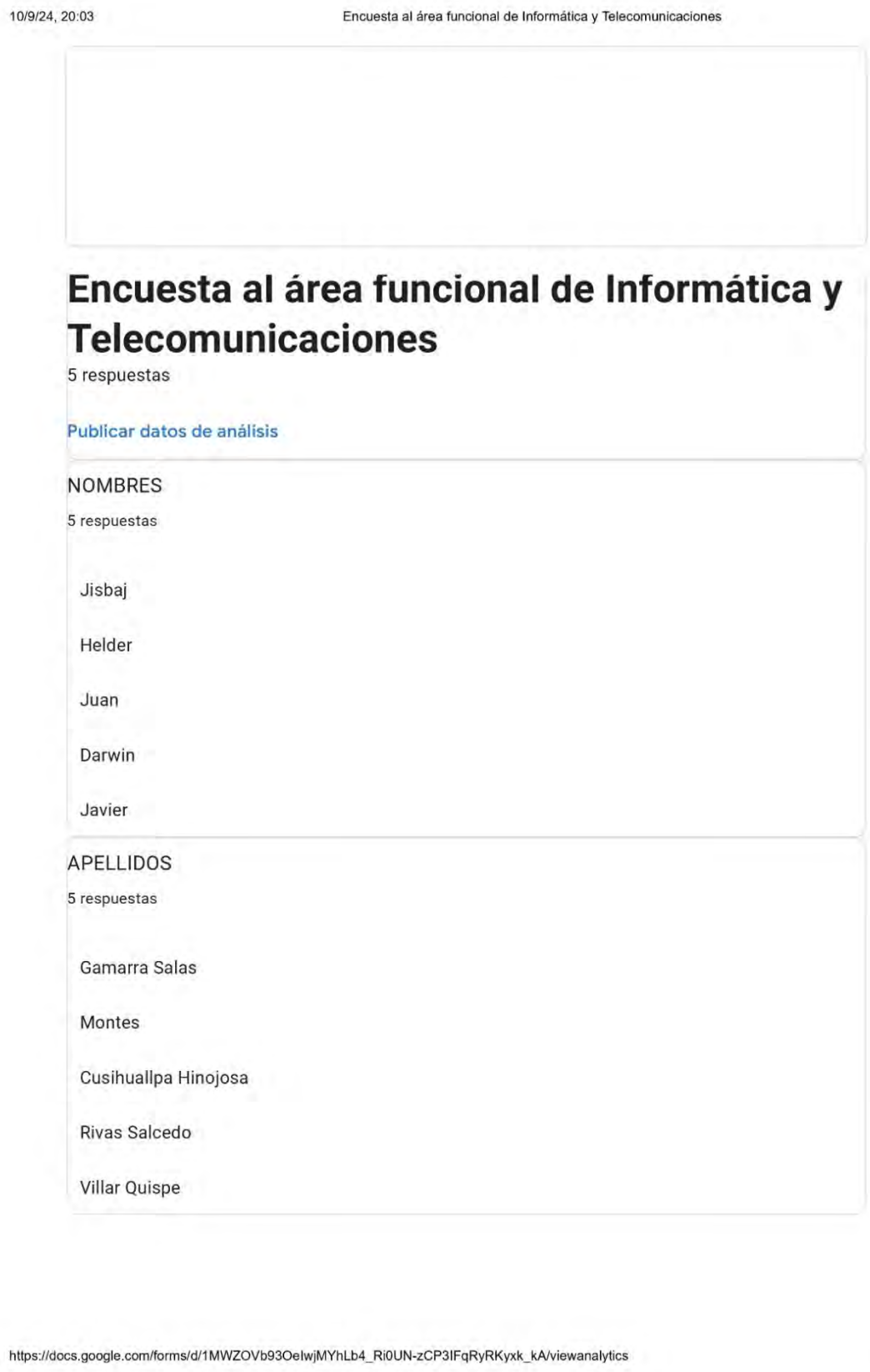
- Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). *MAGERIT – Versión 3.0. Metodología De Análisis Y Gestión De Riesgos De Los Sistemas De Información. Libro I - Método*. Ministerio de Hacienda y Administraciones Públicas.
- Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos*. Ministerio de Hacienda y Administraciones Públicas.
- Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas*. Ministerio de Hacienda y Administraciones Públicas.
- ISO/IEC 2018 & INACAL 2018. (2018). *Tecnología de la información. Técnicas de seguridad. Gestión de riesgos de la seguridad de la información*.
- ISO/IEC 2013 & INDECOPI 2014. (2014). *Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos*.
- Tanenbaum, A. S. (2000). *Organización de computadoras: un enfoque estructurado*. PRENTICE HALL.
- Camapaza Quispe Abdon Anders. (2019). *DISEÑO DEL PLAN DE SEGURIDAD INFORMÁTICA BASADO EN LA NTP ISO/IEC 27001:2014 PARA LA MUNICIPALIDAD DEL CENTRO POBLADO DE SALCEDO - PUNO*. [Tesis de pregrado]. Universidad Andina del Cusco.
- Carmona Torres Leonardo Dante. (2021). *Implementación de una Metodología de Gestión de Riesgos alineada a la ISO 27005 y MAGERIT para el proceso "OSE" de una empresa de facturación electrónica en la ciudad de Lima.* [Tesis de pregrado]. Universidad Tecnológica del Perú.
- Gonzales Auccapuri Fanny. (2016). *Propuesta de un marco de trabajo para la cláusula de adquisición, desarrollo y mantenimiento de sistemas de la ISO/IEC 27002: 2013 "Código de buenas prácticas para la gestión de seguridad de la información" para la oficina de tecnologías de la información y comunicaciones de la EPS. SEDACUSCO S. A.* [Tesis de pregrado]. Universidad Nacional de San Antonio Abad del Cusco.

- Puyén Santos Vicente Raúl y Rivas Palacios Betty Guiliana. (2018). *MODELO DE GESTIÓN DE RIESGOS BASADOS EN LA NORMA ISO/IEC 27005 Y METODOLOGÍA MAGERIT PARA MEJORAR LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL HOSPITAL REGIONAL DE LAMBAYEQUE*. [Tesis de pregrado]. Universidad Nacional Pedro Ruiz Gallo.
- Centro de Escritura Javeriano. (2020). *Normas APA*, (7.ª ed.).
- El Peruano. (2021, Febrero 19). Aprueban el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, modifican el Reglamento de Auditoría Interna, el Reglamento de Auditoría Externa, el TUPA de la SBS, el Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, el Reglamento de Riesgo Operacional, el Reglamento de Tarjetas de Crédito y Débito y el Reglamento de Operaciones con Dinero Electrónico. https://busquedas.elperuano.pe/normaslegales/aprueban-el-reglamento-para-la-gestion-de-la-seguridad-de-la-resolucion-no-504-2021-1929393-1/
- Equipo editorial, Etecé. (2020, Agosto 27). *¿Qué es la información?* Concepto. https://concepto.de/informacion/
- GCFGlobal. (s.f.). *Informática Básica: ¿Qué es hardware y software?* GCFGlobal. https://edu.gcfglobal.org/es/informatica-basica/que-es-hardware-y-software/1/
- Significados.com. (s.f.). *Qué es Información:* Significados. https://www.significados.com/informacion/
- Vélez Martínez, C. (s.f.). *Hardware y Software*. Instituto de Ingeniería UNAM. http://www.ii.unam.mx/es-mx/AlmacenDigital/CapsulasTI/Paginas/hardwareysoftware.aspx
- ERB, M. (s.f.). *2. Gestión de Riesgo en la Seguridad Informática | Gestión de Riesgo en la Seguridad Informática*. Gestión de Riesgo en la Seguridad Informática. https://protejete.wordpress.com/gdr_principal/gestion_riesgo_si/
- CISCO. (s.f.). *¿Qué es la ciberseguridad?* Cisco. https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html
- AMBIT. (2021, Febrero 9). *¿Qué es una auditoría de seguridad informática? Tipos y Fases*. AMBIT - BST. https://www.ambit-bst.com/blog/qu%C3%A9-es-una-auditor%C3%ADa-de-seguridad-inform%C3%A1tica-tipos-y-fases
- infosecurity Mexico. (2020, Junio 29). *Hacking Ético*. Infosecurity Mexico. https://www.infosecuritymexico.com/es/blog/hacking-etico.html

- Villamizar, C. (2022, January 25). *¿Qué es COBIT y para qué sirve?* GlobalSuite Solutions. https://www.globalsuitesolutions.com/es/que-es-cobit/
- OSTEC. (2016, December 30). *ISO27002: Buenas prácticas para gestión de la seguridad de la información*. OSTEC Blog. https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi/
- BSI. (s.f.). *ISO 27002 Tecnología de la información - técnicas de seguridad*. BSI. https://www.bsigroup.com/es-ES/iso-27002-controles-de-seguridad-de-la-informacion/

ANEXOS

Anexo 1: Encuesta al área funcional de informática y telecomunicaciones



10/9/24, 20:03 Encuesta al área funcional de Informática y Telecomunicaciones

Encuesta al área funcional de Informática y Telecomunicaciones

5 respuestas

Publicar datos de análisis

NOMBRES

5 respuestas

Jisbaj

Helder

Juan

Darwin

Javier

APELLIDOS

5 respuestas

Gamarra Salas

Montes

Cusihuallpa Hinojosa

Rivas Salcedo

Villar Quispe

https://docs.google.com/forms/d/1MWZOVb93OelwjMYhLb4_Ri0UN-zCP3IFqRyRKyxk_kA/viewanalytics 1/44

PROFESIÓN

5 respuestas

Ing. Informática y de Sistemas

Electrónico

Ing. Sistemas

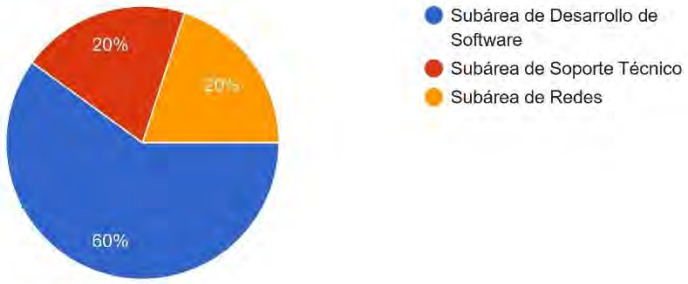
ING. Sistemas e informática

Ing. de Sistemas

SELECCIONAR EL SUBÁREA EN EL QUE LABORA USTED DENTRO DEL ÁREA FUNCIONAL DE INFORMÁTICA Y TELECOMUNICACIONES

Copiar

5 respuestas



CARGO QUE DESEMPEÑA

5 respuestas

Coordinador de Desarrollo de Software

Soporte técnico.

Front End

ADM TI

DESARROLLADOR DE SOFTWARE

a) Datos/ Información

1- ¿Al generar documentos (ya sea en formato Word ,Excel, MS Project, etc.), está es almacenada de manera digital en carpetas dentro de su computador?

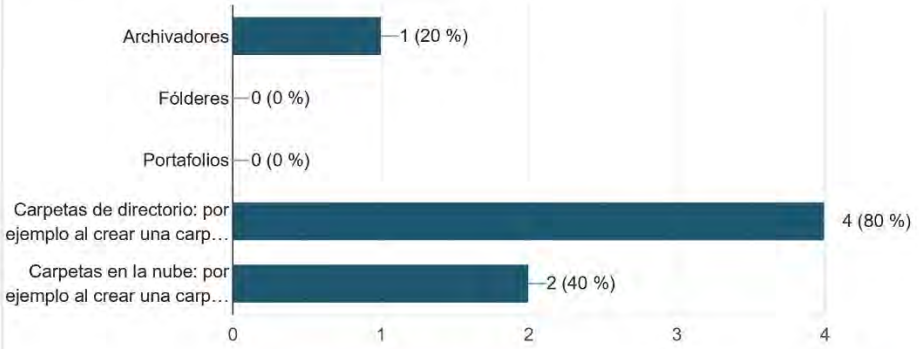
Copiar

5 respuestas

2- ¿De qué manera almacena su información (documentos, imágenes, videos, etc.)?

Copiar

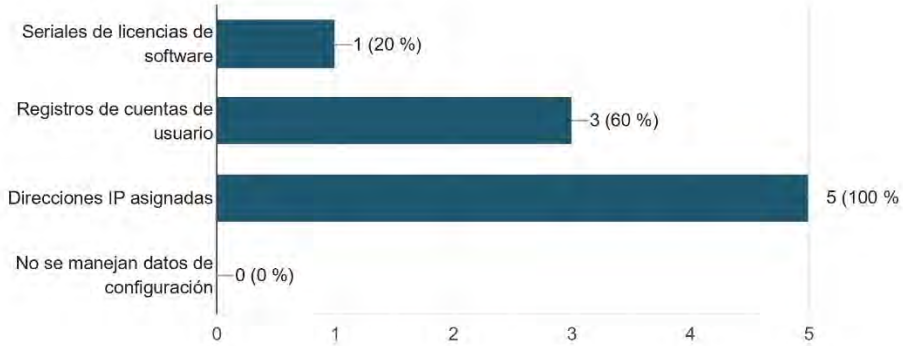
5 respuestas



3- ¿Qué datos de configuración (datos para solucionar problemas de equipos o sistemas) manejan?

Copiar

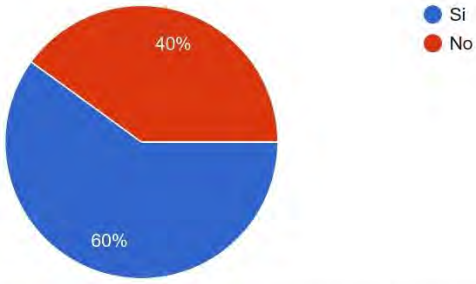
5 respuestas



4- ¿Se cuenta con un registro de contraseñas asignadas por plataforma institucional?

Copiar

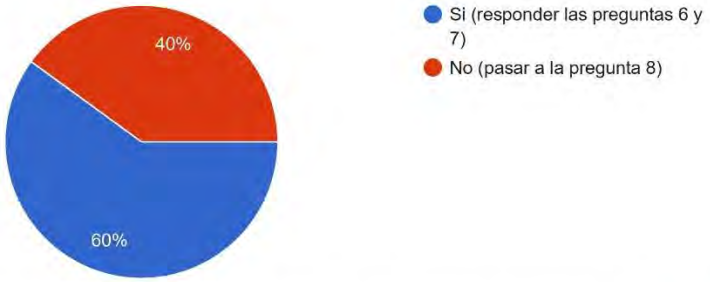
5 respuestas



5- ¿Se permite la modificación de contraseñas en las plataformas institucionales?

Copiar

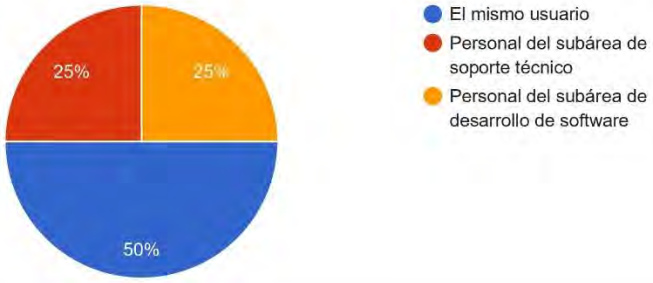
5 respuestas



6- ¿Quién o qué subárea está autorizada para el cambio de contraseñas en las plataformas institucionales?

Copiar

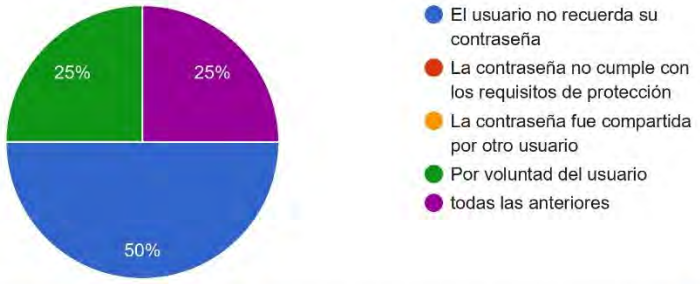
4 respuestas



7- ¿En qué casuística se permite el cambio de contraseñas en las plataformas institusionales?

Copiar

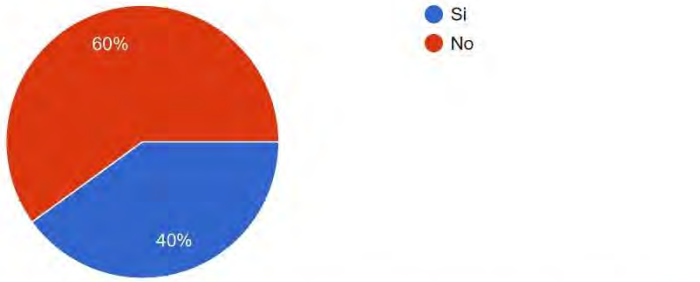
4 respuestas



8- ¿ Se cuenta con un registro de los seriales de licencias de softwares utilizados?

Copiar

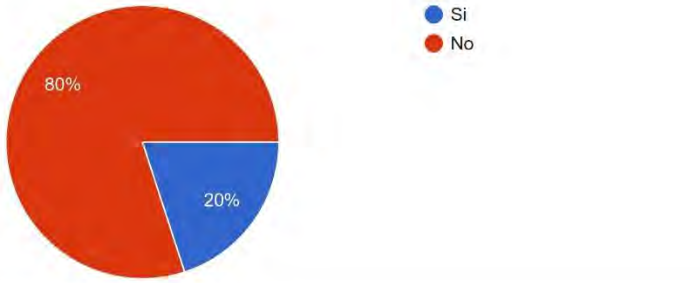
5 respuestas



9- ¿Cuentan con un registro de actividades(es un log de actividad que registra todos los cambios que hacen los usuarios en sus computadoras) del personal de la institución?

Copiar

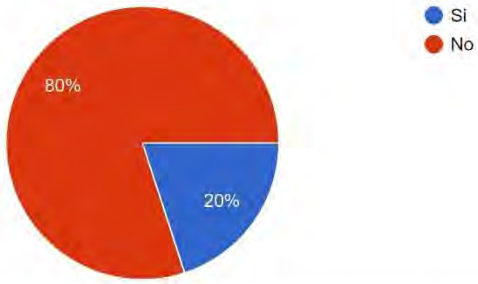
5 respuestas



10- ¿-Cuentan con un registro de actividades (es un log de actividad que registra todos los cambios que hacen los usuarios en sus computadoras) del personal del área funcional de informática y telecomunicaciones?

Copiar

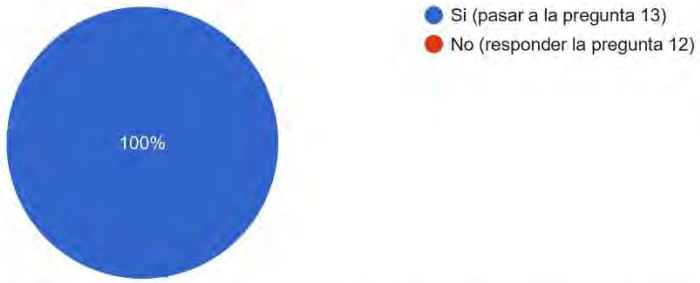
5 respuestas



11- ¿La página HELP DESK genera un reporte sobre las atenciones a los usuarios?

Copiar

5 respuestas



12- ¿De qué manera se puede verificar cuántas personas fueron atendidas?

3 respuestas

Requiriendo una reporte de atención.

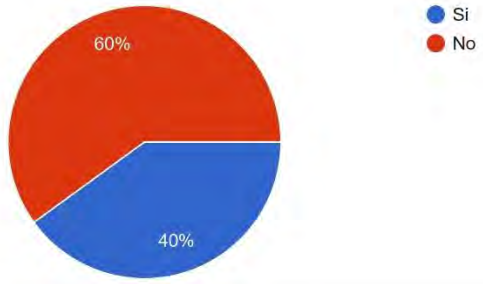
Reporte de Helpdesk

La plataforma ofrece reportes.

13- ¿Cuentan con un registro de datos de prueba (datos que se van a utilizar para probar una determinada pieza de software)?

Copiar

5 respuestas

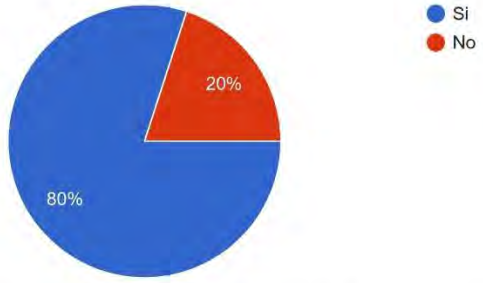


b) Claves criptográficas

1- ¿El manejo de contraseñas de las computadoras de oficina del personal son de manera controlada?

Copiar

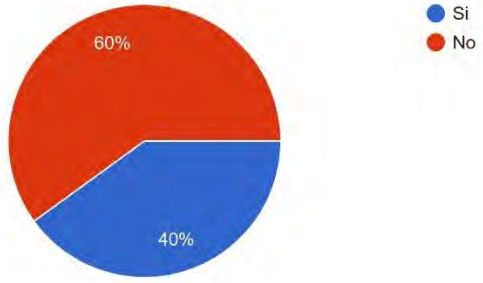
5 respuestas



2- ¿Es obligatoria la obtención de contraseñas en las computadoras de oficina del personal?

Copiar

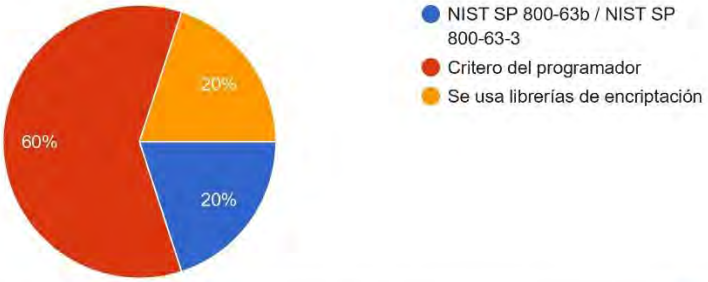
5 respuestas



3- ¿En qué norma(s) se basaron para la creación de contraseñas en las plataformas institucionales?

