Elaboración de un plan de contingencia para la auditoría de los sistemas informáticos del departamento de TICs del Gobierno Autónomo Descentralizado Municipal Intercultural del cantón Saquisilí (GADMICS).

Rivera Reisancho, Jessica Anabel

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Trabajo de Integración Curricular, previo a la obtención del título de Tecnóloga Superior en Redes y Telecomunicaciones

Ing. Viteri Arias, Cristian Santiago

9 de febrero del 2024

Latacunga

Reporte de verificacion de contenido

Copyleaks

Plagiarism report

Tesis_Plan de Contiguencia.pdf

Scan details

Scan time:	Total Pages:	Total Words:
January 31th, 2024 at 19:0 UTC	71	17653

Plagiarism Detection

2.7%

Types of plagiarism		Words
Identical	2.7%	468
Minor Changes	0%	0
Paraphrased	0%	0
Omitted Words	3.3%	587

AI Content Detection

N/A

Text coverage
- AI text
- Human text

Plagiarism Results: (47)

Metodologias Riesgo y Control Informatico: Metodologías en Riesgo y Co... 0.4%

http://hinaluz.blogspot.com/2014/03/metodologias-en-riesgo-y-control.html

Metodologias Riesgo y Control Informatico...

Metodologias Riesgo y Control Informatico: marzo 2014 0.4%

http://hinaluz.blogspot.com/2014/03/

Metodologias Riesgo y Control Informatico...

Introducción a la gestión de sistemas de información en la empresa. Uni... 0.4%

https://www.slideshare.net/julioiglesiaspascual/introduccin-a-la-gestin-de-sistemas-de-informacin-en-la-empr...

Submit Search Upload Introducción a la gestión de sistemas de información en la empresa. Universitat Jaume I Report Share J J...

Tecnologías de la Información aplicada a los negocios 0.4%

https://view.genial.ly/658b06a50af31300148099c/presentation-tecnologias-de-la-informacion-aplicada-a-los-...

You need to enable JavaScript to run this app.Your browser does not support the video tag. Want to make creations as awesome as this o...

.....

Ing, Viteri Arias, Cristian Santiago

C.C.: 0502476914

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Certificación

Certifico que el trabajo de integración curricular: "**Elaboración de un plan de contingencia para la auditoría de los sistemas informáticos del departamento de TICs del Gobierno Autónomo Descentralizado Municipal Intercultural del cantón Saquisilí (GADMICS)**" fue realizado por la señorita **Rivera Reisancho, Jessica Anabel,** el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizada en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Latacunga, 07 de febrero de 2024

.....

Ing. Viteri Arias, Cristian Santiago

C. C.: 0502476914

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Responsabilidad de Autoría

Yo, **Rivera Reisancho, Jessica Anabel**, con cédula de ciudadanía n° 0504310897 declaro que el contenido, ideas y criterios del trabajo de integración curricular: **Elaboración de un plan de contingencia para la auditoría de los sistemas informáticos del departamento de TICs del Gobierno Autónomo Descentralizado Municipal Intercultural del cantón Saquisilí (GADMICS)** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Latacunga, 07 de febrero de 2024

.....

Rivera Reisancho, Jessica Anabel

C.C.: 0504310897

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Tecnología Superior en Redes y Telecomunicaciones.

Autorización de Publicación

Yo **Rivera Reisancho, Jessica Anabel**, con cédula de ciudadanía n° 0504310897, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de integración curricular: **Elaboración de un plan de contingencia para la auditoría de los sistemas informáticos del departamento de TICs del Gobierno Autónomo Descentralizado Municipal Intercultural del cantón Saquisilí (GADMICS)** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Latacunga, 07 de febrero de 2024

.....

Rivera Reisancho, Jessica Anabel

C.C.: 0504310897

Dedicatoria

Con profundo amor y gratitud, dedico este trabajo en primer lugar a Dios por ser el centro de mi vida, quien ha sido el faro que ha iluminado mi camino, infundiendo sabiduría en cada paso de mi viaje. A mis padres, cuyo amor incondicional, apoyo constante y sacrificio desinteresado han sido el cimiento sobre el cual he construido mis sueños. A mis seres queridos, cuya presencia ha sido un bálsamo en tiempos de dificultad y una fuente inagotable de inspiración y alegría. A mis respetados docentes, les agradezco por su confianza en mí y por su dedicación incansable en el noble arte de enseñar. Vuestras palabras de aliento y guía han sido un destello de luz en mi sendero hacia el éxito y el crecimiento personal. Con profunda gratitud, les dedico este trabajo como un tributo en reconocimiento a su invaluable contribución al desarrollo de mi trayectoria académica

RIVERA REISANCHO, JESSICA ANABEL

Agradecimiento

En el transcurso de esta travesía académica, mi corazón se llena de profunda gratitud hacia aquellos que han sido pilares fundamentales en mi camino. Agradezco en primer lugar a Dios, fuente de inspiración y fortaleza, cuya luz me ha guiado en cada paso de este viaje. A mis padres, cuyo amor incondicional y sacrificio han sido el motor de mi crecimiento, les debo una deuda eterna de gratitud. A mis amigos y seres queridos, a quienes considero mi familia extendida, les agradezco por su apoyo inquebrantable y sus palabras de aliento que han sido mi sostén en los momentos más desafiantes. Y a mis respetados docentes, les agradezco por su invaluable ayuda y apoyo en el proceso de culminación de mis estudios. Sus enseñanzas, orientaciones y paciencia han sido fundamentales en mi desarrollo académico y personal. Este logro no hubiera sido posible sin su inestimable contribución. A cada uno de ustedes, mi más sincero reconocimiento y gratitud

RIVERA REISANCHO, JESSICA ANABEL

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Resumen

La monografía aborda la importancia crítica de la elaboración de un plan de contingencia para los sistemas de información del Departamento de Tecnologías de la Información y Comunicaciones (TICs) en las organizaciones modernas. Se destaca la creciente dependencia de las empresas en los sistemas de información y la necesidad de garantizar su disponibilidad y seguridad en todo momento. Se discuten los diferentes tipos de riesgos a los que están expuestos los sistemas de información, incluidos los ciberataques, los fallos de hardware, los desastres naturales y los errores humanos. Se enfatiza la importancia de identificar y evaluar estos riesgos para desarrollar un plan de contingencia efectivo que permita responder de manera rápida y eficiente en caso de un evento adverso. El proceso de desarrollo de un plan de contingencia se examina en detalle, desde la identificación de los activos críticos y los riesgos asociados hasta la definición de estrategias de mitigación y medidas de respuesta. Se destacan las mejores prácticas y metodologías para elaborar un plan de contingencia sólido y efectivo que garantice la continuidad del negocio y la protección de los datos y servicios críticos. Además, se discute la importancia de la formación y el entrenamiento del personal en la ejecución del plan de contingencia, así como la necesidad de realizar pruebas y simulacros periódicos para garantizar su efectividad y relevancia continua. La monografía proporciona una visión integral de la importancia y el proceso de elaboración de un plan de contingencia para los sistemas de información del departamento de TICs, con el objetivo de garantizar la continuidad del negocio y la protección de los activos de la organización en caso de un evento adverso.

Palabras clave: Magerit-Activos, Magerit-Amenazas, Magerit-Impacto, Magerit-Riesgo, Plan Contingencia

Abstract

The monograph addresses the critical importance of developing a contingency plan for the information systems of the Department of Information and Communications Technologies (ICTs) in modern organizations. The growing dependence of companies on information systems and the need to guarantee their availability and security at all times is highlighted. The different types of risks to which information systems are exposed are discussed, including cyberattacks, hardware failures, natural disasters, and human errors. The importance of identifying and evaluating these risks is emphasized to develop an effective contingency plan that allows us to respond quickly and efficiently in the event of an adverse event. The process of developing a contingency plan is examined in detail, from identifying critical assets and associated risks to defining mitigation strategies and response measures. The best practices and methodologies are highlighted to develop a solid and effective contingency plan that guarantees business continuity and the protection of critical data and services. Additionally, the importance of training and training personnel in the execution of the contingency plan is discussed, as well as the need to conduct periodic tests and drills to ensure its effectiveness and continued relevance. The monograph provides a comprehensive view of the importance and process of developing a contingency plan for the information systems of the ICT department, with the aim of guaranteeing business continuity and the protection of the organization's assets in the event of a disaster. an adverse event.

Keywords: Magerit-Assets, Magerit-Threats, Magerit-Impact, Magerit-Risk, Contingency Plan

Capítulo I

Introducción

Tema

ELABORACIÓN DE UN PLAN DE CONTINGENCIA PARA LA AUDITORÍA DE LOS SISTEMAS INFORMÁTICOS DEL DEPARTAMENTO DE TICS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL INTERCULTURAL DEL CANTÓN SAQUISILÍ (GADMICS).

Antecedentes

Los sistemas informáticos se han convertido en un elemento crítico para la mayoría de las organizaciones, ya que están involucrados en una amplia gama de procesos y actividades. Los departamentos de tecnología de la información y las comunicaciones (TICs) son los responsables de garantizar la protección y seguridad de los sistemas informáticos y a su vez los datos que procesan.

En los últimos años, se ha producido un aumento significativo en los ataques cibernéticos y las vulnerabilidades de seguridad informática, lo que ha puesto en riesgo la información y los sistemas informáticos de las organizaciones. Además, la normativa y las regulaciones en torno a la seguridad de la información están cada vez más estrictas, y las organizaciones deben cumplir con estos requisitos o enfrentar multas y sanciones.

En este contexto, la auditoría de los sistemas informáticos se ha vuelto cada vez más importante para evaluar la seguridad y confiabilidad de los sistemas informáticos de una organización. Las auditorías permiten identificar riesgos y debilidades en los sistemas informáticos, y ofrecen recomendaciones para mejorar la seguridad y la protección de los sistemas y datos.

Por lo tanto, es fundamental elaborar un plan de contingencia para la auditoría de los sistemas informáticos del departamento de TICs. De esta forma, de esta forma se asegura la

protección de los sistemas informáticos y la continuidad de las operaciones en caso de sufrir incidentes de seguridad informática. Además, la elaboración del plan de contingencia permite cumplir con los requisitos de auditoria y regulación de seguridad de la información.

Planteamiento del problema

El GADMIC Saquisilí es una institución descentralizada que elabora ordenanzas municipales, fiscalización de los recursos públicos, elaboración del presupuesto del cantón, regularizaciones de propiedades, planificación territorial junto con la realización de obras públicas, todo ello en concordancia con los planes parroquiales, provincial y nacional de desarrollo.

La importancia de los datos almacenados de los sistemas, a menudo se presentan problemas que empeoran su estabilidad y seguridad, así como en 2018, el departamento de TICs del GADMICS sufrió una pérdida de información a gran escala debido a la falta de medidas de seguridad apropiadas. Esta situación resultó en la detención temporal de las actividades de la institución, lo que resultó de la insatisfacción entre los usuarios que dependen de los servicios provistos por el GADMICS

A pesar de este incidente, en la actualidad, el departamento de TICs aún no dispone de un plan de contingencia específico para auditar sus sistemas informáticos y reducir los riesgos de futuros problemas similares en el futuro. Además, la falta de un plan de contingencia puede perjudicar la protección de la información y los activos críticos del departamento de TICs, así como afectar la capacidad de la institución para continuar sus operaciones de manera eficiente y efectiva en caso de interrupciones del servicio.

Por lo tanto, se plantea la elaboración de un plan de contingencia para la auditoría de los sistemas informáticos del departamento de TICs, con la finalidad de que el mismo pueda estar preparado para responder de manera oportuna y efectiva ante incidentes de seguridad informática, minimizando los impactos negativos en la información y activos críticos de la institución, así como la insatisfacción de los usuarios que depende de sus servicios.

Justificación

La creciente dependencia de los sistemas informáticos en las organizaciones ha generado una necesidad cada vez mayor de proteger los datos y sistemas de posibles amenazas y riesgos que pueden afectar su integridad y disponibilidad. Resulta fundamental contar con un plan de contingencia que permita afrontar situaciones de emergencia de manera efectiva y reducir los efectos adversos potenciales que puedan surgir durante la realización de las actividades de una organización

En el caso del GADMICS, una institución que cumple funciones importantes en la planificación y ejecución de proyectos de desarrollo local, la pérdida o inaccesibilidad de la información por problemas en los sistemas informáticos puede afectar el cumplimiento de sus responsabilidades. Por tanto, garantizar la protección de los sistemas informáticos resulta esencial para la continuidad de las operaciones de la institución y la satisfacción de los usuarios.

Además, la elaboración de un plan de contingencia para la auditoría de los sistemas informáticos del departamento de TICs no solo permite afrontar situaciones de emergencia, sino que también contribuye a mejorar la gestión del riesgo en la organización y a garantizar el cumplimiento de las normativas y reglamentos en materia de seguridad de la información. En este sentido, la presente investigación busca aportar al refuerzo de la gestión de los sistemas informáticos en el GADMICS y a la mejora en la calidad de sus servicios a la comunidad.

Objetivos

Objetivo General

Elaborar un plan de contingencia para la auditoria de los sistemas informáticos del departamento de TICs del Gobierno Autónomo Descentralizado Municipal Intercultural del Cantón Saquisilí (GADMICS) con la finalidad de precautelar la información del mismo

Objetivos Específicos

- Identificar y comparar las metodologías de análisis y gestión de riesgos disponibles en el mercado, con el fin de seleccionar la que mejor se adapte a las necesidades del departamento de TICs del GADMICS, para garantizar la protección de su información.
- Identificar los activos críticos del departamento de TICs del GADMICS utilizando la metodología seleccionada para evaluar las amenazas y los riesgos asociados a cada activo.
- Elaboración y entrega del plan de contingencia al departamento de Tics del GADMICS.

Alcance

El presente proyecto incluye el análisis de las metodologías de gestión de riesgos existentes en el mercado y la selección de la más adecuada para proteger la información del departamento de TIC. Además, se llevará a cabo la identificación de los activos críticos del departamento para una gestión adecuada de las amenazas y riesgos a los que se enfrenta.

La elaboración del plan de contingencia será el resultado final del trabajo, el cual producirá la definición de las acciones y los procedimientos a seguir en situaciones de emergencia o contingencia que puedan surgir en los sistemas informáticos. Dicho plan se entregará en el departamento de TICs para su implementación y seguimiento.

Es importante destacar que este trabajo no abarcara la implementación del plan de contingencia, ni la ejecución de la auditoría de los sistemas informáticos del departamento de TICs

Capítulo II

Marco teórico

Sistemas Informáticos

Los sistemas informáticos son conjuntos de hardware y software que trabajan juntos para proporcionar un conjunto de servicios a los usuarios. Los sistemas informáticos pueden variar en complejidad desde dispositivos simples, como un teléfono inteligente o una computadora portátil, hasta sistemas complejos de alta disponibilidad y escalabilidad que pueden soportar aplicaciones empresariales críticas.

Los sistemas informáticos se utilizan en una amplia variedad de aplicaciones, como en la gestión de negocios, la educación, la investigación científica, la comunicación, el entretenimiento, entre otros. En la actualidad, los sistemas informáticos han evolucionado para soportar una amplia gama de dispositivos, incluyendo computadoras personales, servidores, dispositivos móviles, la nube, Internet de las cosas, entre otros.

