Elaboración de un plan de contingencia para los sistemas informáticos de las Juntas administradoras de agua potable de la parroquia de Pastocallle caso de estudio Junta administradora de agua "Miño San Antonio"

Pilatuña Ramos, Edgar Jefferson

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 Tecnólogo Superior en Redes y Telecomunicaciones

Ing. Andaluz Espinosa, Diego Fernando

23 de agosto del 2023

Latacunga

Reporte de verificación de contenido

Copyleaks

Plagiarism report

TESIS_PILATUÑA RAMOS EDGAR JEFFE...

Scan details

Scan time:
August 23th, 2023 at 17:1 UTC

Total Pages:
59

Total Words:
14740

Plagiarism Detection

Types of plagiarism		Words
Identical	3.5%	514
Minor Changes	0%	0
Paraphrased	0%	0
Omitted Words	2.6%	386

AI Content Detection

Text coverage
- AI text
- Human text

Ing. Andaluz Espinosa, Diego Fernando

DIRECTOR

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 los sistemas informáticos de las Juntas administradoras de agua potable de la parroquia de Pastocalle caso de estudio Junta administradora de agua "Miño San Antonio"**, fue realizado por el señor **Pilatuña Ramos, Edgar Jefferson** la cual ha sido revisada y analizada en su totalidad por la herramienta de verificación de similitud de contenido; por lo tanto, cumple con los requisitos legales, teóricos, científicos, tecnológicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Latacunga,23 de agosto del 2023

.....

Ing. Andaluz Espinosa, Diego Fernando

C.C.: 0502352180

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Responsabilidad de Autoría

Yo, **Pilatuña Ramos, Edgar Jefferson**, con cédula de ciudadanía No **1724560220** , declaro que los contenidos, ideas, puntos de vista del presente trabajo de integración curricular: **Elaboración de un plan de contingencia para los sistemas informáticos de las Juntas administradoras de agua potable de la parroquia de Pastocalle caso de estudio Junta administradora de agua "Miño San Antonio"**, es de mi autoría, compromiso y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, metodológicos, y de investigación establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual permitimos acreditar y autorizar para que sustente públicamente.

Latacunga,23 de agosto del 2023

.....

Pilatuña Ramos, Edgar Jefferson

C.C.: 1724560220

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Autorización de Publicación

Yo, **Pilatuña Ramos, Edgar Jefferson**, con cédula de ciudadanía No **1724560220**, autorizo a la Universidad de las Fuerzas Armadas ESPE, publicar el trabajo de integración curricular, **Elaboración de un plan de contingencia para los sistemas informáticos de las Juntas administradoras de agua potable de la parroquia de Pastocalle caso de estudio Junta administradora de agua "Miño San Antonio"**, en el Repositorio Institucional, cuyos contenidos, ideas y puntos de vista es mi responsabilidad.

Latacunga,23 de agosto del 2023

.....

Pilatuña Ramos, Edgar Jefferson

C.C.: 1724560220

Dedicatoria

El presente trabajo lo dedico con todo mi amor y cariño:

Les agradezco a las personas más importantes de mi vida que han estado en todo momento en este proceso de mi vida tanto desde mis inicios con mis estudios y en vida profesional, a mis padres Francisco y Maria quienes desde mi niñez me indujeron los valores que han sido la carta de presentación en todo momento de mi vida y el ejemplo de superación y lucha para convertirme en un profesional, les quedo muy agradecido por todo ese apoyo durante esta etapa estudiantil, por su amor y confianza depositada en mi para cumplir con mi objetivo.

A mis hermanos, por todo el cariño, confianza y el apoyo moral hacia mi persona durante todas las etapas de mi vida como profesional y personal, siempre los llevare en mi corazón cuando estén lejos de casa.

A todas las personas que han depositado su confianza en mi trabajo y mis capacidades para siempre salir adelante y perfeccionarme en todas mis actividades profesionales Dios le pague por sus consejos y ánimos para siempre salir adelante a pesar de las duras circunstancias que me a tocado vivir.

Y como no dedicar este trabajo a las personas que han sido mis mentores durante todos estos años de estudio, han compartido sus conocimientos y experiencias para desenvolverme en el campo laboral actual y enfrentar un futuro competitivo.

Agradecimiento

A gradezco a mi director de tesis, el profesor Ing. Diego Andaluz, por el tiempo entregado a mi persona, para realizar este trabajo. Su conocimiento y experiencia han sido invaluables para mí.

También quiero agradecer a mis mentores que conforman la carrera, Tecnología en Redes y Telecomunicaciones que han dejado sembrada la semilla en mi para poder seguir formándome y perfeccionándome en el ámbito laboral.

También quiero agradecer a mis compañeros de clase por su apoyo y motivación durante el proceso de investigación y escritura. Su entusiasmo y dedicación han sido una gran fuente de inspiración para mí, durante estos años en la universidad.

A mi director de carrera por toda su excelente gestión dentro de la carrera y como docente un agradecimiento fraterno y por acogerme en una de las mejores carreras.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Resumen

Una gran parte de instituciones públicas y privadas no cuenta con un plan de contingencia que permitirá solventar los incidentes que pongan en riesgo las operaciones de la institución donde se vean afectados sus sistemas informáticos, en tal virtud se ve en la necesidad de realizar el estudio y elaboración de un plan de contingencia que pueda ser implantado en instituciones públicas o privadas. A raíz de esta necesidad de resguardo, el Consejo Superior de Administración Electrónica del gobierno de España desarrolló un enfoque metodológico para evaluar y controlar los peligros relacionados con los sistemas de información, conocido como MAGERIT. Su propósito radica en comunicar a los encargados de las actividades de la junta los posibles riesgos y la necesidad de gestionarlos de manera efectiva. El presente caso de estudio es para la junta administradora de agua potable **"**Miño San Antonio", presentará una solución bien definida y estructurada que permita mantener operativa las funciones de la institución cuando ocurra una contingencia sobre la infraestructura tecnológica que se posee. El plan de contingencia propone la aplicación de medidas preventivas y correctivas dentro de los procesos críticos de la institución, los cuales están enfocados a minimizar y reducir el impacto negativo ante la presencia de incidentes o eventos que generen riesgo para el cumplimiento de la misión de la institución.

Palabras clave: Plan de contingencia**,** Mitigación de Riesgos, Respaldos**,** Seguridad informática

Abstract

A large part of public and private institutions does not have a contingency plan that will allow solving incidents that put the operations of the institution at risk where their computer systems are affected, for this reason it is necessary to carry out the study and preparation of a contingency plan that can be implemented in public or private institutions. As a result of this need for safeguards, the Spanish government's High Council for Electronic Administration developed a methodological approach to assessing and controlling information systems-related hazards, known as MAGERIT. Its purpose is to communicate to those in charge of the board's activities the potential risks and the need to manage them effectively. This case study is for the Miño San Antonio potable water management board, it will present a well-defined and structured solution that allows the critical functions of the institution to be kept operational when a contingency occurs on the technological infrastructure that it possesses. The contingency plan proposes the application of preventive and corrective measures within the critical processes of the institution, which are focused on minimizing and reducing the negative impact in the presence of incidents or events that generate risk for the fulfillment of the mission of the institution.

Keywords: Contingency Plan**,** Risk Mitigation**,** Backups**,** IT Security

Capítulo I

Tema: Elaboración de un plan de contingencia para los sistemas informáticos de las Juntas administradoras de agua potable de la parroquia de Pastocallle caso de estudio Junta administradora de agua “Miño San Antonio”

Antecedentes

La mayoría de instituciones a nivel nacional, desde la más grande hasta la más pequeña, cuentan con un infraestructura informática donde se realizan el procesamiento de los datos ya sea propios de la empresa o de los colaboradores, el mismo que debe cumplir con las especificaciones del fabricante y de las normativas internacionales para un correcto funcionamiento, la robustez de la infraestructura también viene acompañada con la seguridad, una de las especificaciones más importe y que muchas de las empresas no lo toman en cuenta.

Las reformas educativas son propuestas del gobierno nacional para lograr un desarrollo de sus funciones, de tal manera se ha visto fundamental hacer énfasis en la consolidación de un sistema educativo formal. Un nuevo modelo educativo basado en tecnología e innovación acoge a ayudantías públicas y así mismo reconoce el interés público. En los centros educativos se debe implementar un sistema estratégico que ayude a descongestionar las áreas apegadas al seguimiento académico de sus escolares (Domínguez, J. 2018).

Fue efectuado un estudio de parte de la Universidad de Minnesota, mostró que aproximadamente 60 empresas que han experimentado el siniestro y no han desarrollado una planeación de restauración quebrarán en 2 a 3 años durante el año. A medida que nos volvamos más dependientes de los recursos informáticos (El Minnesota de Hoy, 2022).

Por ello, es importante destacar que los planes de emergencia incluyen un examen de riesgos a los que se exponen los equipos técnicos e informáticos, incluidos propios archivos, y Determinar qué hacer en caso de accidente.

Un plan de contingencia destaca los aspectos físicos y lógicos donde la mayoría concentran los problemas, también su importancia es establecer pruebas y revisiones periódicas con el fin de mantener un plan de contingencia que pueda ser operativo y actualizado.

Las operaciones previstas en un plan de contingencia se realizan antes, durante y después de la mitigación, pérdida financiera directa o indirecta pérdida de usuarios, costos finales de soporte adicional, costos de compensación, falla de infraestructura técnica, pérdida de información, sistema base defectuosa, entre otros (El Minnesota de Hoy, 2022).

Las empresas públicas y privadas son cada vez más dependientes de su tecnología actual, cambiando la esencia de su negocio a la tecnología, y necesitan una plataforma tecnológica confiable que coopere plenamente para mejorar.

En instituciones, un suceso en las bases tecnológicas puede tener un efecto devastador resultando económico, afectando así el curso de sus actividades en cuestión de minutos (Welington, 2020).

Los desastres tecnológicos no necesariamente tienen que estar relacionados con terremotos, inundaciones, incendios u otros fenómenos naturales de gran magnitud, sino que también pueden ser causados por introducción de un virus o ataque informático, pérdida de información, el peor daño permanente a sistemas de computación o infraestructura técnica. Como tal hay otros tipos de incidentes que tienen el potencial de causar consecuencias muy graves y daños a gran escala a las instituciones.

Las consecuencias de estos eventos en entes que no poseen con planes de contingencia para programas informáticos, podrían llevar a la paralización de los procesos de la agencia, y más aún con respecto a las utilidades básicas que mantiene la plataforma de operaciones, lo que puede generar confusión (Welington, 2020).

Por ello, es importante tener plan de contingencia del sistema informático que permita tener una lista de las acciones que se deben realizar para reducir la recuperación de la infraestructura técnica y reiniciar efectivamente los servicios necesarios. Un sistema en marcha minimizando costos y niveles operativos.

Los planes de contingencia ayudan a ordenar y clasificar responsabilidades y regulaciones para recuperación segura de las composiciones técnicas.

Con este proyecto aplicado en la Junta administradora de agua Miño San Antonio, nuestro caso de estudio de cual partiremos se podrá aplicar la mitigación de riesgos para repoténcialo en las demás juntas aledañas de la parroquia Pastocalle.

Planteamiento de problema

Actualmente, las juntas administradoras de agua potable de la parroquia de Pastocalle cuentan con un sistema informáticos para gestionar la información de los miembros que conforman el diferente número de juntas a su vez conformado una infraestructura tecnológica que la encargada de almacenar un cierto número de activos físicos y lógicos para el procesamiento de los datos.

Las autoridades administrativas y la comuna en general son los encargados de administrar todo el sistema informático que en el caso en concreto no se toman muy para consideración el tema de seguridad informática para la mitigación de los riegos que puede

llegar implicar el poseer un determinado número de componentes ya sean refiriéndonos a el software, hardware, equipamiento de red, sistema de seguridad, video vigencia, etc.

Debido a los eventos que se podrían desarrollarse y dejar sin operación al equipamiento tecnológico se es necesario que todos los activos estén ligados a un plan de contingencia, el mismo que por el momento no cuenta la junta administradora de agua Miño San Antonio, para asegurar su estabilidad de servicios para los contribuyentes de la comunidad, asegurando que todos los sistemas se encuentren operativos a todo momento del día los 365 días del año.