Copiar

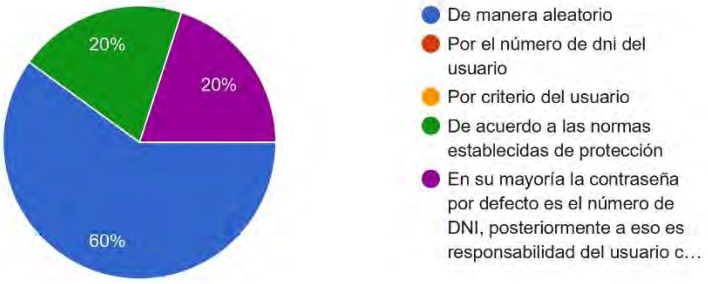
5 respuestas



4- Con respeto a las plataformas del estado, ¿De qué manera son asignadas las contraseñas?

Copiar

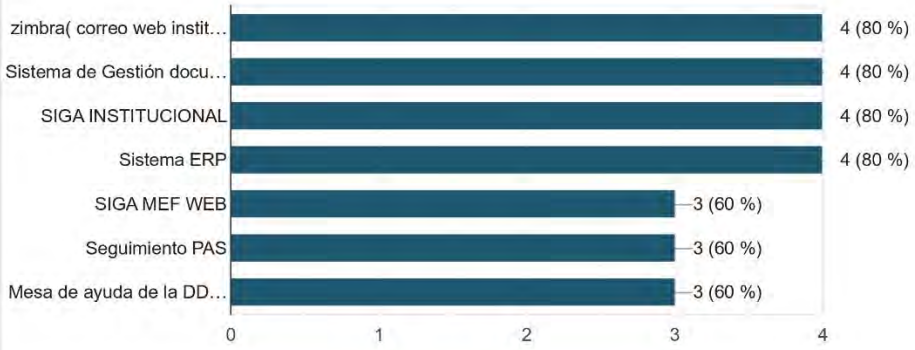
5 respuestas



5- De las plataformas a continuación ,marque cual(es) pertenecen a la institución.

Copiar

5 respuestas

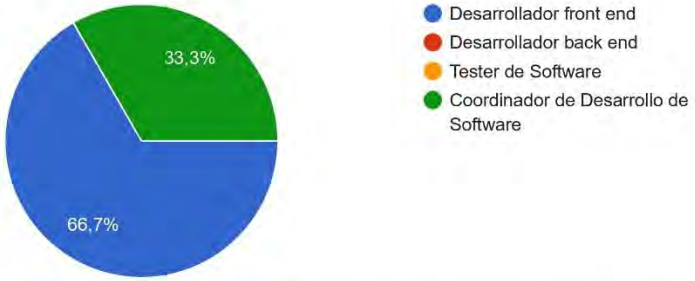


c) Servicios

1- Dentro del subárea de desarrollo de software qué labores desempeña (Si usted no realiza sus actividades dentro de desarrollo de software, pase a la siguiente pregunta)

Copiar

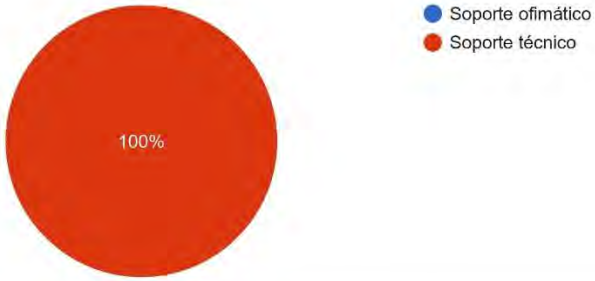
3 respuestas



2- Dentro del subárea de soporte técnico qué labores desempeña (Si usted no realiza sus actividades dentro de soporte técnico pase a la siguiente pregunta)

Copiar

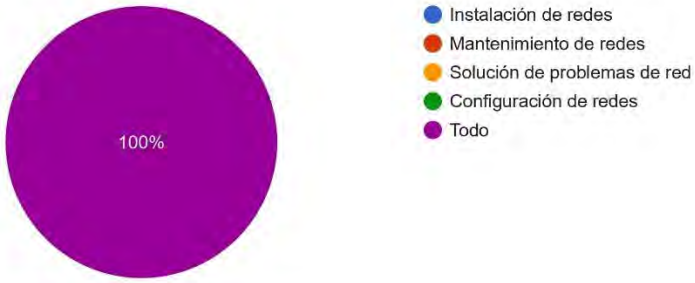
3 respuestas



3- Dentro del subárea de redes qué labores desempeña

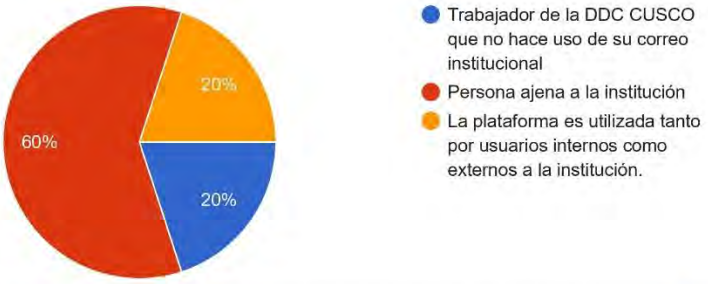
Copiar

1 respuesta



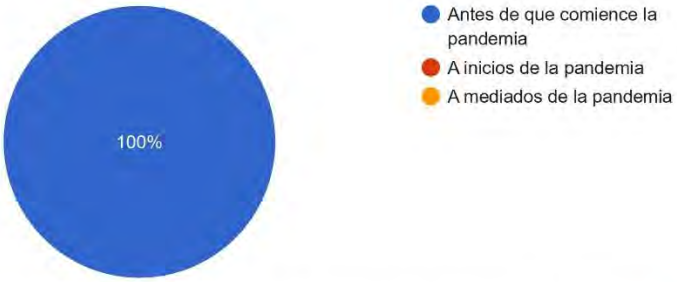
4- Con respecto a la plataforma HELP DESK (mesa de ayuda) , marque la alternativa que defina mejor a un usuario externo: Copiar

5 respuestas



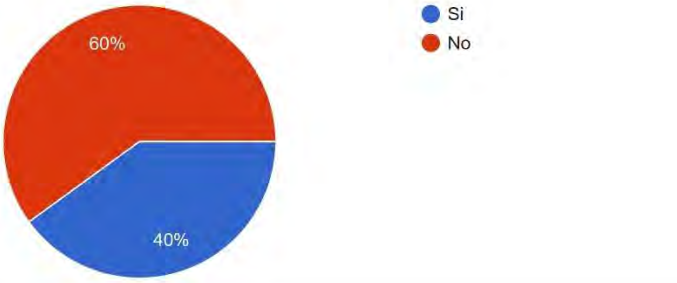
5- Desde cuándo lleva en funcionamiento la plataforma de asistencia técnica HELP DESK (mesa de ayuda) Copiar

5 respuestas



6- ¿Se realiza un control-monitoreo sobre el cambio de contraseñas en las cuentas de los usuarios de las plataformas institucionales? Copiar

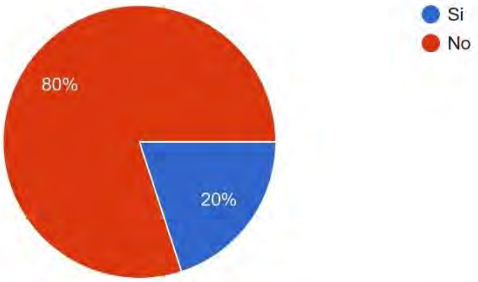
5 respuestas



7- ¿Se realiza un control-monitoreo sobre el cambio de contraseñas en las cuentas de los usuarios de las plataformas del estado?

Copiar

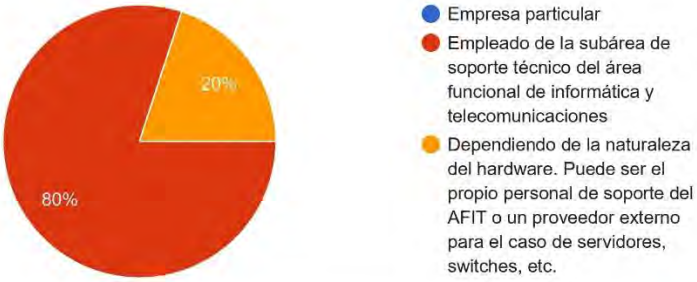
5 respuestas



8- ¿Quién proporciona los servicios de mantenimiento de hardware a la institución?

Copiar

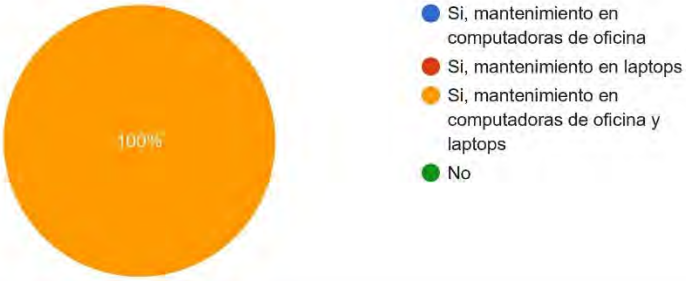
5 respuestas



9- ¿Se brinda mantenimiento de hardware en computadoras de oficinas y laptops a la institución?

Copiar

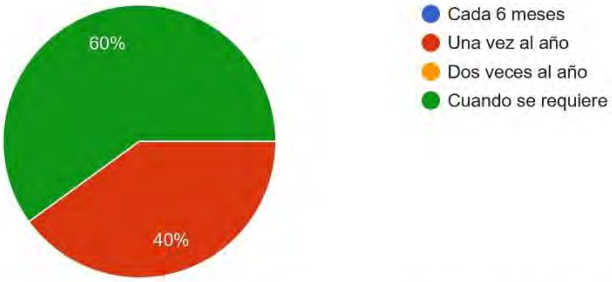
5 respuestas



10- ¿Con qué frecuencia se hace el mantenimiento de hardware?

Copiar

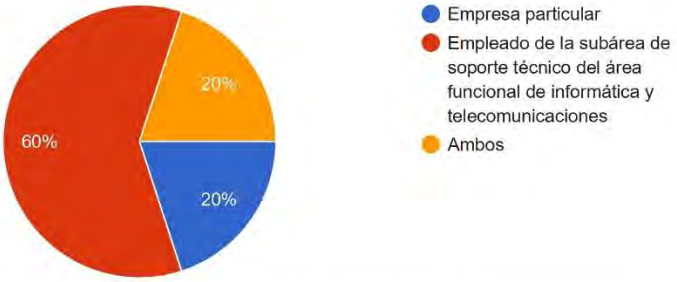
5 respuestas



11- ¿Quién proporciona los servicios de mantenimiento de equipos de reprografía (fotocopiadoras, escáneres, impresoras, etc.) a la institución?

Copiar

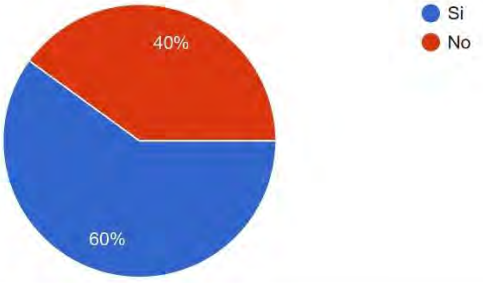
5 respuestas



12- ¿Se brinda mantenimiento de equipos de reprografía(fotocopiadoras, escáneres, impresoras, etc.) ?

Copiar

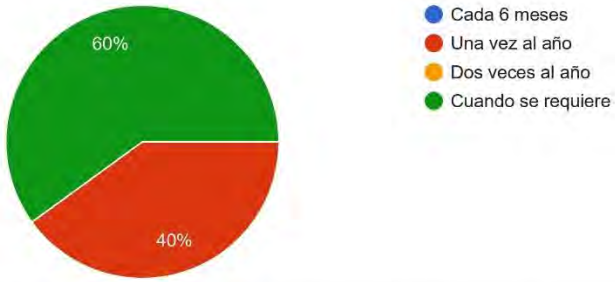
5 respuestas



13- ¿Con qué frecuencia se hace el mantenimiento de equipos de reprografía(fotocopiadoras, escáneres, impresoras, etc.)?

Copiar

5 respuestas



14- ¿Qué tipo de problemas sobre el hardware se dan con mayor frecuencia?

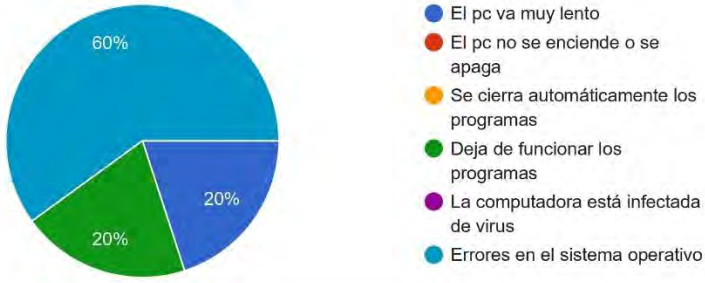
Copiar

5 respuestas

15- ¿Qué tipo de problemas sobre el software se dan con mayor frecuencia?

Copiar

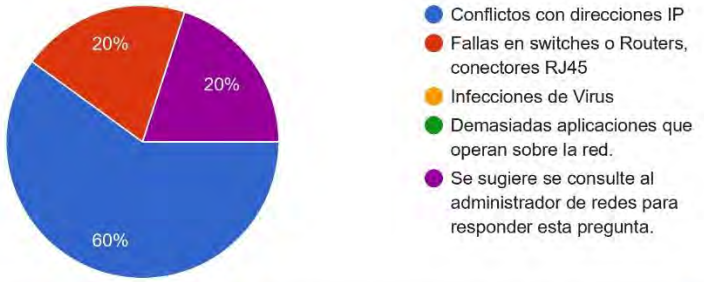
5 respuestas



16- ¿Qué tipo de problemas sobre las redes se dan con mayor frecuencia?

Copiar

5 respuestas



17- ¿Qué tipo de problemas sobre los equipos de reprografía (fotocopiadoras, escáneres, impresoras, etc.) se dan con mayor frecuencia?

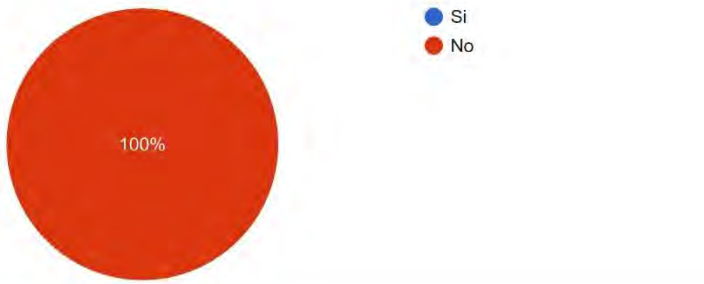
Copiar

5 respuestas

18- ¿Considera que el hardware existente es el adecuado a las necesidades de los empleados de la institución?

Copiar

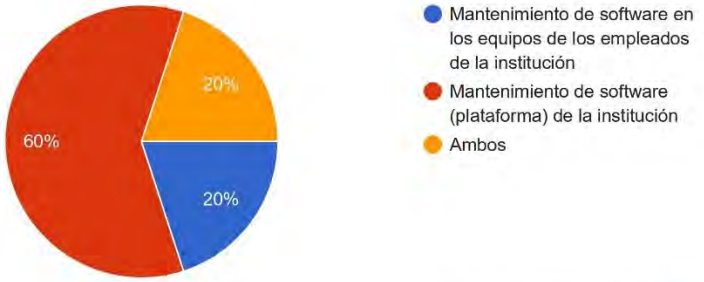
5 respuestas



19- De acuerdo al mantenimiento de software, se cuenta con:

Copiar

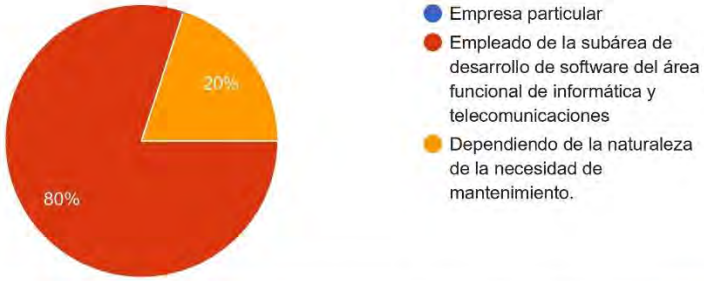
5 respuestas



20- ¿Quién proporciona los servicios de mantenimiento de software a la institución?

Copiar

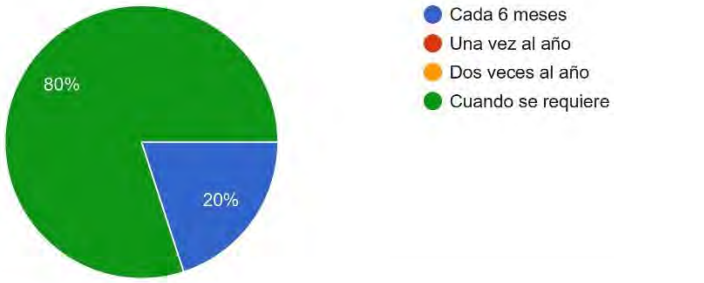
5 respuestas



21- ¿Con qué frecuencia se hace el mantenimiento de software?

Copiar

5 respuestas

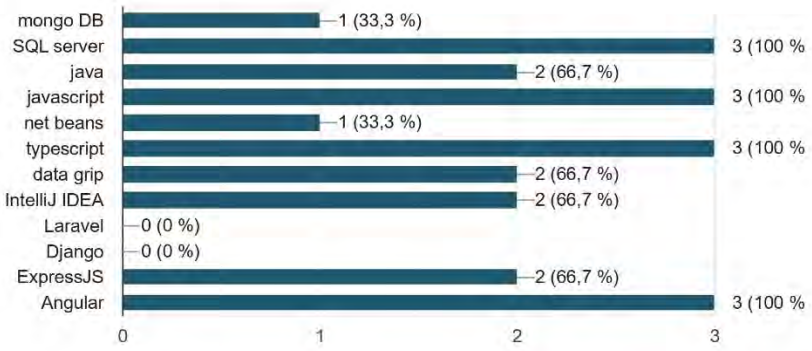


d) Software

1- Para el sub área de desarrollo de software, ¿Qué software utilizan para el desarrollo de sus funciones?

Copiar

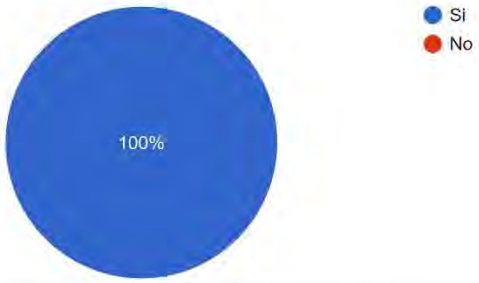
3 respuestas



2- Los antivirus obtenidos y/o usados en las computadoras de las oficinas de la DDC Cusco son versión de paga?

Copiar

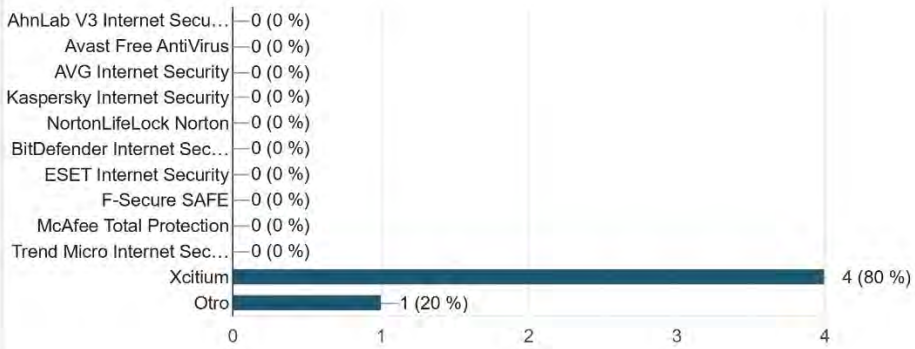
5 respuestas



3- Dentro del área funcional de informática y telecomunicaciones se trabaja con información de gran importancia, ¿Con qué antivirus cuentan para protegerla?

Copiar

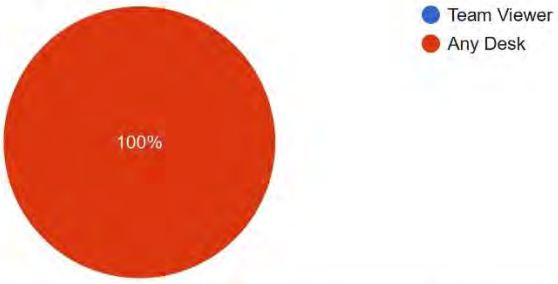
5 respuestas



4- Con respecto a la asistencia técnica brindada, ¿Qué programas de escritorio remoto utilizan para dar solución a las problemáticas encontradas?

Copiar

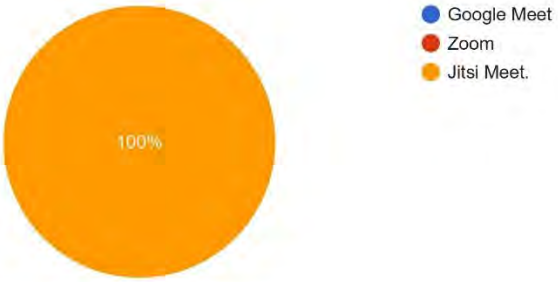
5 respuestas



5- Para las videoconferencias que maneja el personal de la DDC Cusco, ¿Qué software utilizan?

Copiar

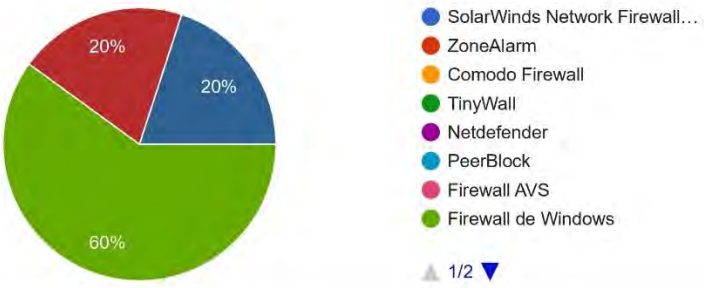
5 respuestas



6- ¿Qué firewall o cortafuego de software se tiene instalado en las computadoras de oficina y laptops de la institución?