Los sistemas informáticos son esenciales para las empresas y organizaciones, ya que pueden ayudar a aumentar la eficiencia, la productividad y la capacidad de innovación. Sin embargo, también pueden ser vulnerables a amenazas como ataques cibernéticos, malware y fallas técnicas, lo que subraya la importancia de la seguridad de los sistemas informáticos

Seguridad Informática

Nos encontramos en una era en donde la información es uno de los recursos más preciados, nuestro mundo está rodeado de millones de datos almacenadas de distintas maneras y distribuidas en diferentes formas; por ende, la información es primordial tanto para personas cotidianas, como para las empresas ya que sin ella el proceso de planificación, control y toma de decisiones, no sería tan sencillo de manejar.

La información es un conjunto de datos transformados en forma significativa que contribuya a reducir la incertidumbre del futuro y, por tanto, ayuda la toma de decisiones y

acciones, la relación entre los datos y la información es equivalente a la que existe entre la materia prima y el producto acabado. Una información será significativa en cuanto que sea útil como materia prima para una decisión determinada. (Lapiedra y Carlos Devece, 2011)

Activos

Los activos informáticos son los recursos digitales que posee una empresa, organización o individuo y que tienen valor económico y se utilizan para generar ingresos o beneficios. Estos activos incluyen todo tipo de recursos informáticos, como hardware, software, redes, datos y cualquier otra infraestructura digital utilizada para apoyar la operación y los procesos de la organización.

Los activos informáticos incluyen:

Hardware: incluye todo el equipo físico que se utiliza en una organización, como ordenadores, portátiles, servidores, impresoras, escáneres, dispositivos móviles y cualquier otro tipo de dispositivo electrónico utilizado para procesar y almacenar datos.

Software: incluye todo el software instalado en los dispositivos informáticos, como sistemas operativos, aplicaciones empresariales, software de seguridad y cualquier otro tipo de software utilizado para automatizar procesos y operaciones.

Redes: incluye los componentes de la red informática, como enrutadores, conmutadores, hubs, firewalls y cualquier otro tipo de dispositivo utilizado para proporcionar conectividad y seguridad a la red.

Datos: son uno de los activos más importantes de la seguridad informática. Esto incluye información confidencial de los clientes, datos financieros, contraseñas, información de identificación personal y cualquier otra información que deba mantenerse segura.

Infraestructura física: la infraestructura física, como los centros de datos, los armarios de servidores, las instalaciones de almacenamiento y cualquier otra infraestructura utilizada para alojar y proteger los sistemas informáticos, también son importantes activos de la seguridad informática.

Los activos informáticos son esenciales para la operación de la mayoría de las organizaciones en la actualidad y, por lo tanto, es importante que se protejan adecuadamente para garantizar la continuidad del negocio y la privacidad de los datos.

Amenazas

En sistemas de información se entiende por amenaza la presencia de uno o más factores, elementos o acciones que de tener la oportunidad atacarían al sistema produciéndole daños (en el peor de los casos irreparables) aprovechándose de su nivel de vulnerabilidad. (López, 2010). A continuación, se describen algunas de las amenazas más comunes que se consideran en el análisis de riesgo:

- Ciberataques: los ciberataques son una amenaza común en el análisis de riesgo y pueden incluir ataques de phishing, malware, ransomware, ataques de denegación de servicio (DDoS) y otros tipos de ataques informáticos.
- Desastres naturales: los desastres naturales, como terremotos, incendios, inundaciones y huracanes, pueden causar daños a la infraestructura de la organización y a los activos.
- Errores humanos: los errores humanos, como el mal uso del software o hardware, la divulgación accidental de información confidencial, el uso inadecuado de los recursos y el mal juicio pueden causar daños a los activos de la organización.
- Amenazas internas: las amenazas internas, como el robo de información confidencial, la mala conducta de los empleados, la negligencia y el sabotaje, pueden ser un riesgo para la seguridad de los activos de la organización.

- Amenazas externas: las amenazas externas, como la competencia desleal, el espionaje industrial, el vandalismo y los robos, pueden afectar la seguridad de los activos de la organización.

Es importante tener en cuenta que las amenazas varían según la organización, la industria y el entorno en el que se encuentra la organización. Por lo tanto, es importante que se realice un análisis de riesgo completo y detallado para identificar las amenazas específicas y mitigar los riesgos de manera efectiva.

Riesgo

Se refiere a la probabilidad de que ocurran eventos no deseados relacionados con los sistemas informáticos y la información que manejan. Los riesgos informáticos pueden incluir la pérdida o corrupción de datos, la interrupción de los servicios, la violación de la privacidad, la infracción de derechos de autor, la exposición a ciberataques, entre otros. El riesgo puede ser causado por diversos factores, como la incertidumbre, la complejidad, la falta de información y la falta de control. El riesgo puede ser mitigado o reducido mediante la aplicación de estrategias y medidas de gestión de riesgos, como la identificación, evaluación, prevención, control y transferencia de riesgos

Impacto

El impacto se refiere al grado de daño o pérdida que se puede producir como resultado de un evento no deseado, como un fallo en el sistema, un ataque cibernético o un desastre natural. El impacto puede manifestarse en diferentes aspectos del sistema, como la disponibilidad, la confidencialidad, la integridad o la funcionalidad. Por ejemplo,

- La disponibilidad se refiere al grado en que el evento afecta la capacidad del sistema para estar disponible y operativo para cumplir con los objetivos del negocio.

- La confidencialidad se refiere al grado en que el evento puede afectar la capacidad del sistema para mantener la privacidad y la confidencialidad de la información que administra.
- La integridad se refiere al grado en que el evento puede afectar la capacidad del sistema para mantener la precisión y la consistencia de la información.

El impacto puede ser medido en diferentes niveles, desde pequeñas interrupciones hasta daños graves en la operación del sistema, pasando por la pérdida de datos, la interrupción de los servicios y la degradación del rendimiento. La evaluación del impacto es una parte importante del análisis de riesgos, se utiliza para identificar y priorizar los riesgos potenciales y las medidas de seguridad necesarias para minimizar o mitigar el impacto en caso de que se produzca un evento no deseado.

Análisis de riesgos

El análisis de riesgos es un procedimiento sistemático que se utiliza para identificar, evaluar y mitigar los riesgos asociados con una actividad o proyecto en particular. El objetivo del análisis de riesgos es identificar los riesgos que podrían afectar el éxito de un proyecto y desarrollar planes para mitigar o eliminar estos riesgos.

El análisis de riesgos se puede dividir en 5 etapas:

- Determinación de los activos de información: En esta etapa se identifican y recopilan los activos de información relevantes, tales como datos, sistemas, redes y aplicaciones.
- Determinación de las amenazas: En esta etapa se identifican las amenazas que pueden afectar a los activos de información. Estas amenazas pueden ser internas o externas y pueden ser causadas por factores como el mal uso, errores humanos, fallos del sistema, desastres naturales o ataques malintencionados.

- Determinación de las vulnerabilidades: se identifican las vulnerabilidades que pueden ser explotadas por las amenazas identificadas. Estas vulnerabilidades pueden ser debilidades en los sistemas, las redes, los procesos o los procedimientos que facilitan el acceso no autorizado a los activos de información.
- Evaluación de los riesgos: se evalúa el nivel de riesgo asociado con cada amenaza y vulnerabilidad identificada. Esta evaluación tiene en cuenta la probabilidad de que se produzca el riesgo, la gravedad de las consecuencias y la efectividad de las medidas de seguridad existentes.
- Identificación de las medidas de seguridad: se identifican las medidas de seguridad necesarias para mitigar los riesgos identificados. Estas medidas pueden incluir la implementación de controles de seguridad técnicos y organizativos, la formación del personal, la implementación de planes de contingencia y la monitorización de la actividad del sistema.

El análisis de riesgos es una herramienta valiosa para ayudar a los proyectos a identificar y mitigar los riesgos que podrían afectar su éxito. Al identificar los riesgos y desarrollar planes para mitigarlos, los proyectos pueden reducir la probabilidad de que ocurran eventos no deseados y aumentar la probabilidad de éxito.

Gestión de riesgo

La gestión de riesgos es un proceso que se utiliza para identificar, evaluar y tomar medidas para reducir los riesgos que una organización puede enfrentar. Es un enfoque sistemático y continuo que implica la identificación de los riesgos potenciales, la evaluación de la probabilidad y el impacto de cada riesgo y la implementación de medidas para reducir el riesgo a un nivel aceptable.

La gestión de riesgos se puede aplicar a una amplia variedad de situaciones, desde la planificación estratégica hasta la gestión de proyectos y la seguridad informática. Las

empresas utilizan la gestión de riesgos para minimizar los riesgos que podrían afectar su capacidad para alcanzar sus objetivos, y para asegurar que estén preparados para enfrentar cualquier situación imprevista.

- Identificación de riesgos: en esta etapa, se identifican todos los riesgos potenciales que podrían afectar el proyecto. Esto se puede lograr mediante la revisión de los registros históricos, el análisis de los informes de los expertos, la realización de entrevistas y el uso de herramientas de análisis.
- Evaluación de riesgos: en esta etapa, se evalúa la probabilidad de que cada riesgo identificado ocurra y el impacto que tendría si ocurriera. Esto ayuda a priorizar los riesgos y desarrollar planes para mitigarlos.
- Mitigación de riesgos: en esta etapa, se desarrollan planes para mitigar o eliminar los riesgos identificados. Estos planes pueden incluir medidas preventivas para reducir la probabilidad de que ocurra un riesgo, o medidas correctivas para reducir el impacto del riesgo si ocurre.
- Monitoreo y revisión: se monitorean y revisan continuamente los riesgos para asegurarse de que las medidas de mitigación sigan siendo efectivas y de que se tomen medidas adicionales si es necesario.

Metodologías de análisis de riesgo

Metodología MAGERIT

Es una metodología de análisis y gestión de riesgos de los sistemas de información fue elaborada por el consejo superior de administración electrónica de España (CSAE) con el propósito de implementar procesos de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información (Gómez et al., 2012).

Los objetivos directos de la metodología Magerit se enfocan en concienciar a los responsables de las organizaciones de la información sobre la existencia de los riesgos y la necesidad de gestionarlos además de ofrecer un método sistemático para realizar un análisis de riesgos derivados del uso de tecnologías de la información y comunicación (TIC) y así mismo de ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control. Magerit está enfocado de igual manera en capacitar a las organizaciones para procesos de evaluación, auditoria, certificación o acreditación. (Administrativa, 2012)

Procesos de la metodología de MAGERIT

La metodología MAGERIT se enfoca en la gestión de riesgos de seguridad de la información por lo que detallaremos a continuación sus dos pasos esenciales

Primer paso: análisis de riesgo

En esta tarea permite determinar lo que posee la organización y se trata de estimar que posibles eventos podrían ocurrir, para el análisis de riesgos se considera los siguientes elementos:

1. Los activos son elementos de valor que posee una organización y que necesitan ser protegidos adecuadamente pueden ser de diferentes tipos, incluyendo información, hardware, software, instalaciones, personal y procesos. La identificación y protección de los activos críticos es esencial en la gestión de los riesgos de la seguridad de la información (2018).
2. Las amenazas son eventos potenciales que pueden causar daño o impacto negativo en los activos de una organización pueden ser de origen natural o humano, y pueden incluir ciberataques, desastres naturales, errores humanos, entre otros. La identificación y evaluación de las amenazas es

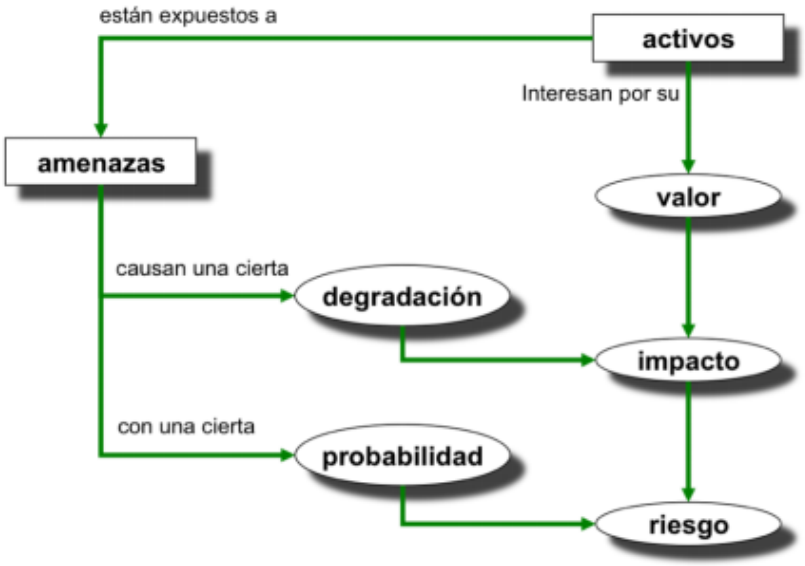
esencial para la gestión efectiva de riesgos de seguridad de la información (2018).

3. Las salvaguardas son medidas o acciones que se implementan para reducir o mitigar los riesgos asociados con las amenazas identificadas pueden ser técnicas, organizativas o legales y pueden incluir la implementación de controles de acceso, la realización de copias de seguridad, el establecimiento de políticas de seguridad, entre otros. La identificación y selección de las salvaguardas adecuadas es esencial para la gestión efectiva de riesgos de seguridad de la información (2018).

Una vez que se han identificado los elementos críticos se puede evaluar el impacto potencial y la probabilidad de que prevengan los riesgos de seguridad de la información. Con esta evaluación, se pueden tomar decisiones informadas sobre cómo tratar los riesgos identificados

Figura 1

Método de análisis de riesgo



Nota. La metodología Magerit sigue una serie de pasos para realizar el análisis de riesgo y determinar los riesgos

Segundo paso: tratamiento del riesgo

Esta etapa consiste en seleccionar y aplicar medidas de seguridad adecuadas para reducir o minimizar los riesgos identificados. Para ello, se deben evaluar las opciones disponibles y seleccionar las medidas más efectivas y rentables para tratar los riesgos identificados.

Es importante destacar que el tratamiento de riesgo no garantiza una protección absoluta contra los riesgos de seguridad de la información, pero ayuda a reducir el impacto y la probabilidad de que se escondan. Además, debe ser un proceso continuo y evolutivo, ya que los riesgos y amenazas cambian constantemente y las medidas de seguridad deben ser actualizadas y mejoradas para garantizar una protección efectiva.

Aspectos importantes de la metodología MAGERIT

MAGERIT se enfoca en la gestión integral de los riesgos de la seguridad de la información, abarcando tanto los aspectos técnicos como los organizativos y legales. Esta perspectiva holística permite una identificación más completa y efectiva de los riesgos y una mitigación más efectiva de los mismos (Muñoz, 2017).

La metodología se enfatiza en la importancia de comprender el contexto en el que se encuentra la organización y cómo influye en su exposición a los riesgos de seguridad de la información lo que nos permite evaluar de manera efectiva los riesgos y su impacto en el negocio, además de proporcionar una estructura clara y sistemática para realizar el análisis de riesgos y establecer medidas de seguridad efectivas (Lopez, 2018). La metodología se compone de seis fases bien definidas, que se enfocan en la identificación de activos, amenazas y vulnerabilidades, la evaluación de los riesgos, el tratamiento de los mismos y el seguimiento continuo (Fuentes, 2019).