Justificación

La elaboración del plan de contingencia brinda una herramienta de apoyo realizada con el fin de tener una reacción oportuna por parte de los administradores y trabajadores de la institución. Dando una solución a este problema se realizará el desarrollo de un manual de plan de contingencia, encontrándose disponible en todo momento de ser requerido. El instrumento de gestión para el manejo de tecnologías planteada será la encargada informar oportunamente para que el personal pueda tener una idea como afrontar problemas con desastres tecnológicos de forma instantánea. Este servicio ayudará a mitigar los riesgos que puede sufrir los sistemas informáticos, reactivando de esa forma los servicios más rápido y efectivo.

El plan de contingencia para los sistemas informáticos antes mencionados debe cumplir con las normas y estándares internacionales establecidos para seguridad informática (ISO), y gestores de calidad de servicio, dando con resultado el garantizar el funcionamiento y asegurando que la Junta administradora de agua” Miño San Antonio no suspenda sus operaciones.

También se debe resaltar que el sistema informático al no poseer un plan de contingencia esta vulnerable a sufrir ataques informáticos y incluso afectaciones físicas, con la

llegada de desastres naturales, desencadenando eventos como perdida de servicio e incluso de información de forma permanente que podría llegar a afectar a los encargados de la junta y a su vez los miembros de la comunidad.

Objetivos

Objetivo general

Elaborar un plan de contingencia para sistemas informáticos de las juntas administradoras de agua potable Pastocalle, caso de estudio administrado de Junta Administradora de Agua Miño San Antonio.

Objetivos específicos

- Evaluar los riegos de tecnología de la información y comunicación que afecten la continuidad del negocio en las instituciones.
- Determinar métricas que permiten gestionar los procesos críticos apoyados en las tecnologías de la información y comunicación.
- Generar procesos, procedimientos y políticas para mantener la operatividad de los servicios de tecnología de la información y comunicación.

Alcance

El proyecto tiene como fin, la creación de un plan de contingencia destinado a la junta administradora de agua Miño San Antonio se originará mediante una evaluación exhaustiva de los activos que poseen actualmente.

Mediante el análisis, se logra identificar los posibles riesgos y se podrá tomar cartas en el asunto dentro de la junta.

Con base en estos aspectos identificados, se articula directrices específicas dirigidas a las afectaciones de mayor relevancia. Los pasos previamente delineados que personal administrativo podrán en marcha cuando se genera un evento que intervenga con la continuidad de las actividades administrativas, mismas que para el desarrollo del plan de riego está regida a las establecidas en la normativa ISO 27000 y 31000, que servirá como marco de referencia.

Visita técnica a la comunidad participante para realizare un evaluó del estado y operación de los componentes de las oficinas de la institución, como son los activos lógicos y físicos del sistema informático para luego gestionar la tabulación y ingreso al software (EAR/PILAR), que será el encargado de realizar el barrido, validación de los activos para poder determinar los riegos presentes dentro de los mismos.

Capítulo II

Marco Teórico

La información

Se define como información al conjunto de datos ordenados y supervisados que son usados para construir un mensaje sobre un determinado fenómeno, suceso o hecho, teniendo como objetivo disminuir la incertidumbre o aumentar el conocimiento sobre algo (León R. d., 2023).

A su vez los datos se no serían nada sin una administración de métodos que los permitan interactuar entre sí.

La información en la informática

La informática gira en torno a la transformación de datos en información valiosa y significativa. Los datos, que pueden abarcar desde números hasta imágenes, carecen de sentido en su estado puro y necesitan ser procesados para cobrar relevancia (Tramullas, 2020). Esta manipulación implica el uso de algoritmos y operaciones lógicas que convierten los datos en información comprensible y útil para la toma de decisiones y la obtención de conocimiento.

El software juega un papel fundamental en este proceso al permitirnos procesar, organizar y presentar la información de maneras diversas. Desde aplicaciones simples hasta sistemas operativos complejos, el software actúa como herramienta para dar vida a los datos y convertirlos en conocimiento aprovechable (Bernal & Rodriguez, 2020).

La información no solo necesita ser procesada, sino también almacenada de manera segura y accesible. Esto se logra a través de dispositivos de almacenamiento, como discos duros y nubes virtuales, que aseguran que la información esté disponible para su uso futuro.

La transmisión de información a través de redes de comunicación, como Internet, permite acceder a la información desde distintas ubicaciones, lo que ha revolucionado la forma en que compartimos y accedemos a los datos.

Las bases de datos son estructuras organizadas para el almacenamiento eficiente de grandes volúmenes de información. Facilitan la búsqueda y recuperación de datos de manera rápida y ordenada.

La seguridad de la información es un aspecto crítico. La protección contra accesos no autorizados y la prevención de pérdida o alteración de datos se logran a través de medidas como el cifrado y la autenticación (Bernal & Rodriguez, 2020).

Visualizar la información a través de gráficos, tablas y diagramas facilita su comprensión y análisis, ayudando a las personas a extraer significado de los datos.

En el mundo actual, el término "Big Data" se refiere a la gestión y análisis de conjuntos de datos masivos y complejos, lo que presenta desafíos y oportunidades únicas (Bernal & Rodriguez, 2020).

Impactos de la información en la informática

La información es un pilar fundamental en el campo de la informática y ejerce una serie de impactos cruciales en múltiples aspectos. Uno de los roles más destacados de la información radica en su capacidad para respaldar la toma de decisiones informadas. En el ámbito informático, sistemas de análisis de datos y algoritmos permiten a las organizaciones

extraer valiosa información a partir de vastos conjuntos de datos, lo cual guía decisiones estratégicas y operativas con fundamentos sólidos (Zarzet, 2020).

Asimismo, la innovación tecnológica se alimenta de la información, tanto existente como nueva. En el mundo de la informática, ideas frescas, conceptos novedosos y descubrimientos en constante evolución se basan en la comprensión y análisis de la información disponible. Por otro lado, la tecnología de la información brinda la oportunidad de establecer comunicación y colaboración a nivel global. Plataformas en línea, aplicaciones de mensajería y redes sociales permiten el intercambio instantáneo de información, potenciando la colaboración y conectividad en diversas áreas.

En términos de eficiencia, la automatización es un resultado directo del procesamiento de información por sistemas informáticos. Automatizar tareas con precisión y rapidez mejora la eficiencia en múltiples sectores, desde la manufactura hasta la administración empresarial. La gestión y organización de información también es crítica, y la tecnología informática posibilita la creación de sistemas de gestión y bases de datos que almacenan, recuperan y organizan información de manera efectiva, un factor clave en la administración de datos empresariales (Peñafiel, 2021).

La accesibilidad a la información se ha revolucionado gracias a la tecnología. Internet y recursos en línea ofrecen acceso instantáneo a una amplia gama de información. Además, el análisis inteligente y la toma de decisiones basada en datos son posibles gracias a la tecnología informática. Esta capacidad de analizar patrones y tendencias en grandes volúmenes de información resulta invaluable para áreas como el análisis financiero, el marketing y la investigación científica.

No obstante, la tecnología también trae desafíos. La gestión segura de información personal y confidencial es fundamental, con tecnologías de seguridad y cifrado empleadas para

proteger la información de amenazas y accesos no autorizados. La información es una fuerza impulsora en la transformación digital de las organizaciones, permitiéndoles adaptarse a las cambiantes demandas empresariales y adoptar nuevas tecnologías para aumentar la eficiencia y la competitividad. En resumen, la información es el alma de la informática y su influencia abarca todos los aspectos de la tecnología y la sociedad moderna, impulsando el avance tecnológico y el éxito organizativo.

Seguridad Informática

La seguridad informática es un campo crucial en el mundo digital actual, que se enfoca en proteger los sistemas, redes, datos y recursos tecnológicos de amenazas cibernéticas y ataques maliciosos. La creciente dependencia de la tecnología y la interconexión global han aumentado la importancia de mantener la integridad, confidencialidad y disponibilidad de la información en entornos digitales (Navas, 2021).

De acuerdo a (Sanchez, 2021)la seguridad informática abarca una amplia gama de prácticas, políticas y tecnologías diseñadas para prevenir, detectar y responder a las amenazas cibernéticas. Los aspectos fundamentales de la seguridad informática incluyen:

- Ciberamenazas y ataques: Esto abarca una variedad de ataques cibernéticos, como el malware (software malicioso), los virus, los gusanos, el phishing (suplantación de identidad), el ransomware (secuestro de datos) y los ataques de denegación de servicio (DDoS). Estos ataques pueden tener graves consecuencias, desde el robo de información hasta el daño a la infraestructura digital.

- Prevención: La prevención implica la implementación de medidas de seguridad proactivas para evitar que las amenazas cibernéticas tengan éxito. Esto incluye la configuración adecuada de cortafuegos, sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS) y sistemas de autenticación fuerte.
- Detección: La detección se centra en identificar y responder a actividades anómalas o potencialmente maliciosas en los sistemas y redes. Esto se logra mediante sistemas de monitoreo y análisis de registros de eventos, así como tecnologías de análisis de comportamiento para identificar patrones de ataque.
- Respuesta: La respuesta implica tomar medidas una vez que se detecta una amenaza. Esto podría implicar la contención del ataque, la eliminación del malware y la restauración de la funcionalidad normal del sistema. La respuesta eficaz puede minimizar el impacto del ataque y reducir el tiempo de inactividad.
- Recuperación: La recuperación involucra la restauración de sistemas y datos a un estado operativo después de un incidente de seguridad. Esto puede implicar la recuperación de datos de respaldo y la evaluación de posibles daños.
- Gestión de riesgos: Evaluar y gestionar los riesgos cibernéticos es una parte esencial de la seguridad informática. Esto incluye la identificación de vulnerabilidades en sistemas y aplicaciones, y la implementación de medidas para mitigar esos riesgos.
- Educación y concienciación: La formación de los usuarios y el personal en las mejores prácticas de seguridad cibernética son cruciales para evitar ataques de

ingeniería social y otros ataques que aprovechan la falta de conocimiento en seguridad.

- Actualización y parches: Mantener el software y los sistemas actualizados con los últimos parches de seguridad es esencial para evitar vulnerabilidades conocidas que puedan ser explotadas por atacantes.

La seguridad informática es un desafío en constante evolución debido a la aparición constante de nuevas amenazas y técnicas de ataque. Por lo tanto, es fundamental para las organizaciones y los individuos mantenerse al día con las últimas tendencias en seguridad y adoptar prácticas sólidas para proteger sus sistemas y datos.

Propiedades de un sistema de información seguro

Para Agudeo (2023), la seguridad informática es una preocupación fundamental en el mundo digital actual. Asegurar la integridad, confidencialidad y disponibilidad de la información es esencial para prevenir amenazas y riesgos cibernéticos. Las propiedades de un sistema de información seguro son:

- Confidencialidad: Esta propiedad garantiza que la información solo sea accesible por personas autorizadas. Se logra a través de medidas como el cifrado de datos, autenticación de usuarios y controles de acceso rigurosos. La confidencialidad evita que información sensible caiga en manos equivocadas.
- Integridad: La integridad asegura que los datos no sean modificados ni alterados de manera no autorizada. Para lograrla, se implementan técnicas de detección de cambios no autorizados en los datos y se utilizan firmas digitales para verificar la autenticidad de la información.

- Disponibilidad: Este aspecto se refiere a asegurar que la información esté disponible cuando se necesite. Se implementan sistemas de respaldo y redundancia para evitar interrupciones no deseadas en el acceso a los datos. Los ataques como los ataques de denegación de servicio (DDoS) buscan interrumpir la disponibilidad.
- Autenticación: La autenticación verifica la identidad de los usuarios que intentan acceder al sistema. Esto se logra mediante contraseñas, códigos de autenticación de dos factores (2FA) o biometría, asegurando que solo las personas autorizadas puedan ingresar al sistema.
- Autorización: La autorización define los niveles de acceso que los usuarios tienen a diferentes partes del sistema o a diferentes tipos de información. Esto evita que usuarios no autorizados tengan acceso a recursos o datos sensibles.
- Auditoría y registro de eventos: La capacidad de rastrear y registrar las acciones realizadas en el sistema es esencial para la detección y respuesta a posibles amenazas. Los registros de eventos permiten reconstruir actividades pasadas y pueden ser cruciales en la investigación de incidentes de seguridad.
- Seguridad física: Además de las medidas electrónicas, la seguridad informática también implica la protección física de los sistemas y dispositivos. Esto incluye la limitación del acceso físico a servidores y equipos, así como la implementación de medidas de seguridad en instalaciones.
- Cifrado: El cifrado de datos convierte la información en un formato ilegible que solo puede ser descifrado por aquellos que tengan la clave de descifrado correcta. Esto

protege la información confidencial en caso de que sea interceptada durante la transmisión o el almacenamiento.