Copiar

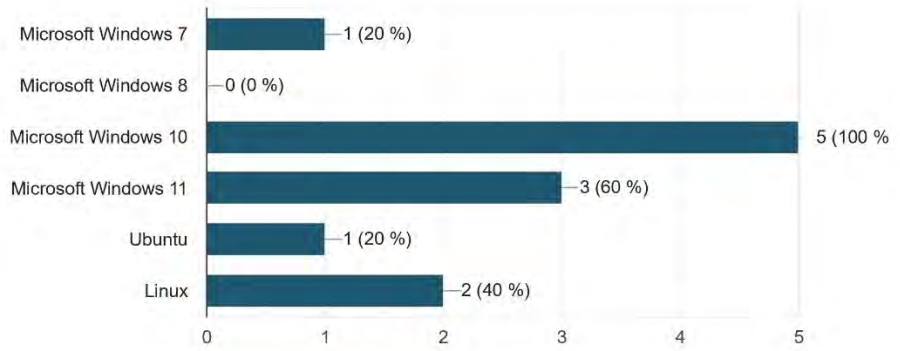
5 respuestas



7- ¿Qué sistema operativo utilizan?

Copiar

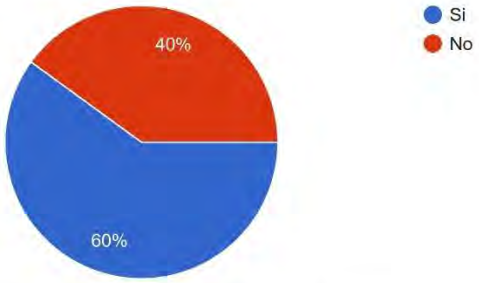
5 respuestas



8- ¿Cuentan con licencias activas de Windows?

Copiar

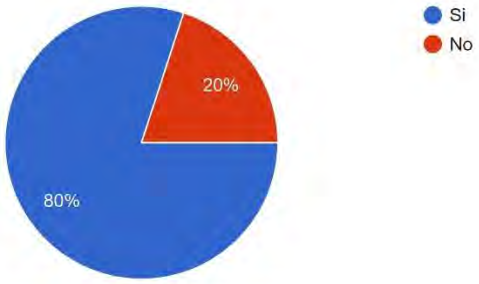
5 respuestas



9- ¿Cuentan con licencias activas de Office (Word,Excel,Power Point,etc)?

Copiar

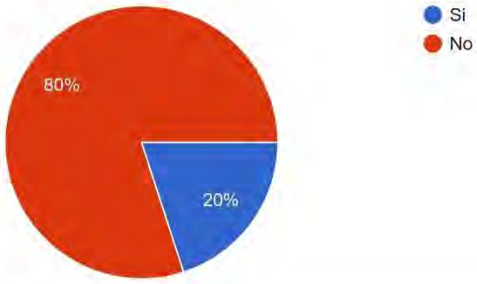
5 respuestas



10- Trabajan con MS Project para administrar los proyectos y gestionar la asignación de tareas en el área funcional de informática y telecomunicaciones?

Copiar

5 respuestas



e) Hardware

1- ¿Cuántas computadoras de escritorio tiene la DDC Cusco?

5 respuestas

--

300

900

800

Se sugiere orientar esta pregunta al área competente que maneja el inventario institucional.

2- ¿Cuántas laptos tiene la DDC Cusco?

5 respuestas

--

200

400

500

Se sugiere orientar esta pregunta al área competente que maneja el inventario institucional.

3- ¿Cuántos cpu's tiene la DDC Cusco?

5 respuestas

--

500

1300

800

Se sugiere orientar esta pregunta al área competente que maneja el inventario institucional.

4- ¿Cuántos teclados tiene la DDC Cusco?

5 respuestas

--

1000

900

800

Se sugiere orientar esta pregunta al área competente que maneja el inventario institucional.

5- ¿Cuántos mouses tiene la DDC Cusco?

5 respuestas

--

1500

900

1300

Se sugiere orientar esta pregunta al área competente que maneja el inventario institucional.

6- ¿Cuántos estabilizadores tiene la DDC Cusco?

5 respuestas

--

300

600

800

Se sugiere orientar esta pregunta al área competente que maneja el inventario institucional.

7- ¿Cuántas cámaras web tiene la DDC Cusco?

5 respuestas

--

50

25

No

Consultar al personal de redes.

8- ¿Cuántos micrófonos tiene la DDC Cusco?

5 respuestas

--

200

0

No

Se sugiere orientar esta pregunta al área competente que maneja el inventario institucional.

9- ¿Cuántos parlantes tiene la DDC Cusco?

5 respuestas

--

50

0

No

Se sugiere orientar esta pregunta al área competente que maneja el inventario institucional.

10- ¿Cuántos monitores tiene la DDC Cusco?

5 respuestas

--

400

900

800

Se sugiere orientar esta pregunta al área competente que maneja el inventario institucional.

11- ¿Cuántos discos duros externos tiene la DDC Cusco?

5 respuestas

--

1000

150

No

Se sugiere orientar esta pregunta al área competente que maneja el inventario institucional.

12- ¿Cuántos lectores de cd 's tiene la DDC Cusco?

5 respuestas

--

100

350

No

Se sugiere orientar esta pregunta al área competente que maneja el inventario institucional.

13- ¿Cuántos proyectores tiene la DDC Cusco?

5 respuestas

--

60

50

No

Se sugiere orientar esta pregunta al área competente que maneja el inventario institucional.

14- ¿Cuántos escáneres tiene la DDC Cusco?

5 respuestas

--

20

5

No

Se sugiere orientar esta pregunta al área competente que maneja el inventario institucional.

15- ¿Cuántas impresoras tiene la DDC Cusco?

5 respuestas

–

400

700

No

Se sugiere orientar esta pregunta al área competente que maneja el inventario institucional.

16- ¿Cuántas fotocopiadoras tiene la DDC Cusco?

5 respuestas

–

100

80

No

Se sugiere orientar esta pregunta al área competente que maneja el inventario institucional.

17- ¿Cuántos equipos funcionales (impresora-escáner-fotocopiadora) tiene la DDC Cusco?

5 respuestas

–

50

80

No

Se sugiere orientar esta pregunta al área competente que maneja el inventario institucional.

18- ¿Cuántos stwiches de red tiene la DDC Cusco?

5 respuestas

–

60

30

30 adm

Se sugiere orientar esta pregunta al área competente que maneja el inventario institucional.

19- ¿Cuántos generadores eléctricos tiene la DDC Cusco?

5 respuestas

1

2

1 data center

20- ¿Cuántos UPS tiene la DDC Cusco?

5 respuestas

–

150

30

1 data center

1

21- ¿Cuántos router mikrotik tiene la DDC Cusco?

5 respuestas

–

15

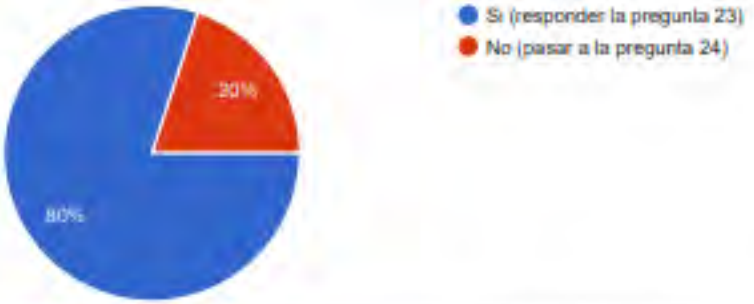
0

No

Se sugiere orientar esta pregunta al área competente que maneja el inventario institucional.

22- ¿Cuentan con firewall o cortafuego de hardware en la DDC Cusco? Copiar

5 respuestas



23- ¿Qué tipo de firewall o cortafuego de hardware tiene la DDC Cusco?

4 respuestas

Hillstone

Nueva generación

Se sugiere orientar esta pregunta al subárea de redes.

24- ¿Cuántos data center tiene la DDC Cusco?

5 respuestas

1

Uno

Se sugiere orientar esta pregunta al subárea de redes.

25- ¿Cuántos servidores tiene la DDC Cusco?

5 respuestas

10

–

45 virtuales

Se sugiere orientar esta pregunta al subárea de redes.

26- ¿Cuántas cintas de backups tiene la DDC Cusco?

5 respuestas

–

0

0

No

Se sugiere orientar esta pregunta al subárea de redes.

27- ¿Cuántos teléfonos IP tiene la DDC Cusco?

5 respuestas

–

200

60

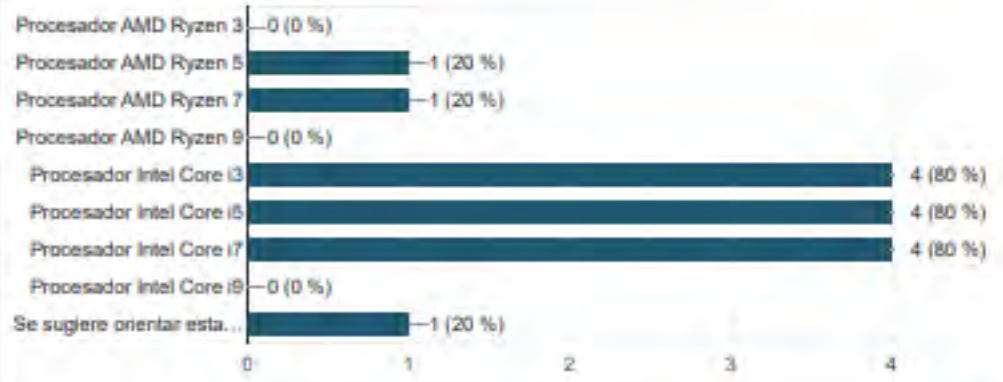
120

Se sugiere orientar esta pregunta al subárea de redes.

28- Marque con qué procesadores cuentan las distintas computadoras de escritorios

Copiar

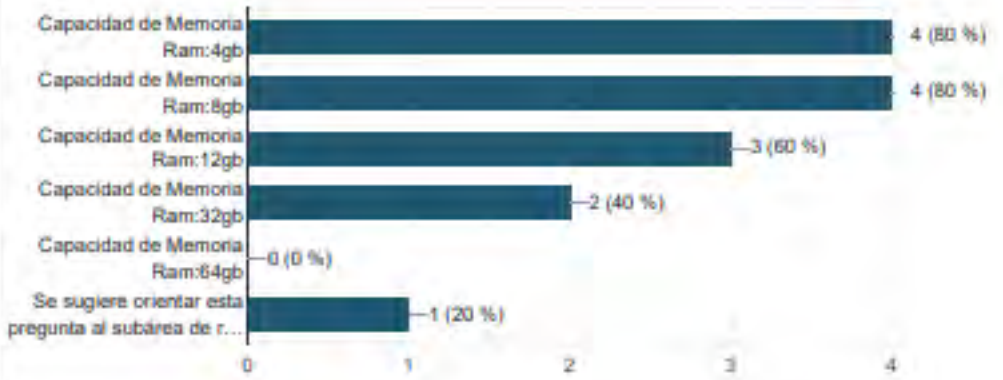
5 respuestas



29- Marque las distintas capacidades de memorias RAM que tengan las computadoras de escritorio

Copiar

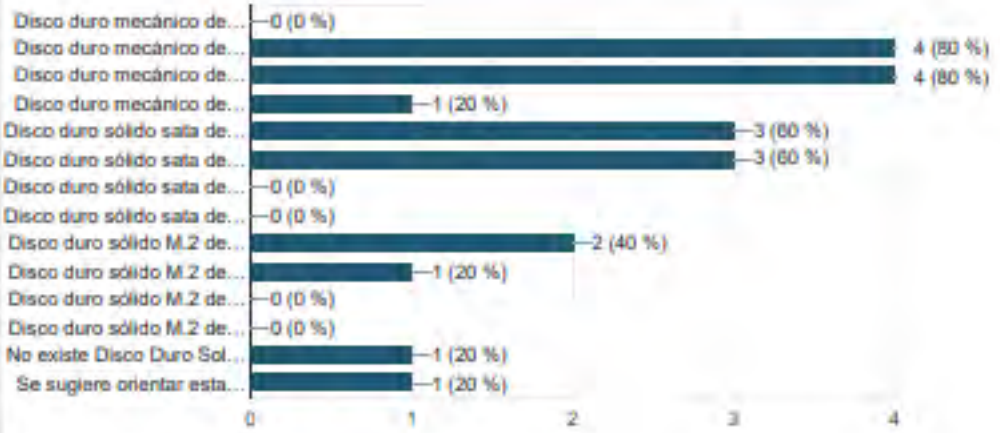
5 respuestas



30- Marque que modelo de disco duro tienen las computadoras de escritorios

Copiar

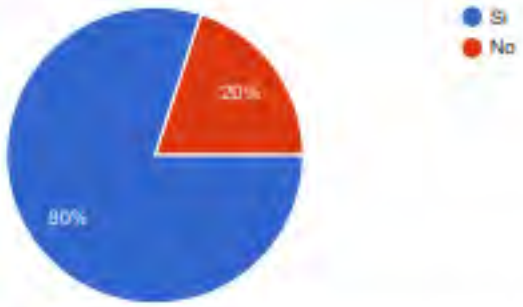
5 respuestas



31- ¿Las computadoras de escritorio cuentan con garantía?

Copiar

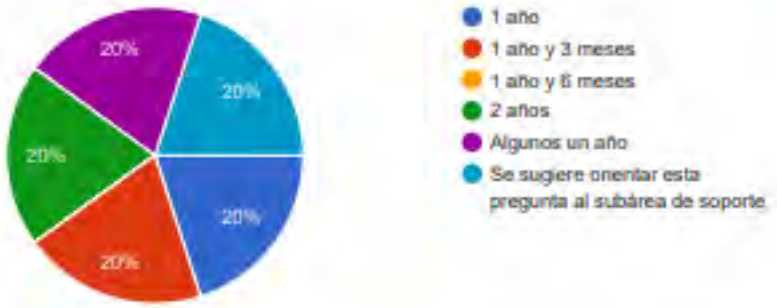
5 respuestas



32- ¿Cuánto tiempo de garantía tienen las computadoras de escritorio?

Copiar

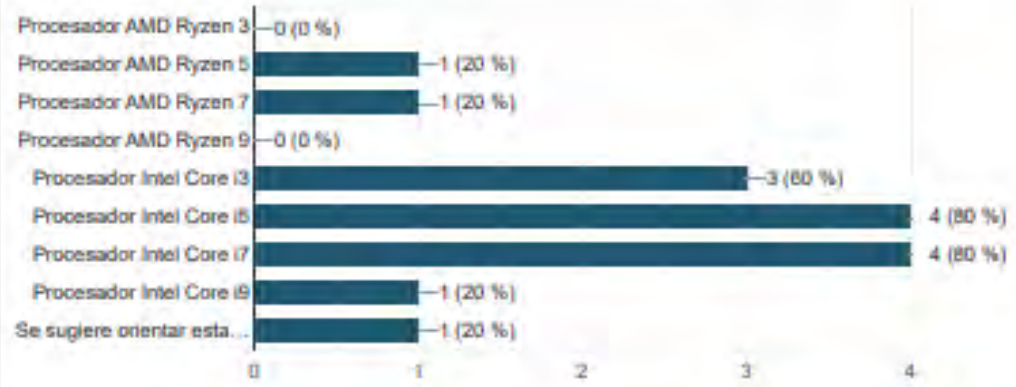
5 respuestas



33- Marque con qué procesadores cuentan las distintas laptops

Copiar

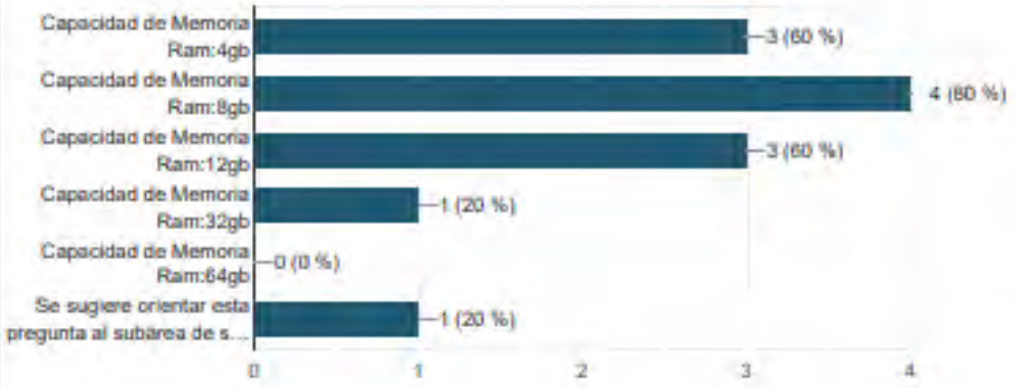
5 respuestas



34- Marque las distintas capacidades de memorias RAM tienen las laptops

Copiar

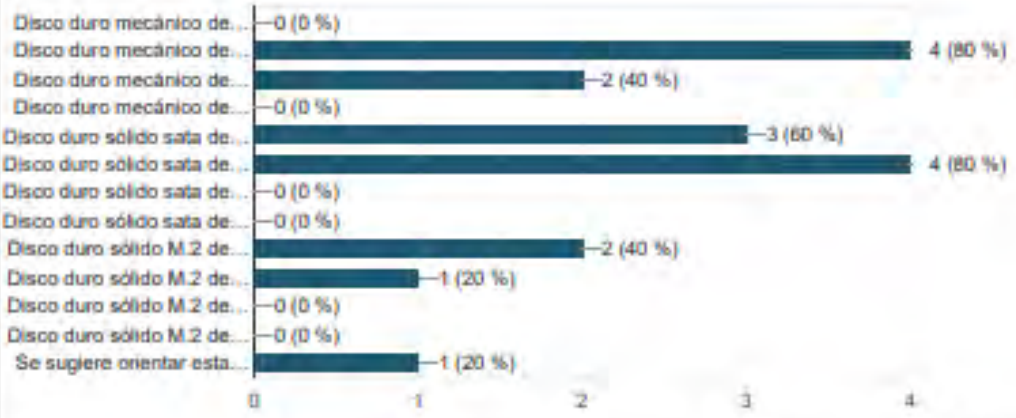
5 respuestas



35- Marque que modelo de disco duro tienen las laptops

Copiar

5 respuestas



36- ¿Las laptops cuentan con garantía?

Copiar

5 respuestas

37- ¿Cuánto tiempo de garantía tienen las laptops?

Copiar

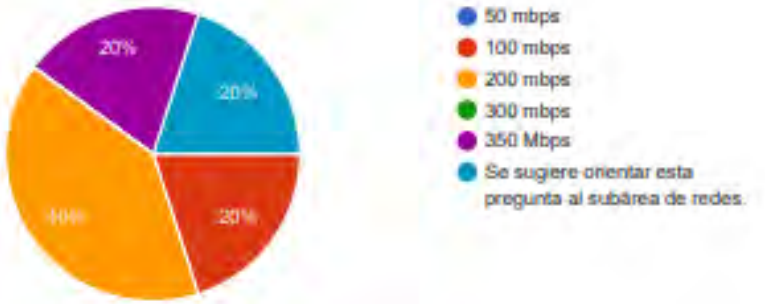
5 respuestas

g) Redes de Comunicaciones

1- ¿Cuál es la velocidad de internet que cuenta el área funcional de informática y telecomunicaciones?

Copiar

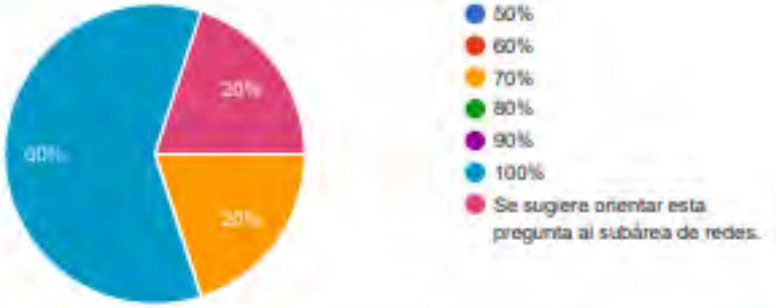
5 respuestas



2- Según el contrato de internet que se tiene con el proveedor del servicio, ¿Cuál porcentaje garantiza de llegada de internet?

Copiar

5 respuestas



3- El servicio de internet adquirido es empresarial/corporativo?

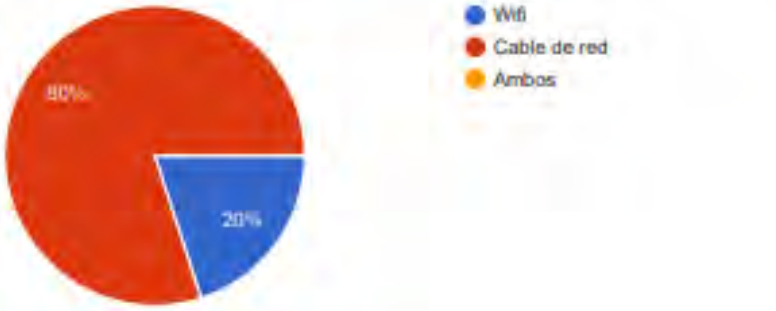
Copiar

5 respuestas

4- La distribución de red en las oficinas de la DDC Cusco es mediante:

Copiar

5 respuestas



5- El servicio de internet que se utiliza en las oficinas de la DDC Cusco es adquirido mediante:

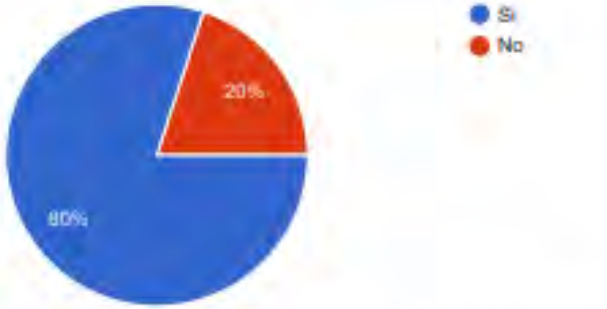
Copiar

5 respuestas

6- ¿El servicio de internet adquirido es simétrico?

Copiar

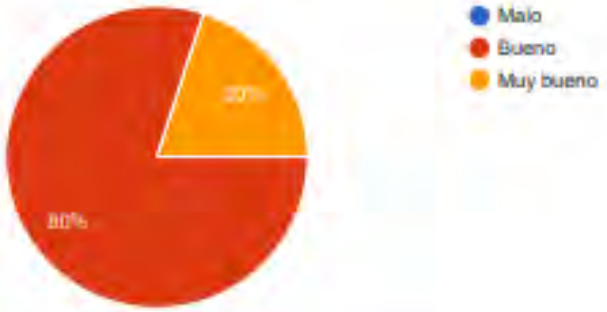
5 respuestas



7- Cómo califica la llegada de internet en las oficinas de la DDC cusco

Copiar

5 respuestas



8- ¿Se presentan constantemente problemas de internet en las oficinas de la DDC Cusco?

Copiar

5 respuestas

9- ¿Cuál es el problema de internet que se presenta con más frecuencia?

4 respuestas

Caidas de red.