Si hablamos de modelos de análisis de riesgos MAGERIT utiliza un modelo basado en la probabilidad de ocurrencia y el impacto que tendría un incidente en el negocio. Esto

permite una evaluación más objetiva y sistemática de los riesgos, lo que a su vez permite establecer medidas de seguridad más efectivas.

Si bien sabemos que MAGERIT es una metodología estructurada, es lo suficientemente flexible como para adaptarse a las necesidades específicas de cada organización. La metodología puede ser aplicada a organizaciones de cualquier tamaño y sector, y se puede ajustar a los requisitos y objetivos específicos de cada organización.

Metodología OCTAVE

Es un método de identificación y evaluación de riesgos desarrollada por el instituto de ingenieros de software o SEI (Software Engineering Institute) en la Universidad de Carnegie Mellon en Estados Unidos orientado a procesos que se utiliza para ayudar a las organizaciones a identificar y gestionar los riesgos de seguridad de la información. La metodología se enfoca en evaluar los riesgos de seguridad de la información en términos de procesos de negocio, y se basa en la comprensión de las amenazas, vulnerabilidades y activos de información crítica.

(Campos y León) describen en su trabajo de titulación algunos de los objetivos de la metodología

- Desarrollar criterios cualitativos de evaluación de riesgos que describan las tolerancias de riesgo operacional de la organización.
- Identificar activos que son importantes para la organización.
- Identificar vulnerabilidades y amenazas a esos activos.
- Determinar y evaluar posibles consecuencias para la organización. (2020)

Etapas de OCTAVE

La metodología OCTAVE cuenta con tres fases que se detallan a continuación

Fase 1: Vista organizacional

Considera la construcción de perfiles activo-amenaza, recopilando los activos más importantes, así como las amenazas y requisitos que pueden afectar negativamente a los activos

Fase 2: Vista tecnológica

A nivel de la infraestructura de las tecnologías de información se identifican las vulnerabilidades a las que están expuestos la organización (Huertas, 2012)

Fase 3: Planificación de las medidas y reducción de los riesgos

Se elabora un plan defensa, en donde se analizan los riesgos en base al impacto que puede llegar a tener los activos críticos de una organización, y posteriormente realizar una estrategia de protección. (Oscar y Edison, 2019)

Metodología EBIOS

Es una metodología francesa que comprende un conjunto de guías y herramienta de software de código abierto gratuito, dedicado a los administradores de riesgos del sistema de información, se utiliza ampliamente tanto en el sector público como en el privado, cumple con los principales estándares de seguridad de TI. (Enisa, 2005)

El método EBIOS permite apreciar y tratar los riesgos relativos a la seguridad de los sistemas de información (SSI). Posibilita también la comunicación dentro del organismo y también con los asociados para contribuir al proceso de la gestión de los riesgos SSI. (nacional, El método EBIOS®, 2003)

Fases de EBIOS

FASE 1: se ocupa del análisis del contexto en términos de la dependencia del proceso empresarial global del sistema de información (contribución a los intereses globales, definición precisa del perímetro, descomposición relevante en flujos de información y funciones). (Enisa, 2005)

FASES 2 Y 3: se llevan a cabo el análisis de necesidades de seguridad y el análisis de amenazas, determinando los puntos de conflicto (Enisa, 2005)

FASES 4 Y 5, Resolución del conflicto, estableciendo los objetivos de seguridad necesarios y suficientes, con pruebas de su cumplimiento y dejando claros cuales son los riesgos residuales. (Solarte, 2016)

Criterio de selección de metodología

Tabla 1

Criterio de evaluación

Parámetros de evaluación	**Metodologías**		
	Magerit	**Ebios**	**Octave**
Identificación de activos	✓	✓	✓
Identificación de amenazas	✓	✓	✓
Identificar salvaguardas	✓		
Determinación de la probabilidad	✓	✓	✓
Análisis del impacto	✓	✓	✓
Establecimiento de parámetros	✓		✓
Determinación del riesgo	✓	✓	✓
Estudio cuantitativo	✓		
Estudio cualitativo	✓		

Dentro del análisis comparativo expuesto en la tabla se llegó a la conclusión que las metodologías Magerit, Octave y Ebios son similares en cuanto a:

- Identificación de activos y amenazas
- Detección de debilidades de los sistemas de informáticos
- Análisis del Impacto

- Resolución del Riesgo
- Establecer parámetros de seguridad informática

Así podemos establecer que cada metodología tiene sus propias características pueden ser utilizadas adecuadamente en la organización, pero para fines del presente proyecto adaptaremos la metodología Magerit con su respectiva herramienta Pilar.

Plan de contingencia

Un plan de contingencia es un conjunto de procedimientos y estrategias preparados de antemano para hacer frente a posibles situaciones de emergencia o crisis que puedan afectar a una organización, empresa, comunidad o cualquier otro ente.

El objetivo principal de un plan de contingencia es minimizar el impacto de un evento imprevisto o desastre en el funcionamiento normal de la organización, la seguridad de las personas y la continuidad del negocio. El plan establece los roles y responsabilidades de las personas involucradas en la gestión de la crisis, así como los recursos necesarios para hacer frente a la situación de emergencia.

El plan de contingencia también identifica los riesgos potenciales y los escenarios de crisis más probables, y establece las medidas preventivas y correctivas necesarias para reducir su impacto y mitigar sus efectos. En resumen, un plan de contingencia es una herramienta esencial para la gestión del riesgo y la preparación para posibles situaciones de emergencia.

Auditoria

La auditoría se refiere a un proceso sistemático de evaluación y verificación de los controles y procedimientos relacionados con los sistemas de información de una organización. Su objetivo principal es evaluar la eficacia, la seguridad y el cumplimiento normativo de los sistemas informáticos y la infraestructura tecnológica de una empresa.

Para garantizar la confiabilidad de la información, la integridad de los sistemas, la protección de los activos digitales y el cumplimiento de las políticas y normas establecidas.

Durante el proceso de auditoría, se analizan diversos aspectos relacionados con los sistemas informáticos, como la seguridad de la red, la gestión de accesos, la protección de datos, el cumplimiento de las normas de privacidad, el backup y la recuperación de datos, entre otros

En resumen, la auditoría informática es un proceso crítico para evaluar y mejorar la seguridad y el cumplimiento normativo de los sistemas de información en una organización, garantizando así la confiabilidad y el adecuado funcionamiento de los sistemas informáticos y protegiendo los activos digitales de la organización.

Capítulo III

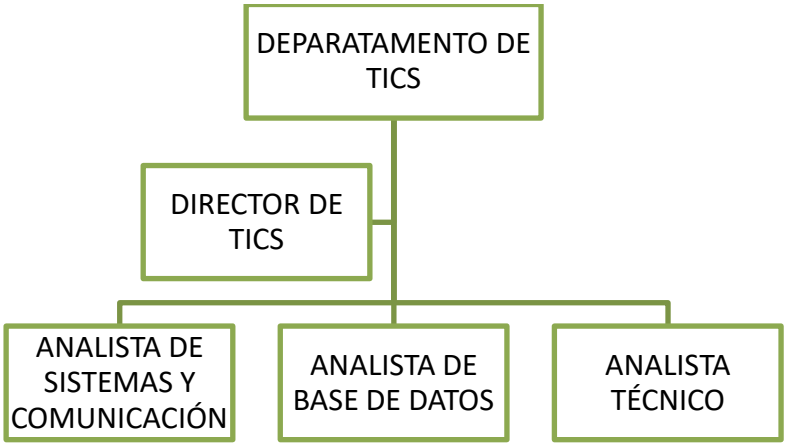
Desarrollo del tema

Situación actual del departamento de TICs del GADMICS

El trabajo de tesis se realizó en el departamento de tecnologías de la información y comunicación (TIC) que depende directamente del gobierno Autónomo Descentralizado Municipal Intercultural del Cantón Saquisilí (GADMICS) el cual es una institución pública cuyo objetivo principal es el desarrollo social, económico y ambiental de dicho cantón; con tal finalidad ejerce una labor eficiente, transparente y confiable que están sujetas a políticas, estrategias u objetivos de un plan de desarrollo de participación; contribuyendo así a la satisfacción de las necesidades de la comunidad

Por ende, el departamento de TIC´s tiene dentro de sus funciones administrar la seguridad, integridad y confiabilidad en el acceso de la base de datos de los sistemas de la organización, creación y autenticación de perfiles de usuario y contraseñas, corrección de inventarios y proyectos en la base de datos al igual que la migración de las mismas; además del mantenimiento de los sistemas informáticos y su infraestructura tecnológica.

Esquema del departamento de TICs



Descripción de los cargos del área de sistemas

A continuación, se detallan las funciones que desempeña el personal del departamento de TICs.

Tabla 2

Descripción del cargo de Director de TICs

Designación del Rol	DIRECTOR DE TICS
Funciones:	Responsable de administrar y representar el departamento de tics Encargado del proceso de contratación de equipos y software Revisión de servidores periódicamente para su óptimo desarrollo Instalación y mantenimiento de equipos

Tabla 3

Descripción del cargo sistemas y comunicación

Designación del Rol	ANALISTA DE SISTEMAS Y COMUNICACIÓN
Funciones:	Inventario de perfiles de usuario Mantenimiento redes lan - wlan Configuraciones de Access Point

Tabla 4

Descripción del cargo de base de datos

Designación del Rol	ANALISTA DE BASE DE DATOS
Funciones:	Responsable de administrar y conceder permisos en las bases de datos de los sistemas informáticos dependiendo de las solicitudes Creación de perfiles de los sistemas de información Respaldos de base de datos Información

Tabla 5

Descripción del cargo de soporte técnico

Designación del Rol	ANALISTA TÉCNICO
Funciones:	Mantenimiento Correctivo y Preventivo de Equipos Instalación de actualizaciones en los Equipos Inventario de Equipos

Incidentes en el departamento de TICs

Actualmente han acontecido varios incidentes como la intrusión en los servidores de base de datos y archivos mediante un virus que no ocasionó problemas mayores; pero el acceso a personal indebido podría llegar a causar problemas irremediables como hace cuatro años que se presentó la caída de uno de los servidores lo que conllevo al daño irremediable, dicho incidente origino la detención en los procesos de cobranza de los predios del GADMIC Saquisilí

Método de análisis de riesgo

Para el buen funcionamiento del plan de contingencia de los sistemas informáticos aplicaremos la metodología Magerit como mencionamos en el análisis de metodologías; el cual nos indica en el libro I que “el análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados” (Administrativa, 2012) los cuales son:

1. Definir los activos importantes para la organización.
2. Definir las amenazas que llegarían a materializarse en aquellos activos.
3. Levantar un plan de salvaguardad ante el riesgo existente
4. Evaluar el impacto sobre los activos ante la amenaza en potencia
5. Evaluar el riesgo de la organización, tales como el riesgo potencial como residual

Para la ejecución del análisis del riesgo informático es importante acoger a las pautas que nos indica el manual de la metodología Magerit: con el apoyo de las entrevistas y visitas técnicas en el departamento de Tics recolectaremos información valiosa que será de gran utilidad para dicho análisis, cabe mencionar que para el análisis de riesgo utilizamos la herramienta Pilar propia de Magerit

Identificación de los activos

Los activos como bien lo mencionamos en el marco teórico son recursos de la organización que pueden estar expuestos a diversas amenazas en el módulo 1 de Magerit se clasifican entre las siguientes categorías:

Tabla 6

Nomenclatura

SIGLAS	DESCRIPCIÓN
[AE]	Activos esenciales
[D]	Datos / Información
[K]	Claves criptográficas
[S]	Servicios
[SW]	Software - Aplicaciones informáticas
[HW]	Equipamiento informático (hardware)
[COM]	Redes de comunicaciones
[Media]	Soportes de información
[AUX]	Equipamiento auxiliar
[L]	Instalaciones
[P]	Personal

Nota. Nomenclatura utilizada por la herramienta EAR/Pilar para clasificar a los activos

Acorde a la clasificación mencionada detallaremos a continuación los activos esenciales del departamento de TIC´s; la herramienta pilar nos permite estructurar los activos mediante capa proporcionando una organización correcta.

Tabla 7

Inventario de activos

ACTIVO	CÓDIGO	NOMBRE
[AE] Activos esenciales	[AE01]	NAS
[D]Datos/ Información	[D001]	Base de datos SQL server
	[D002]	Base de datos PostgreSQL
[S] Servicios	[S001]	Sistema Nacional para la administración de tierras
	[S002]	Sistema de comercialización de servicios
	[S003]	Sistema integrado de tramites al ciudadano
	[S004]	Sistema de gestión administrativa financiera de la asociación de municipalidades ecuatorianas
	[S005]	Sistema integral de catastros
[SW] Software	[SW01]	Anti virus
	[SW02.1]	Windows 2010 pro
	[SW02.2]	Linux
	[SW02.3]	Windows server 2012 R2
	[SW03]	Ofimática
	[SW04]	Monitoreo de red Unifi Network
	[SW05]	Correo electrónico
	[SW06]	Página web Saquisilí
[HW] Hardware	[HW01]	Servidor SIGAME
	[HW02]	Servidor SINAT
	[HW03]	Servidor de aplicación y gestión documental
	[HW04]	Servidor Proxy

ACTIVO	CÓDIGO	NOMBRE
	[HW05]	Servidor de respaldos NAS
	[HW06]	Informática persona
	[HW07]	Medios de impresión
	[modem]	Módems
	[switch]	Conmutador
	[router]	Encaminador
	[anti]	Antenas inalámbricas
[COM] Comunicaciones	[WIFI]	Red inalámbrica
	[LAN]	Red local
	[Inter]	Internet
[AUX] Equipamiento auxiliar	[AUX1]	Fuentes de alimentación
	[AUX2]	sistemas de alimentación ininterrumpida
	[AUX3]	Control antincendios
	[AUX4]	Equipos de climatización
	[AUX5]	Cable eléctrico
	[AUX6]	Cableado de Fibra óptica
[SS] Servicios contratados	[SS01]	Servicio de Internet
[L] Instalaciones	[L001]	Departamento de TIC´s
[P]Personal	[P001]	Administrador de sistema y base de datos
	[P002]	Administrador informativo
	[P003]	Administrador de seguridad
	[P004]	Usuarios externos
	[P005]	Operador

Nota. Listado de los sistemas informáticos del departamento de TIC´s

Dependencia de los activos

Los activos son esenciales en la organización ya que en ellos están almacenados la información y almacenados en diversos sistemas, la dependencia se puede manifestar de diversas formas como, por ejemplo, un sistema informático puede depender de una base de datos para funcionar correctamente, o un activo puede depender de una red de comunicaciones para estar disponible, de igual manera puede haber dependencias de seguridad, donde la seguridad de un activo puede depender de los controles implementados en otros activos

Dicho así, la comprensión de las dependencias de activos es esencial en la gestión de riesgos, ya que permite identificar los posibles impactos en cascada que podrían ocurrir si un activo se ve afectado. Al considerar las dependencias de los activos, se pueden diseñar y aplicar de protección más efectivas para garantizar la disponibilidad, integridad y confidencialidad de los activos de información en su conjunto.

En Magerit disponemos varias formas de representar las dependencias, pero en este caso hemos seleccionado el esquema en mapa porque se observa de mejor manera las dependencias; ya que los activos que se encuentran en la parte superior van a depender de los activos que se encuentras en la parte inferior como muestra la figura.