- Actualizaciones y parches: Mantener el software y los sistemas actualizados con los últimos parches de seguridad es crucial para evitar vulnerabilidades conocidas. Los ciberdelincuentes a menudo aprovechan fallos en el software desactualizado.
- Concientización y capacitación: La educación de los usuarios sobre las mejores prácticas de seguridad y la prevención de amenazas es esencial. Los ataques de ingeniería social a menudo explotan la falta de conciencia de los usuarios

Procesos de seguridad

De acuerdo a Castillo, (2020), los procesos de seguridad informática son una serie de pasos y actividades organizadas que se implementan para garantizar la protección, detección y respuesta ante amenazas y riesgos cibernéticos. Estos procesos son fundamentales para mantener la integridad, confidencialidad y disponibilidad de la información en sistemas y redes. Aquí hay algunos procesos clave en seguridad informática:

- Gestión de riesgos: Este proceso implica la identificación, evaluación y mitigación de los riesgos cibernéticos. Se analizan las amenazas potenciales, las vulnerabilidades y los posibles impactos para determinar qué medidas de seguridad son necesarias y cómo deben implementarse.
- Planificación de seguridad: En este proceso, se definen las políticas y procedimientos de seguridad que guiarán la protección de los sistemas y datos. También se elabora un plan de respuesta a incidentes que detalla cómo se

abordarán las amenazas y cómo se recuperará la funcionalidad después de un ataque.

- Implementación de medidas de seguridad: Este proceso implica la configuración y el despliegue de tecnologías y prácticas de seguridad. Esto incluye la instalación de cortafuegos, sistemas de detección y prevención de intrusiones, sistemas de autenticación y cifrado, entre otros.
- Monitorización y análisis: La monitorización constante de los sistemas y redes es crucial para detectar actividades anómalas o potencialmente maliciosas. Los registros de eventos y el análisis de comportamiento pueden ayudar a identificar patrones de ataque y posibles vulnerabilidades.
- Respuesta a incidentes: En caso de un incidente de seguridad, este proceso establece cómo se abordará la amenaza. Incluye la identificación y aislamiento de la amenaza, la eliminación de malware y la recuperación de sistemas.
- Recuperación y continuidad del negocio: Después de un incidente, se debe trabajar en la recuperación de los sistemas y la restauración de la funcionalidad normal. Además, se pueden establecer planes de continuidad del negocio para garantizar que las operaciones críticas continúen incluso después de un incidente.
- Capacitación y concienciación: Educación constante para el personal y los usuarios finales es esencial. Esto incluye la capacitación sobre las mejores prácticas de seguridad y cómo reconocer y responder a las amenazas.
- Evaluación y mejora continua: Después de implementar medidas de seguridad, es crucial evaluar su efectividad y realizar ajustes en función de las lecciones

aprendidas de los incidentes pasados. La seguridad informática es un proceso en constante evolución.

- Gestión de acceso: Este proceso se refiere a la administración de los permisos y niveles de acceso de los usuarios a sistemas y datos. Esto asegura que solo las personas autorizadas tengan acceso a la información adecuada.
- Auditoría de seguridad: La auditoría regular de sistemas y redes ayuda a identificar posibles debilidades y asegura que las políticas de seguridad se estén aplicando correctamente.

Estos procesos de seguridad trabajan en conjunto para crear una estrategia sólida de seguridad informática, protegiendo sistemas y datos de manera integral y efectiva.

Análisis de seguridad

De acuerdo a Izquierdo, (2020), el análisis de seguridad es un proceso fundamental en el campo de la seguridad informática que implica evaluar y comprender la postura de seguridad de sistemas, redes, aplicaciones y otros activos digitales. El objetivo principal del análisis de seguridad es identificar vulnerabilidades, debilidades y riesgos potenciales en un entorno tecnológico para tomar medidas proactivas y proteger eficazmente la información y los activos digitales. Aquí hay algunos aspectos clave del análisis de seguridad:

- Evaluación de riesgos: El análisis de seguridad comienza con la evaluación de riesgos. Esto implica identificar amenazas potenciales que podrían explotar vulnerabilidades y causar daños, ya sea a nivel de software, hardware o procesos.
- Identificación de vulnerabilidades: Durante el análisis, se buscan vulnerabilidades conocidas y desconocidas en sistemas y aplicaciones. Esto puede incluir

debilidades en el código, configuraciones inseguras o cualquier aspecto que pueda ser aprovechado por atacantes.

- Pruebas de penetración: Las pruebas de penetración (pen testing) son una parte importante del análisis de seguridad. Implican simular ataques reales para evaluar la resistencia de un sistema. Los expertos en seguridad intentan explotar vulnerabilidades y luego proporcionan recomendaciones para mitigar los riesgos.
- Evaluación de la arquitectura: Se analiza la arquitectura de los sistemas y redes para identificar posibles puntos débiles en el diseño. Esto podría incluir evaluaciones de la seguridad de red, la configuración de cortafuegos y la separación adecuada de redes.
- Análisis de código: Se examina el código fuente de aplicaciones y software para identificar posibles vulnerabilidades y errores de programación que podrían ser explotados por atacantes.
- Análisis de registros y eventos: Se revisan los registros de eventos y actividades en sistemas y redes para identificar patrones de actividad sospechosa. Esto puede ayudar a detectar amenazas en tiempo real o identificar actividades anómalas después de un incidente.
- Análisis de comportamiento: Se utilizan técnicas de análisis de comportamiento para identificar actividades que se desvían de los patrones normales. Esto puede ser útil para detectar amenazas internas o externas que evaden las medidas de seguridad tradicionales.
- Evaluación de políticas y procedimientos: Además de la tecnología, se evalúan las políticas y los procedimientos de seguridad establecidos en una organización. Esto

asegura que haya una alineación entre las prácticas operativas y las necesidades de seguridad.

- Informe y recomendaciones: Después del análisis, se genera un informe detallado que resalta las vulnerabilidades identificadas, los riesgos potenciales y las recomendaciones para abordarlos. Este informe es esencial para tomar decisiones informadas sobre cómo mejorar la seguridad.
- Mejora continua: El análisis de seguridad no es un evento único. Debe ser un proceso continuo para mantenerse al día con las amenazas emergentes y los cambios en el entorno tecnológico.

Gestión de riegos

Para Pazmiño (2022), la gestión de riesgos es un proceso fundamental en el ámbito de la seguridad informática y la seguridad en general. Consiste en identificar, evaluar y mitigar los riesgos potenciales que pueden afectar los sistemas, activos digitales, datos y operaciones de una organización. El objetivo principal de la gestión de riesgos es tomar medidas proactivas para reducir la probabilidad y el impacto de posibles amenazas y eventos adversos. Aquí están los componentes clave de la gestión de riesgos:

- Identificación de riesgos: El proceso comienza por identificar las posibles amenazas y vulnerabilidades que podrían afectar la seguridad de los activos digitales y la operación de una organización. Esto implica examinar tanto factores internos como externos.
- Análisis de riesgos: Una vez identificados los riesgos, se realiza un análisis más profundo para evaluar su probabilidad de ocurrencia y su impacto potencial. Esto

ayuda a priorizar qué riesgos son más críticos y merecen una atención inmediata.

- Evaluación de impacto: Se determina cómo cada riesgo podría afectar la operación de la organización, la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas. Esto permite comprender las posibles consecuencias y tomar medidas adecuadas.
- Evaluación de probabilidad: Se evalúa la probabilidad de que un riesgo específico se materialice. Esto ayuda a comprender cuán probable es que ocurra un evento adverso y qué nivel de preparación se necesita.
- Mitigación de riesgos: Una vez que los riesgos han sido identificados y evaluados, se toman medidas para reducir su probabilidad y su impacto. Esto puede implicar la implementación de controles de seguridad, políticas, procedimientos y tecnologías específicas.
- Transferencia de riesgos: En algunos casos, una organización puede optar por transferir parte del riesgo a terceros, como compañías de seguros o proveedores de servicios de seguridad. Esto permite que la organización comparta la carga financiera en caso de que ocurra un evento adverso.
- Aceptación de riesgos: Algunos riesgos pueden ser difíciles de mitigar o costosos de abordar completamente. En tales casos, una organización puede optar por aceptar cierto nivel de riesgo y estar preparada para responder adecuadamente en caso de que ocurra un evento adverso.

- Monitoreo y revisión: La gestión de riesgos es un proceso continuo. Se debe monitorear constantemente el entorno de seguridad para detectar cambios en los riesgos y ajustar las estrategias de mitigación según sea necesario.
- Planificación de contingencia: Como parte de la gestión de riesgos, se deben desarrollar planes de contingencia y de respuesta a incidentes. Estos planes describen cómo la organización responderá a eventos adversos y cómo se recuperará de ellos.
- Comunicación y concienciación: Es importante que todos los niveles de la organización comprendan los riesgos y las medidas de seguridad implementadas. La comunicación y la concienciación son esenciales para crear una cultura de seguridad.

La gestión de riesgos es esencial para mantener la seguridad y la continuidad de las operaciones en un entorno tecnológico en constante evolución. Al abordar proactivamente los riesgos, las organizaciones pueden reducir la exposición a amenazas cibernéticas y minimizar los impactos de posibles incidentes.

Variables de la seguridad

La seguridad informática se sustenta en una serie de variables esenciales que trabajan en conjunto para salvaguardar sistemas, datos y recursos contra amenazas y riesgos. La confidencialidad se ocupa de restringir el acceso no autorizado a información sensible, mientras que la integridad garantiza que los datos permanezcan inalterados y consistentes. La disponibilidad se concentra en asegurar que sistemas y recursos estén disponibles cuando se necesiten, evitando interrupciones imprevistas (More, 2022).

La autenticación verifica la identidad de usuarios o sistemas, mientras que la autorización define sus permisos de acceso. La auditoría y monitorización vigilan actividades para detectar actividades sospechosas. La criptografía cifra y protege datos, y la seguridad física resguarda activos como servidores y centros de datos de daños y accesos no autorizados.

La prevención de intrusiones bloquea accesos no deseados, y la detección y respuesta a incidentes se encargan de actuar rápidamente ante amenazas. La educación y concienciación del personal son cruciales para prevenir ataques como el phishing. Las políticas y el cumplimiento establecen reglas claras, y la gestión de riesgos evalúa y mitiga amenazas potenciales.

Mantener actualizados sistemas y software con parches de seguridad, así como respaldar datos, son componentes vitales. En un entorno de nube, comprender y aplicar medidas de seguridad específicas es clave.

Retención de fuga de datos

Para Villaseca (2023), la retención de fuga de datos, también conocida como "Data Loss Prevention" (DLP) en inglés, es una estrategia y conjunto de tecnologías diseñadas para prevenir la filtración no autorizada de información sensible y confidencial fuera de una organización. La retención de fuga de datos se centra en identificar, supervisar y controlar la transferencia de datos sensibles, ya sea intencional o accidentalmente, a través de diversos canales de comunicación, como correos electrónicos, redes, dispositivos de almacenamiento y más. El objetivo es proteger la integridad y confidencialidad de los datos críticos de una organización. Aquí hay aspectos clave de la retención de fuga de datos:

- Identificación de datos sensibles: El primer paso en la retención de fuga de datos es identificar qué tipos de datos se consideran sensibles y confidenciales para la organización. Esto puede incluir información financiera, datos personales, propiedad intelectual, secretos comerciales y más.
- Supervisión de canales de comunicación: Las soluciones de retención de fuga de datos monitorean activamente las comunicaciones internas y externas para detectar patrones y comportamientos que puedan indicar la transferencia no autorizada de datos sensibles.

Políticas de seguridad: Se establecen políticas y reglas que definen qué acciones están permitidas y cuáles no en relación con la transferencia de datos sensibles. Esto podría incluir bloquear ciertos tipos de archivos adjuntos en correos electrónicos o prevenir la carga de ciertos tipos de datos en plataformas en la nube.