Falta de cableado estructurado en los edificios alquilados

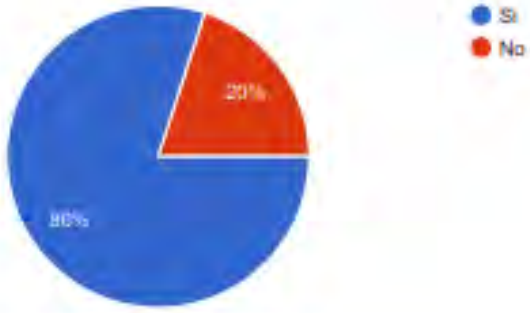
Casos fortuitos

En la sede de machupicchu hay cortes de luz y a raiz de los derrumbes existe muchas veces fracturas de fibra.

10- ¿Se cuenta con algún servicio de internet de respaldo?

Copiar

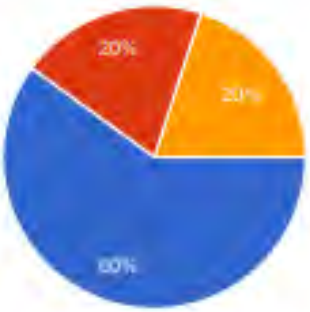
5 respuestas



11- ¿El internet de respaldo es simétrico?

Copiar

5 respuestas



- Si
- No
- No se cuenta con un servicio de internet de respaldo

12- ¿Cuál es la velocidad de internet de respaldo?

Copiar

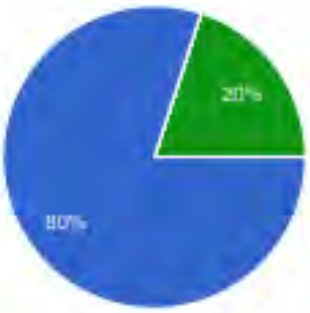
5 respuestas

- 50 mbps
- 100 mbps
- 200 mbps
- 300 mbps
- No se cuenta con un servicio de internet de respaldo
- 350 Mbps
- Se sugiere orientar esta pregunta al subárea de redes.

13- El servicio de internet de respaldo que utilizan en las oficinas de la DDC Cusco es adquirida mediante:

Copiar

5 respuestas

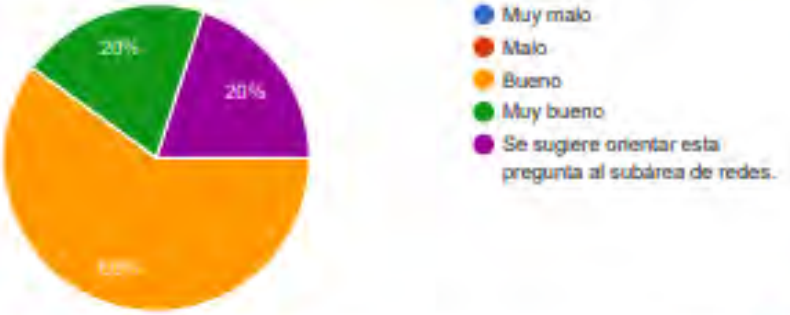


- Fibra óptica
- Satelital
- Coaxial
- Se sugiere orientar esta pregunta al subárea de redes.

14- Cómo califica la llegada de internet de respaldo en las oficinas de la DDC cusco

Copiar

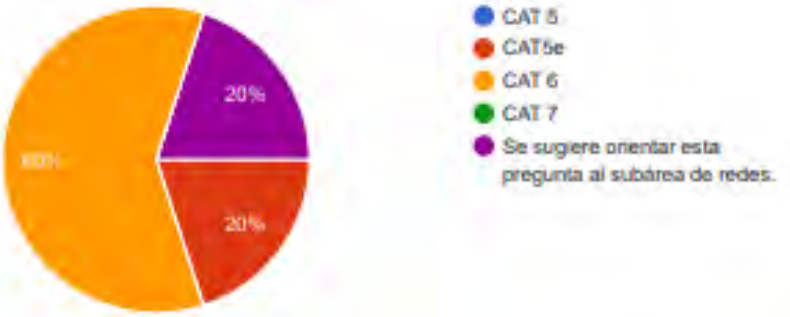
5 respuestas



15- ¿Con que categoria de cable de red cuenta ?

Copiar

5 respuestas

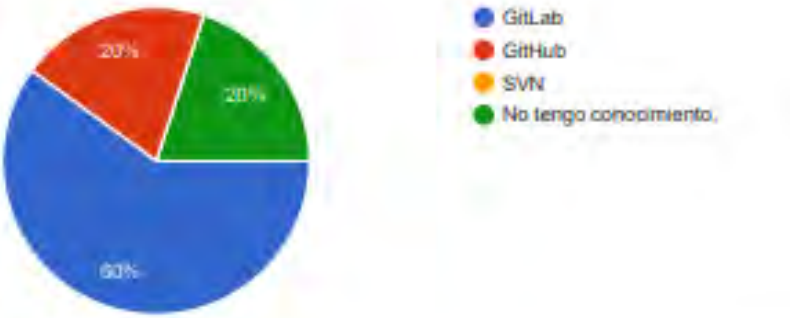


f) Soportes de Información

1- ¿En qué tipo de repositorio guardan su código fuente trabajado de manera personal en el área funcional de informática y telecomunicaciones?

Copiar

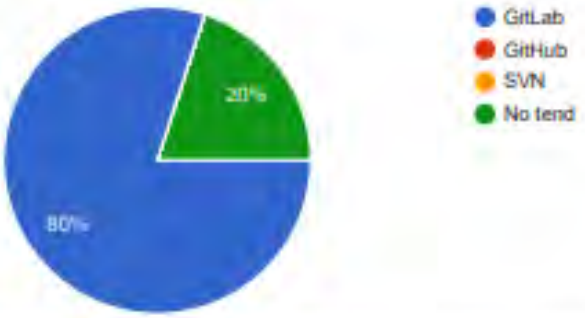
5 respuestas



2- ¿En qué tipo de repositorio guardan su código fuente trabajado de manera grupal en el área funcional de informática y telecomunicaciones

Copiar

5 respuestas



3- En caso de que el código fuente guardado se pierda o tenga un inconveniente, ¿Tienen alguna copia de seguridad o respaldo?

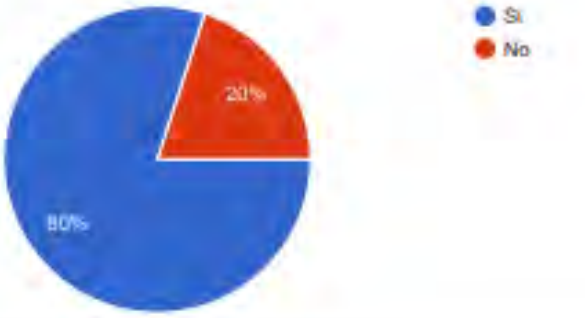
Copiar

5 respuestas

4- ¿Se tiene guardado ese respaldo de código fuente en un data center?

Copiar

5 respuestas



5- ¿Con qué frecuencia recibe mantenimiento el data center? Copiar

5 respuestas

6- ¿Quién proporciona los servicios de mantenimiento del data center a la institución? Copiar

5 respuestas

7- ¿Se utiliza USB para compartir algún tipo de información? Copiar

5 respuestas

h) Equipamiento Auxiliar

1- ¿Cuentan con data center?

Copiar

5 respuestas

2- ¿Cuentan con generador eléctrico?

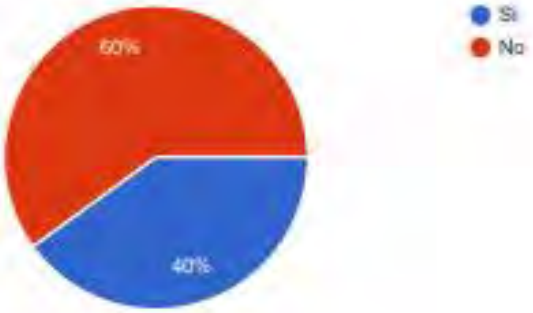
Copiar

5 respuestas

3- ¿Cuentan con un UPS de alimentación de emergencia por computadora de escritorio?

Copiar

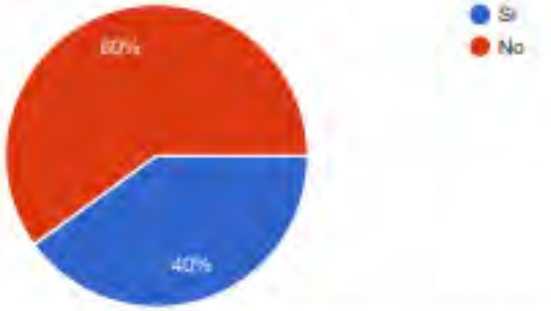
5 respuestas



Copiar

4- ¿Cuentan con aire acondicionado en las oficinas de la DDC Cusco?

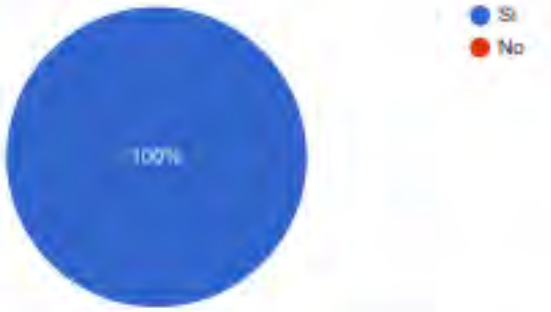
5 respuestas



Copiar

5- ¿Cuentan con mobiliarios (armarios, estantes, cajas fuertes) donde guardan información física o equipos informáticos?

5 respuestas



Copiar

6- ¿Cuentan con equipos de destrucción de soportes de información?

5 respuestas

7- ¿Qué tipo de equipo de destrucción de soportes de información utilizan?

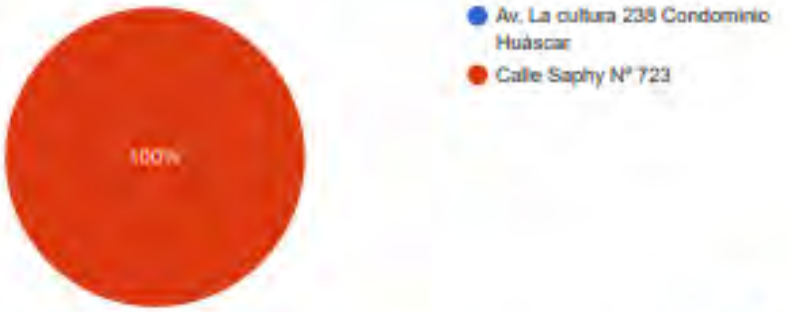
0 respuestas

Aún no hay respuestas para esta pregunta.

i) Instalaciones

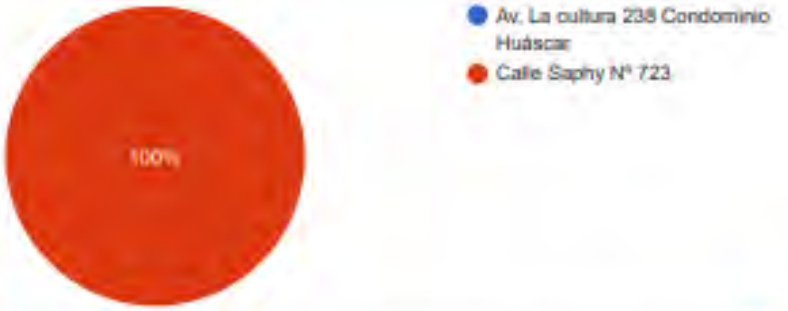
1- ¿En qué local se encuentra ubicado el data center? Copiar

5 respuestas



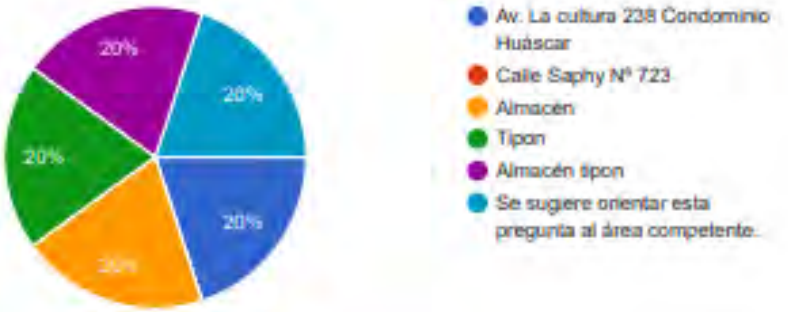
2- ¿En qué local se encuentra la fuente de alimentación de emergencia (generador eléctrico) Copiar

5 respuestas



3- ¿En qué local se almacenan los equipos informáticos en desuso o nuevos? Copiar

5 respuestas



j) Personal

1- ¿Cuántas personas trabajan en el local?

5 respuestas

6

–

12

Se sugiere orientar esta pregunta al área competente.

2- Dentro del subárea de desarrollo de software, ¿Quiénes lo conforman?

5 respuestas

4

Profesionales técnicos

Programdores

6

5 ingenieros de sistemas.

3- Dentro del subárea de soporte técnico, ¿Quiénes lo conforman?

4 respuestas

2

Tecnicos informaticos

5

Se sugiere orientar esta pregunta al subárea de soporte.

4- Dentro del subárea de redes, ¿Quiénes lo conforman?

4 respuestas

4

Ing. de Sistemas

1 y otro de apoyo parcial

Se sugiere orientar esta pregunta al subárea de redes.

Anexo 2: Encuesta al personal de la Dirección Desconcentrada de Cultura de Cusco

Encuesta

Somos bachilleres de la carrera
Ingeniería Informática y de Sistemas de la Universidad Nacional de San Antonio Abad del Cusco, para la elaboración de nuestra tesis necesitamos recabar información por medio de las siguientes preguntas en el cual cada usuario debe llenar de manera responsable. Solicitando su colaboración, para poder recolectar datos requeridos en la realización del proyecto de tesis denominado: **"Propuesta de implementación de la NTP-ISO/IEC 27005:2018 aplicando la metodología MAGERIT para el Área Funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco"**, el cual tiene como objetivo: **identificar, evaluar y clasificar los riesgos, amenazas y vulnerabilidades que puedan existir dentro de la Dirección Desconcentrada de Cultura del Cusco,** donde realizaremos la recolección de datos como primera fase la cual consiste en poder identificar la información y equipamiento informático pertenecientes a la institución y de esa forma evaluar y clasificar y realizar una valoración de los riesgos y/o amenazas que se puedan encontrar.
Atentamente:

Alexander Pavel Ibarra Huaman

Sharom Mitchel Nolazco Sandoval

* Indica que la pregunta es obligatoria

1. Correo *

2. NOMBRES *

3. APELLIDOS *

4. AREA LABORAL *

5. PROFESIÓN *

6. CARGO QUE DESEMPEÑA *

7. TELÉFONO *

8. CORREO ELECTRÓNICO *

Salta a la pregunta 9

A- DATOS

Datos: conjunto de letras, números y/o símbolos.
En este sección se va a recabar toda la información(es la unión de datos que forma un mensaje o mensajes) que manejan en el área de trabajo

9. 1- ¿Qué tipo de información manejan? *

Selecciona todos los que correspondan.

- [ ] Información confidencial o clasificada (Información de carácter privado de acceso a un número limitado de personas)
- [ ] Información pública (Información de acceso general)
- [ ] Información del personal (Información de cada persona como: DNI, nombre, dirección, etc)
- [ ] Información interna (Información compartida con los trabajadores de la institución)
- [ ] Información externa (Información compartida con otras instituciones)
- [ ] Otro:

10. 2.- Con respecto a la pregunta 1 según su área de trabajo. ¿Ud hace uso de información publica? *

Marca solo un óvalo.

- Si
- No

11. 3.- Con respecto a la pregunta 1 según su área de trabajo. ¿Ud hace uso de información privada? *

Marca solo un óvalo.

- Si
- No

12. 4- ¿Qué tipo de datos manejan según su área de trabajo? *

Selecciona todos los que correspondan.

- [ ] Inventario de bienes e inmuebles
- [ ] Registro de asistencia
- [ ] Documentos administrativos
- [ ] Otro: _____

13. 5- ¿En que tipo o tipos de formato maneja usted su información? *

Selecciona todos los que correspondan.

- [ ] PDF
- [ ] Word
- [ ] Excel
- [ ] Power Point
- [ ] Otro: _____

14. 6- ¿El área en el que está laborando cuenta con una base de datos del personal? *

Marca solo un óvalo.

- Verdadero
- Falso
- Otro: _____

Salta a la pregunta 15

B- CLAVES CRIPTOGRÁFICAS

Son contraseñas para proteger la información.

15. 5- ¿Maneja alguna contraseña para ingresar a su computadora? *

Marca solo un óvalo.

- Si
- No

16. 6- ¿Con qué frecuencia cambia su contraseña de su computadora? *

Marca solo un óvalo.

- Nunca
- Cada mes
- Cada 6 meses
- Una vez al año
- Otro: _____

17. 7- ¿Comparte con algún otro trabajador su acceso con respecto a su correo web institucional? *

Marca solo un óvalo.

- Si
- No
- Otro: _____

18. 8- ¿Comparte con algún otro trabajador su acceso con respecto a SIGA(Sistema Integrado de Gestión Administrativa)? *

Marca solo un óvalo.

- Si
- No
- Otro: _____

19. 9- ¿Comparte con algún otro trabajador su acceso con respecto a SGD(Sistema de Gestión Documental)? *

Marca solo un óvalo.

- Si
- No
- Otro: _____

20. 10- De acuerdo a las preguntas anteriores ¿Comparte con algún otro trabajador su acceso con respecto a otra plataforma? *

_____

_____

_____

_____

_____

Salta a la pregunta 21

C- SERVICIOS

Función que ayuda a las necesidades de los usuarios o persona externa

21. 11- ¿Qué tipo de servicios ofrecen para el público? *

Selecciona todos los que correspondan.

- [ ] Atención al público
- [ ] Reservas de ticktes y/o boletos
- [ ] Consultas web
- [ ] Otro: _____

22. 12- ¿Su computadora recibe mantenimiento periódicamente? *

Marca solo un óvalo.

- ◯ Si
- ◯ No

23. 13- ¿Cuentan con soporte técnico? *

Marca solo un óvalo.

- ◯ Si
- ◯ No

24. 14- Que calificación darías a atención en soporte técnico? *

Marca solo un óvalo.

- ◯ Muy malo
- ◯ Mala
- ◯ Bueno
- ◯ Muy bueno

Salta a la pregunta 25

D- SOFTWARE- APLICACIONES INFORMÁTICAS

SOTWARE: Programa que se usan en la computadora.

25. 15- ¿Su computadora cuenta con un antivirus? *

Marca solo un óvalo.

- ◯ Si
- ◯ No

26. 16- Con respecto a la pregunta anterior ¿Puede decirnos que tipo de software de seguridad cuenta (antivirus)? *

Selecciona todos los que correspondan.

- ☐ ESET
- ☐ Avast
- ☐ MCAfee
- ☐ Otro: _____

27. 17- ¿Tiene conocimiento si el antivirus de su computadora esta activo (licencia vigente)? *

Marca solo un óvalo.

- ◯ Sí
- ◯ No

28. 18- ¿Cuentan con software de manejo de información institucional? *

Selecciona todos los que correspondan.

- [ ] Correo web institucional
- [ ] SIGA(Sistema Integrado de Gestión Administrativa)
- [ ] SGD(Sistema de Gestión Documental)
- [ ] Otro: _____

29. 19- ¿Su computadora cuentan con programas de uso de escritorios remotos? *

Marca solo un óvalo.

- ◯ Sí
- ◯ No

30. 20- Con respecto a la pregunta anterior, indique que programas de uso de escritorios remotos utiliza? *

Selecciona todos los que correspondan.

- [ ] Team Viewer
- [ ] Any Desk

Salta a la pregunta 31

E- SOPORTES DE INFORMACIÓN

Son dispositivos físicos y/o virtuales que permiten almacenar información de forma permanente, o largos periodos de tiempo.

31. 21- ¿De qué manera guardan la información física? *

Selecciona todos los que correspondan.

- [ ] Papeles
- [ ] Archivadores
- [ ] Folder catalogo
- [ ] Folder manila
- [ ] Folder plastificado
- [ ] Folder con sujetador
- [ ] Otro: _____

32. 22- ¿De qué manera guardan la información digital? *

Selecciona todos los que correspondan.

- [ ] USB
- [ ] CD
- [ ] DVD
- [ ] Tarjetas de memoria (SD, microSD, etc.)
- [ ] Disco duro
- [ ] Google Drive
- [ ] One Drive
- [ ] Computadora personal
- [ ] Computadora de oficina
- [ ] Otro: _____

F. EQUIPAMIENTO AUXILIAR

Se consideran otros equipos que sirven de soporte a los sistemas de información (

conjunto de elementos que interactúan entre sí con un fin común, que permite que la información esté disponible para satisfacer las necesidades en una organización)

33. 23- ¿Tiene acceso a internet? *

Marca solo un óvalo.

- Si
- No

34. 24- ¿Qué tan buena es la conexión (es estable sin cortes) de internet en tu computadora? *

Marca solo un óvalo.

- Si
- No

35. 25- ¿Qué tan buena es la velocidad (velocidad en la que carga al entrar a una página web) de internet en tu computadora? *

Marca solo un óvalo.

- Si
- No

*Salta a la sección 8 (**GRACIAS POR RESPONDER LA ENCUESTA**)*

GRACIAS POR RESPONDER LA ENCUESTA

Anexo 3: Políticas

- Políticas para el uso seguro de aplicaciones de mensajería instantánea en el área funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco
- Políticas para el manejo seguro de información clasificada en el área funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco
- Políticas disciplinarias para incidentes de seguridad de la información en el área funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco
- Políticas para una adecuada gestión de contraseñas en el área funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco
- Políticas sobre la contratación de software a terceros en el área funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco
- Políticas de desarrollo, mantenimiento de software en el área funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco
- Políticas sobre el correcto manejo de equipos informáticos (hardware, software) de la Dirección Desconcentrada de Cultura de Cusco
- Políticas sobre la descarga no controlada de software de la Dirección Desconcentrada de Cultura de Cusco
- Políticas para la asignación de derechos de acceso, limitación y uso de cuentas en plataformas en el área funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco
- Políticas disciplinarias para incidentes con el cuidado de activos de la Dirección Desconcentrada de Cultura de Cusco
- Políticas en contra de la ingeniería social de la Dirección Desconcentrada de Cultura de Cusco
- Políticas de Derechos de Autor de la Dirección Desconcentrada de Cultura de Cusco

Políticas para el uso seguro de aplicaciones de mensajería instantánea en el área funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco

1. Autorización de Aplicaciones

a. Política:

-Establecer el tipo de aplicación de mensajería instantánea.

b. Procedimiento:

-Solo se permitirá el uso de aplicaciones de mensajería instantánea autorizadas y aprobadas por el área funcional de Informática y Telecomunicaciones.