Representamos en la figura la tabla de colores para una mejor interpretación de las dependencias en Ear/Pilar

Figura 2

Dependencia entre activos

Nota. Esquema en mapa de las dependencias entre activos en la herramienta EAR/Pilar

Valoración de activos

La valoración de activos consiste en identificar y asignar un valor a los activos de información de una organización, es decir, a los recursos que se utilizan para el almacenamiento, procesamiento y transmisión de información; se realiza con el objetivo de poder establecer un orden de prioridades para la gestión de los riesgos, identificar los activos más críticos, establecer los recursos necesarios para protegerlos y definir las medidas de seguridad adecuadas para protegerlos.

Dimensiones de valoración de los activos

Cada dimensión se utiliza para valorar las consecuencias de la materialización de una amenaza porque representa una faceta o aspecto independiente del activo, dependiendo del análisis de riesgos que requiere la organización se puede valor un activo en todas las dimensiones o como se puede centrar en una única dimensión; pero la

valoración que reciba dicho activo en una determinada dimensión, es una medida del perjuicio para la organización si el activo se ve dañado en esa dimensión.

En el catálogo II de Magerit nos explica las dimensiones de valoración al igual de una serie de preguntas para realizar la valoración:

Tabla 8

Dimensiones de valoración

DIMENSIÓN	**PREGUNTAS**
[D] Disponibilidad	¿Qué importancia tendría que el activo no estuviera disponible?
[I] Integridad de los datos	¿Qué importancia tendría que los datos fueran modificados fuera de control?
[C] Confidencialidad de la información	¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?
[A] Autenticidad	¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree? ¿Qué importancia tendría que los datos no fueran realmente imputables a quien se cree?
[T] Trazabilidad	¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio? ¿Qué importancia tendría que no quedara constancia del acceso a los datos?

Nota. Descripción de las dimensiones y preguntas recomendada por Magerit

Tabla 9

Criterio de valorización

Valor		Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
8-6	Alto	Daño grave
5-3	Medio	Daño importante
2-1	Bajo	Daño menor
0	Despreciable	Irrelevante

Nota. Escala de valores utilizada por la herramienta EAR/pilar

A continuación, se aprecia la valoración propia de los activos; cuyo valor establecido se estimó dependiendo de la información recolectada en las entrevistas realizadas al departamento de TICs

Tabla 10

Valoración de activos

	D	I	C	A	T
[AE] ACTIVOS ESENCIALES					
[AE01] NAS	[2]	[9]	[7]	[9]	[9]
[D]DATOS/ INFORMACIÓN					
[D001] Base de datos SQL server	[9]	[9]	[9]	[8]	[8]
[D002] Base de datos PostgreSQL	[9]	[9]	[9]	[9]	[9]
[S] SERVICIOS					
[S001] Sistema Nacional para la administración de tierras	[9]	[9]	[9]	[9]	[9]

	D	I	C	A	T
[S002] Sistema de comercialización de servicios	[9]	[9]	[9]	[9]	[9]
[S003] Sistema integrado de tramites al ciudadano	[9]	[9]	[9]	[9]	[9]
[S004] Sistema de gestión administrativa financiera de la asociación de municipalidades ecuatorianas	[9]	[9]	[9]	[9]	[8]
[S005] Sistema integral de catastros	[9]	[9]	[9]	[9]	[9]
[SW] SOFTWARE					
[SW01] Anti virus	[4]				
[SW02.1]Windows 2010 pro	[8]	[9]	[7]	[8]	[8]
[SW02.2] Linux	[9]	[8]	[7]	[8]	[8]
[SW02.3] Windows server 2012 R2	[9]	[9]	[7]	[9]	[9]
[SW03] Ofimática					[7]
[SW04] Monitoreo de red Unifi Network					[7]
[S006] Correo electrónico	[8]	[7]	[8]	[7]	[7]
[S007] Pagina web Saquisilí		[7]			
[HW] HARDWARE					
[HW01] Servidor SIGAME	[9]	[7]	[8]	[9]	
[HW02] Servidor SINAT	[9]	[7]	[8]	[9]	
[HW03] Servidor de aplicación y gestión documental	[9]	[7]	[7]	[9]	
[HW04] Servidor Proxy	[8]	[6]	[7]	[8]	
[HW05] Servidor de respaldos NAS	[9]	[7]	[8]	[9]	
[HW06] Informática persona	[9]	[7]	[7]	[7]	[8]
[HW07] Medios de impresión	[7]			[3]	[5]
[modem] Módems	[7]				[8]
[switch] Conmutador	[8]				[7]

	D	I	C	A	T
[router] Encaminador	[7]				[7]
[anti] Antenas inalámbricas	[7]				[7]
[COM] COMUNICACIONES					
[WIFI] Red inalámbrica					[7]
[LAN] Red local					[7]
[Inter] Internet	[7]			[8]	[7]
[AUX] EQUIPAMIENTO AUXILIAR					
[AUX1] Fuentes de alimentación	[8]				
[AUX2] Sistemas de alimentación ininterrumpida	[8]				
[AUX3] Sistema de detección y extinción de antincendios	[7]				
[AUX4] Equipos de climatización	[8]				
[AUX5] Cableado de datos (Fibra óptica y Alimentación)	[8]				
[AUX6]Cerradura electromagnética	[8]				[8]
[SS] SERVICIOS CONTRATADOS					
[SS01] Servicio de Internet	[6]	[3]	[3]		
[L] INSTALACIONES					
[L001] Departamento de TICs	[9]				
[P]PERSONAL					
[P001] Administradora de sistema y base de datos	[8]	[9]	[9]		
[P002] Administrador informativo	[6]	[6]	[8]		
[P003] Administrador de seguridad	[8]	[9]	[9]		
[P004] Usuarios externos		[6]			

	D	I	C	A	T
[P005] Operador	[7]	[6]	[8]		

Nota. Valoración de activos por dimensiones en la herramienta EAR/pilar

Características de las amenazas

El objetivo de esta actividad es definir el entorno que los sistemas están probablemente expuesto, identificar posibles amenazas ante determinados activos y que consecuencias acarrearía a la institución ante la posible materialización de dichas amenazadas

Las amenazadas se dividen en cuatro grupos según lo que nos manifiesta la herramienta pilar estandarizada por Magerit

- [N] desastres naturales
- [I] de Origen industrial
- [E] errores y fallos no intencionados
- [A] ataques intencionados

En Magerit, la identificación de las amenazas es una etapa fundamental en el proceso de gestión de riesgos. Consiste en identificar las posibles fuentes o eventos que pueden causar daños o impactos negativos en los activos de información de una organización. La identificación de amenazas se realiza con el objetivo de comprender y evaluar los riesgos a los que están expuestos los activos, a continuación, en la tabla se resume las categorías de amenazas que nos muestra los libros de MAGERIT

Valoración de las amenazas

El objetivo propuesto en la presente tarea es la estimación de la probabilidad y degradación que tienen las amenazas ante su posible materialización sobre determinados

activos. Para valorar las amenazas nos regimos a una escala cualitativa de la probabilidad y la degradación de ocurrencia de las amenazas sobre los activos, los cuales son:

Tabla 11

Criterios de valoración de la probabilidad

Nivel	Criterio
CS	Casi seguro
MA	Muy alta
P	Posible
PP	Poco posible
MR	Muy rara

Nota. La metodología Magerit nos recomienda utilizar una escala de valores para identificar la probabilidad de las amenazas

A continuación, detallamos la escala nominal de la degradación de los activos ante amenaza materializada

Tabla 12

Criterios de valoración de la degradación

Nivel		Porcentaje
T	Total	100%
MA	Muy alta	90%
A	Alta	50%
M	Media	10%
B	Baja	1%

Nota. La metodología Magerit nos proporciona una escala de valorización para la degradación de las amenazas

Valores Acumulados y Repercutidos

De acuerdo con MAGERIT, es posible calcular tanto el impacto como el riesgo, ya sea de forma acumulada o repercutida, en la tabla se redactan las diferencias existentes entre ambas formas de calculo

Tabla 13

Diferencias Impacto Acumulado y Repercutido

	Impacto acumulado	**Impacto repercutido**
Calculado	Para cada activo, por cada amenaza y en cada dimensión	Sobre un activo específico que es afectado por una amenaza determinada
Referencia	Valor acumulado de los activos	Valor propio del activo
Representación	Acumulativo del efecto de múltiples amenazas	El efecto específico de una amenaza

Tabla 14

Diferencias Riesgo Acumulado y Repercutido

	Riesgo acumulado	**Riesgo repercutido**
Calculo	Se calcula el valor de riesgo total de los activos afectados por una amenaza específica	Se calcula el valor de riesgo para un activo específico que es afectado por una amenaza determinada.

	Riesgo acumulado	Riesgo repercutido
Enfoque	Se enfoca en la amenaza y la evaluación de los posibles impactos que tendría en los activos involucrados.	Se enfoca en el activo en sí y se evalúa la magnitud del daño o impacto que tendría sobre él una amenaza específica
Valores	En este caso, se utilizan valores relativos y acumulados por amenaza	En este caso, se utilizan valores absolutos para el activo afectado.
Consideración	Este enfoque es más útil cuando se busca evaluar la escala del impacto de una amenaza en la organización en general.	Este enfoque se enfoca más en evaluar los riesgos específicos para un activo determinado.

Estado de riesgo

Dentro de esta actividad se evaluará y determinará el nivel actual de riesgo asociado a los activos de información en departamento de Tic´s, considerando varios factores, como la probabilidad de que una amenaza se materialice, el impacto potencial que tenga en los activos y las medidas de seguridad existentes para mitigar el riesgo. Con ello se busca obtener una visión clara del nivel de riesgo y comprender la situación de seguridad que se debe emplear en los activos

Determinación del impacto potencial

Es una medida de la gravedad de las consecuencias que podrían derivarse de la materialización de una amenaza sobre un activo, y su valoración es clave para la gestión efectiva de los riesgos en el departamento de Tic´s. (Cañon y Calderón)

Para determinar el impacto potencial, MAGERIT utiliza una escala de valores definida para cada dimensión. Estos valores se utilizan para autorizar un nivel de impacto numérico a cada dimensión en caso de que se produzca una amenaza.

Tabla 15

Escala Impacto Potencial (EAR/Pilar)

Criterio	Valor
	[10] Nivel10
MA: Muy alto	[9] Nivel 9
	[8] Nivel 8
A: Alto	[7] Alto
	[6] Alto (-)
M: Medio	[5] Medio (+)
	[4] Medio
B: Bajo	[3] Medio (-)
	[2] Bajo (+)
MB: Muy bajo	[1] Bajo
	[0] Despreciable

Nota. Escala de valores del impacto potencial y su nomenclatura de código de colores

Los cálculos proporcionados por pilar fueron determinados en base al valor de los activos y la degradación que provocan las amenazas, cabe recalcar que la valoración se determina en función de las dimensiones de valoración de los activos, tales como:

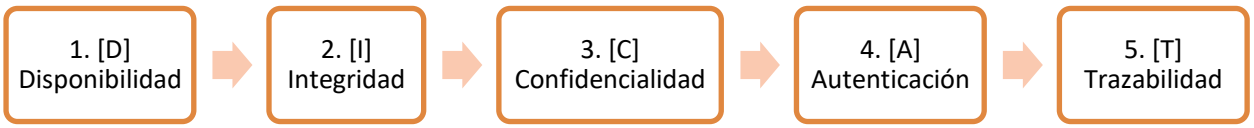


Tabla 16

Impacto Potencial

	D	I	C	A	T
[AE] ACTIVOS ESENCIALES					
[AE01] NAS	[2]	[9]	[7]	[9]	
[D]DATOS/ INFORMACIÓN					
[D001] Base de datos SQL server	[9]	[9]	[9]	[8]	
[D002] Base de datos PostgreSQL	[9]	[9]	[9]	[9]	
[S] SERVICIOS					
[S001] Sistema Nacional para la administración de tierras	[9]	[9]	[9]	[9]	
[S002] Sistema de comercialización de servicios	[9]	[9]	[9]	[9]	
[S003] Sistema integrado de tramites al ciudadano	[9]	[9]	[9]	[9]	
[S004] Sistema de gestión administrativa financiera de la asociación de municipalidades ecuatorianas	[9]	[9]	[9]	[9]	
[S005] Sistema integral de catastros	[9]	[9]	[9]	[9]	
[SW] SOFTWARE					
[SW01] Anti virus	[3]				
[SW02.1] Windows 2010 pro	[8]	[9]	[7]		
[SW02.2] Linux	[9]	[8]	[7]		

	D	I	C	A	T
[SW02.3] Windows server 2012 R2	[9]	[9]	[7]		
[SW03] Ofimática	[6]				
[SW04] Monitoreo de red Unifi Network	[7]				
[S006] Correo electrónico	[8]	[7]	[8]	[7]	
[S007] Pagina web Saquisilí		[7]		[7]	
[HW] HARDWARE					
[HW01] Servidor SIGAME	[9]	[9]	[9]	[9]	
[HW02] Servidor SINAT	[9]	[9]	[9]	[9]	
[HW03] Servidor de aplicación y gestión documental	[9]	[9]	[8]	[9]	
[HW04] Servidor Proxy	[8]	[8]	[8]	[8]	
[HW05] Servidor de respaldos NAS	[9]	[9]	[9]	[9]	
[HW06] Informática personal	[9]	[7]	[7]		
[HW07] Medios de impresión	[7]				
[modem] Módems	[7]				
[switch] Conmutador	[8]				
[router] Encaminador	[7]				
[anti] Antenas inalámbricas	[7]				
[COM] COMUNICACIONES					
[WIFI] Red inalámbrica	[7]				
[LAN] Red local	[8]				
[Inter] Internet	[6]				
[AUX] EQUIPAMIENTO AUXILIAR					
[AUX1] Fuentes de alimentación	[7]				
[AUX2] sistemas de alimentación ininterrumpida	[7]				

	D	I	C	A	T
[AUX3] Control antincendios	[6]				
[AUX4] Equipos de climatización	[7]				
[AUX5] Cableado de datos (Fibra óptica y Alimentación)	[7]				
[AUX6]Cerradura electromagnética	[8]				
[SS] SERVICIOS CONTRATADOS					
[SS01] Servicio de Internet	[5]				
[L] INSTALACIONES					
[L001] Departamento de TICs	[8]				
[P]PERSONAL					
[P001] Administradora de sistema y base de datos		[8]	[8]		
[P002] Administrador informativo		[8]	[8]		
[P003] Administrador de seguridad		[8]	[8]		
[P004] Usuarios externos		[5]			
[P005] Operador		[5]	[7]		

Nota. Tabla de resultado del Impacto potencial calculado por la herramienta EAR/Pilar

Determinación del riesgo potencial

El riesgo se calcula al multiplicar la probabilidad de una amenaza por el impacto potencial en el activo afectado, mientras más alto el impacto y la probabilidad el riesgo es mayor, así como se muestra en la figura

La herramienta PILAR para identificar los niveles de criticidad utiliza una escala de colores que está estructurado de la siguiente manera

Figura 3

Código de color del Riesgo

Nota. La herramienta EAR/Pilar utiliza una escala de valores para clasificar los riesgos