- Detección de patrones: Las soluciones DLP utilizan algoritmos y análisis de contenido para detectar patrones que podrían indicar la transferencia no autorizada de datos. Esto puede incluir la detección de números de tarjetas de crédito, información médica o información confidencial en los correos electrónicos.
- Prevención de filtraciones: Si se detecta una transferencia no autorizada de datos sensibles, las soluciones DLP pueden tomar medidas para prevenir la fuga. Esto podría incluir bloquear la transferencia, notificar a los administradores de seguridad o aplicar acciones correctivas.
- Monitorización de actividades: Las soluciones DLP también pueden proporcionar informes y análisis sobre las actividades relacionadas con la retención de fuga de datos. Esto ayuda a las organizaciones a entender los patrones y áreas de riesgo.

- Educación y concienciación: Junto con las tecnologías DLP, es esencial educar y concienciar al personal sobre las políticas de seguridad y las mejores prácticas para prevenir la fuga de datos. Muchas filtraciones ocurren por errores humanos involuntarios.
- Adaptabilidad: La retención de fuga de datos debe ser adaptable a los cambios en la tecnología y las necesidades de la organización. Las soluciones DLP deben actualizarse regularmente para abordar nuevas amenazas y tipos de datos sensibles.

La retención de fuga de datos es especialmente importante en entornos en línea y digitales, donde la transferencia de información puede ocurrir de manera rápida y a menudo inadvertida. Al implementar estrategias y tecnologías DLP, las organizaciones pueden minimizar el riesgo de exposición de datos sensibles y mantener la confianza de sus clientes y socios comerciales.

Ingeniería social

La ingeniería social de acuerdo a Olmedo (2020), es una técnica utilizada por atacantes cibernéticos y delitos informáticos para manipular a las personas y obtener información confidencial o acceso a sistemas y redes. A diferencia de los ataques que se centran en explotar debilidades técnicas, la ingeniería social se basa en la manipulación psicológica y la explotación de la confianza de las personas. Los atacantes utilizan diversos métodos para engañar a sus víctimas y lograr sus objetivos. Algunas formas comunes de ingeniería social incluyen:

- Phishing: Los ataques de phishing involucran el envío de correos electrónicos o mensajes falsificados que parecen provenir de fuentes legítimas, como empresas o instituciones financieras. Estos mensajes intentan convencer a las personas de hacer clic en enlaces maliciosos o proporcionar información personal y financiera.
- Pretexto: En este enfoque, los atacantes crean una historia convincente o un "pretexto" para engañar a la víctima. Pueden hacerse pasar por colegas, empleados de soporte técnico o incluso amigos y familiares para obtener información confidencial.
- Ingeniería social telefónica: Los atacantes pueden llamar a las víctimas haciéndose pasar por representantes de empresas legítimas o autoridades, como agentes de policía. Pueden solicitar información confidencial o instruir a la víctima a tomar ciertas acciones que beneficien al atacante.
- Manipulación emocional: Los atacantes pueden explotar las emociones humanas, como el miedo o la empatía, para obtener información o persuadir a las víctimas a realizar acciones no deseadas. Esto puede involucrar historias tristes, amenazas o situaciones de urgencia.
- Ingeniería social en redes sociales: Los atacantes pueden recopilar información personal sobre una víctima de redes sociales y luego utilizar esa información para diseñar un enfoque personalizado. Esto puede aumentar la probabilidad de éxito del ataque.

Ataques de ingeniería social cara a cara: En este enfoque, los atacantes interactúan directamente con las víctimas en persona. Pueden hacerse pasar por contratistas, repartidores o empleados de mantenimiento para ganar acceso a instalaciones o sistemas.

- Manipulación de confianza: Los atacantes pueden ganarse la confianza de las víctimas a lo largo del tiempo, haciéndose pasar por amigos o colegas. Luego, pueden explotar esa confianza para obtener información confidencial o acceso a sistemas.

La ingeniería social es peligrosa porque se basa en la naturaleza humana y nuestra tendencia a confiar en otros. Los ataques de este tipo pueden ser difíciles de detectar y defender debido a su enfoque en la manipulación psicológica. La mejor defensa contra la ingeniería social es la educación y la concienciación. Las personas deben estar alerta a las señales de posibles ataques y ser cautelosas al proporcionar información confidencial o tomar acciones en línea o fuera de línea.

Resguardo de información

El resguardo de información, también conocido como "backup", es un proceso esencial en la seguridad informática que implica crear copias de seguridad de datos y archivos importantes con el propósito de protegerlos contra la pérdida, daño o acceso no autorizado. El resguardo de información es fundamental para asegurar la disponibilidad y la integridad de los datos, ya que los sistemas y dispositivos pueden sufrir fallas técnicas, ataques cibernéticos, errores humanos u otras eventualidades que puedan poner en riesgo la información crítica (Garcia, 2021). Aquí están los aspectos clave del resguardo de información:

- Identificación de datos críticos: El primer paso es identificar los datos y archivos que son críticos para la operación de la organización. Esto podría incluir datos financieros, registros de clientes, documentos legales, información de proyectos y más.

- Frecuencia de respaldo: Se debe determinar con qué frecuencia se realizarán las copias de seguridad. Esto dependerá de la importancia de los datos y de la cantidad de cambios que se realicen en ellos. Algunas organizaciones realizan copias de seguridad diarias, mientras que otras lo hacen semanal o mensualmente.
- Métodos de respaldo: Existen varios métodos de respaldo, que incluyen respaldo en disco duro externo, respaldo en servidores en la nube, respaldo en cintas magnéticas, entre otros. La elección del método depende de las necesidades y recursos de la organización.

Estrategia de retención: Se debe definir cuánto tiempo se mantendrán las copias de seguridad. Algunos datos pueden requerir un período de retención más largo que otros, debido a regulaciones legales u otros requisitos.

- Pruebas de recuperación: No basta con crear copias de seguridad; es importante probar regularmente la capacidad de restaurar los datos desde las copias de seguridad. Esto asegura que los datos puedan ser recuperados de manera efectiva en caso de una pérdida real.
- Almacenamiento seguro: Las copias de seguridad deben almacenarse en un lugar seguro que esté protegido contra el acceso no autorizado, el daño físico y los desastres naturales. Las copias de seguridad en la nube pueden proporcionar una protección adicional contra desastres locales.
- Automatización: Utilizar soluciones de respaldo automatizado es fundamental para asegurarse de que las copias de seguridad se realicen de manera regular y consistente, sin depender de la intervención manual.

- Documentación: Es importante llevar un registro de los procedimientos de respaldo, las frecuencias, los métodos y otros detalles importantes. Esto facilita la recuperación de datos y la planificación en caso de una pérdida.
- Actualización de copias de seguridad: A medida que los datos cambian y se actualizan, es importante asegurarse de que las copias de seguridad también se actualicen para reflejar la información más reciente.

Copias de seguridad

Las copias de seguridad, de acuerdo a Amate (2020), expresa que también son conocidas como backups, son duplicados de datos y archivos importantes almacenados en una ubicación secundaria o en un medio diferente al de los datos originales. El propósito principal de las copias de seguridad es asegurar que los datos estén protegidos contra pérdidas accidentales, daños, corrupción, ataques cibernéticos u otros eventos adversos. Aquí hay aspectos clave relacionados con las copias de seguridad:

Tipos de copias de seguridad

- Copia completa: Se copian todos los datos y archivos en su totalidad.
- Copia incremental: Solo se copian los datos nuevos o modificados desde la última copia.
- Copia diferencial: Se copian los datos nuevos o modificados desde la última copia completa.
- Copia en espejo: Se crea una réplica exacta de los datos en tiempo real.

Importancia de las copias de seguridad:

Protección contra pérdida de datos debido a fallas de hardware, errores humanos, malware, ransomware y otros eventos.

Facilitan la recuperación después de desastres naturales, robos o daños físicos en los dispositivos.

Frecuencia de las copias de seguridad

La frecuencia depende de la cantidad y la importancia de los datos, así como de la velocidad de cambio en los archivos.

Datos críticos pueden requerir copias de seguridad.

- Medios de almacenamiento:

Discos duros externos, unidades USB y otros medios físicos.

Almacenamiento en la nube, que ofrece accesibilidad desde cualquier lugar y protección contra desastres locales.

- Automatización:

Es importante configurar sistemas de copias de seguridad automáticas para garantizar que las copias se realicen regularmente sin intervención manual.

- Verificación y restauración:

Después de cada copia de seguridad, se debe verificar su integridad para asegurarse de que los datos se copiaron correctamente.

Realizar pruebas de restauración periódicas para asegurarse de que las copias de seguridad sean recuperables.

- Almacenamiento seguro:

Las copias de seguridad deben almacenarse en lugares seguros, protegidos contra acceso no autorizado, daños físicos y desastres.

- Retención de copias de seguridad:

Definir cuánto tiempo se mantendrán las copias de seguridad antiguas antes de eliminarlas.

Algunos datos pueden requerir retenciones más largas debido a regulaciones o requisitos legales.

- Enfoque en datos críticos:

Priorizar la copia de seguridad de datos y archivos que son esenciales para la operación y la continuidad del negocio.

- Política de copias de seguridad:

Establecer una política clara que defina quién es responsable de las copias de seguridad, cuándo se deben realizar y cómo se deben manejar los procedimientos de recuperación.

Las copias de seguridad son una parte esencial de la estrategia de seguridad informática y deben ser implementadas tanto por organizaciones como por individuos. La pérdida de datos puede tener consecuencias devastadoras, y las copias de seguridad bien gestionadas pueden proporcionar una forma efectiva de mitigar esos riesgos.

Respaldos

Es otro aspecto muy importante que va relacionado con la planificación de problemas, es el apoyo información pueden ser interna o externa.

Respaldo interno

El objetivo de las copias de seguridad internas es resolver contingencias menores que no requieran la reubicación externa de los elementos informáticos afectados (Palacios Pacheco, 2013).

Respaldo externo

El objetivo de las copias de seguridad fuera del sitio es resolver emergencias críticas que requieren viajar fuera del sitio a una ubicación distinta a la ubicación normal cuando la gravedad de la emergencia impide la aplicación de una solución de copia de seguridad interna (Palacios Pacheco, 2013).

Infraestructura tecnológica

Para Cando (2020), la infraestructura tecnológica se refiere a la base tecnológica y los recursos necesarios para operar sistemas, aplicaciones y servicios en una organización. Esta infraestructura proporciona el soporte técnico necesario para que las operaciones comerciales sean eficientes y efectivas. La infraestructura tecnológica incluye una variedad de componentes y elementos interconectados que permiten la comunicación, el procesamiento de datos y la entrega de servicios digitales. Aquí hay algunos aspectos clave de la infraestructura tecnológica:

- Hardware:

Servidores: Dispositivos que proporcionan servicios y recursos a través de una red.

Estaciones de trabajo: Computadoras utilizadas por los empleados para realizar tareas.

Dispositivos de red: Enrutadores, conmutadores, puntos de acceso inalámbrico, etc.

Dispositivos de almacenamiento: Unidades de disco duro, sistemas de almacenamiento en red, unidades de estado sólido, etc.

- Redes:

Infraestructura de red: Cables, enrutadores, conmutadores y otros componentes que permiten la comunicación entre dispositivos.

Redes locales (LAN): Redes dentro de un lugar específico, como una oficina.

Redes de área amplia (WAN): Redes que abarcan distancias más grandes, como conexiones entre ubicaciones geográficas.

- Software:

Sistemas operativos: Plataformas de software que gestionan recursos de hardware y permiten la ejecución de aplicaciones.

Aplicaciones: Software diseñado para tareas específicas, como suites de productividad, software de gestión y más.

Software de seguridad: Soluciones antivirus, firewalls, sistemas de prevención de intrusiones, etc.

- Virtualización:

Permite ejecutar múltiples sistemas operativos y aplicaciones en un mismo hardware físico.

Reduce los costos, mejora la utilización de recursos y facilita la administración.

- Nube:

Uso de recursos informáticos (como almacenamiento y procesamiento) a través de Internet en lugar de infraestructura local.

Modelos de nube incluyen SaaS (Software como Servicio), PaaS (Plataforma como Servicio) e IaaS (Infraestructura como Servicio).