- correo electrónico institucional
- WhatsApp (meta) institucional

-Cualquier nueva aplicación debe ser revisada y aprobada antes de su implementación.

2. Clasificación de la Información

a. Política:

-La información debe ser clasificada antes de compartirla a través de aplicaciones de mensajería.

b. Procedimiento:

Los usuarios deben clasificar la información identificando si es confidencial, interna o pública.

-La información confidencial sólo deberá ser compartida a través del correo electrónico institucional

- La información interna o pública puede ser compartida a través de los medios de mensajería instantáneos autorizados.

3. Encriptación y Seguridad

a. Política:

-Implementar métodos de seguridad para proteger la información.

b. Procedimiento:

-Se exigirá el uso de aplicaciones de mensajería instantánea que implementen encriptación de extremo a extremo para proteger la confidencialidad de la información.

-Se realizarán auditorías periódicas para garantizar el cumplimiento de estas medidas de seguridad.

4. Gestión de Cuentas

a. Política:

-Establecer directrices claras para la gestión de cuentas de acceso.

b. Procedimiento:

-Se fomentará el uso de cuentas oficiales y corporativas para las comunicaciones laborales.

-Los empleados deben informar de inmediato cualquier actividad sospechosa o pérdida de credenciales asociadas con sus cuentas de mensajería.

5. Auditorías y Supervisión

a. Política:

-Realizar auditorías y supervisiones regulares de manera controlada.

b. Procedimiento:

-Se implementarán herramientas de auditoría y supervisión para rastrear las actividades en las aplicaciones de mensajería instantánea utilizadas en el ámbito laboral.

-Estas auditorías se realizarán de manera regular, y los empleados deben ser conscientes de que sus comunicaciones pueden ser revisadas con fines de seguridad.

6. Capacitación Continua

a. Política:

-Brindar capacitaciones sobre el uso seguro de aplicaciones de mensajería instantánea.

b. Procedimiento:

Se proporcionará formación regular sobre las políticas de seguridad de la información y el uso adecuado de las aplicaciones de mensajería.

Los empleados deben estar al tanto de los riesgos asociados con la fuga de información clasificada y conocer las mejores prácticas para prevenir tales incidentes.

7. Comunicación Transparente

a. Política:

-La comunicación transparente es fundamental para una respuesta rápida y efectiva a posibles amenazas.

b. Procedimiento:

Los usuarios deben informar inmediatamente sobre cualquier incidente de seguridad, pérdida de dispositivo o sospecha de fuga de información.

8. Gestión de Dispositivos Móviles

a. Políticas:

-Establecer directrices claras para la gestión de dispositivos móviles.

b. Procedimiento:

-Implementar la adquisición de dispositivos móviles para el uso de una cuenta de WhatsApp institucional por personal

-Los dispositivos móviles institucionales y las aplicaciones de mensajería instaladas en estos estarán sujetos a auditorías y supervisión periódicas por parte del departamento de TI

Implementar medidas de seguridad en dispositivos móviles, como bloqueo remoto y borrado de datos en caso de pérdida o robo.

Políticas para el manejo seguro de información clasificada en el área funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco

1. Identificación y resguardo

a. Política:

-Todo documento o dato que contenga información clasificada debe ser debidamente identificado y resguardado.

b. Procedimiento:

Los usuarios deben clasificar la información identificando si es confidencial, interna o pública.

-La información confidencial sólo deberá ser compartida a través del correo electrónico institucional

- La información interna o pública puede ser compartida a través de los medios de mensajería instantáneos autorizados

2. Control de Acceso

a. Política:

- Implementar un sistema de control de acceso para garantizar la seguridad de la información clasificada.

b. Procedimiento:

-Se implementarán métodos de acceso basados en roles, garantizando que solo aquellos con la autorización adecuada tengan acceso a la información clasificada.

-Se revisarán y actualizarán regularmente los privilegios de acceso de acuerdo con los cambios en la estructura organizativa y las responsabilidades laborales.

3. Registro de Acceso

a. Política:

- Implementar un registro de acceso para rastrear y auditar las actividades de los usuarios.

b. Procedimiento:

-Se mantendrá un registro detallado de cada acceso a la información clasificada, incluyendo quién accedió, cuándo y con qué propósito.

-Los registros serán revisados periódicamente para identificar cualquier actividad sospechosa.

4. Protección contra Escape de Información

a. Políticas:

-Implementar medidas de seguridad digital para prevenir el escape no autorizado de información clasificada.

b. Procedimiento:

-Utilizar métodos de autenticación fuertes para asegurar que solo usuarios legítimos tengan acceso.

-Establecer protocolos claros y procedimientos de respuesta a incidentes en caso de que se detecte una fuga de información clasificada.

-Implementar medidas de seguridad física, como acceso restringido al área funcional de Informática y Telecomunicaciones.

-Encriptación de soportes de almacenamiento.

5. Destrucción Segura

a. Política:

-Los documentos o medios que contengan información clasificada y ya no sean necesarios serán destruidos de manera segura.

b. Procedimiento:

-Se aplicarán métodos de eliminación segura como:

- Borrado seguro
- Formateo seguro
- Eliminación física de dispositivos

6. Abuso de Privilegios de Acceso

a. Política

-El acceso a la información confidencial está sujeto a restricciones y seguimiento.

b. Procedimiento:

-El abuso de privilegios de acceso será tratado como una violación grave.

-Se realizarán auditorías regulares para detectar y prevenir posibles abusos, y las sanciones por violaciones se aplicarán de manera consistente.

7. Capacitación Continua

a. Política:

-Brindar capacitaciones sobre el manejo seguro de información clasificada.

b. Procedimiento:

-Todos los empleados que manejen información clasificada deberán recibir formación continua sobre las políticas y procedimientos de seguridad.

-La formación incluirá pautas específicas sobre el manejo adecuado de la información clasificada y la conciencia sobre las consecuencias de su mal uso.

8. Modificación Deliberada de la Información

a. Política:

- La modificación deliberada de la información puede dar lugar a sanciones disciplinarias encargadas por la autoridad competente de acuerdo a la gravedad del hecho.

b. Procedimiento:

- Establecer un proceso claro y equitativo para investigar y abordar el caso.
- Aplicar sanciones de manera consistente y proporcional a la gravedad de la violación.

9. Divulgación de Información

a. Política:

- La divulgación de la información puede dar lugar a sanciones disciplinarias encargadas por la autoridad competente de acuerdo a la gravedad del hecho.

b. Procedimiento:

- Establecer un proceso claro y equitativo para investigar y abordar el caso.
- Aplicar sanciones de manera consistente y proporcional a la gravedad de la violación.

Políticas disciplinarias para incidentes de seguridad de la información en el área funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco

1. Escapes de Información

a. Política:

- El personal responsable de la filtración de información confidencial estará sujeto a acciones disciplinarias.

b. Procedimiento:

- Investigación interna para determinar la causa y el alcance.
- Acciones disciplinarias proporcionales a la gravedad del incidente.
- Colaboración con las autoridades legales según sea necesario.

2. Destrucción de Información (Errores y fallos no intencionados)

a. Política:

- Se espera que el personal responsable notifique inmediatamente cualquier destrucción accidental de información.

b. Procedimiento:

- Investigación para comprender la naturaleza del error.
- Acciones correctivas y acciones disciplinarias en casos de negligencia.

3. Abuso de Privilegios de Acceso

a. Política:

- El acceso a la información confidencial está sujeto a restricciones y monitoreo.

b. Procedimiento:

- Revisión de privilegios de acceso y actividades relacionadas.
- Acciones disciplinarias proporcionales, desde capacitación hasta sanciones, según la intencionalidad y repetición.

4. Modificación Deliberada de la Información

a. Política:

- Cualquier modificación no autorizada de datos está estrictamente prohibida.

b. Procedimiento:

- Identificación de la modificación y restauración de datos.
- Acciones disciplinarias, incluida sanciones rígidas según lo permitido por la ley, en casos graves.

5. Destrucción de Información (Ataques Intencionados)

a. Política:

- Atacar o destruir intencionadamente información resultará en acciones disciplinarias severas.

b. Procedimiento:

- Colaboración con equipos de seguridad para rastrear el origen del ataque.
- Acciones disciplinarias legales y administrativas según lo permitido por la ley.

6. Fugas de Información

a. Política:

- Cualquier intento de exfiltración de datos será tratado con seriedad.

b. Procedimiento:

- Detección temprana y mitigación de fugas.
- Acciones disciplinarias, incluida sanciones rígidas, junto con medidas legales según sea necesario.

7. Divulgación de Información

a. Política:

- La divulgación no autorizada de información confidencial será sancionada.

b. Procedimiento:

- Investigación para determinar la intencionalidad y el alcance.
- Acciones disciplinarias y medidas correctivas, incluida la formación adicional sobre la importancia de la confidencialidad.

Políticas para una adecuada gestión de contraseñas en el área funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco

1. Contraseñas Fuertes

a. Política:

- Se requiere el uso de contraseñas fuertes y se deben cambiar regularmente.
- Sólo se permite compartir contraseñas dentro del área funcional de Informática y Telecomunicaciones

b. Procedimiento:

- Auditorías regulares para evaluar la complejidad y el cambio periódico de contraseñas.
- Formación sobre la importancia de contraseñas sólidas y la gestión segura de las mismas.

2. Escapes de Información

a. Política:

- El personal es responsable de proteger sus credenciales de acceso(contraseñas).

b. Procedimiento:

- Investigación interna para determinar cómo se produjo el escape de información.
- Acciones disciplinarias en caso de negligencia o incumplimiento de políticas.

3. Alteración Accidental de la Información

a. Política:

- Se deben tomar precauciones adicionales al manipular datos críticos.

b. Procedimiento:

- Revisión de procesos y procedimientos para prevenir alteraciones accidentales.
- Acciones disciplinarias proporcionales a la gravedad del incidente.

4. Destrucción de Información (Errores y Fallos No Intencionados)

a. Política:

- Se prohíbe la eliminación de información sin la debida autorización.

b. Procedimiento:

- Revisiones de actividades para detectar eliminaciones no autorizadas.
- Acciones disciplinarias y medidas correctivas según la gravedad.

5. Fugas de Información

a. Política:

- Reportar inmediatamente cualquier sospecha de fuga de información.

b. Procedimiento:

- Procedimientos claros para la notificación de fugas de información.
- Acciones disciplinarias según el grado de colaboración y cumplimiento.

6. Abuso de Privilegios de Acceso

a. Política:

- El acceso a datos sensibles está restringido y monitorizado.

b. Procedimiento:

- Auditorías periódicas de privilegios de acceso.
- Acciones disciplinarias, incluyendo la revocación de privilegios en casos de abuso.

7. Acceso No Autorizado

a. Política:

- El acceso a sistemas y datos está limitado a personal autorizado.

b. Procedimiento:

- Monitoreo constante de intentos de acceso no autorizado.
- Acciones disciplinarias y medidas legales según sea necesario.

Políticas sobre la contratación de software a terceros en el área funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco

Para garantizar una adquisición segura y eficaz, es importante establecer políticas claras que aborden el proceso antes, durante y después de la contratación.

Antes de la Contratación:

- Evaluación de Necesidades:

  Antes de buscar software externo, realiza una evaluación exhaustiva de las necesidades y requisitos específicos de la institución.

-Análisis de Riesgos:

  Realiza una evaluación de riesgos para identificar posibles amenazas a la seguridad, privacidad y cumplimiento normativo asociadas con el software.

-Investigación del Proveedor:

  Investiga a fondo a los proveedores de software potenciales, considerando su reputación, experiencia, seguridad y estabilidad financiera.

-Cumplimiento Normativo:

  Asegúrate de que el software cumpla con los estándares y regulaciones relevantes de la institución y la empresa.

-Contratos y Acuerdos:

  Establece contratos claros y acuerdos de nivel de servicio (SLA) que incluyan cláusulas sobre seguridad, mantenimiento, actualizaciones y términos de rescisión.

Durante la Contratación:

-Pruebas y Evaluación:

  Realiza pruebas piloto o evaluaciones para asegurarte de que el software cumple con los requisitos técnicos y funcionales de la institución.

-Seguridad y Privacidad:

  Asegúrate de que el software cumpla con los estándares de seguridad y privacidad de la institución. Realiza evaluaciones de seguridad si es necesario.

-Formación del Personal:

Proporciona formación adecuada al personal que utilizará el nuevo software para garantizar un uso eficiente y seguro.

-Gestión de Cambios:

Implementa un plan de gestión de cambios para minimizar interrupciones y resistencia por parte de los usuarios.

-Monitoreo Continuo:

Establece un sistema de monitoreo continuo para evaluar el rendimiento y la seguridad del software después de la implementación.

Después de la Contratación:

-Soporte Continuo:

Asegúrate de que el proveedor ofrezca soporte continuo para abordar problemas técnicos y actualizaciones de seguridad.

-Gestión de Riesgos Continua:

Mantén una gestión de riesgos continua para identificar y abordar nuevas amenazas o vulnerabilidades que puedan surgir.

-Actualizaciones y Parches:

Implementa regularmente actualizaciones y parches de seguridad proporcionados por el proveedor para mantener el software protegido contra nuevas vulnerabilidades y/o amenazas.

-Auditorías Periódicas:

Realiza auditorías periódicas de seguridad y rendimiento para garantizar que el software siga cumpliendo con los estándares y requisitos de la institución.

-Evaluación de Resultados:

Evalúa regularmente el rendimiento del software en relación con los objetivos de la institución y la satisfacción del usuario.

Al seguir estas políticas a lo largo del ciclo de vida de la contratación de software de terceros, una empresa puede minimizar riesgos y maximizar los beneficios de la nueva adquisición.

Políticas de desarrollo, mantenimiento de software en el área funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco

1. Ciclo de Vida del Desarrollo de Software

a. Política:

- Se debe seguir un enfoque estructurado del ciclo de vida del desarrollo de software, que incluya fases de planificación, diseño, implementación, prueba y despliegue.

b. Procedimiento:

- Establecer procesos formales para cada fase del ciclo de vida del desarrollo.
- Realizar revisiones regulares para evaluar y mejorar el proceso.

2. Gestión de Proyectos

a. Política:

- Adoptar metodologías de gestión de proyectos, como Agile o Scrum, para optimizar la eficiencia y la entrega de resultados.

b. Procedimiento:

- Asignar roles y responsabilidades claras en cada proyecto.
- Utilizar herramientas de gestión de proyectos para el seguimiento del progreso y la colaboración del equipo.

3. Estándares de Desarrollo

a. Política:

- El código debe seguir estándares de desarrollo acordados, garantizando consistencia y facilitando el mantenimiento futuro.

b. Procedimiento:

- Realizar revisiones de código periódicas para garantizar la adhesión a los estándares.
- Proporcionar capacitación regular sobre las mejores prácticas de codificación.

4. Seguridad del Software

a. Política:

- La seguridad del software debe ser una prioridad, integrando prácticas de seguridad desde las fases iniciales del desarrollo.

b. Procedimiento:

- Realizar análisis de riesgos de seguridad y pruebas regulares.
- Implementar prácticas de desarrollo seguro y garantizar el cumplimiento de estándares de seguridad.

5. Mantenimiento y Actualización

a. Política:

- Se debe implementar un plan de mantenimiento proactivo para garantizar que el software esté actualizado y funcione correctamente con el tiempo.

b. Procedimiento:

- Establecer ciclos regulares de actualización y parches.
- Monitorear proactivamente la salud del software y corregir problemas identificados.

6. Gestión de Configuración

a. Política:

- Se deben establecer prácticas de gestión de configuración para rastrear y controlar cambios en el software.

b. Procedimiento:

- Utilizar sistemas de control de versiones para gestionar cambios en el código y otros artefactos.
- Mantener registros detallados de cambios y versiones.

7. Documentación

a. Política:

- La documentación completa y actualizada es esencial para facilitar el mantenimiento y la comprensión del software.

b. Procedimiento:

- Requerir documentación detallada para el código, diseño y procedimientos de despliegue.
- Mantener manuales de usuario y documentación técnica actualizados.

8. Evaluación de Desempeño

a. Política:

- Implementar métricas de evaluación de desempeño para medir la calidad y eficiencia del desarrollo de software.

b. Procedimiento:

- Realizar revisiones de desempeño periódicas y ajustar los procesos según los resultados.
- Utilizar métricas para identificar áreas de mejora continua.

Políticas sobre el correcto manejo de equipos informáticos (hardware, software) de la Dirección Desconcentrada de Cultura de Cusco

1. Adquisición y Mantenimiento del Hardware

a. Política:

- La adquisición de hardware debe basarse en requisitos específicos.

b. Procedimiento:

- Realizar evaluaciones regulares de las necesidades de hardware.
- Establecer un programa de mantenimiento preventivo para prolongar la vida útil de los equipos.

2. Instalación y Configuración del Software

a. Política:

- Solo se deben instalar y configurar software licenciado y autorizado.

b. Procedimiento:

- Mantener un inventario actualizado de software instalado.
- Asegurarse de que la instalación cumpla con los requisitos de seguridad y políticas internas.

3. Actualizaciones y Parches

a. Política:

- Todos los sistemas deben estar actualizados con los últimos parches de seguridad y actualizaciones de software.

b. Procedimiento:

- Implementar un programa de actualización periódico para aplicar parches y actualizaciones.
- Realizar pruebas antes de aplicar actualizaciones críticas.

4. Seguridad del Hardware y Software

a. Política:

- Implementar medidas de seguridad física y lógica para proteger tanto el hardware como el software.

b. Procedimiento:

- Utilizar sistemas de autenticación robustos y controles de acceso físico.
- Realizar auditorías de seguridad de forma regular.

5. Gestión de Contraseñas

a. Política:

- Establecer directrices claras para la gestión de contraseñas seguras y cambiarlas regularmente.

b. Procedimiento:

- Educar a los usuarios sobre la importancia de proteger sus contraseñas.

6. Gestión de Inventarios

a. Política:

- Mantener inventarios precisos de hardware y software.

b. Procedimiento:

- Utilizar herramientas de gestión de activos para rastrear equipos y licencias de software.
- Actualizar el inventario después de cada cambio significativo.

7. Uso Aceptable de Recursos

a. Política:

- Establecer directrices claras sobre el uso aceptable de los recursos informáticos.

b. Procedimiento:

- Informar a los empleados sobre las políticas de uso aceptable.
- Monitorear el uso de recursos y tomar medidas correctivas según sea necesario.

8. Capacitación del Personal

a. Política:

- Proporcionar capacitación regular sobre el manejo adecuado de equipos informáticos.

b. Procedimiento:

- Ofrecer sesiones de formación sobre las políticas y procedimientos.
- Mantener al personal informado sobre las últimas amenazas de seguridad y mejores prácticas.

9. Eliminación Segura

a. Política:

- Establecer procedimientos para la eliminación segura de hardware y datos obsoletos.

b. Procedimiento:

- Realizar un borrado seguro de datos antes de deshacerse de los dispositivos.
- Cumplir con los requisitos legales y medioambientales para la eliminación de equipos.

Políticas sobre la descarga no controlada de software de la Dirección Desconcentrada de Cultura de Cusco

1. Aprobación Previa

a. Política:

- Todo software debe ser aprobado por el área funcional de Informática y Telecomunicaciones antes de ser descargado e instalado en los sistemas de la institución.

b. Procedimiento:

- Establecer un proceso formal para solicitar y obtener la aprobación de nuevos programas.
- Designar un punto de contacto en el área funcional de Informática y Telecomunicaciones para gestionar las solicitudes.

2. Lista de Software Aprobado

a. Política:

- Mantener una lista actualizada de software aprobado para uso en la institución.

b. Procedimiento:

- Revisar y actualizar regularmente la lista de software aprobado.
- Proporcionar acceso fácil a la lista a todo el personal de la institución.

3. Restricciones de Privilegios

a. Política:

- Restringir los privilegios de instalación de software a usuarios autorizados.

b. Procedimiento:

- Configurar sistemas para que solo el área funcional de Informática y Telecomunicaciones tengan la potestad de instalar software.
- Establecer procedimientos para solicitar privilegios temporales cuando sea necesario.

4. Monitoreo de Actividades

a. Política:

- Monitorear las actividades relacionadas con la descarga e instalación de software para detectar comportamientos inusuales.

b. Procedimiento:

- Implementar herramientas de monitoreo y auditoría de sistemas.
- Revisar regularmente los registros para identificar posibles descargas no controladas.

5. Educación y Concientización

a. Política:

- Educar a los empleados sobre los riesgos asociados con la descarga no controlada de software.

b. Procedimiento:

- Proporcionar formación regular sobre la importancia de seguir las políticas de descarga de software.
- Destacar los riesgos de seguridad y las consecuencias de incumplir las políticas.

6. Sanciones por Incumplimiento

a. Política:

- Establecer consecuencias claras para el incumplimiento de las políticas de descarga de software.

b. Procedimiento:

- Aplicar sanciones proporcionales a la gravedad del incumplimiento.
- Garantizar la consistencia en la aplicación de sanciones para todo el personal de la institución.

7. Actualizaciones y Parches

a. Política:

- Todas las actualizaciones y parches de software deben gestionarse a través de procesos formales.

b. Procedimiento:

- Notificar a los usuarios sobre las actualizaciones y parches aprobados.
- Establecer un programa regular de aplicación de actualizaciones para mantener la seguridad y la compatibilidad.

8. Cumplimiento Legal y Licencias

a. Política:

- Cumplir con todas las leyes de propiedad intelectual y requisitos de licencia asociados con el software.

b. Procedimiento:

- Realizar auditorías periódicas para garantizar el cumplimiento de las licencias.
- Mantener registros precisos de las licencias de software utilizadas.

Políticas para la asignación de derechos de acceso, limitación y uso de cuentas en plataformas en el área funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco

1. Asignación de Derechos de Acceso

a. Política:

- La asignación de derechos de acceso debe basarse en el principio de menor privilegio, otorgando solo los permisos necesarios para realizar las funciones laborales.

b. Procedimiento:

- Realizar evaluaciones periódicas para revisar y ajustar los derechos de acceso según las responsabilidades del usuario.
- Documentar y aprobar formalmente cualquier cambio en los privilegios de acceso.