Tabla 17

Riesgo Potencial

	D	I	C	A	T
[AE] ACTIVOS ESENCIALES					
[AE01] NAS	{2,1}	{6,2}	{5,1}	{6,2}	
[D]DATOS/ INFORMACIÓN					
[D001] Base de datos SQL server	{6,2}	{6,2}	{6,2}	{5,7}	
[D002] Base de datos PostgreSQL	{6,2}	{6,2}	{6,2}	{6,2}	
[S] SERVICIOS	{6,2}	{6,2}	{6,2}	{6,2}	

	D	I	C	A	T
[S001] Sistema Nacional para la administración de tierras	{6,2}	{6,2}	{6,2}	{6,2}	
[S002] Sistema de comercialización de servicios	{6,2}	{6,2}	{6,2}	{6,2}	
[S003] Sistema integrado de tramites al ciudadano	{6,2}	{6,2}	{6,2}	{6,2}	
[S004] Sistema de gestión administrativa financiera de la asociación de municipalidades ecuatorianas	{6,2}	{6,2}	{6,2}	{6,2}	
[S005] Sistema integral de catastros	{6,2}	{6,2}	{6,2}	{6,2}	
[SW] SOFTWARE					
[SW01] Anti virus	{2,8}				
[SW02.1] Windows 2010 pro	{5,7}	{6,2}	{5,1}		
[SW02.2] Linux	{6,2}	{5,7}	{5,1}		
[SW02.3] Windows server 2012 R2	{6,2}	{6,2}	{5,1}		
[SW03] Ofimática	{4,5}				
[SW04] Monitoreo de red Unifi Network	{5,1}				
[S006] Correo electrónico	{5,7}	{5,1}	{6,0}	{4,2}	
[S007] Pagina web Saquisilí		{5,1}		{4,2}	
[HW] HARDWARE					
[HW01] Servidor SIGAME	{6,2}	{6,2}	{6,2}	{6,2}	
[HW02] Servidor SINAT	{6,2}	{6,2}	{6,2}	{6,2}	
[HW03] Servidor de aplicación y gestión documental	{6,2}	{6,2}	{5,7}	{6,2}	

	D	I	C	A	T
[HW04] Servidor Proxy	{5,7}	{4,8}	{5,1}	{5,7}	
[HW05] Servidor de respaldos NAS	{6,2}	{6,2}	{6,2}	{6,2}	
[HW06] Informática persona	{6,2}	{5,1}	{5,1}		
[HW07] Medios de impresión	{6,8}				
[modem] Módems	{5,1}				
[switch] Conmutador	{5,7}				
[router] Encaminador	{5,1}				
[anti] Antenas inalámbricas	{5,1}				
[COM] COMUNICACIONES					
[WIFI] Red inalámbrica	{5,1}				
[LAN] Red local	{5,7}				
[Inter] Internet	{4,5}				
[AUX] EQUIPAMIENTO AUXILIAR					
[AUX1] Fuentes de alimentación	{4,2}				
[AUX2] sistemas de alimentación ininterrumpida	{4,2}				
[AUX3] Control antincendios	{3,7}				
[AUX4] Equipos de climatización	{4,2}				
[AUX5] Cableado de datos (Fibra óptica y Alimentación)	{4,2}				
[AUX6]Cerradura electromagnética	{5,4}				
[SS] SERVICIOS CONTRATADOS					
[SS01] Servicio de Internet	{3,0}				
[L] INSTALACIONES					

	D	I	C	A	T
[L001] Departamento de TICs	{5,7}				
[P]PERSONAL					
[P001] Administradora de sistema y base de datos		{4,8}	{4,8}		
[P002] Administrador informativo		{4,8}	{4,8}		
[P003] Administrador de seguridad		{4,8}	{4,8}		
[P004] Usuarios externos		{3,0}			
[P005] Operador		{3,9}	{4,2}		

Nota. Tabla de resultados del riesgo potencial en la herramienta EAR/Pilar

Caracterización de salvaguardas

Las salvaguardas o contramedidas se definen como procedimientos o mecanismos tecnológicos que ayudan a reducir el riesgo asociado a un activo y permiten hacer frente a las amenazas (Amutio & Candau, 2012).

Esta actividad se compone de dos pasos específicos:

- Identificación de las salvaguardas: Consiste en reconocer y enumerar las medidas de protección disponibles que pueden contrarrestar las amenazas identificadas.
- Valoración de las salvaguardas: Implica evaluar y determinar la eficacia y relevancia de cada salvaguarda en relación con las amenazas específicas.

Para llevar a cabo esta tarea, utilizaremos la herramienta Pilar, que nos proporcionará el apoyo necesario. Mediante esta herramienta, seleccionaremos las salvaguardas más apropiadas que nos permitan atenuar y enfrentar las amenazas identificadas.

Identificación y valoración de salvaguardas

Las salvaguardas existentes se han determinado considerando los criterios de clasificación de seguridad especificados por MAGERIT. Estos criterios se dividen en diferentes aspectos que abordan distintas áreas de protección. Para facilitar la identificación y selección de las salvaguardas apropiadas, se utilizan las siguientes designaciones:

G	Salvaguardas relacionadas con la gestion de la seguridad de la información a nivel estratégico y organizacional. Incluye políticas de seguridad, marcos de gobierno, procedimientos de gestión de riesgos y capacitación del personal
T	Salvaguardas de naturaleza técnica, que se implementan a nivel de infraestructura y sistemas de información. Incluye medidas como firewalls, sistemas de detección de intrusiones, cifrado, autenticación de usuarios y copias de segurida
F	Salvaguardas que abordan aspectos físicos de seguridad, como el control de acceso a instalaciones, sistemas de vigilancia, protección contra incendios y seguridad de los equipos físicos
P	Salvaguardas centradas en la gestión de las personas y el factor humano en la seguridad de la información. Incluye políticas de contratación, programas de concienciación en seguridad, políticas de uso aceptable y procedimientos de manejo de incidentes.

Además de los aspectos detallados anteriormente en la metodología MAGERIT se pueden identificar diferentes tipos de medidas de protección para reducir el riesgo. Algunos de los tipos de protección que se pueden considerar son los siguientes:

Tabla 18

Tipos de Protección

[PR]	Prevención
[DR]	Disuasión
[EL]	Eliminación
[IM]	Minimización del impacto

[CR]	Corrección
[RC]	Recuperación
[AD]	Administrativa
[AW]	Concienciación
[DC]	Detección
[MN]	Monitorización

Nota. La herramienta EAR/Pilar utiliza una escala de medidas de protección para clasificar y tratar los riesgos

Para evaluar el grado de efectividad y eficiencia de las salvaguardas implementadas en las amenazas la herramienta Pilar utiliza los siguientes niveles de madurez, cabe mencionar que cuanto más alto sea el nivel de madurez de una salvaguarda, mayor será su eficacia para mitigar el riesgo asociado a una amenaza identificada.

Tabla 19

Niveles de eficacia y madurez

Factor	**Nivel**	**Significado**
0%	L0	Inexistente
10%	L1	Iniciado
30%	L2	Reproducible, pero no intuitivo
50%	L3	Proceso definido
75%	L4	Gestionado y medible
100%	L5	Optimizado

Valoración de salvaguardas

En la tabla 20 se ingresaron las escalas de madurez en la herramienta lo cual tuvieron un rango de L2 a L5 en donde:

L2: Reproducible, pero no intuitivo. En este nivel, la salvaguarda se ha documentado y se ha implementado, pero su aplicación puede ser inconsistente y puede haber dificultades para entender cómo y cuándo se debe aplicar.

L3: Proceso definido. En este nivel, la salvaguarda se ha integrado en un proceso de gestión de seguridad establecido, se entiende cómo y cuándo se debe aplicar, y se han definido indicadores para evaluar su eficacia.

L4: Gestionado y mediano. En este nivel, la salvaguarda se gestiona y se mide periódicamente, se han establecido objetivos de mejora continua y se utiliza la retroalimentación para ajustar la aplicación de la salvaguarda y mejorar su eficacia.

L5: Optimizado. Es el nivel más alto de madurez de la gestión de la seguridad de la información y representa una organización altamente eficiente y efectiva en la gestión de sus riesgos de seguridad de la información.

Si bien es cierto que alcanzar un nivel L5 sería lo ideal, en este caso nos alinearemos con las recomendaciones de la herramienta Pilar. Lo esencial es tener una idea realista de lo que se puede lograr para poder avanzar gradualmente hacia un nivel de madurez superior que mejore el desempeño de la organización. A continuación, identificaremos cada activo correspondiente a cada salvaguarda dependiendo de los puntos tratados anteriormente

Tabla 20

Salvaguardas para la Identificación y autenticación

Salvaguarda:	[IA] Identificación y autenticación
Activos:	[D] Datos / Información [SW] Aplicaciones (software)
Aspecto:	[G] gestión
Tipo de protección:	[EL] Eliminación

Niveles de seguridad: L2-L5

- Política de contraseñas: Establecer una política de contraseñas para que los usuarios de la red utilicen contraseñas seguras y cambien periódicamente.
- Monitorización de actividades: Monitorizar las actividades de los usuarios para detectar intentos de acceso no autorizados o inusuales
- Certificados digitales: Uso de certificados digitales para garantizar la autenticidad de los usuarios y dispositivos que acceden a la red.
- Protección de las credenciales: Proteger las credenciales guardadas en la red mediante técnicas de cifrado y otros métodos de protección

Tabla 21

Salvaguarda para el control de acceso lógico

Salvaguarda:	[AC] Control de acceso lógico
Activos:	[D] Datos / Información [S] Servicios [SW] Aplicaciones (software) [COM] Redes de comunicación
Aspecto:	[T] técnica
Tipo de protección:	[EL] Eliminación

Niveles de seguridad: L4

- Política de control de acceso: Establecer una política de control de acceso que defina los requisitos de seguridad para acceder a los sistemas y datos
- Política de contraseñas: Establecer una política de contraseñas que exija contraseñas seguras, el cambio periódico de contraseñas y la limitación de intentos de acceso fallidos

- Separación de funciones: Separar las funciones de los usuarios para evitar conflictos de interés y reducir el riesgo de fraude.
- Auditoría de acceso: Realizar auditorías periódicas para verificar el acceso de los usuarios y detectar cualquier actividad sospechosa.

Tabla 22

Salvaguarda para la protección de la información

Salvaguarda:	[D] Protección de la Información
Activos:	[D] Datos / Información
Aspecto:	[G] gestión
Tipo de protección:	[PR] Prevención

Niveles de seguridad: L4

- Clasificación de la información: Clasificar la información según su nivel de confidencialidad y establecer medidas de seguridad apropiadas para cada nivel.
- Análisis de vulnerabilidades: Realizar análisis periódicos de vulnerabilidades para identificar posibles brechas de seguridad y tomar medidas para mitigarlas.
- Monitorización de eventos: Implementar sistemas de monitorización de eventos para detectar posibles intrusiones o actividades inusuales en los sistemas.

Tabla 23

Salvaguarda para la protección de los Servicios

Salvaguarda:	[S] Protección de los Servicios
Activos:	[S] Servicios
Aspecto:	[G] gestión
Tipo de protección:	[PR] Prevención
Niveles de seguridad: L4	

- Gestión de la continuidad de los servicios: Establecer planes y procedimientos para la continuidad de los servicios en caso de interrupciones, fallas o desastres.
- Gestión de la monitorización de los servicios: Implementar sistemas de monitorización de los servicios para detectar posibles interrupciones o fallas.
- Gestión de la seguridad de los servicios: Implementar medidas de seguridad para proteger los servicios de posibles amenazas externas e internas.
- Pruebas de seguridad: Realice pruebas de seguridad periódicas para identificar posibles brechas de seguridad y tomar medidas para reducirlas.

Tabla 24

Salvaguardas para la protección de las aplicaciones informáticas

Salvaguarda:	[SW] Protección de las Aplicaciones Informáticas
Activos:	[SW] Aplicaciones (software)

Aspecto:	[G] gestión
Tipo de protección:	[PR] Prevención

Niveles de seguridad: L2-L4

- Verificación y validación de la seguridad de las aplicaciones: Realizar pruebas de seguridad para verificar y validar la seguridad de las aplicaciones antes de ponerlas en producción.
- Gestión de los accesos y permisos: Establecer un proceso de gestión de los accesos y permisos para las aplicaciones que permita controlar quién tiene acceso a las aplicaciones y qué permisos tienen.
- Protección de la memoria: Use técnicas de protección de la memoria para evitar que las aplicaciones puedan ser vulneradas a través de ataques de buffer, overflow u otras técnicas similares.
- Prevención de inyección de código: Implementar medidas para evitar la inyección de código malicioso en las aplicaciones, por ejemplo, mediante la validación de datos de entrada.

Tabla 25

Salvaguardas para protección de los equipos informáticos

Salvaguarda:	[HW] Protección de los Equipos Informáticos (HW)
Activos:	[HW] Equipamiento informático (hardware)
Aspecto:	[G] gestión
Tipo de protección:	[PR] Prevención

Niveles de seguridad: L4

- Actualización de software y firmware: Mantenga actualizado el software y el firmware de los equipos para corregir posibles vulnerabilidades de seguridad
- Gestión de contraseñas: Establecer una política de gestión de contraseñas que permita controlar quién tiene acceso a los equipos y qué permisos tienen.
- Monitorización de eventos: Implementar sistemas de monitorización de eventos para detectar posibles intrusiones o actividades inusuales en los equipos.

Tabla 26

Salvaguarda para la protección de las comunicaciones

Salvaguarda:	[COM] Protección de las Comunicaciones
Activos:	[COM] Redes de comunicación
Aspecto:	[G] gestión
Tipo de protección:	[PR] Prevención

Niveles de seguridad: L5

- Encriptación de datos: La encriptación de los datos durante la transmisión es una medida muy efectiva para proteger la información durante el proceso de comunicación.
- Gestión de claves y certificados: Establecer una política de gestión de claves y certificados para la encriptación de las comunicaciones, con el fin de garantizar la seguridad y autenticidad de los datos.

- Monitoreo de la red: Monitorear periódicamente la red, para detectar posibles intrusiones o ataques.
- Uso de VPN: Use redes privadas virtuales para establecer comunicaciones seguras y privadas a través de Internet.

Tabla 27

Salvaguarda para los elementos auxiliares

Salvaguarda:	[AUX] Elementos Auxiliares
Activos:	[AUX] Elementos Auxiliares
Aspecto:	[G] gestión
Tipo de protección:	[PR] Prevención

Niveles de seguridad: L4

- Establecer fuentes de alimentación alternativas, como baterías o generadores eléctricos de emergencia, para mantener la energía en caso de fallo del suministro eléctrico.
- Instalar sistemas de detección y control de temperatura, humedad y otros factores ambientales, para garantizar que los equipos estén funcionando en un ambiente adecuado.
- Realice pruebas rigurosas y de calidad después de cada actualización o mantenimiento, para garantizar que los equipos sigan funcionando correctamente.

Tabla 28

Salvaguarda para la protección física de equipos

Salvaguarda:	[PPE] Protección física de los equipos
Activos:	[HW] Equipamiento informático (hardware)
Aspecto:	[F] física
Tipo de protección:	[EL] Eliminación

Niveles de seguridad: L4

- Ubicación segura: Almacenar los equipos en una ubicación segura, como una sala de servidores o un centro de datos, para protegerlos de posibles robos o daños.
- Protección contra agua y humedad: Implementar medidas para proteger los equipos contra posibles daños por agua o humedad, como impermeabilizar las paredes o techos y utilizar barreras impermeables para aislar los equipos.
- Cámaras de vigilancia: Instalar cámaras de vigilancia en la ubicación donde se encuentran los equipos para disuadir posibles robos y facilitar la identificación de los responsables en caso de incidentes.
- Registro de visitantes: Mantener un registro de las visitas a la ubicación donde se encuentran los equipos para permitir la trazabilidad de las acciones realizadas.