- Centros de datos:

Instalaciones que albergan servidores, almacenamiento y otros componentes de infraestructura.

Pueden ser propios o administrados por terceros proveedores de servicios.

- Seguridad:

Medidas y tecnologías para proteger la infraestructura contra amenazas cibernéticas.

Incluye firewalls, sistemas de detección de intrusos, autenticación y cifrado.

- Respaldo y recuperación:

Estrategias y tecnologías para realizar copias de seguridad de datos y sistemas, y para recuperarlos en caso de fallos.

- Gestión de sistemas:

Herramientas y procesos para administrar, monitorear y mantener los componentes de la infraestructura.

- Escalabilidad y planificación:

Diseñar la infraestructura para permitir un crecimiento futuro y para acomodar cambios en las necesidades tecnológicas.

La infraestructura tecnológica es fundamental para el funcionamiento de las organizaciones en la era digital. La planificación, implementación y gestión adecuadas de la infraestructura son esenciales para asegurar que los sistemas sean seguros, confiables y eficientes en el cumplimiento de los objetivos comerciales.

Activos tecnológicos

De acuerdo a León (2021), los activos tecnológicos son recursos y componentes de tecnología que una organización posee y utiliza para respaldar sus operaciones y alcanzar sus objetivos comerciales. Estos activos pueden incluir hardware, software, datos, redes y otros recursos relacionados con la tecnología de la información. Los activos tecnológicos son esenciales para la eficiencia, la innovación y la competitividad en la era digital. Aquí hay varios tipos de activos tecnológicos:

- Hardware:
- Servidores: Computadoras potentes utilizadas para almacenar y procesar datos y aplicaciones en redes.
- Estaciones de trabajo: Computadoras utilizadas por los empleados para tareas diarias.
- Dispositivos móviles: Teléfonos inteligentes, tabletas y otros dispositivos utilizados para la comunicación y la productividad.
- Dispositivos de red: Enrutadores, conmutadores, puntos de acceso inalámbrico, etc.
- Software:

Sistemas operativos: Plataformas que gestionan los recursos de hardware y permiten que las aplicaciones se ejecuten.

- Aplicaciones:

Software utilizado para realizar tareas específicas, como procesadores de texto, hojas de cálculo, software de diseño, etc.

Software de seguridad: Soluciones antivirus, firewalls, sistemas de prevención de intrusiones, etc.

- Datos:

Información almacenada en bases de datos, archivos y otros sistemas.

Datos de clientes, información financiera, registros de ventas y más.

Los datos son un activo crítico para la toma de decisiones y la operación de la organización.

- Redes:

Infraestructura de red: Componentes como cables, enrutadores y conmutadores que permiten la comunicación entre dispositivos.

Redes locales (LAN) y de área amplia (WAN) utilizadas para la comunicación y el acceso a recursos compartidos.

- Recursos en la nube:

Almacenamiento y recursos informáticos (como servidores virtuales) proporcionados a través de Internet por proveedores de servicios en la nube.

Plataformas como Amazon Web Services (AWS), Microsoft Azure y Google Cloud.

- Aplicaciones personalizadas:

Software diseñado y desarrollado específicamente para satisfacer las necesidades únicas de una organización.

Puede incluir aplicaciones internas, herramientas de gestión y sistemas personalizados.

Dispositivos IoT (Internet de las cosas):

Dispositivos conectados a Internet que recopilan y transmiten datos, como sensores en fábricas, cámaras de seguridad, termostatos inteligentes, etc.

- Propiedad intelectual y software patentado:

Derechos de propiedad intelectual relacionados con software, invenciones tecnológicas y otros activos de propiedad intelectual.

- Licencias y derechos de uso:

Permisos para utilizar software y servicios bajo ciertas condiciones y términos.

Recursos de seguridad:

Herramientas de seguridad como firewalls, sistemas de detección de intrusos y soluciones de autenticación.

La gestión adecuada de los activos tecnológicos es fundamental para garantizar su utilización efectiva, seguridad y eficiencia. Las organizaciones deben llevar a cabo un seguimiento, una planificación y una inversión cuidadosos para mantener sus activos tecnológicos actualizados y alineados con sus objetivos comerciales a largo plazo.

Activos Físicos

Los activos físicos son elementos tangibles que una organización posee y utiliza para llevar a cabo sus operaciones y cumplir sus objetivos comerciales. Estos activos son recursos valiosos que pueden ser utilizados para generar ingresos, mejorar la eficiencia y respaldar las operaciones diarias de una organización (Loyola, 2022).

Activos lógicos

Dentro de las organizaciones, después de la valoración de los activos se debe tomar encuentra que para su funcionamiento total y continuo se debe crear un plan que mitigue los riesgos y amenazas que este podría sufrir (Cartuche, 2022).

Plan de Contingencia

El plan de contingencia es conjunto de políticas permiten una resolución rápida para restaurar los servicios de la agencia o de la organización en caso de contingencias que interrumpan parcialmente o interrumpan las actividades de la agencia o de la organización, y/o puede definirse como una estrategia que incluye pasos, un plan de contingencia de sistemas y equipos informáticos son definidos por Fernández (2015) como un objeto que garantiza que los procesos continúen en funcionamiento en caso de un problema del sistema de información".

Todos los entes pueden presentar a distintos problemas en sistemas informáticos, ya sean estos incendios, inundaciones, sabotajes, etc. cómo virus, información, software, almacenamiento inadecuado, etc. Puede paralizar parcial o completamente la actividad normal, lo que resulta en daño tisular.

Los incidentes imprevistos en los sistemas y equipos informáticos pueden tener diferentes impactos en una institución según las afectaciones, y si no predefine varias medidas para minimizar este impacto, su organización puede afectar su supervivencia. Los planes de contingencia están diseñados para minimizar el impacto de un incidente en los sistemas informáticos de una empresa, para garantizar el servicio y la productividad en caso de desastre, y para proteger la infraestructura crítica. alcanzando (Ayudaley, 2020).

Figura 1

Valoraciónes de un plan de contingencia

Nota. En la imagen se demuestra un plan de contingencia y las valoraciones de cada proceso. Tomado de (Ayudaley, 2020).

Objetivos del plan de contingencia

El objetivo de la planificación de una contingencia es dejar que una organización continúe con su actividad normal lo más rápido posible después de un evento imprevisto.

Garantice la integridad de los colaboradores y visitantes.

Protección de los datos es confidencial.

Protección de documentos, suministros.

Garantía de la pronta reanudación de las operaciones causado por error humano, destrucción intencional y falla del equipo. Mitigación de riesgos debido a desastres.

Capacidad para continuar las operaciones posteriores a un evento desastroso.

Metodología del plan de contingencia

La construcción de planes contingentes se guía de la metodología. Esto le permite adaptarse a las bases proporcionada por la instalación como a los servicios (Ortega, 2011).

Figura 2

Fases de plan de contingencia

Nota. En la fotografía se representa las fases de un plan de contingencia. Tomado de (Ayudaley, 2020).

Hay varias consideraciones importantes al modelar e implementar un plan de contingencia.

Le recomendamos que utilice una herramienta para realizar un análisis de riesgo.

Deben definirse los procesos de disponibilidad y continuidad de TI para garantizar que los planes se mantengan actualizados frente al cambio constante.

También debe definir los criterios de lanzamiento para el plan.

También es importante definir una estrategia para recuperar y cumpla con estándares de calidad.

Riesgos

El riesgo lo define la Universidad Simón Bolívar (2009) como "la probabilidad de que una amenaza pueda explotar una vulnerabilidad particular". Técnicamente, el riesgo generalmente se considera solo como una amenaza que determina el grado de riesgo de que ocurra una pérdida.

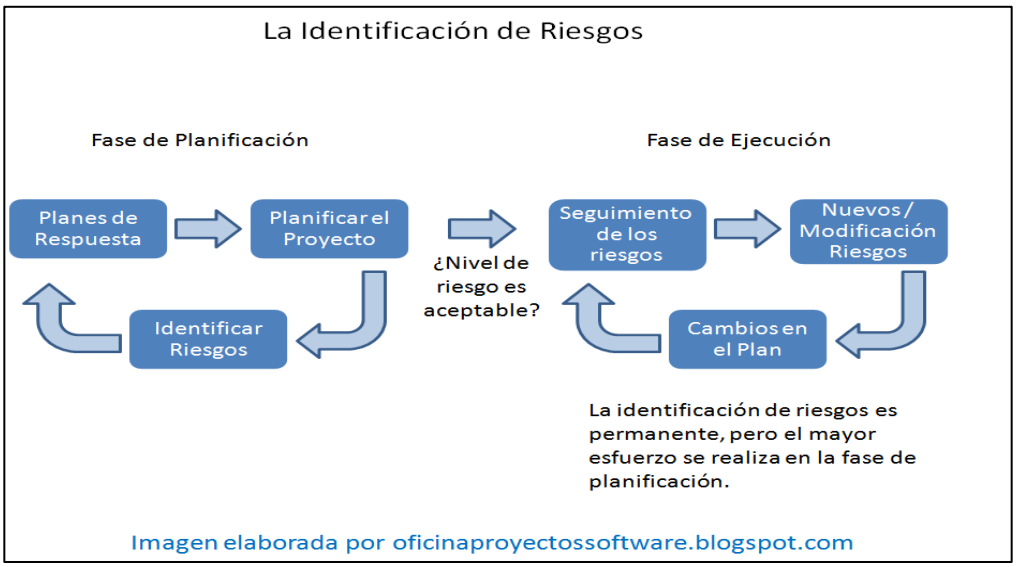
Evaluación, tratamiento y monitoreo del riesgo

Los riesgos a los que están expuestos los activos son fundamentales para poder gestionarlos. Así, han surgido numerosos métodos e instrumentos que tienen como objetivo el análisis que permite ver qué tan inseguros pueden ser estos (Universidad Simón Bolívar, 2009).La serie ISO 27000 es ahora una unión de las pautas que brindan las bases para los sistemas de organización de seguridad de información y, de manera similar, ISO 31000 se centra en la gestión de riesgos en sí. Como tal proporciona información crítica para que las empresas conozcan los riesgos que corren archivos de información y estén preparados para evitarlos.

En resumen, estos estándares establecen que los archivos de información serán evaluados para conocer el impacto. posteriormente se realiza un análisis para conocer qué esta en peligro. la Universidad Simón Bolívar (2009) define como "En ese momento, se deben tomar decisiones sobre los riesgos que aceptará la organización y qué controles se implementarán para mitigar esos riesgos". Además, otras amenazas de evaluación de riesgo, por lo que la vulnerabilidad equivale a una condición en cuanto a vulnerabilidad para cada de amenaza (Gobierno del encuentro, 2013).

Figura 3

Proceso para tratamiento de riegos



Nota. La fotografía demuestra la identificación de riesgos y su tratamiento para detener. Tomado de (PMOinformatica.com).

Las siguientes áreas se consideran para determinar los parámetros para evaluar los controles según la acción asignada.

- Gestión TI.
- Seguridad de información.
- Desarrollo del sistema informático.

En cuanto se refiere al seguimiento y gestión de riesgos, cabe destacar que son regulares. Además, la persona responsable de seguir debe estar definida. Para que tengan éxito, debe contener los aspectos de gestión de riesgos:

- Asegurar controles efectivos y eficientes.
- Conseguir datos para la evaluación de riesgos.
- Analizar los eventos incluidos en accidentes.
- Reconocer nuevos riesgos

Metodología para la gestión de riesgos tecnológicos

Octave

Una actualización de Software Engineering Institute (SEI), cubre problemas organizativos y examina que las personas usan la infraestructura de en su trabajo diario. (Sordo) define "El objetivo de OCTAVE es el riesgo organizacional y se enfoca en temas relacionados con la estrategia y la práctica".

Cramm

Se basa en la norma ISO 27001, pretende permitir a agentes de seguridad, reconocer riesgos y reducirlos a niveles aceptables (Guglieri, 1999).

Risk It

Ahorra tiempo, dinero y esfuerzo al proporcionar una metodología clara para centrarse en los riesgos asociados con tecnología de información. Metodología de asociación de auditoría que controla los sistemas de información (Isaca).