2. Control y Supervisión de Accesos

a. Política:

- Implementar sistemas de control y supervisión de accesos para rastrear y auditar las actividades de los usuarios.

b. Procedimiento:

- Monitorear regularmente los registros de acceso para detectar patrones inusuales o actividades sospechosas.
- Realizar auditorías internas y externas periódicas para evaluar la eficacia de los controles de acceso.

3. Limitación de Privilegios de Administrador

a. Política:

- Restringir el acceso de administrador solo a las personas que necesitan esos privilegios para cumplir con sus funciones laborales.

b. Procedimiento:

- Implementar un sistema de aprobación formal para otorgar y revocar privilegios de administrador.
- Monitorear y auditar regularmente las actividades de los administradores.

4. Cambios en la Configuración del Sistema

a. Política:

- Todos los cambios en la configuración del sistema deben seguir un proceso formal y documentado.

b. Procedimiento:

- Realizar pruebas y evaluaciones de impacto antes de implementar cambios en la configuración.
- Documentar y revisar todos los cambios en la configuración del sistema.

5. Destrucción de Información

a. Política:

- Establecer procedimientos claros para la eliminación segura de información confidencial y registros.

b. Procedimiento:

- Utilizar métodos seguros para eliminar o destruir datos, como la sobrescritura segura o la destrucción física de medios.
- Realizar auditorías periódicas para verificar el cumplimiento de los procedimientos de destrucción de datos.

6. Protección contra Robo de Cuentas

a. Política:

- Implementar medidas de seguridad robustas para prevenir el robo de cuentas, como autenticación multifactor (MFA) y controles de acceso basados en roles.

b. Procedimiento:

- Educar a los usuarios sobre la importancia de proteger sus credenciales y la forma de utilizar medidas de seguridad como MFA.
- Establecer un proceso para la revocación inmediata de cuentas en caso de robo o compromiso.

7. Informe de Incidentes

a. Política:

- Establecer un proceso formal para informar y manejar incidentes de seguridad, incluidos errores del administrador y situaciones de robo de cuentas.

b. Procedimiento:

- Implementar un sistema de notificación de incidentes que permita a los empleados informar de manera confidencial cualquier actividad sospechosa.
- Responder rápidamente a los informes de incidentes, investigar y tomar medidas correctivas.

8. Formación Continua

a. Política:

- Proporcionar formación continua al personal sobre seguridad de la información y buenas prácticas de gestión de cuentas.

b. Procedimiento:

- Ofrecer sesiones de formación regular sobre seguridad de TI y gestión de cuentas.
- Mantener al personal actualizado sobre las amenazas emergentes y las mejores prácticas de seguridad.

Políticas disciplinarias para incidentes con el cuidado de activos de la Dirección Desconcentrada de Cultura de Cusco

1. Política de Cuidado de Activos

a. Política:

- Todo el personal de la institución tienen la responsabilidad de cuidar y proteger los activos de la organización, incluidos equipos, dispositivos, datos y propiedades.

b. Procedimiento:

- Definir qué se considera activos de la organización y proporcionar orientación sobre su uso y manejo adecuados.
- Establecer directrices específicas sobre la responsabilidad individual y colectiva en relación con el cuidado de activos.

2. Uso Aceptable de Equipos y Recursos

a. Declaración:

- El personal de la institución debe utilizar los equipos y recursos de la institución para fines laborales.

b. Procedimiento:

- Proporcionar una lista clara de usos aceptables y no aceptables de equipos y recursos.
- Informar al personal de la institución sobre las consecuencias de un uso inadecuado.

3. Protección de Datos y Confidencialidad

a. Declaración:

- Los empleados deben proteger la confidencialidad e integridad de los datos de la organización y los activos de información.

b. Procedimiento:

- Establecer protocolos para el manejo seguro de información confidencial.
- Especificar las sanciones para la divulgación no autorizada o la pérdida de información sensible.

4. Seguridad Física

a. Declaración:

- Todos los empleados son responsables de mantener la seguridad física de los activos, como edificios, instalaciones y equipos.

b. Procedimiento:

- Establecer procedimientos para el acceso seguro a las instalaciones.
- Especificar las acciones disciplinarias en caso de negligencia que conduzca a daños físicos a los activos.

5. Reporte de Incidentes

a. Declaración:

- El personal de la institución debe informar de inmediato cualquier incidente que pueda afectar la seguridad o integridad de los activos.

b. Procedimiento:

- Establecer un canal de comunicación claro y confidencial para informar incidentes.
- Garantizar que los informantes estén protegidos contra represalias y reconozcan la importancia del reporte oportuno.

6. Capacitación Continua

a. Declaración:

- Proporcionar formación regular para garantizar que el personal de la institución esté al tanto de las políticas y prácticas relacionadas con el cuidado de activos.

b. Procedimiento:

- Realizar sesiones de formación periódicas sobre seguridad de activos y prácticas seguras.
- Mantener al personal de la institución informado sobre las actualizaciones y cambios en las políticas.

7. Sanciones Disciplinarias

a. Política:

- El incumplimiento de las políticas de cuidado de activos puede dar lugar a sanciones disciplinarias encargadas por la autoridad competente de acuerdo a la gravedad del hecho.

b. Procedimiento:

- Establecer un proceso claro y equitativo para investigar y abordar violaciones de las políticas.
- Aplicar sanciones de manera consistente y proporcional a la gravedad de la violación.

8. Auditorías y Evaluaciones

a. Política:

- La institución se reserva el derecho de realizar auditorías y evaluaciones para garantizar el cumplimiento de las políticas de cuidado de activos.

b. Procedimiento:

- Realizar auditorías periódicas para evaluar el cumplimiento de las políticas y corregir posibles desviaciones.
- Informar al personal de la institución sobre el propósito y la naturaleza de las auditorías.

Políticas en contra de la ingeniería social de la Dirección Desconcentrada de Cultura de Cusco

1. Definición de Ingeniería Social

a. Política:

- Definir claramente qué se considera ingeniería social y sus diversas formas, como el phishing, el pretexting, la suplantación de identidad, entre otros.

b. Procedimiento:

- Proporcionar ejemplos concretos de técnicas de ingeniería social.
- Educar a los empleados sobre cómo identificar y reportar intentos de ingeniería social.

2. Sensibilización y Formación

a. Política:

- Establecer programas regulares de sensibilización y formación para educar al personal de la institución sobre los riesgos de la ingeniería social.

b. Procedimiento:

- Realizar sesiones de formación interactivas y prácticas.
- Proporcionar actualizaciones periódicas para abordar nuevas tácticas de ingeniería social.

3. Gestión de Incidentes

a. Política:

- Establecer un proceso formal para la gestión de incidentes relacionados con ingeniería social.

b. Procedimiento:

- Definir los pasos a seguir al identificar o sospechar de un intento de ingeniería social.
- Garantizar que el personal de la institución sepa a quién informar y cómo hacerlo.

4. Pruebas de Concientización

a. Política:

- Realizar pruebas regulares de concientización para evaluar la resistencia del personal de la institución a los ataques de ingeniería social.

b. Procedimiento:

- Simular ataques y evaluar la respuesta del personal de la institución.
- Proporcionar retroalimentación y orientación para mejorar la conciencia.

5. Sanciones Disciplinarias

a. Política:

- Establecer consecuencias disciplinarias claras para el personal de la institución que violen las políticas de ingeniería social.

b. Procedimiento:

- Aplicar sanciones proporcionales a la gravedad de la violación.
- Garantizar la consistencia en la aplicación de sanciones.

Políticas de Derechos de Autor de la Dirección Desconcentrada de Cultura de Cusco

1. Alcance

-Estas políticas se aplican a todas las obras creativas, incluyendo información documentaria y software, producidas por personal de la institución en el curso de sus funciones laborales.

2. Propiedad Intelectual

-La institución será considerada el titular de los derechos de autor de las obras creativas, incluyendo documentación y software, creadas por sus empleados en el desempeño de sus funciones laborales, a menos que se acuerde lo contrario por escrito.

3. Registro de Obras

-Se alienta a los creadores, especialmente en el desarrollo de software, a registrar sus obras con la institución para facilitar la gestión de derechos de autor y demostrar la titularidad en caso de disputas.

4. Uso Justo y Deber de Cuidado

-Los empleados deben seguir los principios del uso justo y actuar con cuidado al utilizar o incorporar obras de terceros en la documentación o software para evitar infringir derechos de autor.

5. Política de Cumplimiento

-Las violaciones a estas políticas pueden dar lugar a medidas disciplinarias, que van desde advertencias y capacitación adicional hasta acciones legales, según la gravedad de la infracción.

6. Educación y Concientización

-La institución proporcionará capacitación periódica sobre estas políticas para garantizar que todos los empleados estén informados y cumplan con las normas establecidas.

7. Colaboración con Terceros

- Las colaboraciones con terceros en el desarrollo de software deben establecer claramente los términos de uso y respetar los derechos de autor de ambas partes.

Revisiones Periódicas de Políticas

a. Política general:

- Establecer un proceso de revisión y actualización regular de las políticas.

b. Procedimiento:

- Revisar las políticas en respuesta a nuevas amenazas o cambios en el entorno de seguridad.
- Obtener retroalimentación de incidentes y pruebas de concientización para mejorar las políticas.

Estas políticas deben ser comunicadas de manera efectiva a todo el personal y formar parte integral de la cultura de seguridad de la institución.

Anexo 4: Ejemplos tipificados de amenazas que afectan a los activos

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Datos / Información		
Activos	**Errores y fallos no intencionados**	**Ejemplos**
Datos de configuración	Errores de los usuarios	El personal de soporte y redes al tener un archivo digital (de direcciones ip, licencias, cuentas de registro de usuarios) si digita mal o elimina algo está haciendo un mal uso de los datos de configuración.
	Errores del administrador	El administrador (persona que crea, actualiza el documento) al tener ese archivo digital (de direcciones ip, licencias, cuentas de registro de usuarios) si digita mal o elimina algo está haciendo un mal uso de los datos de configuración.
	Errores de configuración	Al configurar una dirección ip a una computadora, abre el archivo digital de las direcciones ip, digita mal o copia una dirección ip de otra computadora.
	Escapes de información	Compartir el archivo digital (de direcciones ip, licencias, cuentas de registro de usuarios) por un medio a personas que no tengan conocimiento.
	Alteración accidental de la información	Modificar el archivo digital (de direcciones ip, licencias, cuentas de registro de usuarios).

	Destrucción de información	Eliminar el archivo digital (de direcciones ip, licencias, cuentas de registro de usuarios).
	Fugas de información	Comentar el archivo digital (de direcciones ip, licencias, cuentas de registro de usuarios), indiscreción, medio electrónico o papel.
Base de datos de la página web de la DDC	Errores de los usuarios	Los programadores o personas que tengan acceso limitado a la base de datos cometen errores de digitación, editar, copiar o eliminar en base de datos o consultas.
	Errores del administrador	El gestor de base de datos o la persona que tenga acceso total a la base de datos cometen errores de digitación, editar, copiar o eliminar en base de datos o consultas.
	Escapes de información	Compartir la base de datos por un medio a personas que no tengan conocimiento.
	Alteración accidental de la información	Cuando se esté usando la base de datos sin querer modifiques los DNIs de las personas, y se desordene la información de las personas con los DNIs. Son los errores sobre la información que guarda la base de datos.
	Destrucción de información	Eliminar la información que guarda o almacena la base de datos.
	Fugas de información	Comentar la información que guarda o almacena la base de datos por indiscreción, medio electrónico o papel.
	Errores de los usuarios	El personal digita, modifica el log de actividades (registro de actividades).

Log de actividades	Errores del administrador	El jefe de área digita, modifica el log de actividades (registro de actividades) de su persona o personal.
	Errores de monitorización	El jefe de área al hacer un monitoreo modifica el log de actividades (registro de actividades).
	Escapes de información	Compartir el log de actividades (registro de actividades) por un medio a personas que no tengan conocimiento.
	Alteración accidental de la información	Modificar el log de actividades (registro de actividades) .
	Destrucción de información	Eliminar el log de actividades (registro de actividades).
	Fugas de información	Comentar el log de actividades (registro de actividades) por indiscreción, medio electrónico o papel.
Datos de prueba	Errores de los usuarios	El personal programador al tener un archivo digital (líneas de código, configuraciones, direcciones ip de prueba) digita mal o elimina algo.
	Errores del administrador	El administrador (persona que crea, actualiza el documento) al crear un archivo digital (direcciones ip de prueba para probar si llega internet a una computadora) digital mal.
	Escapes de información	Compartir un archivo digital (líneas de código, configuraciones, direcciones ip de prueba) por un medio a personas que no tengan conocimiento.

	Alteración accidental de la información	Modificar un archivo digital (líneas de código, configuraciones, direcciones ip de prueba).
	Destrucción de información	Eliminar un archivo digital (líneas de código, configuraciones, direcciones ip de prueba).
	Fugas de información	Comentar un archivo digital (líneas de código, configuraciones, direcciones ip de prueba) por indiscreción, medio electrónico o papel.
Documentos digitales (memos, informe mensual)	Errores de los usuarios	El personal del área de informática al hacer un mal uso del editor del texto, digita mal el documento generado y/o recibido por el personal interno u otras áreas.
	Errores del administrador	El administrador (jefe de área) al hacer un mal uso del documento digital del editor del texto, digita mal el documento generado y/o recibido por el personal interno u otras áreas.
	Escapes de información	Compartir el documento digital por un medio a personas que no tengan conocimiento.
	Alteración accidental de la información	Modificar, digitar mal el documento generado y/o recibido por el personal.
	Destrucción de información	Eliminar el documento digital.

	Fugas de información	Comentar el documento digital por indiscreción, medio electrónico o papel.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Datos / Información		
Activos	**Ataques intencionados**	**Ejemplos**
Datos de configuración	Suplantación de la identidad del usuario	Que un personal interno pida acceso de ese activo mintiendo que requiere una persona de alto cargo y así conseguir ese activo. Persona que se hace pasar por otra para obtener ese activo.
	Abuso de privilegios de acceso	Que una persona de alto cargo (director, jefe de área) pida acceso a ese activo, o el mismo personal que tiene acceso abusa de su poder.
	Modificación deliberada de la información	Modificar el archivo digital (de direcciones ip, licencias, cuentas de registro de usuarios).
	Destrucción de información	Eliminar el archivo digital (de direcciones ip, licencias, cuentas de registro de usuarios).
	Suplantación de la identidad del usuario	Que un personal interno pida acceso de ese activo mintiendo que requiere una persona de alto cargo y así conseguir ese activo. Persona que se hace pasar por otra para obtener ese activo.

Base de datos de la página web de la DDC	Abuso de privilegios de acceso	Que una persona de alto cargo (director, jefe de área) pida acceso a ese activo, o el mismo personal que tiene acceso abusa de su poder.
	Modificación deliberada de la información	Modificar la base de datos o consultas.
	Destrucción de información	Eliminar la base de datos o consultas.
	Divulgación de información	Divulgar la información que almacena la base de datos (DNIs, nombres, id y contraseñas).
Log de actividades	Manipulación de los registros de actividad (log)	Manipular el log de actividades.
	Manipulación de la configuración	Manipular la configuración del archivo que está guardado en un drive. Ejemplo: si es privado o público.
	Suplantación de la identidad del usuario	Que un personal interno pida acceso de ese activo mintiendo que requiere una persona de alto cargo y así conseguir ese activo. Persona que se hace pasar por otra para obtener ese activo.
	Abuso de privilegios de acceso	Que una persona de alto cargo (director, jefe de área) pida acceso a ese activo, o el mismo que tiene acceso abusa de su poder.
	Repudio	Que uno del personal interno envíe su log de actividades al jefe de área y el jefe niegue haber recibido.
	Modificación deliberada de la información	Modificar el log de actividades.
	Destrucción de información	Eliminar el log de actividades.

Datos de prueba	Suplantación de la identidad del usuario	Que un personal interno pida acceso de ese activo mintiendo que requiere una persona de alto cargo y así conseguir ese activo. Persona que se hace pasar por otra para obtener ese activo.
	Abuso de privilegios de acceso	Que una persona de alto cargo (director, jefe de área) pida acceso a ese activo, o el mismo que tiene acceso abusa de su poder.
	Modificación deliberada de la información	Modificar datos de prueba (datos de códigos que se usen en otras aplicaciones, datos ya compilados).
	Destrucción de información	Eliminar datos de prueba (datos de códigos que se usen en otras aplicaciones, datos ya compilados).
Documentos digitales	Suplantación de la identidad del usuario	Cuando un personal recibe un documento que tiene una firma digital del jefe de área y usa esa firma para otros fines.
	Abuso de privilegios de acceso	Que una persona de alto cargo (director, jefe de área) pida acceso a ese activo, o el mismo que tiene acceso abusa de su poder. Ejemplo: Jefe de área le llega un memo de llamado de atención a uno de su personal y guardó ese documento, no informa y como resultado hace que despidan a ese personal.
	Modificación deliberada de la información	Una persona modifica el documento recibido o elaborado por el personal.
	Destrucción de información	Una persona elimina el documento recibido o elaborado por el personal.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Claves Criptográficas		
Activos	**Errores y fallos no intencionados**	**Ejemplos**
Contraseña de acceso a la base de datos de la página web de la DDC	Errores de los usuarios	Responder a los correos electrónicos de Phishing, guardar contraseñas en un lugar no seguro como bloc de notas en escritorio o navegador web.
	Errores del administrador	Que la persona al crear ponga una contraseña débil o repita la misma contraseña en otras aplicaciones. Falta de cambio periódico de contraseñas.
	Escapes de información	Compartir la contraseña por un medio a personas que no tengan conocimiento.
	Alteración accidental de la información	Si olvidas tu contraseña y tratas de establecerla es posible que accidentalmente cambies tu contraseña anterior por una nueva sin darte cuenta. Si utilizas un administrador de contraseñas, como LastPass o 1Password, y accidentalmente guardas una contraseña incorrecta. Sobrescribir la contraseña correcta con información incorrecta, esto puede llevar a una alteración accidental.
	Destrucción de información	Suponiendo que se tenga un archivo donde está guardada la contraseña ya sea en escritorio o drive el cual no se tenga copias y se elimina por equivocación.

		Se tiene un archivo donde está guardada la contraseña en el escritorio, la computadora falla y se pierde el archivo por lo tanto no se puede recuperar.
	Fugas de información	Que se revele la contraseña por indiscreción, medio electrónico o papel.
Contraseña de acceso al NVR	Errores del administrador	Que la persona al crear ponga una contraseña débil o repita la misma contraseña en otras aplicaciones.
	Escapes de información	Compartir la contraseña por un medio a personas que no tengan conocimiento.
	Alteración accidental de la información	Si olvidas tu contraseña y tratas de establecerla es posible que accidentalmente cambies tu contraseña anterior por una nueva sin darte cuenta.
	Destrucción de información	Suponiendo que se tenga un archivo donde está guardada la contraseña ya sea en escritorio o drive el cual no se tenga copias y se elimina por equivocación. Se tiene un archivo donde está guardada la contraseña en el escritorio, la computadora falla y se pierde el archivo por lo tanto no se puede recuperar.
	Fugas de información	Que se revele la contraseña por indiscreción, medio electrónico o papel.

Contraseña de acceso al router	Errores de los usuarios	Responder a los correos electrónicos de Phishing, guardar contraseñas en un lugar no seguro como bloc de notas en escritorio o navegador web.
	Errores del administrador	Que la persona al cambiar la contraseña designada del router ponga una contraseña débil o repita la misma contraseña en otras aplicaciones.
	Escapes de información	Compartir la contraseña por un medio a personas que no tengan conocimiento.
	Alteración accidental de la información	Si olvidas tu contraseña y tratas de establecerla es posible que accidentalmente cambies tu contraseña anterior por una nueva sin darte cuenta.
	Destrucción de información	Suponiendo que se tenga un archivo donde está guardada la contraseña ya sea en escritorio o drive el cual no se tenga copias y se elimina por equivocación. Se tiene un archivo donde está guardada la contraseña en el escritorio, la computadora falla y se pierde el archivo por lo tanto no se puede recuperar.
	Fugas de información	Que se revele la contraseña por indiscreción, medio electrónico o papel.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Claves Criptográficas		
Activos	**Ataques intencionados**	**Ejemplos**
Contraseña de acceso a la base de datos de la página web de la DDC	Suplantación de la identidad del usuario	Que un personal interno pida acceso de ese activo mintiendo que requiere una persona de alto cargo y así conseguir ese activo. Persona que se hace pasar por otra para obtener ese activo.
	Abuso de privilegios de acceso	Que una persona de alto cargo (director, jefe de área) pida acceso a ese activo, o el mismo que tiene acceso abusa de su poder.
	Acceso no autorizado	Por medio de Phishing. Que una persona externa sin autorización acceda esa contraseña por medio de suplantación de la identidad del usuario.
	Modificación deliberada de la información	El atacante ya tiene acceso a la base de datos y contraseña, puede cambiar a otra contraseña.
	Destrucción de información	Suponiendo que se tenga un archivo donde está guardada la contraseña ya sea en escritorio o drive el cual no se tenga copias y se elimina por equivocación por lo tanto el atacante elimina ese único archivo.
Contraseña de acceso al NVR	Suplantación de la identidad del usuario	Que un personal interno pida acceso de ese activo mintiendo que requiere una persona de alto cargo y así conseguir ese activo. Persona que se hace pasar por otra para obtener ese activo.
	Acceso no autorizado	Que una persona externa sin autorización acceda a esa contraseña por medio de suplantación de la identidad del usuario.
	Modificación deliberada de la información	El atacante ya tiene acceso al NVR y contraseña, puede cambiar a otra contraseña.
	Destrucción de información	Suponiendo que se tenga un archivo donde está guardada la contraseña ya sea en escritorio o drive el cual no se tenga copias; por lo tanto, el atacante elimina ese único archivo.

		Eliminar la contraseña del NVR.
Contraseña de acceso al router	Suplantación de la identidad del usuario	Que un personal interno pida acceso de ese activo mintiendo que requiere una persona de alto cargo y así conseguir ese activo. Persona que se hace pasar por otra para obtener ese activo.
	Abuso de privilegios de acceso	Que una persona de alto cargo (director, jefe de área) pida acceso a ese activo, o el mismo que tiene acceso abusa de su poder. Ejemplo: quitar el internet a una persona.
	Acceso no autorizado	Que una persona externa sin autorización acceda a esa contraseña por medio de suplantación de la identidad del usuario.
	Modificación deliberada de la información	El atacante ya se conectó a la red y tiene acceso al usuario de cuenta y contraseña, puede cambiar a otra contraseña.
	Destrucción de información	Que el atacante resetea el router y al resetearlo se elimina la contraseña de acceso al router.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Servicios		
Activos	**Errores y fallos no intencionados**	**Ejemplos**
	Errores de los usuarios	Cuando el personal de soporte técnico completa mal los campos de un formulario al responder un ticket. Al distribuir mal la información (enviar a otra área que no corresponde).
	Errores del administrador	Falta de actualización de la página del help desk por medio de la empresa contratada.