Tabla 29

Salvaguarda para protección de las instalaciones

Salvaguarda:	[L] Protección de las Instalaciones

Activos:	[L] Instalaciones
Aspecto:	[F] física
Tipo de protección:	[PR] Prevención
Niveles de seguridad: L4	

- Identificación y control de accesos: Establecer un proceso de identificación y control de accesos a las instalaciones para permitir el acceso solo a personas autorizadas y evitar intrusiones no deseadas.
- Seguridad física: Establecer medidas de seguridad física en las, como la instalación de cerraduras seguras para garantizar la seguridad de los usuarios y de los activos.
- Evaluación de riesgos: Realice una evaluación de riesgos periódica para identificar posibles vulnerabilidades en las instalaciones y establecer medidas de protección adecuadas.

Tabla 30

Salvaguarda para gestión del personal

Salvaguarda:	[P] Gestión del Personal
Activos:	[P] personal
Aspecto:	[P]Personal
Tipo de protección:	[PR] Prevención
Niveles de seguridad: L4	

- Procesos de selección adecuados: Establecer de selección adecuados para el personal, que permitan la identificación de personas capacitadas y confiables para desempeñar sus funciones en la organización.
- Acuerdos de confidencialidad: Establecer acuerdos de confidencialidad con el personal, que permitan la protección de la información confidencial de la organización.
- Formación en seguridad: Proporcionar formación en seguridad al personal, que les permita conocer las medidas de seguridad establecidas y su importancia.

Tabla 31

Salvaguarda para gestión de vulnerabilidades

Salvaguarda:	[V] Gestión de vulnerabilidades
Activos:	[SW] Aplicaciones (software)
Aspecto:	[G] gestión
Tipo de protección:	[CR] Corrección

Niveles de seguridad: L2-L4

- Evaluación de vulnerabilidades: Realice una evaluación periódica de vulnerabilidades en los sistemas y componentes de la organización, con el fin de identificar vulnerabilidades posibles y establecer medidas para su mitigación
- Corrección de vulnerabilidades: Establecer un proceso de corrección de vulnerabilidades, que permita la identificación, análisis y mitigación de las vulnerabilidades identificadas en los sistemas y componentes.

Impacto residual

Se refiere al nivel de daño o pérdida que puede ocurrir después de haber implementado las salvaguardas y medidas de mitigación necesarias para hacer frente a una amenaza. La metodología MAGERIT utiliza el concepto de "valoración de riesgos residuales" para evaluar el nivel de riesgo que queda después de la implementación de las salvaguardas y medidas de mitigación. Esta valoración se realiza después de haber evaluado la probabilidad e impacto inicial de la amenaza, y haber aplicado las medidas de seguridad necesarias para reducir el riesgo

Tabla 32

Escala de valores

Valor
[10] Nivel10
[9] Nivel 9
[8] Nivel 8
[7] Alto
[6] Alto (-)
[5] Medio (+)
[4] Medio
[3] Medio (-)
[2] Bajo (+)
[1] Bajo
[0] Despreciable

Tabla 33

Impacto Residual

	D	I	C	A	T
[AE] ACTIVOS ESENCIALES					
[AE01] NAS	[0]	[5]	[3]	[5]	
[D]DATOS/ INFORMACIÓN					
[D001] Base de datos SQL server	[4]	[4]	[4]	[3]	
[D002] Base de datos PostgreSQL	[4]	[4]	[4]	[4]	
[S] SERVICIOS	[4]	[4]	[4]	[5]	
[S001] Sistema Nacional para la administración de tierras	[4]	[3]	[4]	[5]	
[S002] Sistema de comercialización de servicios	[4]	[4]	[4]	[5]	
[S003] Sistema integrado de tramites al ciudadano	[4]	[4]	[4]	[5]	
[S004] Sistema de gestión administrativa financiera de la asociación de municipalidades ecuatorianas	[4]	[4]	[4]	[5]	
[S005] Sistema integral de catastros	[4]	[4]	[4]	[5]	
[SW] SOFTWARE					
[SW01] Anti virus	[0]				
[SW02.1] Windows 2010 pro	[3]	[4]	[2]		
[SW02.2] Linux	[4]	[3]	[2]		
[SW02.3] Windows server 2012 R2	[4]	[4]	[2]		
[SW03] Ofimática	[1]				
[SW04] Monitoreo de red Unifi Network	[2]				
[S006] Correo electrónico	[3]	[2]	[3]	[2]	
[S007] Pagina web Saquisilí		[2]		[2]	
[HW] HARDWARE					

	D	I	C	A	T
[HW01] Servidor SIGAME	[4]	[4]	[4]	[4]	
[HW02] Servidor SINAT	[4]	[4]	[4]	[4]	
[HW03] Servidor de aplicación y gestión documental	[4]	[4]	[3]	[4]	
[HW04] Servidor Proxy	[3]	[3]	[3]	[3]	
[HW05] Servidor de respaldos NAS	[4]	[5]	[5]	[5]	
[HW06] Informática persona	[4]	[2]	[2]		
[HW07] Medios de impresión	[2]				
[modem] Módems	[2]				
[switch] Conmutador	[3]				
[router] Encaminador	[2]				
[anti] Antenas inalámbricas	[2]				
[COM] COMUNICACIONES					
[WIFI] Red inalámbrica	[2]				
[LAN] Red local	[3]				
[Inter] Internet	[1]				
[AUX] EQUIPAMIENTO AUXILIAR					
[AUX1] Fuentes de alimentación	[2]				
[AUX2] sistemas de alimentación ininterrumpida	[2]				
[AUX3] Control antincendios	[1]				
[AUX4] Equipos de climatización	[2]				
[AUX5] Cableado de datos (Fibra óptica y Alimentación)	[2]				
[AUX6]Cerradura electromagnética	[3]				
[SS] SERVICIOS CONTRATADOS					
[SS01] Servicio de Internet	[0]				

	D	I	C	A	T
[L] INSTALACIONES					
[L001] Departamento de TICs	[3]				
[P]PERSONAL					
[P001] Administradora de sistema y base de datos		[3]	[3]		
[P002] Administrador informativo		[3]	[3]		
[P003] Administrador de seguridad		[3]	[3]		
[P004] Usuarios externos		[0]			
[P005] Operador		[0]	[2]		

Nota. Tabla de resultados del impacto residual en la herramienta EAR/pilar

Riesgo residual

Se refiere al nivel de riesgo que queda después de haber implementado las medidas de seguridad y salvaguardas para hacer frente a una amenaza de seguridad de la información. En otras palabras, es el nivel de riesgo que queda después de haber aplicado medidas de mitigación y reducción de riesgos para minimizar la probabilidad y el impacto de una amenaza.

El riesgo residual nos permite determinar si las medidas de mitigación aplicadas son adecuadas o si se necesitan medidas adicionales para reducir aún más el riesgo. También puede ayudar a identificar las áreas que necesitan más atención y recursos para mejorar la seguridad de la información.

Figura 4

Escala de valoración

Nota. Niveles de criticidad que utiliza la herramienta EAR/Pilar

Tabla 34

Riesgo Residual

	D	I	C	A	T
[AE] ACTIVOS ESENCIALES					
[AE01] NAS	{0,40}	{2,4}	{1,2}	{2,4}	
[D]DATOS/ INFORMACIÓN					
[D001] Base de datos SQL server	{2,1}	{1,9}	{1,9}	{1,5}	
[D002] Base de datos PostgreSQL	{2,1}	{1,9}	{1,9}	{2,1}	
[S] SERVICIOS					
[S001] Sistema Nacional para la administración de tierras	{2,2}	{1,9}	{1,9}	{2,4}	
[S002] Sistema de comercialización de servicios	{2,2}	{1,9}	{1,9}	{2,4}	
[S003] Sistema integrado de tramites al ciudadano	{2,2}	{1,9}	{1,9}	{2,4}	

	D	I	C	A	T
[S004] Sistema de gestión administrativa financiera de la asociación de municipalidades ecuatorianas	{2,2}	{1,9}	{1,9}	{2,4}	
[S005] Sistema integral de catastros	{2,2}	{1,9}	{1,9}	{2,4}	
[SW] SOFTWARE					
[SW01] Anti virus	{0,47}				
[SW02.1] Windows 2010 pro	{1,3}	{1,9}	{0,95}		
[SW02.2] Linux	{1,9}	{1,3}	{0,95}		
[SW02.3] Windows server 2012 R2	{1,9}	{1,9}	{0,95}		
[SW03] Ofimática	{0,82}				
[SW04] Monitoreo de red Unifi Network	{0,99}				
[S006] Correo electrónico	{1,6}	{0,94}	{1,8}	{0,82}	
[S007] Pagina web Saquisilí		{0,95}		{0,82}	
[HW] HARDWARE					
[HW01] Servidor SIGAME	{2,1}	{1,9}	{1,9}	{2,1}	
[HW02] Servidor SINAT	{2,1}	{1,9}	{1,9}	{2,1}	
[HW03] Servidor de aplicación y gestión documental	{2,2}	{1,9}	{1,4}	{2,1}	
[HW04] Servidor Proxy	{1,6}	{0,85}	{1,1}	{1,5}	
[HW05] Servidor de respaldos NAS	{2,2}	{2,4}	{2,4}	{2,4}	
[HW06] Informática persona	{1,9}	{0,94}	{0,95}		
[HW07] Medios de impresión	{2,7}				
[modem] Módems	{0,99}				
[switch] Conmutador	{1,6}				
[router] Encaminador	{0,99}				
[anti] Antenas inalámbricas	{0,99}				

	D	I	C	A	T
[COM] COMUNICACIONES					
[WIFI] Red inalámbrica	{0,99}				
[LAN] Red local	{1,6}				
[Inter] Internet	{0,84}				
[AUX] EQUIPAMIENTO AUXILIAR					
[AUX1] Fuentes de alimentación	{0,76}				
[AUX2] sistemas de alimentación ininterrumpida	{0,76}				
[AUX3] Control antincendios	{0,65}				
[AUX4] Equipos de climatización	{0,76}				
[AUX5] Cableado de datos (Fibra óptica y Alimentación)	{0,76}				
[AUX6]Cerradura electromagnética	{0,95}				
[SS] SERVICIOS CONTRATADOS					
[SS01] Servicio de Internet	{0,49}				
[L] INSTALACIONES					
[L001] Departamento de TIC´s	{1,5}				
[P]PERSONAL					
[P001] Administradora de sistema y base de datos		{0,84}	{0,84}		
[P002] Administrador informativo		{0,84}	{0,84}		
[P003] Administrador de seguridad		{0,84}	{0,84}		
[P004] Usuarios externos		{0,47}			
[P005] Operador		{0,68}	{0,74}		

Nota. Tabla de resultados de los riesgos residuales del departamento de TICs proporcionados por la herramienta EAR/pilar

Gestión de riesgo

Una vez identificado los activos, amenazas, la evaluación del impacto potencial y la implementación de medidas de seguridad identificaremos los riesgos críticos del departamento de TIC´s de GADMICS para ello se debe evaluar el riesgo residual después de aplicar las salvaguardas. los riesgos críticos son aquellos que aún representan un alto nivel de riesgo después de haber aplicado todas las medidas de seguridad posibles.

Tabla 35

Riesgos críticos del departamento de TICs

Activos	**Amenazas**	D	V	D	I	P	R
[AE01] NAS	[A.5] suplantación de identidad	[A]	[9]	T	[4]	PP	{2,3}
	[A.6] Abuso de privilegios de acceso	[I]	[9]	T	[5]	PP	{2,4}
	[A.6] Abuso de privilegios de acceso	[A]	[9]	T	[5]	PP	{2,1}
	[A.11] Acceso no autorizado	[I]	[9]	T	[4]	MR	{2,1}
	[A.11] Acceso no autorizado	[A]	[9]	T	[4]	MR	{2,1}
	[N.*] Desastres naturales	[D]	[9]	T	[4]	MR	{1,9}
[D001] Base de datos SQL server	[I.6] Corte del suministro eléctrico	[D]	[9]	T	[4]	MR	{2,1}
	[I.2] Daños por agua	[D]	[9]	T	[4]	MR	{2,1}
	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	T	[4]	MR	{2,1}
	[I.*] Desastres industriales	[D]	[9]	T	[4]	MR	{2,1}
	[N.*] Desastres naturales	[D]	[9]	T	[4]	MR	{1,9}

Activos	Amenazas	D	V	D	I	P	R
[D002] Base de datos PostgreSQL	[I.6] Corte del suministro eléctrico	[D]	[9]	T	[4]	MR	{2,1}
	[I.2] Daños por agua	[D]	[9]	T	[4]	MR	{2,1}
	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	T	[4]	MR	{2,1}
	[I.*] Desastres industriales	[D]	[9]	T	[4]	MR	{2,1}
	[A.11] Acceso no autorizado	[A]	[9]	T	[4]	MR	{2,1}
	[N.*] Desastres naturales	[D]	[9]	T	[4]	MR	{1,9}
[S001] Sistema Nacional para la administración de tierras	[A.6] Abuso de privilegios de acceso	[A]	[9]	T	[5]	MR	{2,4}
	[I.6] Corte del suministro eléctrico	[D]	[9]	T	[4]	MR	{2,2}
	[I.2] Daños por agua	[D]	[9]	T	[4]	MR	{2,1}
	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	T	[4]	MR	{2,1}
	[I.*] Desastres industriales	[D]	[9]	T	[4]	MR	{2,1}
	[A.11] Acceso no autorizado	[A]	[9]	T	[4]	MR	{2,1}
	[N.*] Desastres naturales	[D]	[9]	T	[4]	MR	{1,9}
[S002] Sistema de comercialización de servicios	[A.6] Abuso de privilegios de acceso	[A]	[9]	T	[5]	MR	{2,4}
	[I.6] Corte del suministro eléctrico	[D]	[9]	T	[4]	MR	{2,2}
	[I.2] Daños por agua	[D]	[9]	T	[4]	MR	{2,2}

Activos	Amenazas	D	V	D	I	P	R
	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	T	[4]	MR	{2,2}
	[I.*] Desastres industriales	[D]	[9]	T	[4]	MR	{2,2}
	[A.11] Acceso no autorizado	[A]	[9]	T	[4]	MR	{2,1}
	[N.*] Desastres naturales	[D]	[9]	T	[4]	MR	{1,9}
[S003] Sistema integrado de tramites al ciudadano	[A.6] Abuso de privilegios de acceso	[A]	[9]	T	[5]	MR	{2,4}
	[I.6] Corte del suministro eléctrico	[D]	[9]	T	[4]	MR	{2,1}
	[I.2] Daños por agua	[D]	[9]	T	[4]	MR	{2,1}
	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	T	[4]	MR	{2,1}
	[I.*] Desastres industriales	[D]	[9]	T	[4]	MR	{2,1}
	[A.11] Acceso no autorizado	[A]	[9]	T	[4]	MR	{2,1}
	[N.*] Desastres naturales	[D]	[9]	T	[4]	MR	{1,9}
[S004] Sistema de gestión administrativa financiera de la asociación de municipalidades ecuatorianas	[A.6] Abuso de privilegios de acceso	[A]	[9]	T	[5]	MR	{2,4}
	[I.6] Corte del suministro eléctrico	[D]	[9]	T	[4]	MR	{2,2}
	[I.2] Daños por agua	[D]	[9]	T	[4]	MR	{2,2}
	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	T	[4]	MR	{2,2}
	[I.*] Desastres industriales	[D]	[9]	T	[4]	MR	{2,2}