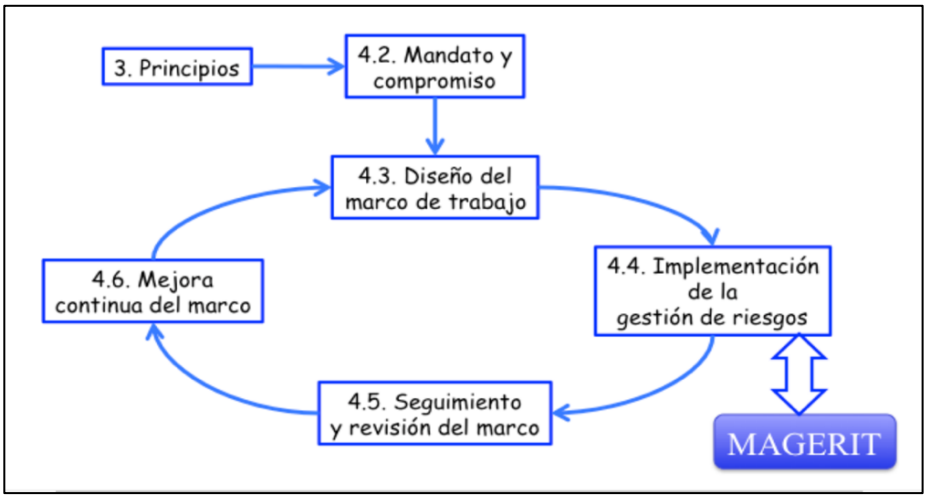
Magerit

La norma ISO 31000, Magerit incluye procesos para identificar riesgos dentro del marco para permitir que las agencias gubernamentales tomen decisiones que consideren los riesgos resultantes del uso de la tecnología de información (Miguel, 2012).

La herramienta MAGERIT se utiliza para implementar bajo las especificaciones del Centro Nacional de Inteligencia apoya la examinación de riesgo de información MAGERIT.

Figura 4

Proceso de implementación de metodología Magerit



Nota. En la imagen se demuestra el proceso de gestión de riesgos por parte de magerit. Tomado de (MAGERIT, 2012)

ISO/IEC

La Organización Internacional de Normalización ISO y la Comisión Electrotécnica Internacional IEC, son las responsables de un sistema de normalización especializado a nivel mundial que constituyen estándares para las gestiones de servicios de las tecnologías de la información (Bsi).

Estas dos instituciones desarrollan normas internacionales con la finalidad de realizar acuerdos en la actividad técnica. El autor (Navas, 2021)define las normas ISO como un conjunto de estándares que tienen la finalidad de contribuir a los procesos de gestión de las instituciones.

Norma ISO 31000

La norma ISO 31000 brinda orientación integral para el manejo de riesgos y proporciona orientación para las organizaciones, ya sean públicas, privadas o entidades comunitarias, para realizar análisis y evaluación de riesgos. Esta recomendación de mejores prácticas del estándar ayuda a mejorar las prácticas de administración y garantizar la seguridad del propia (Bsi).

ISO 27001

La norma ISO 27001:2013, es utilizada como un marco de referencia para los sistemas de seguridad de la información y tiene varios objetivos como el cumplimiento legal de la norma, además de asegurar la protección de la información y los activos más importantes de la institución (Guglieri, 1999). Es importante recalcar que se puede implementar en todo tipo de institución o empresa y se adapta al tamaño de esta.

Las Normas ISO permiten:

- Realizar un análisis y valoración de riesgos.
- Identificar amenazas para la institución.
- Medir las consecuencias que representan los riesgos para la institución.
- Implantar controles de seguridad.
- La elaboración de un plan que permita el tratamiento de riesgos.

ISO 9001

La normativa ISO 9001, según (Martínez, 2016) contribuyen a la adopción de un enfoque de procesos que es necesario cuando se planea la mejora e implementación de un sistema de gestión de calidad. Esta norma permite el uso de la metodología Planificar, Hacer, Verificar, Actuar (PHVA).

En el mercado actualmente existen muchos softwares que ayudan al procesamiento de los datos de seguridad.

Software AER (Entorno de Análisis de Riesgos) /Pilar

EAR/PILAR es un software que implementa y amplía la Metodología RA/RM de Magerit, diseñado para apoyar el proceso de gestión de riesgos en períodos prolongados. Las herramientas PILAR apoyan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit. Pilar García y Pilar Klarmann son personas con experiencia en diferentes campos, como la adquisición de talento y el conocimiento de la aviación, respectivamente, y no están directamente relacionadas con el software EAR/PILAR

EAR/PILAR apoya el proceso de gestión de riesgos proporcionando herramientas para el análisis y gestión de los sistemas de información siguiendo la metodología Magerit. El software evalúa los riesgos en varias dimensiones, incluida la confidencialidad, la integridad, la disponibilidad, la autenticidad y la responsabilidad.

La metodología Magerit estima la frecuencia con la que se materializan las amenazas y deduce el riesgo al que está expuesto el sistema. La degradación y la frecuencia califican la vulnerabilidad del sistema. El software también ayuda al administrador del sistema de información a implementar salvaguardas que reducen la frecuencia de ocurrencia o reducen o limitan el impacto de las amenazas. Dependiendo del grado de implementación de estas salvaguardas, el sistema pasa a una nueva estimación de riesgo, que se denomina riesgo residual. En general, EAR/PILAR proporciona un conjunto de herramientas especializadas en sistemas de información y comunicaciones y están diseñadas para apoyar el proceso de gestión de riesgos durante largos períodos.

Capítulo III

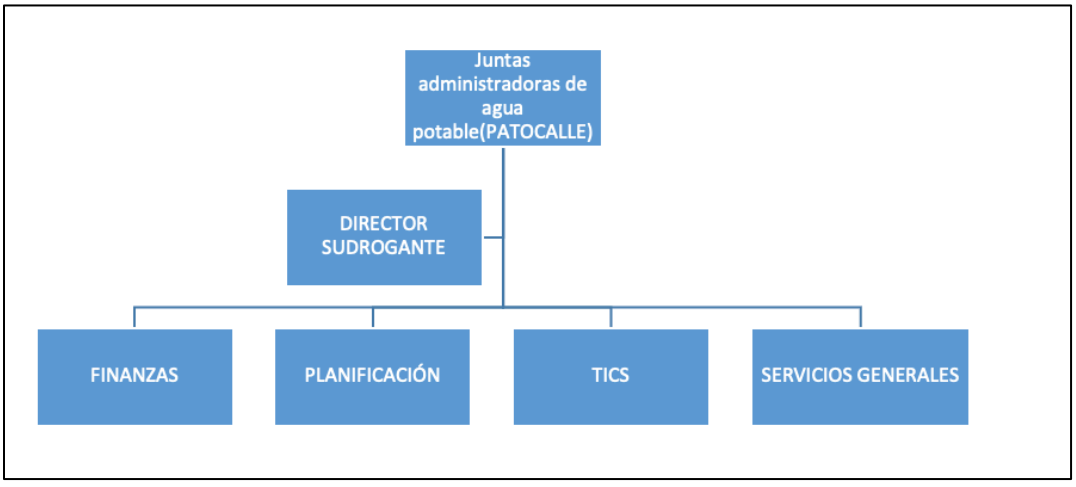
Desarrollo del tema

Antecedentes

La parroquia de Pastocalle cuenta con un organización de las comunidades para realizar una gestión del uso del agua, llamadas también juntas de agua y en específico vamos a hablar de la Junta de agua potable “Miño San Antonio” ,la misma que se encuentra bajo la dirección de agua potable y Alcantarillado (DIMAPAL),que está ubicada en provincia de Cotopaxi, cantón Latacunga, parroquia Pastocalle, la administración se encuentra a cargo del señor Segundo Gabriel Yánez Chiriboga, ente encargado de entregar el servicio de agua potable para la comunidad, y que hoy en día cuenta con 338 socios y su administración que se encuentra constituida de la siguiente forma:

Figura 5

Organigrama de la junta administradoras de agua



Nota. En la imagen se muestra la estructura de la administración de la junta de agua. Tomado de (Junta administradora de agua “Miño San Antonio”)

Situación inicial

Como se me mencionaba anteriormente en los anteriores hechos en la parroquia Pastocalle, para iniciar con nuestro proceso de evaluación del estado de integración de seguridad, pudimos constatar que su infraestructura tecnológica muchos de los equipos se encuentran documentados y algunos otros no, y que en su mayoría son equipamiento ofimático y de seguridad del inmueble, además que se puede evidenciar que debido a las ordenanzas administrativas del SRI la junta de agua cuenta con la implementación facturación electrónica, un software privado propio de la junta de agua(aplicativo web).

Debido al gran número de socios la administración está viendo la opción futura de la construcción de una nueva oficina administrativa para el bien de común de todos los asociados.

Después de la visita técnica a las instalaciones cada dejar claro que la institución carece de los siguientes puntos como:

- Correo institucional.
- Desconocimiento de las Normativas y lineamientos internacionales para la gestión de seguridad y control de riesgos informáticos.
- Programas sin licenciamiento.
- Aplicativo web que no cuenta con un respaldo bien implementado de toda la información anexada en el mismo.

Previamente al realizar el análisis la junta de agua proporciona un inventario de bienes donde constan activos de software, hardware, comunicaciones y mueblería tal y como se muestra a continuación:

Figura 6

Inventario de activos de información tipo software, hardware,comunicaciones y muebleria del JAMSA

Fecha de elaboración/validación: 5/01/2023

Nombre del Activo de Información	Descripción del activo de información	Tipología			Clasificación del activo de información						Localización del activo de información
					El activo es crítico para las operaciones internas			El activo es crítico para el servicio a terceros			
		Software	Hardware	Servicios	Bajo	Medio	Alto	Bajo	Medio	Alto	
Aplicativo wed (Junta)	Sofware de facturación electronica privado	X					X			X	Servidor Web y Ordenador
SAT Empresarial	Es el software por el cual se gestionan de documentación	X			X					X	Servidor Web y Ordenador
ROUTER TP-LINK/AC 1200	El equipo ideal para la conectividad de red y conectividad a doble banda 2.4 G Y 5G.		X				X			X	Oficina
COMPIESCRITORIO/HP	PC de escritorio con componentes basicos		X				X			X	Oficina
FAX	utiliza una línea telefónica para enviar originales escaneados (papel) o recibir datos enviados desde máquinas remotas.		X			X				X	Oficina
PORTATIL HP	Ordenador de oficina		X				X			X	Oficina
IMPRESORA HP/WF-2850	impresión de documentos por via de cable		X			X				X	Oficina
ROUTER TP-LINK/AC 1600	El equipo ideal para la conectividad de red y conectividad a doble banda 2.4 G.		X				X			X	Oficina
TELEFONO ANALOGO	Un teléfono analogode alta gama potentes funciones		X				X			X	Oficina
CAMARAS DE VIDEO VIGILANCIA	Equipos de video vigilancia po wifi a aplicativo movil		X				X			X	Oficinas

Nota. Inventario de activos y bienes del JAMS, Tomado de (Junta administradora de agua “Miño San Antonio”).

Figura 7

Número de bienes utilizados en el JAMSA

Fecha de elaboración/ validación: 05 de enero de 2023

Nombre del Activo de Información	Descripción del activo de información	Tipología			Clasificación del activo de información						Estado y custodia del activo de información	
					El activo es crítico para las operaciones internas			El activo es crítico para el servicio a terceros			Custodio del Activo del información	Localización del activo de información
		Software	Hardware	Servicios	Bajo	Medio	Alto	Bajo	Medio	Alto		
2 Computadores de escritorio	Equipos de cómputo utilizados para la gestión del dia a dia en la entidad y donde se realiza todo el ingreso de información que se genera en las juntas		X				X			X	Técnico operativo de la Oficina Asesora de Planeación	Puestos de trabajo en la junta
1 Computadores portátiles	Equipos de cómputo utilizados para la gestión del dia a dia en la entidad y donde se realiza todo el ingreso de información que se genera en		X				X			X	Funcionarios y contratistas de planta	Puestos de trabajo en las juntas y/o en custudia en Sistemas para préstamos de los
1 Impresoras	Equipos de contingencia para la salida física de la documentación generada en las juntas		X			X			X		Técnico operativo de la Oficina Asesora de Planeación	Algunos puestos de trabajo en la junta
3 camaras	Equipos de video vigilancia		X				X			X	Técnico operativo de la Oficina Asesora de Planeación	Técnico operativo de la Oficina Asesora de Planeación
1Switches	Equipos de comunicación alámbrico de la red LAN de las juntas.		X				X		X		Técnico operativo de la Oficina Asesora de Planeación	Cuarto de Servidores y comunicaciones
2 Routers inalámbricos	Equipos de comunicación inalámbrico hacia la red LAN de las juntas.		X				X			X	Técnico operativo de la Oficina Asesora de Planeación	Repartidos el las diferentes oficinas de la junta
1 Firewall físico	Equipo usado para la seguridad perimetral de datos de las juntas		X			X			X		Técnico operativo de la Oficina Asesora de Planeación	Cuarto de Servidores y comunicaciones
2 discos duros de 2Tb c/u	Equipos de almacenamiento masivo donde se realiza el Backup de todos los datos generados en las juntas.		X			X		X			Técnico operativo de la Oficina Asesora de Planeación	Cuarto de Servidores y comunicaciones

Nota. En la imagen se muestra el número de activos en la infraestructura tecnológica del JAMSA. Tomado de (Junta administradora de agua “Miño San Antonio”).