Página Help Desk	Errores de [re-]encaminamiento	El personal soporte técnico al responder los tickets generados por usuarios externos envía ese mensaje por otro medio. Ejemplo: correo electrónico, llamada, WhatsApp.
	Escapes de información	Compartir reportes de atención a personas que no tengan conocimiento.
	Alteración accidental de la información	Modificar los tickets al poner si fue atendido o no, archivar un mensaje de los tickets.
	Destrucción de información	Eliminar los mensajes de los tickets generados y reportes de atención.
	Fugas de información	Comentar reportes de atención por indiscreción, medio electrónico o papel.
	Caída del sistema por agotamiento de recursos	Cuando la empresa contratada no brinda soporte inmediato por agotamiento de sus recursos.
Páginas web institucionales	Errores del administrador	Escribir mal un código, bugs, equivocarse al hacer mantenimiento, por el personal de desarrolladores /programadores.
	Errores de [re-]encaminamiento	Redirección incorrecta (al entrar a un link me envía a otro link que no corresponde).
	Errores de secuencia	Al entrar a un link para realizar un trámite, que no me dirija al orden correcto de pasos (del paso 1 al paso 3).

	Escapes de información	Compartir la información generada de los usuarios externos, o información generada de la institución a personas que no tengan conocimiento.
	Alteración accidental de la información	Modificación en el código de las páginas.
	Destrucción de información	Eliminar una parte del código de la página.
	Fugas de información	Comentar la información generada de los usuarios externos, o información generada de la institución por indiscreción, medio o papel.
	Errores de mantenimiento / actualización de programas (software)	Errores de mantenimiento: Dar un mal mantenimiento a la página Actualización de programas: olvidar actualizar java o algún programa con el que se trabaje la página.
	Caída del sistema por agotamiento de recursos	Cuando el servidor de las páginas web cae por saturación de sus recursos.
Soporte técnico	Errores de los usuarios	El personal interno solicita un servicio incorrecto.
	Errores del administrador	El personal de soporte se equivoca al brindar el servicio de soporte técnico.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Servicios		
Activos	**Ataques intencionados**	**Ejemplos**
Página Help Desk	Suplantación de la identidad del usuario	Que una persona consiga el id y contraseña de un personal de soporte para hacerse pasar por otra persona.
	Alteración de secuencia	Modificar el orden de alguna solicitud.
	Acceso no autorizado	Que una persona externa sin autorización acceda a esa página por medio de suplantación de la identidad del usuario. Ejemplo: acceder a una cuenta de usuario del personal.
	Modificación deliberada de la información	Modificar los tickets al poner si fue atendido o no, archivar un mensaje de los tickets.
	Destrucción de información	Eliminar las solicitudes presentadas por los usuarios y reportes de atención.
	Divulgación de información	Divulgar la información que almacena los tickets de los usuarios.
	Suplantación de la identidad del usuario	Que una persona consiga el id y contraseña de un personal de desarrolladores /programadores para hacerse pasar por otra persona.
	Uso no previsto	El programador en la página publica algún anuncio que sea de su beneficio.
	Acceso no autorizado	Que una persona externa sin autorización acceda a esa página por medio de suplantación de la identidad del usuario. Ejemplo:

Páginas web institucionales		acceder a una cuenta de usuario del personal, o que acceda al mismo código.
	Modificación deliberada de la información	Modificar el código, modificar la información publicada en la página.
	Destrucción de información	Eliminar una parte o todo el código, eliminar información publicada en las plataformas institucionales.
	Denegación de servicio	Ataques de saturación de sistema
Soporte técnico	Suplantación de la identidad del usuario	Que una persona se haga pasar por un personal de soporte técnico y brinde un mal servicio.
	Abuso de privilegios de acceso	Que una persona de alto cargo (director, jefe de área) pida soporte técnico para él o un familiar.
	Uso no previsto	Que la persona que da el soporte técnico lo use para sus familiares o para él, y al hacer eso no cumple con el soporte técnico que debería brindar a los demás trabajadores.
	Alteración de secuencia	No cumpla con una secuencia de atención al realizar un soporte.
	Repudio	No querer hacer el servicio de soporte técnico a un personal.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Software		
Activos	**De origen industrial**	**Ejemplos**
Aplicaciones	Avería de origen físico o lógico	Físico: que se cuelgue la máquina, que se malogre el disco duro, actualización del Windows. Lógico: que falle la aplicación por tener errores en su código por lo tanto tendría errores lógicos.
Antivirus	Avería de origen físico o lógico	Físico: que se cuelgue la máquina, que se malogre el disco duro, actualización del Windows. Lógico: que falle la aplicación por tener errores en su código por lo tanto tendría errores lógicos.
Sistemas Operativos	Avería de origen físico o lógico	Físico: Hardware defectuoso, sobrecalentamiento puede provocar bloqueos o problemas en el Sistema Operativo Lógico: errores de configuración, virus
Ofimática	Avería de origen físico o lógico	Físico: que se cuelgue la máquina, que se malogre el disco duro, actualización del Windows Lógico: que falle la aplicación por tener errores en su código por lo tanto tendría errores lógicos.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Software		
Activos	**Errores y fallos no intencionados**	**Ejemplos**
Aplicaciones	Errores de los usuarios	El personal de desarrolladores/programadores al compilar un programa (bucle infinito) pueden colgarlo.
	Difusión de software dañino	Propagación inocente de virus.
	Alteración accidental de la información	Cambio de configuración de manera no intencionada, y hacer algunos clicks erróneos en las aplicaciones que utilicen.
	Vulnerabilidades de los programas (software)	Defectos de la misma aplicación que no esté bien desarrollada en aspectos de seguridad.
	Errores de mantenimiento / actualización de programas (software)	Errores de mantenimiento: no brindar mantenimiento periódico. Actualización de programas: que los mismos programas no se actualicen correctamente o falta de actualización por desconocimiento.
Antivirus	Errores de los usuarios	Al instalar un programa se desactiva por un momento el antivirus y sin volver a activarlo. Al instalar un programa aparece una alerta de virus el cual es ignorado.
	Errores del administrador	El administrador que tiene control del antivirus de todas las máquinas, puede quitar el antivirus a alguien de manera accidental.

	Difusión de software dañino	El antivirus captura a un virus y lo pone en cuarentena accidentalmente sacas esos virus.
	Alteración accidental de la información	Alterar la configuración del antivirus.
	Destrucción de información	Desinstalar la aplicación de manera no intencionada.
	Errores de mantenimiento / actualización de programas (software)	Errores de mantenimiento: que una persona se olvide de hacer un análisis, revisar, las alertas o actualizaciones del antivirus. Actualización de programas: que no actualice regularmente el antivirus.
Sistemas Operativos	Errores de los usuarios	Error de los trabajadores al momento de la actualización de su sistema operativo (apagar su computadora de manera imprudente).
	Errores del administrador	El personal de Soporte técnico no actualiza el SO, se le olvida.
	Difusión de software dañino	Propagación inocente de virus.
	Alteración accidental de la información	Errores de los trabajadores al eliminar de manera accidental la carpeta System32. Modificar el Windows update.
	Vulnerabilidades de los programas (software)	Mala actualización del mismo sistema operativo.
	Errores de mantenimiento / actualización de programas (software)	Errores de mantenimiento: no realizar el mantenimiento (revisar constantemente) sistema operativo Actualización de programas: no actualizar a nuevas versiones del sistema operativo.

Ofimática	Errores de los usuarios	Instalar o descargar complementos no confiables.
	Errores del administrador	Instalación incorrecta del paquete office.
	Difusión de software dañino	Propagación inocente de virus, al descargar archivos o complementos.
	Alteración accidental de la información	Instalar o descargar complementos no confiables.
	Destrucción de información	Desinstalar la aplicación de manera no intencionada.
	Errores de mantenimiento / actualización de programas (software)	Actualización de programas: no hacer una actualización a una versión más reciente que cumpla con las necesidades de cada área.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Software		
Activos	**Ataques intencionados**	**Ejemplos**
Aplicaciones	Uso no previsto	Usar la aplicación de paga para realizar otros trabajos a otra empresa.
	Difusión de software dañino	Propagación intencionada de virus para afectar a la aplicación.
	Manipulación de programas	Alteración intencionada del funcionamiento de los programas, quitar algunas de las funciones como ocultar o cambiar el lenguaje.

Antivirus	Abuso de privilegios de acceso	Que una persona de alto cargo (director, jefe de área) o el mismo administrador que tiene control del antivirus de todas las máquinas, puede quitar el antivirus a alguien.
	Difuso de software dañino	Propagación intencionada de virus para afectar al antivirus. Liberar virus que están en cuarentena.
	Modificación deliberada de la información	Modificar la configuración del antivirus.
	Destrucción de información	Desinstalar la aplicación.
	Manipulación de programas	Desactivar alguna función del antivirus.
Sistemas Operativos	Difuso de software dañino	Propagación intencionada de virus para afectar al sistema operativo.
	Modificación deliberada de la información	Modificación de archivos críticos: el atacante cambia algún archivo del sistema operativo para poder debilitar la seguridad.
	Destrucción de información	Eliminar la carpeta System32 o formatear.
	Manipulación de programas	Selección de la edición incorrecta de Windows. Ejemplo: (Windows home en lugar de Windows pro) ya que limita algunas características. Idioma y distribución del teclado incorrecto. No activar Windows.
	Uso no previsto	Usar el office de paga para realizar otros trabajos a otra empresa.

Ofimática	Difuso de software dañino	Propagación intencionada de virus para afectar office, descargar e instalar complementos no confiables como macros maliciosos que se usan en Word y en Excel, estos afectan a la función del office.
	Destrucción de información	Desinstalar la aplicación.
	Manipulación de programas	Manipular la configuración de los programas del office, desactivar o algunas herramientas de los programas.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Hardware		
Activos	**De origen industrial**	**Ejemplos**
Computadoras desktops	Fuego	Daños por fuego.
	Daños por agua	Daños por agua.
	Desastres industriales	Daños por explosiones, derrumbes.
	Contaminación mecánica	Daños por polvo, suciedad.
	Contaminación electromagnética	Que al haber otros aparatos electrónicos que generan emanaciones electromagnéticas, ambos al estar en funcionamiento generan radiación electromagnética.
	Avería de origen físico o lógico	Avería física: que falle algunos de los componentes de la computadora, golpes, caídas.

		Avería lógica: problemas del software, sistema operativo, aplicaciones.
	Corte del suministro eléctrico	Pérdida del suministro eléctrico.
	Condiciones inadecuadas de temperatura o humedad	Daños por exceso de calor, frío, humedad.
	Emanaciones electromagnéticas	Dentro de la computadora no tiene buena ventilación y se sobrecalientan los componentes internos como procesador, tarjeta gráfica.
Laptops	Fuego	Daños por fuego.
	Daños por agua	Daños por agua.
	Desastres industriales	Daños por explosiones, derrumbes.
	Contaminación mecánica	Daños por polvo, suciedad.
	Contaminación electromagnética	Que al haber otros aparatos electrónicos que generan emanaciones electromagnéticas, ambos al estar en funcionamiento generan radiación electromagnética.
	Avería de origen físico o lógico	Avería física: que falle algunos de los componentes de las laptops, golpes, caídas. Avería lógica: problemas del software, sistemas operativos, aplicaciones.
	Corte del suministro eléctrico	Pérdida del suministro eléctrico.

	Condiciones inadecuadas de temperatura o humedad	Daños por exceso de calor, frío, humedad.
	Emanaciones electromagnéticas	Dentro de la laptop no tiene buena ventilación y se sobrecalientan los componentes internos como procesador, tarjeta gráfica.
Equipos de reprografía	Fuego	Daños por fuego.
	Daños por agua	Daños por agua.
	Desastres industriales	Daños por explosiones, derrumbes.
	Contaminación mecánica	Daños por polvo, suciedad.
	Contaminación electromagnética	Que al haber otros aparatos electrónicos que generan emanaciones electromagnéticas, ambos al estar en funcionamiento generan radiación electromagnética.
	Avería de origen físico o lógico	Avería física: golpes, falle algún componente. Avería lógica: que falle el funcionamiento lógico de los equipos.
	Corte del suministro eléctrico	Pérdida del suministro eléctrico.
	Condiciones inadecuadas de temperatura o humedad	Daños por exceso de calor, frío, humedad.
	Emanaciones electromagnéticas	Una fotocopiadora defectuosa o mal apantallada emite radiación electromagnética.
	Fuego	Daños por fuego.
	Daños por agua	Daños por agua.

Firewall	Desastres industriales	Daños por explosiones, derrumbes.
	Contaminación mecánica	Daños por polvo, suciedad.
	Contaminación electromagnética	Si un firewall de hardware mal protegido emite radiación electromagnética no deseada que interfiere con dispositivos electrónicos cercanos como router servidores u otros componentes de red, ahí hay contaminación electromagnética.
	Avería de origen físico o lógico	Avería física: un disco duro defectuoso daña el funcionamiento, golpes, caídas. Avería lógica: problemas de conectividad, fallos en conexiones de red, problemas con servidores, problemas de enrutamiento de fábrica que venga.
	Corte del suministro eléctrico	Pérdida del suministro eléctrico.
	Condiciones inadecuadas de temperatura o humedad	Daños por exceso de calor, frío, humedad.
	Emanaciones electromagnéticas	Que presente algunas fallas en el blindaje electromagnético (componente que se encarga de reducir la emanación electromagnética).
	Fuego	Daños por fuego.
	Daños por agua	Daños por agua.
	Desastres industriales	Daños por explosiones, derrumbes.

Router	Contaminación mecánica	Daños por polvo, suciedad.
	Contaminación electromagnética	Que esté en contacto el router donde está un laboratorio que realicen experimentos con equipos electrónicos de alta potencias.
	Avería de origen físico o lógico	Avería física: fallo en los componentes como la placa base o memoria ram, golpes, caídas. Avería lógica: fallas en el software interno del router.
	Corte del suministro eléctrico	Pérdida del suministro eléctrico.
	Condiciones inadecuadas de temperatura o humedad	Daños por exceso de calor,frío, humedad.
	Emanaciones electromagnéticas	Se sobrecalientan los componentes internos como Radiación térmica.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Hardware		
Activos	**Errores y fallos no intencionados**	**Ejemplos**
Computadoras desktops	Errores del administrador	Desconectar antes de que termine de apagarse la computadora.
	Errores de mantenimiento / actualización de equipos (hardware)	Errores de mantenimiento: no darle mantenimiento, no limpiar, no cambiar pasta térmica. Actualización de equipos: no actualizar a nuevas versiones de componentes.

	Caída del sistema por agotamiento de recursos	Cuando se llena la capacidad de memoria de algún componente (memoria RAM, disco duro) se acaba ese recurso.
	Pérdida de equipos	Que se pierda el activo de manera no intencionada.
Laptops	Errores del administrador	Bajar la pantalla antes de que termine de apagar la laptop, esto causa daño en el disco duro.
	Errores de mantenimiento / actualización de equipos (hardware)	Errores de mantenimiento: no darle mantenimiento, no limpiar, no cambiar pasta térmica. Actualización de equipos: no actualizar a nuevas versiones de componentes.
	Caída del sistema por agotamiento de recursos	Cuando se llena la capacidad de memoria de algún componente (memoria RAM, disco duro) se acaba ese recurso.
	Pérdida de equipos	Que se pierda el activo de manera no intencionada.
Equipos de reprografía	Errores del administrador	Desconectar sin apagar los equipos.
	Errores de mantenimiento / actualización de equipos (hardware)	Errores de mantenimiento: no darle mantenimiento, no cambiar rodillos. Actualización de equipos: no actualizar a nuevas versiones de componentes.
	Caída del sistema por agotamiento de recursos	Cuando ya no hay tóner, tinta.
	Pérdida de equipos	Que se pierda el activo de manera no intencionada.

Firewall	Errores del administrador	Configurar mal el firewall de manera no intencionada malogra el funcionamiento.
	Errores de mantenimiento / actualización de equipos (hardware)	Errores de mantenimiento: no realizar copias de seguridad de configuraciones, no supervisar y registrar los eventos del firewall.
	Caída del sistema por agotamiento de recursos	No tener capacidad suficiente en el procesamiento o en la memoria.
	Pérdida de equipos	Que se pierda el activo de manera no intencionada.
Router	Errores del administrador	Configurar mal el router.
	Errores de mantenimiento / actualización de equipos (hardware)	Errores de mantenimiento: no darle mantenimiento Actualización de equipos: no actualizar a nuevas versiones de componentes
	Caída del sistema por agotamiento de recursos	Saturación de la memoria del router.
	Pérdida de equipos	Que se pierda el activo de manera no intencionada.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Hardware		
Activos	**Ataques intencionados**	**Ejemplos**
	Abuso de privilegios de acceso	Que una persona de alto cargo (director, jefe de área) pida acceso a ese activo de otra persona, o el mismo personal que tiene acceso

Computadoras desktops		abusa de su poder. Y se daña la privacidad que hay en las computadoras.
	Uso no previsto	Usar la computadora para ver videos, escuchar música.
	Acceso no autorizado	El atacante consigue acceder al activo sin tener autorización.
	Manipulación de los equipos	Hacer un mal uso de la computadora desktop como apagar mal o sabotear el hardware.
	Denegación de servicio	Agotar los recursos para que deje de funcionar la computadora. Agotar la capacidad de almacenamiento de disco duro o memoria.
	Robo	Robo del activo.
	Ataque destructivo	Destrucción del activo.
Laptops	Abuso de privilegios de acceso	Que una persona de alto cargo (director, jefe de área) pida acceso a ese activo de otra persona, o el mismo personal que tiene acceso abusa de su poder. Y se daña la privacidad que hay en las laptops.
	Uso no previsto	Usar la laptop para ver videos, escuchar música.
	Acceso no autorizad	El atacante consigue acceder al activo sin tener autorización.
	Manipulación de los equipos	Sabotaje del hardware. Ejemplo: desensamblar la laptop.
	Denegación de servicio	Agotar los recursos para que deje de funcionar la laptop. Agotar la capacidad de almacenamiento de disco duro o memoria.

	Robo	Robo del activo.
	Ataque destructivo	Destrucción del activo.
Equipos de reprografía	Abuso de privilegios de acceso	Que una persona de alto cargo (director, jefe de área) pida acceso a ese activo de otra persona, o el mismo personal que tiene acceso abusa de su poder. Ejemplo: tener acceso completo para usar los equipos, sin dar acceso a otro personal.
	Uso no previsto	Use para su beneficio, imprimir o escanear archivos que no competen con su trabajo.
	Acceso no autorizado	Que una persona de otra área use el equipo de otra área y pueda malograr al no saber usar.
	Manipulación de los equipos	Sabotaje del hardware. Ejemplo: Poner mal el tóner, las tintas.
	Denegación de servicio	Agotar los recursos del equipo de reprografía para que deje de funcionar. Sobrecarga de las solicitudes de impresión, saturación de la cola de impresión.
	Robo	Robo del activo.
	Ataque destructivo	Destrucción del activo.
	Acceso no autorizado	Tenga acceso al firewall.
	Manipulación de los equipos	Manipular la configuración como desactivar.

Firewall	Denegación de servicio	Agotar los recursos del firewall, ataque de inundación de solicitudes y de saturar la capacidad de procesamiento del firewall.
	Robo	Robo del activo.
	Ataque destructivo	Destrucción del activo.
Router	Uso no previsto	Que lo use para su beneficio aprovechándose de la distribución del internet.
	Acceso no autorizado	Tenga acceso al router una persona no autorizada.
	Manipulación de los equipos	Resetear el router.
	Denegación de servicio	Sobrecargar los dispositivos, agotar la capacidad de almacenamiento, CPU, memoria.
	Robo	Robo del activo.
	Ataque destructivo	Destrucción del activo.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Redes de comunicaciones		
Activos	**De Origen Industrial**	**Ejemplos**
Internet	Fallo de servicios de comunicaciones	Interrupciones del proveedor de servicios, la empresa tiene problemas técnicos que afectan la conectividad.
Internet de respaldo	Fallo de servicios de comunicaciones	Interrupciones del proveedor de servicios, la empresa tiene problemas técnicos que afectan la conectividad.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Redes de comunicaciones		
Activos	**De errores y fallos no intencionados**	**Ejemplos**
Internet	Errores del administrador	Mal configuración en distribución de red y que no llegue internet al personal.
	Errores de [re-]encaminamiento	Introducción de rutas incorrectas, omisión de partes de configuración.
	Errores de secuencia	Mal configuración del tcp.
	Escapes de información	Cuando hay un cable suelto existe la posibilidad de que se conecten a internet.
	Fugas de información	Revelar contraseña del wifi.
	Errores de mantenimiento / actualización de equipos (hardware)	Errores de mantenimiento: mal mantenimiento de cableado de red. Actualización de equipos: actualización de nuevo equipo router, actualización de velocidad del internet.
	Caída del sistema por agotamiento de recursos	Cuando varias personas usan y saturan internet.
	Errores del administrador	Mal configuración en distribución de red y que no llegue internet al personal.

Internet de respaldo	Errores de [re-]encaminamiento	Introducción de rutas incorrectas, omisión de partes de configuración.
	Errores de secuencia	Mal configuración del tcp.
	Escapes de información	Cuando hay un cable suelto existe la posibilidad de que se conecten a internet.
	Fugas de información	Revelar contraseña del wifi.
	Errores de mantenimiento / actualización de equipos (hardware)	Errores de mantenimiento: mal mantenimiento de cableado de red. Actualización de equipos: actualización de nuevo equipo router, actualización de velocidad del internet.
	Caída del sistema por agotamiento de recursos	Cuando varias personas usan y saturan internet.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Redes de comunicaciones		
Activos	**Ataques intencionados**	**Ejemplos**
Internet	Abuso de privilegios de acceso	El mismo personal abusa de su poder, no dan internet a personas que no quieren.
	Uso no previsto	Lo usan para descargar, ver videos música, etc.
	[Re-]encaminamiento de mensajes	Tcp protocolo mal configuración.