Activos	Amenazas	D	V	D	I	P	R
	[A.11] Acceso no autorizado	[A]	[9]	T	[4]	MR	{2,1}
	[N.*] Desastres naturales	[D]	[9]	T	[4]	MR	{1,9}
[S005] Sistema integral de catastros	[A.6] Abuso de privilegios de acceso	[A]	[9]	T	[5]	MR	{2,4}
	[I.6] Corte del suministro eléctrico	[D]	[9]	T	[4]	MR	{2,2}
	[I.2] Daños por agua	[D]	[9]	T	[4]	MR	{2,1}
	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	T	[4]	MR	{2,1}
	[I.*] Desastres industriales	[D]	[9]	T	[4]	MR	{2,1}
	[A.11] Acceso no autorizado	[A]	[9]	T	[4]	MR	{2,1}
	[N.*] Desastres naturales	[D]	[9]	T	[4]	MR	{1,9}
[HW01] Servidor SIGAME	[I.6] Corte del suministro eléctrico	[D]	[9]	T	[4]	MR	{2,1}
	[I.2] Daños por agua	[D]	[9]	T	[4]	MR	{2,1}
	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	T	[4]	MR	{2,1}
	[I.*] Desastres industriales	[D]	[9]	T	[4]	MR	{2,1}
	[A.11] Acceso no autorizado	[A]	[9]	T	[4]	MR	{2,1}
	[N.*] Desastres naturales	[D]	[9]	T	[4]	MR	{1,9}
[HW02] Servidor SINAT	[I.6] Corte del suministro eléctrico	[A]	[9]	T	[4]	MR	{2,1}
	[I.2] Daños por agua	[D]	[9]	T	[4]	MR	{2,1}

Activos	Amenazas	D	V	D	I	P	R
	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	T	[4]	MR	{2,1}
	[I.*] Desastres industriales	[D]	[9]	T	[4]	MR	{2,1}
	[A.11] Acceso no autorizado	[A]	[9]	T	[4]	MR	{2,1}
	[N.*] Desastres naturales	[D]	[9]	T	[4]	MR	{1,9}
[HW03] Servidor de aplicación y gestión documental	[I.6] Corte del suministro eléctrico	[D]	[9]	T	[4]	MR	{2,2}
	[I.*] Desastres industriales	[D]	[9]	T	[4]	MR	{2,1}
	[I.2] Daños por agua	[D]	[9]	T	[4]	MR	{2,1}
	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	T	[4]	MR	{2,1}
	[A.11] Acceso no autorizado	[A]	[9]	T	[4]	MR	{2,1}
	[[N.*] Desastres naturales	[D]	[9]	T	[4]	MR	{1,9}
HW05] Servidor de respaldos NAS	[A.6] Abuso de privilegios de acceso	[A]	[9]	T	[5]	MR	{2,4}
	[A.6] Abuso de privilegios de acceso	[I]	[9]	T	[5]	MR	{2,4}
	[A.6] Abuso de privilegios de acceso	[C]	[9]	T	[5]	MR	{2,4}
	[I.6] Corte del suministro eléctrico	[D]	[9]	T	[4]	MR	{2,2}
	[I.2] Daños por agua	[D]	[9]	T	[4]	MR	{2,1}

Activos	Amenazas	D	V	D	I	P	R
	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	T	[4]	MR	{2,1}
	[I.*] Desastres industriales	[D]	[9]	T	[4]	MR	{2,1}
	[A.11] Acceso no autorizado	[I]	[9]	T	[5]	MR	{2,1}
	[A.11] Acceso no autorizado	[C]	[9]	T	[5]	MR	{2,1}
	[A.11] Acceso no autorizado	[A]	[9]	T	[5]	MR	{2,1}
	[N.*] Desastres naturales	[D]	[9]	T	[4]	MR	{1,9}

Nota. Tabla de resultados de los riesgos críticos del departamento de TICs proporcionado por la herramienta EAR/pilar

Contingencia de los sistemas informáticos

Tabla 36

Suplantación de identidad

Plan #01	Contingencia	
Versión 1.0	Suplantación de identidad	GADMIC Saquisilí Ñawpaman Katishun

1. Plan de prevención

1.1. Eventualidad

La emergencia se activará cuando se:

- Detecte actividad inusual en los sistemas informáticos
- Alertas de seguridad en el sistema
- Informes de las personas afectadas

1.2. Objetivo

Proteger la información sensible del GADMICS y colaborar con las autoridades pertinentes para tomar acciones específicas dependiendo de la gravedad del incidente

1.3. Entorno

Este evento afectara a toda la oficina del departamento de TICs

1.4. Encargados

Los principales representantes que llevarán al cumplimiento de todas las medidas que se establecerán en dicho, estarán a cargos los miembros del departamento de TICS del GADMICS

1.5. Actividad de mitigación

- Desarrollar programas de formación continua para educar a los empleados y usuarios sobre las tácticas de suplantación de identidad y cómo reconocerlas.
- Implementar sistemas de monitoreo continuo para identificar patrones inusuales de actividad, alertando sobre posibles casos de suplantación.
- Establecer un proceso para garantizar la aplicación regular de actualizaciones y parches de seguridad en todos los sistemas.
- Desarrollar y hacer cumplir políticas de contraseñas que requieran combinaciones sólidas de caracteres y cambios de periódicos.

2. Plan de emergencia

2.1. Activación del plan

Plan #01	Contingencia
Versión 1.0	Suplantación de identidad

El plan dará inicio cuando se detecte actividades inusuales o anómalas en los registros de actividad que sugieren una posible suplantación de identidad

2.2. Activación para la contingencia

- Definir indicadores clave que puedan señalar una posible suplantación de identidad, como intentos de acceso desde ubicaciones inusuales, patrones de actividad inusuales o cambios en la información de la cuenta.
- Designar un equipo de respuesta a incidentes que pueda realizar una evaluación preliminar de la situación al recibir una notificación
- En caso de confirmación o fuerte sospecha, aísle inmediatamente las cuentas afectadas y restrinja el acceso no autorizado

2.3. Proceso de mitigación

Realizar un análisis posterior del incidente para identificar las lecciones aprendidas y realizar mejoras continuas en los procedimientos de respuesta.

3. Plan de restauración

3.1. Personal responsable

Personal del departamento de TICs

3.2. Actividades

- Identificar y verificar posibles incidentes de suplantación de identidad mediante sistemas de monitoreo, alertas de seguridad, informes de usuarios u otras fuentes

Plan #01	Contingencia	
Versión 1.0	Suplantación de identidad	

- Iniciar el proceso de restablecimiento de credenciales para las cuentas afectadas y asegurar que los usuarios legítimos recuperen el control de sus cuentas

3.3. Recomendaciones

- Implementar medidas para restaurar la normalidad en el servicio tan pronto como sea posible, asegurando que las operaciones críticas puedan reanudarse de manera segura.

Tabla 37

Abuso de privilegios de acceso

Plan #02	Contingencia	
Versión 1.0	Abuso de privilegios de acceso	

1. Plan de prevención

1.1. Eventualidad

Activar de manera rápida y eficiente el plan de contingencia ante la detección de un abuso de privilegios de acceso

1.2. Objetivo

Detectar y notificar de manera rápida y efectiva cualquier indicio de abuso de privilegios de acceso

1.3. Entorno

Plan #02	Contingencia	
Versión 1.0	Abuso de privilegios de acceso	

Este evento afectara a toda la oficina del departamento de TICS

1.4. Encargados

Los principales representantes que llevarán al cumplimiento de todas las medidas que se establecerán en dicho, estarán a cargos los miembros del departamento de TICs del GADMICS

1.5. Actividad de mitigación

- Asignar a los usuarios solo los privilegios necesarios para realizar sus funciones.
- Clasificar los privilegios de acceso en función de la criticidad y la sensibilidad de los datos o sistemas a los que otorgan acceso
- Establecer políticas claras y concisas que rijan el acceso a sistemas y datos, incluyendo quién tiene acceso a qué y bajo qué circunstancias
- Revisar y actualizar periódicamente los privilegios en base a las responsabilidades laborales

2. Plan de emergencia

2.1. Activación del plan

El plan dará inicio cuando se detecte actividades inusuales o anómalas en los registros de actividad que sugieren un posible abuso de privilegios

2.2. Actividades de contingencia

Plan #02	Contingencia	
Versión 1.0	Abuso de privilegios de acceso	GADMIC Saquisilí Ñawpaman Katishun

- Identificar y verificar posibles incidentes de abuso de privilegios mediante sistemas de monitoreo continuo, alertas de seguridad, o informes de usuarios u otros canales.
- Establecer un mecanismo claro y rápido para que los usuarios y el personal notifiquen cualquier sospecha de abuso de privilegios.
- Active el equipo de respuesta a incidentes designados tan pronto como se confirme o se sospeche fuertemente de un abuso de privilegios.
- Aislar las cuentas o sistemas afectados para evitar la propagación del incidente a otras partes de la red o a otros usuarios.
- Recopilar toda la información disponible sobre el incidente, incluyendo registros de actividad, archivos afectados y cualquier evidencia relacionada.

3. Plan de restauración

3.1. Personal responsable

Se creará un equipo responsable dentro del departamento de TICs para la restauración de los sistemas afectados por el riesgo

3.2. Actividades

- Iniciar el proceso de restablecimiento de credenciales para las cuentas afectadas y asegurar que los usuarios legítimos recuperen el control de sus cuentas.

Plan #02	Contingencia	
Versión 1.0	Abuso de privilegios de acceso	

- Realice un análisis forense para entender el alcance del incidente, cómo ocurrió y si hay otros sistemas o usuarios afectados.
- Establecer un plan de comunicación interna y externa para informar a los empleados, usuarios y, si es necesario, al público en general sobre el incidente.
- Colaborar estrechamente con equipos de seguridad internos y externos para compartir información sobre amenazas y mejores prácticas de prevención.

3.3. Recomendaciones

Actualizar el plan de contingencia en base a las revisiones y análisis del daño generado por el riesgo y la capacidad de respuesta ante abusos futuros.

Tabla 38

Acceso no autorizado

Plan #03	Contingencia	
Versión 1.0	Acceso no autorizado	

1. Plan de prevención

1.1. Eventualidad

Recepción de alertas automáticas o notificaciones de sistemas de seguridad que indican posibles intentos de intrusión, como violaciones de políticas de acceso, intentos de penetración externa o comportamientos sospechosos en la red.

1.2. Objetivo

Proteger la información sensible del GADMICS y colaborar con las autoridades pertinentes para tomar acciones específicas dependiendo de la gravedad del incidente

1.3. Entorno

Este evento afectara a toda la oficina del departamento de TICs

1.4. Encargados

Los principales representantes que llevarán al cumplimiento de todas las medidas que se establecerán en dicho, estarán a cargos los miembros del departamento de TICs del GADMICS.

1.5. Actividad de mitigación

- Establecer políticas claras y documentadas de acceso, definiendo quién tiene acceso a qué recursos y bajo qué condiciones.
- Implementar la autenticación multifactorial para aumentar la seguridad de las credenciales de usuario y reducir el riesgo de acceso no autorizado.
- Mantener actualizados todos los sistemas y aplicaciones con los últimos parches de seguridad para mitigar vulnerabilidades conocidas.

Plan #03	Contingencia
Versión 1.0	Acceso no autorizado

- Configurar sistemas de monitoreo de registros para detectar patrones inusuales en los intentos de acceso, lo que podría indicar un acceso no autorizado.

2. Plan de emergencia

2.1. Activación del plan

Detección de actividad anormal a gran escala que afecta múltiples sistemas o afecta críticamente las operaciones de la organización.

2.2. Actividades de contingencia

- Active el equipo de respuesta a incidentes designados tan pronto como se confirme o se sospeche de un acceso no autorizado
- Aislar rápidamente los sistemas o cuentas comprometidas para evitar la propagación del acceso no autorizado
- Recopilar evidencia relacionada con el acceso no autorizado, incluyendo registros de actividad, direcciones IP involucradas y cualquier otro dato relevante.

3. Plan de restauración

3.1. Personal responsable

Se creará un equipo responsable dentro del departamento de TICs para la restauración de los sistemas afectados por el riesgo

3.2. Actividades

Plan #03	Contingencia
Versión 1.0	Acceso no autorizado

- Iniciar el proceso de restablecimiento de credenciales para las cuentas afectadas y garantizar que los usuarios legítimos recuperen el control.
- Evaluar la necesidad y la obligación legal de notificar a las autoridades y reguladores sobre el acceso no autorizado.

3.3. Recomendaciones

Realizar una evaluación post-incidente para identificar lecciones aprendidas, áreas de mejora y ajustar las políticas y procedimientos según sea necesario.

Tabla 39

Corte del suministro eléctrico

Plan #04	Contingencia
Versión 1.0	Corte del suministro eléctrico

1. Plan de prevención

1.1. Eventualidad

Recepción de alertas por parte de servicios públicos o proveedores de energía sobre mantenimientos programados, cortes de emergencia o problemas en la infraestructura eléctrica.

1.2. Objetivo

Proteger la información sensible del GADMICS y colaborar con las autoridades pertinentes para tomar acciones específicas dependiendo de la gravedad del incidente

Plan #04	Contingencia
Versión 1.0	Corte del suministro eléctrico

1.3. Entorno

Este evento afectara a toda la oficina del departamento de TICs

1.4. Encargados

Los principales representantes que llevarán al cumplimiento de todas las medidas que se establecerán en dicho, estarán a cargos los miembros del departamento de TICs del GADMICS

1.5. Actividad de mitigación

- Establecer fuentes de energía alternativa, como generadores eléctricos, baterías de respaldo y sistemas de energía renovable, para mantener operaciones críticas durante los cortes de suministro.
- Implementar un programa regular de mantenimiento preventivo en la infraestructura eléctrica para reducir la probabilidad de fallas y maximizar la confiabilidad.
- Instalar sistemas de protección, como reguladores de voltaje y supresores de sobretensiones, para salvar equipos sensibles contra daños durante cortes de energía y picos de voltaje.

2. Plan de emergencia

2.1. Activación del plan

Ocurrencia de un corte no planificado en el suministro eléctrico que afecta las operaciones críticas de la organización.

2.2. Actividades de contingencia

Plan #04	Contingencia
Versión 1.0	Corte del suministro eléctrico

- Evaluar rápidamente el impacto del corte de energía en las operaciones críticas y determinar la magnitud del incidente.
- Iniciar el uso de fuentes de energía alternativa de manera inmediata para mantener en funcionamiento sistemas críticos y minimizar la interrupción de servicios.

3. Plan de restauración

3.1. Personal responsable

Se creará un equipo responsable dentro del departamento de TICs para la restauración de los sistemas afectados por el riesgo

3.2. Actividades

- Coordinar con las autoridades locales y proveedores de servicios para restaurar el suministro eléctrico de manera segura y eficiente.
- Realice una verificación exhaustiva de equipos y sistemas afectados para asegurar que no haya daños y que estén listos para funcionar una vez que se restablezca el suministro eléctrico.