Activos

Dentro de las Junta administradora de agua su infraestructura tecnológica se encuentra documentada ya que cada cierto tiempo se realiza un mantenimiento preventivo y renovación de los mismos en caso de ser necesarios para nuestro caso de estudio se destinará los siguientes activos:

Tabla 1

Activos de Software del JAMSA

SOFWARE	
Cantidad	**Descripción**
4	Programas de ofimática (PAQUETE OFFICE)
2	Programas de contabilidad (FACTURACIÓN)
3	Sistemas Operativos (WINDOWS)

Nota. La tabla muestra el equipamiento activos software.

Tabla 2

Activos de Hardware del JAMSA

HADWARE	
Cantidad	**Descripción**
1	Telefonía Análoga
2	Computadores de escritorio
	Impresoras (CABLE)
2	Laptops
	Switch
1	Router
1	Kit de cámaras de seguridad (3CAMARAS)

Nota. La tabla muestra el equipamiento activos hardware.

Tabla 3

Equipamiento de Comunicaciones

COMUNICACIONES	
Cantidad	**Descripción**
10m	Cableado UTP cap 5
1	swich
2	Telefonía Análoga
1	Fax

Nota. La tabla muestra el equipamiento activo de comunicaciones.

Infraestructura

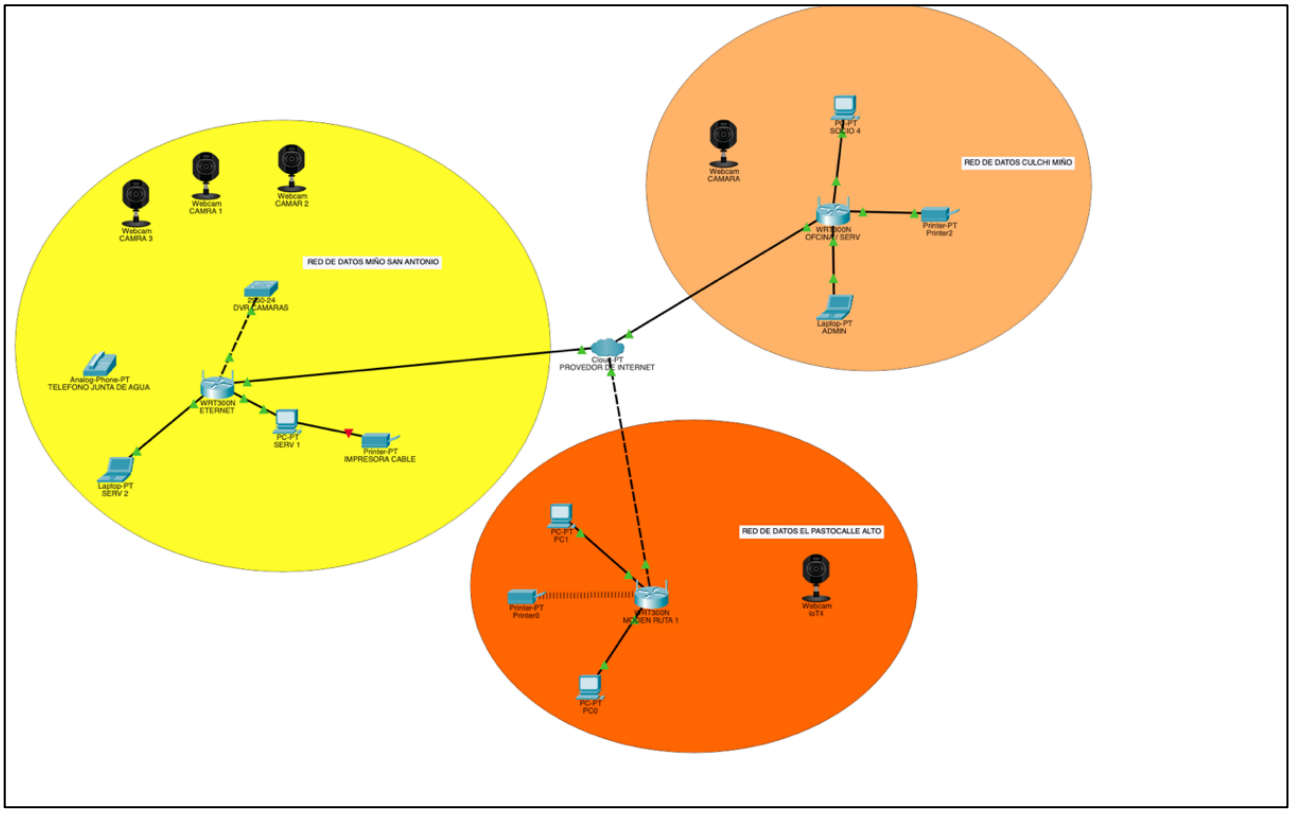
Con el paso de los tiempos muchas entidades tanto públicas y privadas renuevan su equipamiento porque las nuevas funcionalidades que les podría aportar a su crecimiento para optimizar su trabajo en las actividades diarias, así como muchas que no las hacen debido al incremento de costo de las mismas que los hacen siempre mantener el mismo equipamiento hasta que su uso ya no sea el ideal para desempeñar las funciones.

También cabe mencionar que se pudo realizar una visita a las juntas aledañas donde puedo evidenciar equipamiento que podría también ser candidato para aplicar el presente proyecto.

Con este breve despliegue de la visualización de los activos encontrados en el lugar, JAMSA como se le denomina para el presente proyecto la junta administradora de agua potable “Miño San Antonio”, se puedo determinar que posee la infraestructura de continuación:

Figura 8

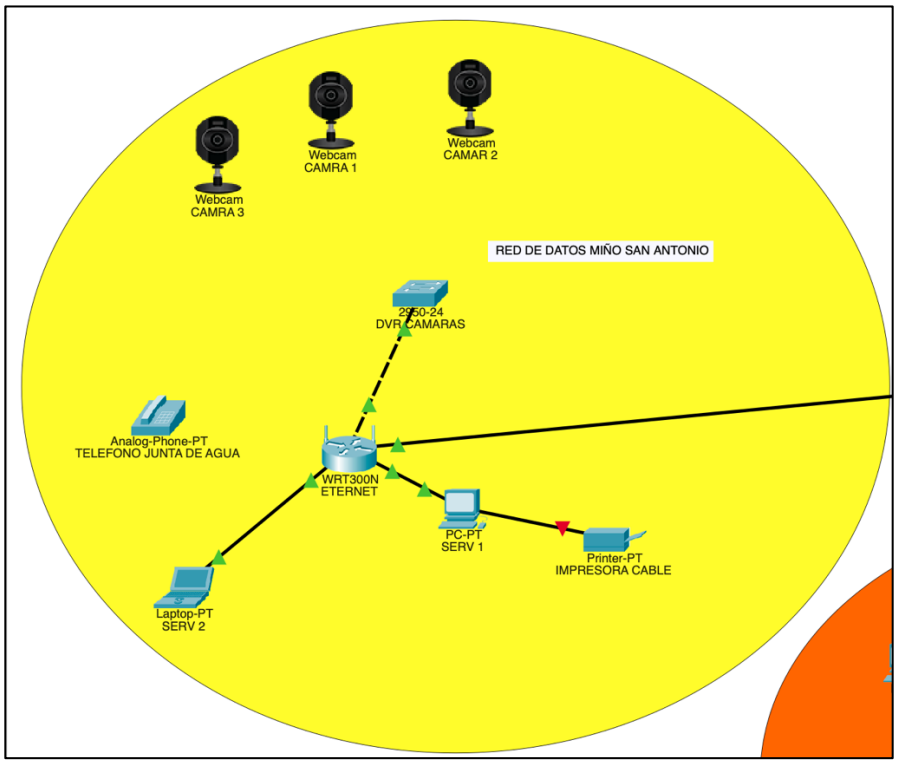
Bosquejo de toda la red de las juntas de agua" Pastocalle"



Nota. La imagen se evidencia los activos de las juntas aledañas de las juntas de agua Pastocalle.

Figura 9

Bosquejo de la red de la junta de agua" Miño San Antonio"



Nota. La ilustración se evidencia los activos del JAMSA.

Proceso gestión de riegos (ISO 27001 Y 31000_Magerit_Pilar)

Bajo nuestra visualización de nuestros sistemas informáticos para el análisis, gestión y tratamiento de los riegos tomaremos como pilar la ISO 27001 la misma que bajo su acreditación de servicios que nos ofrece, esta aliada con la base metodológica MAGERIT, la misma que se apoya con la herramienta PILAR, permitiendo un trabajo eficiente y eficaz. Para llevar a cabo este análisis, se han establecido tres etapas:

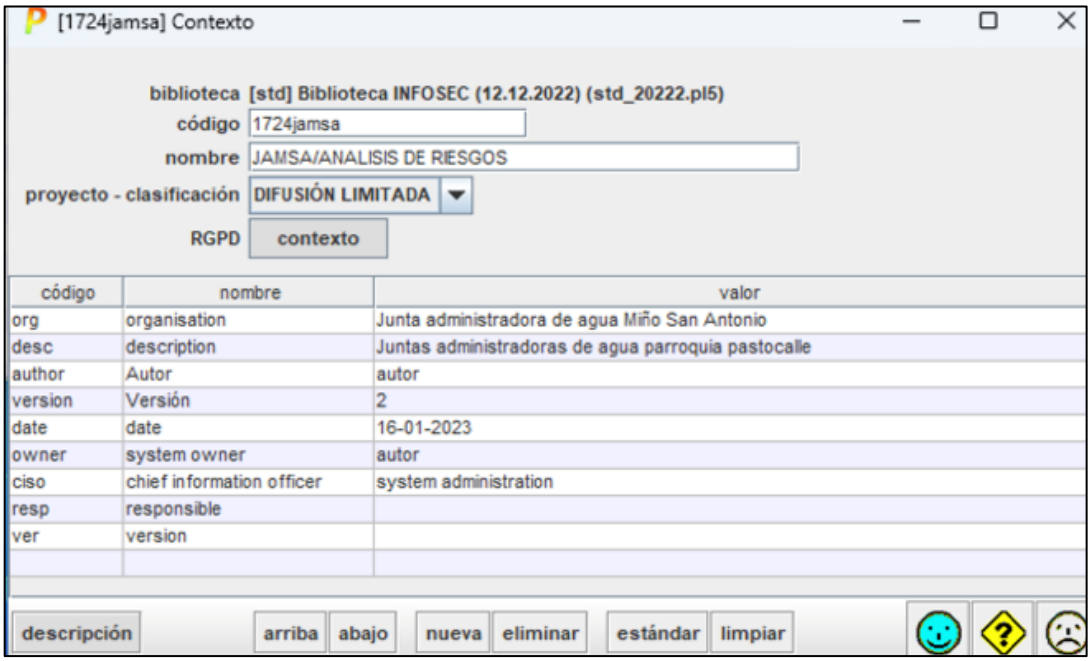
- Identificación de los activos más importantes de JAMSA.

- Determinación de las amenazas a los activos.
- Evaluación del impacto de las amenazas y evaluación del riesgo en función a valores determinados por el software.