	Alteración de secuencia	No cifrado de datos.
	Acceso no autorizado	Al obtener contraseña de wifi.
	Análisis de tráfico	El atacante al hacer un análisis de tráfico se puede recopilar información de cómo se utiliza la red, detectar los problemas de rendimiento, identificar amenazas de seguridad.
	Interceptación de información (escucha)	Un atacante se interpone entre la comunicación entre dos partes lo que le permite interceptar y a veces modificar los datos que se transmitan entre ellos. Se llama ataque MITM (hombre en el medio, man in the middle.
	Modificación deliberada de la información	Entrar y modificar mal lo que ya está configurado.
	Denegación de servicio	Ataque de agotamiento de recursos, el atacante utiliza técnicas para agotar los recursos del servidor o la infraestructura de red.
Internet de respaldo	Abuso de privilegios de acceso	El mismo personal abusa de su poder, no dan internet a personas que no quieren.
	Uso no previsto	Lo usan para descargar, ver videos música, etc.
	[Re-]encaminamiento de mensajes	Tcp protocolo mal configuración.
	Alteración de secuencia	Cifrado de datos.
	Acceso no autorizado	Al obtener contraseña de wifi.

	Análisis de tráfico	El atacante al hacer un análisis de tráfico se puede recopilar información de cómo se utiliza la red, detectar los problemas de rendimiento, identificar amenazas de seguridad.
	Interceptación de información (escucha)	Un atacante se interpone entre la comunicación entre dos partes lo que le permite interceptar y a veces modificar los datos que se transmitan entre ellos. Se llama ataque MITM (hombre en el medio, man in the middle.
	Modificación deliberada de la información	Entrar y modificar mal lo que ya está configurado.
	Denegación de servicio	Ataque de agotamiento de recursos, el atacante utiliza técnicas para agotar los recursos del servidor o la infraestructura de red.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Soportes de información		
Activos	**Desastres naturales**	**Ejemplos**
USB	Fuego	Daños por fuego.
	Daños por agua	Daños por agua.
	Desastres naturales	Daños por desastres naturales.
Disco duro externo	Fuego	Daños por fuego.
	Daños por agua	Daños por agua.
	Desastres naturales	Daños por desastres naturales.

Servidores	Fuego	Daños por fuego.
	Daños por agua	Daños por agua.
	Desastres naturales	Daños por desastres naturales.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Soportes de información		
Activos	**De Origen Industrial**	**Ejemplos**
USB	Fuego	Daños por fuego.
	Daños por agua	Daños por agua.
	Desastres industriales	Daños por explosiones, derrumbes.
	Contaminación mecánica	Daños por polvo, suciedad.
	Contaminación electromagnética	Que al haber un motor o un microondas que estos emitan ondas electromagnéticas y eso malogra al USB (que no pueda guardar o quemarse).
	Avería de origen físico o lógico	Avería física: golpes caídos. Avería lógica: que no funcione bien el USB, que esté mal formateado.
	Condiciones inadecuadas de temperatura o humedad	Daños por exceso de calor, frío, humedad.

	Degradación de los soportes de almacenamiento de información	Como consecuencia del paso del tiempo.
	Emanaciones electromagnéticas	Cuando el USB está en funcionamiento genera emanaciones electromagnéticas. Ejemplo: computadora encendida y USB siendo utilizada al mismo tiempo.
Disco duro externo	Fuego	Daños por fuego.
	Daños por agua	Daños por agua.
	Desastres industriales	Daños por explosiones, derrumbes.
	Contaminación mecánica	Daños por polvo, suciedad.
	Contaminación electromagnética	Que al haber un motor o un microondas que estos emitan ondas electromagnéticas y eso malogra al disco duro externo (que no pueda guardar o quemarse).
	Avería de origen físico o lógico	Avería física: golpes, caídas. Avería lógica: que no funcione bien el disco duro externo, que esté mal formateado.
	Condiciones inadecuadas de temperatura o humedad	Daños por exceso de calor, frío, humedad.
	Degradación de los soportes de almacenamiento de información	Como consecuencia del paso del tiempo.

	Emanaciones electromagnéticas	Cuando el disco duro externo está en funcionamiento genera emanaciones electromagnéticas. Ejemplo: computadora encendida y disco duro externo siendo utilizada al mismo tiempo.
Servidores	Fuego	Daños por fuego.
	Daños por agua	Daños por agua.
	Desastres industriales	Daños por explosiones, derrumbes.
	Contaminación mecánica	Daños por polvo, suciedad.
	Contaminación electromagnética	Que al haber un motor o un microondas que estos emitan ondas electromagnéticas y eso malogra los servidores.
	Avería de origen físico o lógico	Avería física: golpes, caídas, que de fábrica venga defectuoso algunos de sus componentes del servidor. Avería lógica: que esté mal formateado.
	Condiciones inadecuadas de temperatura o humedad	Daños por exceso de calor, frío, humedad.
	Degradación de los soportes de almacenamiento de información	Como consecuencia del paso del tiempo.
	Emanaciones electromagnéticas	El servidor emite emanaciones electromagnéticas.
Repositorios de código fuente	Fallo de servicios de comunicaciones	Que no haya internet.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Soportes de información		
Activos	**De errores y fallos no intencionados**	**Ejemplos**
USB	Errores de los usuarios	No expulsar correctamente el USB.
	Alteración accidental de la información	Que formatee en un formato no válido en vez de FAT32 en NTFS Que modifique de manera no intencionada alguna de las propiedades o funciones del USB.
	Destrucción de información	Que se caiga y se rompa.
	Errores de mantenimiento / actualización de equipos (hardware)	Errores de mantenimiento: darle un mal mantenimiento.
	Pérdida de equipos	Que se pierda el activo de manera no intencionada.
Disco duro externo	Errores de los usuarios	No expulsar correctamente el disco duro externo.
	Alteración accidental de la información	Que modifique de manera no intencionada alguna de las propiedades o funciones del disco duro externo.
	Destrucción de información	Que se caiga y se rompa.
	Errores de mantenimiento / actualización de equipos (hardware)	Errores de mantenimiento: darle un mal mantenimiento.
	Pérdida de equipos	Que se pierda el activo de manera no intencionada.
	Errores de los usuarios	(Personal desarrolladores/ programadores)

Servidores		Actualizaciones inadecuadas del software, errores de configuración (al configurar incorrectamente el sistema operativo).
	Errores del administrador	(Personal de red) Actualizaciones inadecuadas del software, errores de configuración (al configurar incorrectamente el sistema operativo).
	Errores de mantenimiento / actualización de equipos (hardware)	Errores de mantenimiento: cambios de discos duros. Actualización de equipos: mala actualización de software o del sistema operativo.
	Pérdida de equipos	Que se pierda el activo de manera no intencionada.
	Indisponibilidad del personal	Cuando el personal no se encuentra disponible para el monitoreo.
Repositorios de código fuente	Errores del administrador	Modifique el acceso a otros desarrolladores/programadores.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Soportes de información		
Activos	**Ataques intencionados**	**Ejemplos**
USB	Uso no previsto	Que use el USB para guardar archivos personales.
	Acceso no autorizado	Que alguien agarre el USB de otra persona.
	Manipulación de los equipos	Manipular la configuración del USB.

	Robo	Que roben el activo.
	Ataque destructivo	Destruyen el activo, vandalismo.
Disco duro externo	Uso no previsto	Que use el disco duro externo para guardar archivos personales.
	Acceso no autorizado	Que alguien agarre el disco duro externo de otra persona.
	Manipulación de los equipos	Manipular la configuración del disco duro externo.
	Robo	Que roben el activo.
	Ataque destructivo	Destruyen el activo, vandalismo.
Servidores	Uso no previsto	Que un trabajador guarde su propia página web en el servidor para evitar pagar un servidor.
	Acceso no autorizado	Que una persona acceda a la cuenta de usuario y contraseña para poder cargar su aplicación o eliminarlo.
	Modificación deliberada de la información	Manipular la configuración, quitar las medidas de seguridad que tiene el servidor, dar un mal mantenimiento.
	Destrucción de información	Eliminar la información del servidor.
	Divulgación de información	Divulgar la información del servidor.
	Manipulación de los equipos	Desconectar algún cable que esté conectado al servidor.
	Robo	Que roben el activo.
	Ataque destructivo	Destruyen el activo, vandalismo.
	Uso no previsto	Guardar proyectos ajenos a la institución.
	Acceso no autorizado	Que una persona acceda al repositorio.

Repositorios de código fuente	Modificación deliberada de la información	Modifique la configuración del repositorio.
	Destrucción de información	Eliminar el repositorio.
	Divulgación de información	Divulgar la cuenta de usuario y contraseña.
	Robo	Robar la cuenta.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Equipamiento Auxiliar		
Activos	**Desastres naturales**	**Ejemplos**
Generador eléctrico	Fuego	Daños por fuego.
	Daños por agua	Daños por agua.
	Desastres naturales	Daños por desastres naturales.
UPS	Fuego	Daños por fuego.
	Daños por agua	Daños por agua.
	Desastres naturales	Daños por desastres naturales.
Equipo de climatización	Fuego	Daños por fuego.
	Daños por agua	Daños por agua.
	Desastres naturales	Daños por desastres naturales.
Mobiliario	Fuego	Daños por fuego.
	Daños por agua	Daños por agua.
	Desastres naturales	Daños por desastres naturales.

NVR	Fuego	Daños por fuego.
	Daños por agua	Daños por agua.
	Desastres naturales	Daños por desastres naturales.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Equipamiento Auxiliar		
Activos	**De Origen Industrial**	**Ejemplos**
Generador eléctrico	Fuego	Daños por fuego.
	Daños por agua	Daños por agua.
	Desastres industriales	Daños por explosiones, derrumbes.
	Contaminación mecánica	Daños por polvo, suciedad.
	Contaminación electromagnética	Campos electromagnéticos intensos cerca al generador eléctrico, interferencias de voltaje.
	Avería de origen físico o lógico	Avería física: golpes, caídas, problemas en los componentes. Avería lógica: falla del sensor de temperatura.
	Condiciones inadecuadas de temperatura o humedad	Daños por exceso de calor, frío, humedad.
	Interrupción de otros servicios y suministros esenciales	Que no haya combustible.
	Emanaciones electromagnéticas	El activo emite interferencias electromagnéticas.
	Fuego	Daños por fuego.

UPS	Daños por agua	Daños por agua.
	Desastres industriales	Daños por explosiones, derrumbes.
	Contaminación mecánica	Daños por polvo, suciedad.
	Contaminación electromagnética	Que al haber un motor o un microondas que estos emitan ondas electromagnéticas y eso malogra al UPS.
	Avería de origen físico o lógico	Avería física: batería dañada del UPS, que se desgasta. Avería lógica: falla del software de gestión (controla su funcionamiento y permite configurar parámetros), es decir que no avise cuando se esté usando el UPS o cuando este baja la batería.
	Condiciones inadecuadas de temperatura o humedad	Daños por exceso de calor, frío, humedad.
	Corte de suministro eléctrico	Que no haya electricidad y no se pueda cargar.
	Emanaciones electromagnéticas	El activo emite interferencias electromagnéticas.
Equipo de climatización	Fuego	Daños por fuego.
	Daños por agua	Daños por agua.
	Desastres industriales	Daños por explosiones, derrumbes.
	Contaminación mecánica	Daños por polvo, suciedad.
	Contaminación electromagnética	Que al haber un motor o un microondas que estos emitan ondas electromagnéticas y eso malogra al equipo de climatización.
	Avería de origen físico o lógico	Avería física: compresor dañado.

		Avería lógica: fallo del termostato es decir mal configurado, problemas del control electrónico.
	Corte de suministro eléctrico	Que se vaya la electricidad.
	Interrupción de otros servicios y suministros esenciales	Que se acabe el refrigerante (gas).
	Emanaciones electromagnéticas	El activo emite ondas electromagnéticas.
Mobiliario	Fuego	Daños por fuego.
	Daños por agua	Daños por agua.
	Desastres industriales	Daños por explosiones, derrumbes.
	Contaminación mecánica	Daños por polvo, suciedad.
	Avería de origen físico o lógico	Avería física: golpes, caídas.
NVR	Fuego	Daños por fuego.
	Daños por agua	Daños por agua.
	Desastres industriales	Daños por explosiones, derrumbes.
	Contaminación mecánica	Daños por polvo, suciedad.
	Contaminación electromagnética	Que al haber un motor o un microondas que estos emitan ondas electromagnéticas y eso malogra al NVR.
	Avería de origen físico o lógico	Avería física: golpes, caídas, que venga por defecto un componente dañado.

		Avería lógica: Fallos en la configuración del software (que no esté grabando).
	Corte de suministro eléctrico	Que no haya electricidad.
	Condiciones inadecuadas de temperatura o humedad	Daños por exceso de calor, frío, humedad.
	Fallo de servicios de comunicaciones	Cuando no hay conexión entre el NVR y la cámara (analógicamente o por problemas de red.
	Interrupción de otros servicios y suministros esenciales	Que no haya cámaras ip o disco duro lleno de almacenamiento.
	Degradación de los soportes de almacenamiento de información	Como consecuencia del paso del tiempo, falla del servidor.
	Emanaciones electromagnéticas	El activo emite interferencias electromagnéticas.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Equipamiento Auxiliar		
Activos	**De errores y fallos no intencionados**	**Ejemplos**
	Errores de los usuarios	Sobrecarga del generador con demasiados equipos.
	Errores del administrador	No controlar el combustible disponible.

Generador eléctrico	Errores de mantenimiento / actualización de equipos (hardware)	Errores de mantenimiento: dar un mal mantenimiento de manera no intencionada.
	Pérdida de equipos	Que se pierda el activo.
UPS	Errores de los usuarios	(Mala manipulación) conectar demasiados dispositivos, ignorar alarmas de baja batería.
	Errores de administrador	Mala instalación, mala monitorización.
	Errores de mantenimiento / actualización de equipos (hardware)	Errores de mantenimiento: dar un mal mantenimiento de manera no intencionada.
	Pérdida de equipos	Que se pierda el activo.
Equipo de climatización	Errores de los usuarios	Uso inadecuado del termostato en circunstancias no adecuadas.
	Errores del administrador	Ignorar problemas de refrigerante y fuga.
	Errores de mantenimiento / actualización de equipos (hardware)	Errores de mantenimiento: dar un mal mantenimiento de manera no intencionada.
	Pérdida de equipos	Que se pierda el activo.
Mobiliario	Errores de mantenimiento / actualización de equipos (hardware)	No tener barnizado los armarios.
	Pérdida de equipos	Que se pierda el activo.
	Errores de administrador	No configurar adecuadamente las alertas, no mantener un registro de usuario y respaldo de datos.

NVR	Errores de mantenimiento / actualización de equipos (hardware)	Errores de mantenimiento: dar un mal mantenimiento físico o lógico de manera no intencionada.
	Pérdida de equipos	Que se pierda el activo.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Equipamiento Auxiliar		
Activos	**Ataques intencionados**	**Ejemplos**
Generador eléctrico	Uso no previsto	Sabiendo que no hay luz cargas tu teléfono usando el generador eléctrico.
	Acceso no autorizado	Que una persona externa haga uso de la energía eléctrica generada por el generador eléctrico.
	Manipulación de los equipos	Al apagar incorrectamente de manera intencionada, llenar otro tipo de combustible.
	Robo	Que roben el activo.
	Ataque destructivo	Destruyen el activo, vandalismo.
UPS	Uso no previsto	Sabiendo que no hay luz cargas tu teléfono usando el UPS.
	Acceso no autorizado	Que otra persona de otra área o externa haga uso de la energía eléctrica del UPS.
	Manipulación de los equipos	Sustitución de baterías por otro que no corresponde.
	Robo	Que roben el activo.

	Ataque destructivo	Destruyen el activo, vandalismo.
Equipo de climatización	Manipulación de los equipos	Realizar un mantenimiento incorrecto del equipo de climatización
	Robo	Que roben el activo.
	Ataque destructivo	Destruyen el activo, vandalismo.
Mobiliario	Uso no previsto	Usar el mobiliario para guardar tus cosas personales.
	Acceso no autorizado	Que otra persona de otra área use ese mobiliario para guardar sus cosas.
	Manipulación de los equipos	Hacer un mal uso del mobiliario (sobrecargar el peso del activo).
	Robo	Que roben el activo.
	Ataque destructivo	Destruyen el activo, vandalismo.
	Ocupación enemiga	Que invadan las instalaciones.
NVR	Manipulación de la configuración	Manipulación de la configuración general del NVR.
	Uso no previsto	Borrar algún video del NVR.
	Acceso no autorizado	Que alguien sin autorización ingrese y tenga acceso total al NVR.
	Divulgación de información	Divulgar la información que tiene el NVR como por ejemplo cuántas cámaras hay, cuántos puntos graban, si hay puntos ciegos.
	Manipulación de los equipos	Manipular cámaras como bloquear, mover, desconectarlo del NVR.
	Robo	Que roben el activo.
	Ataque destructivo	Destruyen el activo, vandalismo.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Instalaciones		
Activos	**Desastres naturales**	**Ejemplos**
Oficina	Fuego	Daños por fuego.
	Daños por agua	Daños por agua.
	Desastres naturales	Daños por explosiones, derrumbes.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Instalaciones		
Activos	**De Origen Industrial**	**Ejemplos**
Oficina	Fuego	Daños por fuego.
	Daños por agua	Daños por agua.
	Desastres industriales	Daños por explosiones, derrumbes.
	Contaminación mecánica	Daños por polvo, suciedad.
	Corte de suministro eléctrico	Que no haya electricidad.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Instalaciones		
Activos	**De errores y fallos no intencionados**	**Ejemplos**
Oficina	Errores de los usuarios	No mantener un entorno limpio y organizado.
	Errores del administrador	Pérdida de llave.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Instalaciones		
Activos	**Ataques intencionados**	**Ejemplos**
Oficina	Uso no previsto	Usar la oficina para asuntos personales, como guardar tus cosas o traer personas.
	Acceso no autorizado	Acceso de personal no autorizado a la oficina.
	Ataque destructivo	Que destruyan la oficina, vandalismo.
	Ocupación enemiga	Que invadan las instalaciones.
	Indisponibilidad del personal	Ausencia del personal como huelga, bajas no justificadas.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Personal		
Activos	**Desastres naturales**	**Ejemplos**
Jefe de área	Fuego	Daños por fuego.
	Desastres naturales	Daños por explosiones, derrumbes.
P.Desarrolladores / Programadores	Fuego	Daños por fuego.
	Desastres naturales	Daños por explosiones, derrumbes.
P.Soporte técnico	Fuego	Daños por fuego.
	Desastres naturales	Daños por explosiones, derrumbes.
P.Redes	Fuego	Daños por fuego.
	Desastres naturales	Daños por explosiones, derrumbes.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Personal		
Activos	**De Origen Industrial**	**Ejemplos**
Jefe de área	Fuego	Daños por fuego (a causa de explosión, corto circuito).
P.Desarrolladores / Programadores	Fuego	Daños por fuego (a causa de explosión, corto circuito).
P.Soporte técnico	Fuego	Daños por fuego (a causa de explosión, corto circuito).
P.Redes	Fuego	Daños por fuego (a causa de explosión, corto circuito).

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Personal		
Activos	**De errores y fallos no intencionados**	**Ejemplos**
Jefe de área	Deficiencias en la organización	Cuando no está claro quién tiene que hacer exactamente qué y cuándo puede afectar a su cargo.
	Escapes de información	Comparta alguna información que maneje.
	Indisponibilidad del personal	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica.
P.Desarrolladores / Programadores	Deficiencias en la organización	Cuando no está claro quién tiene que hacer exactamente qué y cuándo puede afectar a su cargo (organizarse quien hace tal código).
	Escapes de información	Comparta alguna información que maneje.

	Indisponibilidad del personal	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica.
P.Soporte técnico	Deficiencias en la organización	Cuando no está claro quién tiene que hacer exactamente qué y cuándo puede afectar a su cargo (distribuir las labores de soporte técnico).
	Indisponibilidad del personal	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica.
P.Redes	Deficiencias en la organización	Cuando no está claro quién tiene que hacer exactamente qué y cuándo puede afectar a su cargo (distribuir las labores de redes).
	Indisponibilidad del personal	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica.

Ejemplos tipificados de amenazas que afectan a los activos del tipo: Personal		
Activos	**Ataques intencionados**	**Ejemplos**
Jefe de área	Repudio	Que no quiera realizar sus funciones.
	Indisponibilidad del personal	Ausencia del personal como huelga, bjas no justificadas.
	Extorsión	Que sea extorsionado para hacer algo incorrecto como robar información.
	Ingeniería social (picaresca)	Abuso de la buena fe de las personas para que realicen actividades indebidas.
P.Desarrolladores / Programadores	Repudio	Que no quiera realizar sus funciones.
	Indisponibilidad del personal	Ausencia del personal como huelga, bajas no justificadas.
	Extorsión	Que sea extorsionado para hacer algo incorrecto como robar información.
	Ingeniería social (picaresca)	Abuso de la buena fe de las personas para que realicen actividades indebidas.
P.Soporte técnico	Repudio	Que no quiera realizar sus funciones.
	Indisponibilidad del personal	Ausencia del personal como huelga, bajas no justificadas.
	Extorsión	Que sea extorsionado para hacer algo incorrecto como robar información.
	Ingeniería social (picaresca)	Abuso de la buena fe de las personas para que realicen actividades indebidas.

P.Redes	Repudio	Que no quiera realizar sus funciones.
	Indisponibilidad del personal	Ausencia del personal como huelga, bajas no justificadas.
	Extorsión	Que sea extorsionado para hacer algo incorrecto como robar información.
	Ingeniería social (picaresca)	Abuso de la buena fe de las personas para que realicen actividades indebidas.

Anexo 5: Carta de conformidad del Anexo 4

CARTA DE CONFORMIDAD

El que suscribe, Ing. Jisbaj Gamarra Salas, en mi condición de profesional certificado como *Certified Risk Management Professional* (ISO31000) por Global Trust Association, por medio de la presente, doy la validez del **Anexo 4: Ejemplos tipificados de amenazas que afectan a los activos**, que elaboraron los bachilleres Sharom Mitchel Nolazco Sandoval y Alexander Pavel Ibarra Huamán como parte del desarrollo de su proyecto de tesis titulado «Propuesta de implementación de la NTP-ISO/IEC 27005:2018 aplicando la metodología Magerit para el Área Funcional de Informática y Telecomunicaciones de la Dirección Desconcentrada de Cultura de Cusco».

Conformidad que se expide única y exclusivamente con fines académicos.

Cusco, 21 de marzo de 2024.

Ing. Jisbaj Gamarra Salas