3.3. Recomendaciones

Conducir una revisión post-evento para evaluar la respuesta al corte de suministro eléctrico, identificar áreas de mejora y actualizar el plan de contingencia según sea necesario.

Tabla 40

Condiciones inadecuadas de temperatura o humedad

Plan #05 Versión 1.0	**Contingencia** Condiciones inadecuadas de temperatura o humedad	GADMIC saquisilí Ñawpaman Katishun

1. Plan de prevención

1.1. Eventualidad

Detección de problemas en el sistema de climatización de las instalaciones, lo que podría afectar la capacidad de mantener condiciones adecuadas de temperatura y humedad.

1.2. Objetivo

Proteger la información sensible del GADMICS y colaborar con las autoridades pertinentes para tomar acciones específicas dependiendo de la gravedad del incidente

1.3. Entorno

Este evento afectara a toda la oficina del departamento de TICs

1.4. Encargados

Los principales representantes que llevarán al cumplimiento de todas las medidas que se establecerán en dicho, estarán a cargos los miembros del departamento de TICs del GADMICS

1.5. Actividad de mitigación

- Implementar sistemas de monitoreo ambiental para medir y registrar continuamente los niveles de temperatura y humedad en áreas críticas.

Plan #05 Versión 1.0	Contingencia Condiciones inadecuadas de temperatura o humedad	GADMIC saquisilí Ñawpaman Katishun

- Establecer un programa regular de mantenimiento preventivo para equipos de climatización y sistemas de control ambiental, minimizando así la probabilidad de fallos.
- Garantizar la disponibilidad de respaldo de energía, como generadores eléctricos, para mantener operativos los sistemas de control ambiental durante cortes de energía.

2. Plan de emergencia

2.1. Activación del plan

Falla crítica en el sistema de climatización que compromete la capacidad de mantener condiciones adecuadas de temperatura y humedad en las instalaciones

2.2. Actividades de contingencia

- Active el equipo de respuesta a incidentes designados tan pronto como se detecten condiciones adversas para la temperatura o humedad.
- Estabilizar gradualmente las condiciones ambientales hasta alcanzar niveles aceptables para la operación segura de equipos y procesos.
- Evaluar rápidamente el impacto de las condiciones inadecuadas en áreas críticas y determinar la magnitud del incidente.

3. Plan de restauración

3.1. Personal responsable

Se creará un equipo responsable dentro del departamento de TICs para la restauración de los sistemas afectados por el riesgo

Plan #05	Contingencia	
Versión 1.0	Condiciones inadecuadas de temperatura o humedad	

3.2. Actividades

Realice una evaluación de daños en equipos y áreas afectadas para identificar cualquier impacto duradero y tomar medidas correctivas adicionales si es necesario

3.3. Recomendaciones

Conducir una revisión post-evento para evaluar la respuesta, identificar áreas de mejora y actualizar el plan de contingencia según sea necesario

Tabla 41

Desastres industriales

Plan #06	Contingencia	
Versión 1.0	Desastres industriales	

1. Plan de prevención

1.1. Eventualidad

Cambios inesperados en las condiciones ambientales que podrían afectar la estabilidad de procesos industriales, como temperaturas extremas o eventos climáticos adversos.

1.2. Objetivo

Proteger la información sensible del GADMICS y colaborar con las autoridades pertinentes para tomar acciones específicas dependiendo de la gravedad del incidente

Plan #06	Contingencia
Versión 1.0	Desastres industriales

1.3. Entorno

Este evento afectara a toda la oficina del departamento de TICs

1.4. Encargados

Los principales representantes que llevarán al cumplimiento de todas las medidas que se establecerán en dicho, estarán a cargos los miembros del departamento de TICs del GADMICS

1.5. Actividad de mitigación

Implementar programas de inspección y mantenimiento preventivo para equipos críticos, infraestructuras y sistemas que puedan ser fuente de desastres industriales.

Proporcionar entrenamiento regular a empleados sobre prácticas seguras, protocolos de emergencia y el uso adecuado de equipos de seguridad.

2. Plan de emergencia

2.1. Activación del plan

Ocurrencia de explosiones, incendios u otros eventos catastróficos que amenazan la seguridad de los trabajadores, la infraestructura y la comunidad circundante.

2.2. Actividades de contingencia

- Evaluar rápidamente el alcance del desastre, identificando áreas afectadas, posibles víctimas y determinando la magnitud del incidente.

Plan #06	Contingencia	
Versión 1.0	Desastres industriales	

- Implementar procedimientos de evacuación y rescate según sea necesario, priorizando la seguridad de las personas y minimizando la exposición a riesgos.
- Implementar procedimientos de evacuación y rescate según sea necesario, priorizando la seguridad de las personas y minimizando la exposición a riesgos.

3. Plan de restauración

3.1. Personal responsable

Se creará un equipo responsable dentro del departamento de TICs para la restauración de los sistemas afectados por el riesgo

3.2. Actividades

- Brindar atención médica a los afectados, coordinar con servicios de emergencia médica y proporcionar apoyo psicológico a empleados y personas afectadas.
- Realizar una evaluación detallada de los daños a instalaciones, equipos y el medio ambiente para determinar las acciones necesarias para la restauración.
- Establecer un sistema de comunicación interna y externa para informar sobre la situación después del desastre, las medidas tomadas y las expectativas de recuperación.

3.3. Recomendaciones

Plan #06	Contingencia
Versión 1.0	Desastres industriales

Realizar una evaluación del desastre para evaluar las respuestas al riesgo de tal manera que el plan de contingencia pueda ser actualizado y acoplado a las necesidades latentes de la entidad

Tabla 42

Desastres Naturales

Plan #07	Contingencia
Versión 1.0	Desastres Naturales

1. Plan de prevención

1.1. Eventualidad

Recepción de alertas emitidas por autoridades meteorológicas sobre la proximidad de un desastre natural, como huracanes, tornados, terremotos, inundaciones, entre otros.

1.2. Objetivo

Proteger la información sensible del GADMICS y colaborar con las autoridades pertinentes para tomar acciones específicas dependiendo de la gravedad del incidente

1.3. Entorno

Este evento afectara a toda la oficina del departamento de TICs

1.4. Encargados

Los principales representantes que llevarán al cumplimiento de todas las medidas que se establecerán en dicho, estarán a cargos los miembros del departamento de TICs del GADMICS

1.5. Actividad de mitigación

- Implementar sistemas de monitoreo meteorológico para recibir alertas anticipadas de eventos climáticos extremos y permitir una respuesta proactiva.
- Desarrollar y comunicar planes de evacuación y refugio para empleados, clientes y visitantes, considerando rutas seguras y lugares seguros.

2. Plan de emergencia

2.1. Activación del plan

Ocurrencia de un desastre natural, como un terremoto, inundación o tormenta, que impacta directamente la infraestructura industrial, provocando daños significativos y aumentando el riesgo de desastres industriales asociados.

2.2. Actividades de contingencia

- Activar procedimientos de evacuación y rescate de acuerdo con el tipo de desastre, priorizando la seguridad de las personas y minimizando la exposición a riesgos.
- Coordinar la apertura de refugios seguros y la prestación de primeros auxilios, asegurando el bienestar de empleados y otras personas presentes en la instalación.

- Coordinar con las autoridades locales, servicios de emergencia y otros organismos relevantes para una respuesta conjunta y eficaz.

3. Plan de restauración

3.1. Personal responsable

Se creará un equipo responsable dentro del departamento de TICs para la restauración de los sistemas afectados por el riesgo

3.2. Actividades

- Realizar una evaluación rápida y detallada de los daños causados por el desastre natural en instalaciones, equipos y entorno.
- Establecer prioridades para la restauración de operaciones críticas, asegurando que la infraestructura es segura y los sistemas son funcionales.
- Establecer un sistema de comunicación interna y externa para informar sobre la situación después del desastre, las medidas tomadas y las expectativas de recuperación.

3.3. Recomendaciones

Realizar una evaluación del desastre para evaluar las respuestas al riesgo de tal manera que el plan de contingencia pueda ser actualizado y acoplado a las necesidades latentes de la entidad

Capitulo IV

Conclusiones y Recomendaciones

Conclusiones

- Se ha realizado una investigación exhaustiva para identificar y comparar las metodologías de análisis y gestión de riesgos disponibles en el mercado. Como resultado, se ha seleccionado la metodología MAGERIT que se adapta a las necesidades específicas del departamento de TICs del GADMICS, lo que garantizará una adecuada protección de su información.
- Mediante la aplicación de PILAR de la metodología MAGERIT, se ha logrado identificar de manera precisa y detallada los activos críticos del departamento de TICs del GADMICS, así como las amenazas y riesgos asociados a cada uno de ellos. Esto proporciona una visión clara de los posibles escenarios de riesgo que pueden afectar la seguridad de la información.
- Se ha elaborado un plan de contingencia completo y detallado que incluye estrategias y controles para mitigar los riesgos identificados. El plan de contingencia proporciona un marco sólido para responder eficazmente a incidentes de seguridad informática y garantizar la continuidad de las operaciones del departamento de TICs del GADMICS en caso de emergencias.

Recomendaciones

- Mantenimiento y Actualización Continua: Es fundamental que el plan de contingencia se mantenga actualizado y se revise de manera periódica para asegurar que refleje los cambios en la infraestructura tecnológica y las nuevas amenazas de seguridad. Asignar responsabilidades claras para la revisión y actualización del plan garantizará su efectividad a lo largo del tiempo.
- Capacitación y Concientización: Es importante llevar a cabo programas de capacitación y concientización periódicos para el personal del departamento de TICs, así como para otros usuarios de los sistemas informáticos. Esto asegurará que todos estén familiarizados con el plan de contingencia y sepan cómo actuar en caso de un incidente de seguridad.
- Respuesta a Incidentes: Establecer un equipo de respuesta a incidentes bien entrenado y coordinado para asegurar una acción rápida y efectiva en caso de que ocurra algún incidente. Definir roles y responsabilidades claras para cada miembro del equipo facilitará una respuesta eficiente.

Bibliografía

Administrativa, D. G. (02 de octubre de 2012). *EAR/PILAR.* EAR/PILAR: https://www.ar-tools.com/doc/magerit/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

Amutio Gómez, M. A., Candau, J., & Mañas, J. A. (2012). MAGERIT. En M. d. Miguel Angel Amutio Gómez, J. Gonzáles Barroso, & D. y. Subdirección General de Información (Edits.), *MAGERIT - versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información Libro I - Método* (responsable edición digital: Subdirección General de Información, Documentación y Publicaciones ed., pág. 127). Madrid, España: © Ministerio de Hacienda y Administraciones Públicas, Secretaría General Técnica, Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones. Retrieved 31 de agosto de 2018, from https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Amutio, M., & Candau, J. (12 de octubre de 2012). *PAE portal, administración electrónica.* PAE Portal Administración Electrónica: https:///2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8%20.pdf

Andrés Rodrigo Reinoso. (2017). *Análisis y Evaluación de Riesgos de Seguridad Informática a través del Análisis de tráfico de datos en redes de área local (LAN).* QUITO.

Campos, C., & León, D. (2020). https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/8244/BC-4644%20CAMPOS%20CRUZ-LEON%20TESEN.pdf?sequence=1&isAllowed=y

Cañon, J., & Calderón, W. (2017). http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2998/Dise%c3%b1o%20de%20un%20sistema%20de%20gestion%20de%20seguridadde%20la%20informacion.pdf?isAllowed=y&sequence=1

Enisa. (02 de Junio de 2005). *Agencia de la Unión Europea para la ciberseguridad*. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_ebios.html

Erb, M. (2010). *Gestión de Riesgo en la Seguridad Informática*. Gestión de Riesgo en la Seguridad Informática: https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

Fuentes, M. (2019). https://stadium.unad.edu.co/preview/UNAD.php?url=%2Fbitstream%2F10596%2F14448%2F1%2F80029231.pdf

Gaona Vásquez, K. d. (octubre de 2013). Retrieved mayo de 2018, from https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf

Gómez, M. A., Candau, J., & Mañas, J. A. (2012). *Magerit, Libro I.* Madrid: © Ministerio de Hacienda y Administraciones Públicas.

Helena Alemán Novoa, C. R. (2015). *Metodologías para el análisis de riesgos en los SGSi*. http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

Huertas, A. (2 de abril de 2012). *Security Artwork*. https://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%E2%80%93-metodologias-ii/

Lapiedra, R., & Carlos Devece, J. G. (2011). Biblioteca Universitat Jaume. En R. Lapiedra, & J. G. Carlos Devece, *Introducción a la gestion de sistemas de informacion en la empresa* (pág. 6). QUITO, PICHINCHA, Ecuador. Retrieved 8 de Mayo de 2018, from https://libros.metabiblioteca.org/bitstream/001/193/8/978-84-693-9894-4.pdf

Lopez, F. (21 de 08 de 2018). *Repositorio de Universidad Nacional.* Interpolados: https://repository.unad.edu.co/bitstream/handle/10596/20419/13748364.pdf?sequence=4&isAllowed=y

López, P. A. (2010). *Seguridad informática.* Editex,S. A.,.

Muñoz, J. (2017). https://stadium.unad.edu.co/preview/UNAD.php?url=%2Fbitstream%2F10596%2F14448%2F1%2F80029231.pdf

nacional, S. g. (2003). *El método EBIOS®.* Paris: desconocida.

nacional, S. g. (2004). *EBIOS.* Francia: consultoria de la DCSSI.

Oscar, S., & Edison, Á. (26 de julio de 2019). *Repositorio, Universidad Tecnica de Ambato.* http://192.188.46.193/bitstream/123456789/69721/1/Silva%20Miranda%20Oscar%20Marcelo%20-%202019.pdf

PILAR Análisis y Gestión de Riesgos Ayuda Versión 7.2. (26 de noviembre de 2018). PILAR Análisis y Gestión de Riesgos Ayuda Versión 7.2: file:///C:/Program%20Files%20(x86)/PILAR_7.2/help_es/cia/WebHelp/index.html#!1089

Prieto, J. A. (Enero de 2018). *Implementación de la metodología octave* . http://fcqi.tij.uabc.mx/usuarios/revistaaristas/numeros/N12/articulos/56-64.pdf

Quintero Villarroya, J. L., & SDG TIC. Ministerio de Defensa. (2012). *Análisis y Gestión de Risgos. Pilar.* Madrid, España: Asociación Española de Calidad CSTIC 2012. Retrieved 10 de Enero de 2019, from https://www.aec.es/c/document_library/get_file?uuid=b3945e58-17f2-4dc0-88ac-863ae9f998cb&groupId=10128

Rodríguez, J. M., Peralta, I., & Consejo Superior de Administración Electrónica. (2013). Gestión de Riesgos Magerit. En J. M. Rodríguez, I. Peralta, Consejo Superior de ADministración Electrónica, & t. P. Peralta (Ed.), *Gestión de Riesgos Magerit* (pág. 38). ©tiThink 2013. Retrieved 31 de agosto de 2018, from https://www.tithink.com/publicacion/MAGERIT.pdf

Solarte, F. N. (04 de Julio de 2016). *Sistema de gestión de seguridad*. http://blogsgsi.blogspot.com/2016/07/v-behaviorurldefaultvmlo_93.html

Anexos