El software presenta varias versiones (BASIC, RM, BCM, RMAT), mismo que están bajo una licencia de evolución, para llevar a cabo este proyecto, ayudándonos a generar los informes de análisis de riegos de nuestros activos para lo cual se inicia creado un proyecto con los datos proporcionados por la junta de agua tal y como se muestra a continuación:

Figura 10

Interfaz principal PILAR(Inicio de analisis)



Nota. La ilustración evidencia la parte de inicio del análisis en PILAR.

Los activos se ingresan en la herramienta PILAR para su posterior análisis, y todos ellos se encuentran en el mismo dominio de seguridad por defecto, por lo que los requisitos de seguridad son los más altos en cada dimensión de seguridad.

Tabla 4

Ingreso de activos

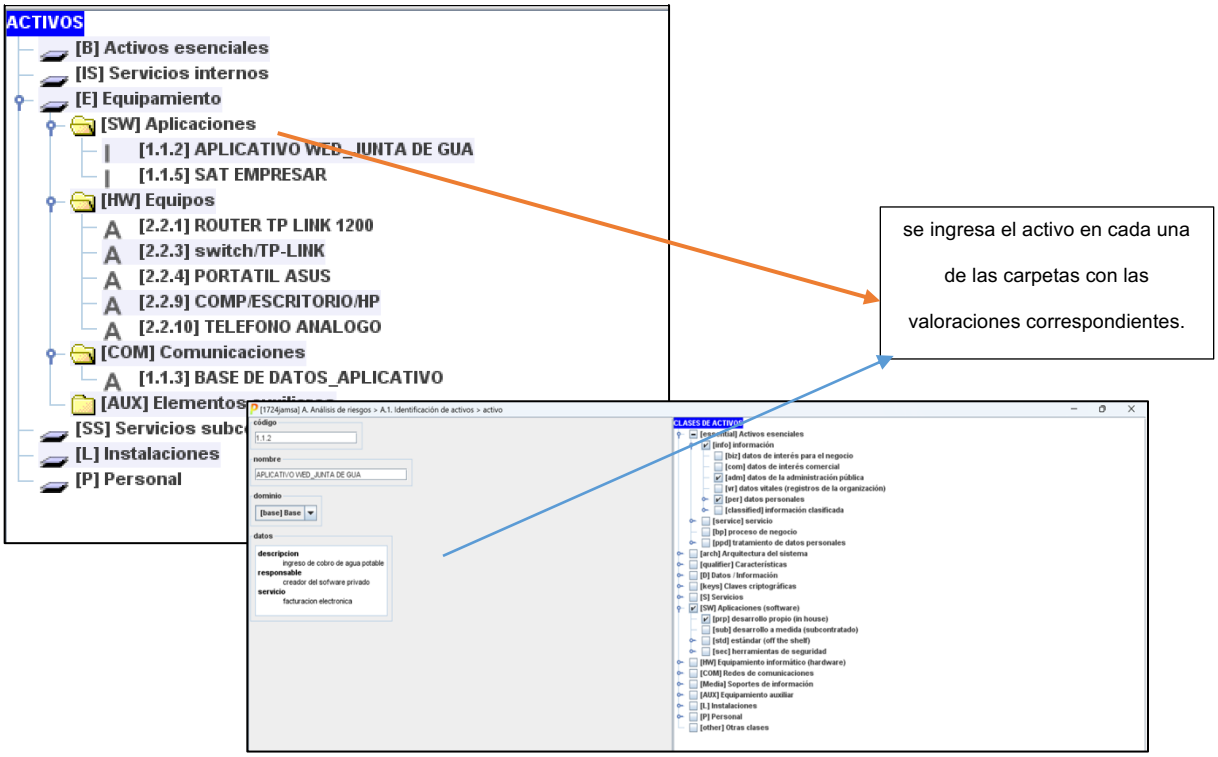
Activos	Tipo	Detalle	Cantidad
Software	Aplicativo web	Facturación	
	Switch		3
	Modem	Comunicaciones	
	Telefonía		
Hardware	Análoga	1PC de	
	Impresoras	administración	2 PCs de
	Estaciones		trabajo
	de trabajo		
	Oficina		
Infraestructura		Matriz	1
Datos	Respaldos	Documentos y	----------
	BDD	registros	-----

Nota. La tabla muestra el equipamiento del JAMSA.

Los recuadros de pilar determinan que se ingrese valores como su operatividad, tipo de activo, actividad que realiza, y versión del mismo para el ingreso de cada uno de ellos, misma información que se puede encontrar en manuales de marca de los equipos o su vez con su operatividad con el acercamiento a la comunidad y conocimiento de cada uno de los activos.

Figura 11

Ingreso de activos en PILAR



Nota. En la imagen se evidencia la interfaz de PILAR para el ingreso de los activos.

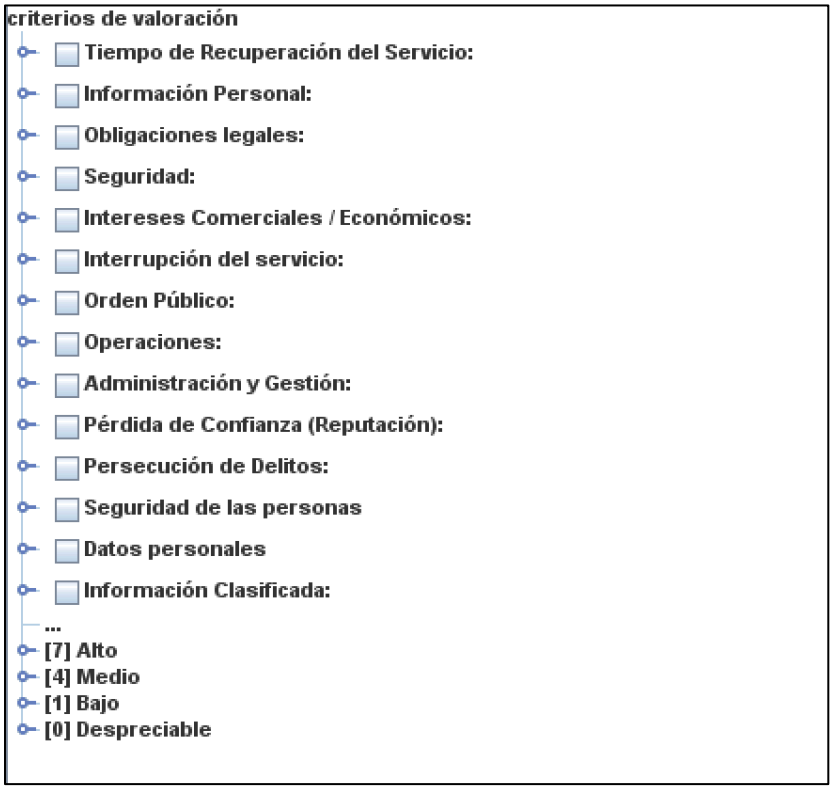
Dominios de Seguridad

El JAMSA al ser una institución que se maneja de manera autónoma, tiende a regirse a diversos cambios continuos debido a sus representantes, por que basado en el uso de la norma ISO 9001 se utiliza un nivel de seguridad 3 a 8 para los activos que el programa determina puntos altos para asignar dominios de seguridad de manera manual.

Pilar cuenta con una infinidad de valoraciones que se les puede dar a los activos dependiendo del campo o tipo de entidad a la que se vaya a realizar el análisis de riegos, tal y como se puede evidenciar en la siguiente ilustración.

Figura 12

Dominios de seguridad para los activos informáticos



Nota. La imagen se observa las valoraciones de seguridad aplicados a los activos del JAMSA, Tomado del Software PILAR(EAR).

Diagnóstico de Amenazas

A continuación, detallamos en la siguiente imagen, los criterios de evaluación de amenazas, que el software usara.

Figura 13

Valoración de amenazas

Nota. La imagen evidencia las valoraciones que esta determinados por el software PILAR, Tomado del Software PILAR(EAR).

Identificación de Amenazas

A continuación, se describirán las potenciales amenazas que podrían tener impacto en el JAMSA:

Eventos naturales como incendios, inundaciones, terremotos y erupción volcánica.

Mal funciones en componentes de hardware y software.

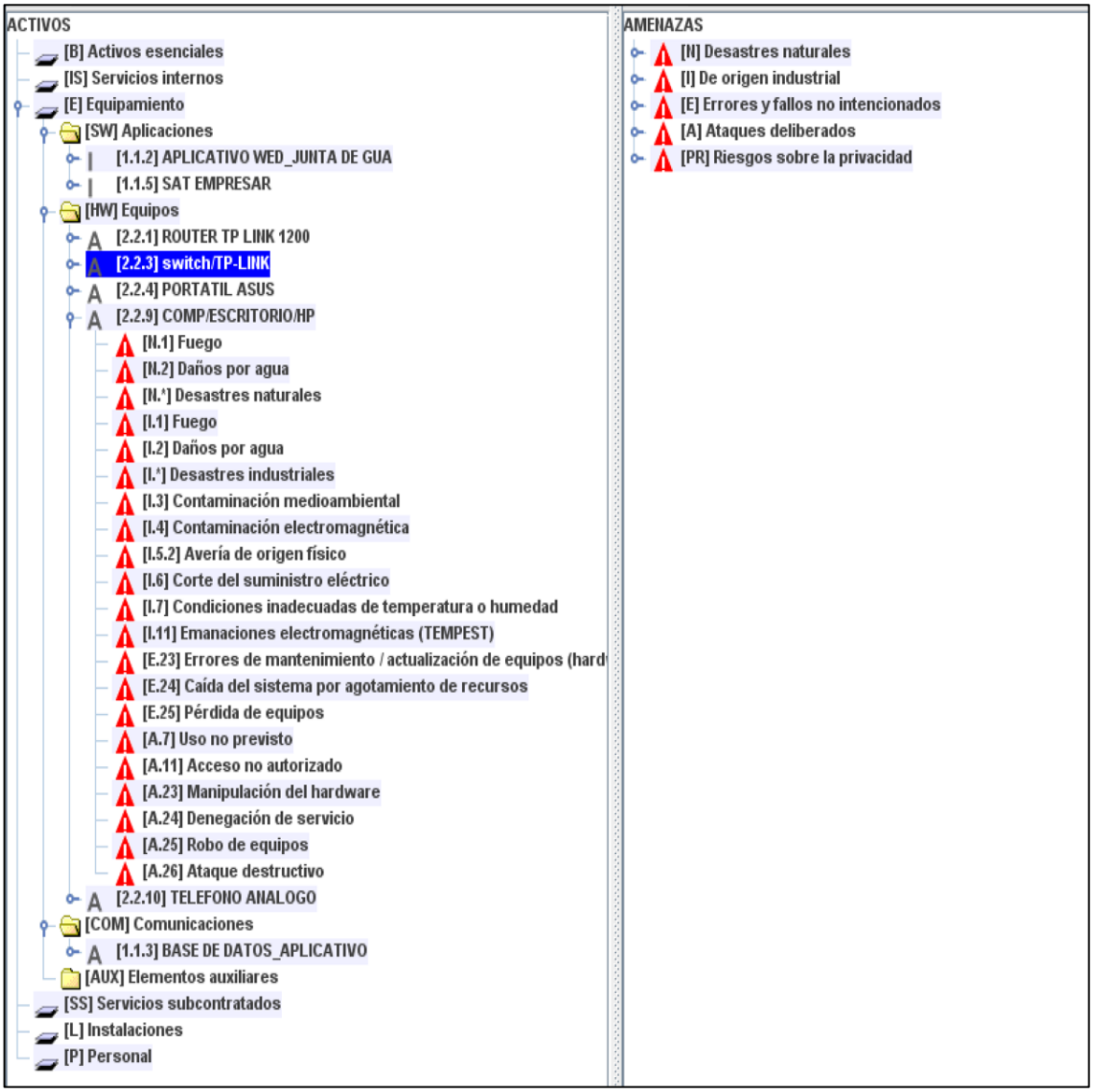
Acceso a la información por parte de individuos no autorizados.

Corte de servicios internet/energía eléctrica

El software asigna de manera automática las amenazas que podría sufrir el sistema informático tal y como se muestra a continuación:

Figura 14

Amenazas agregadas por el programa por defecto



Nota. La imagen evidencia las valoraciones que están determinados por el software PILAR en relación con las amenazas.

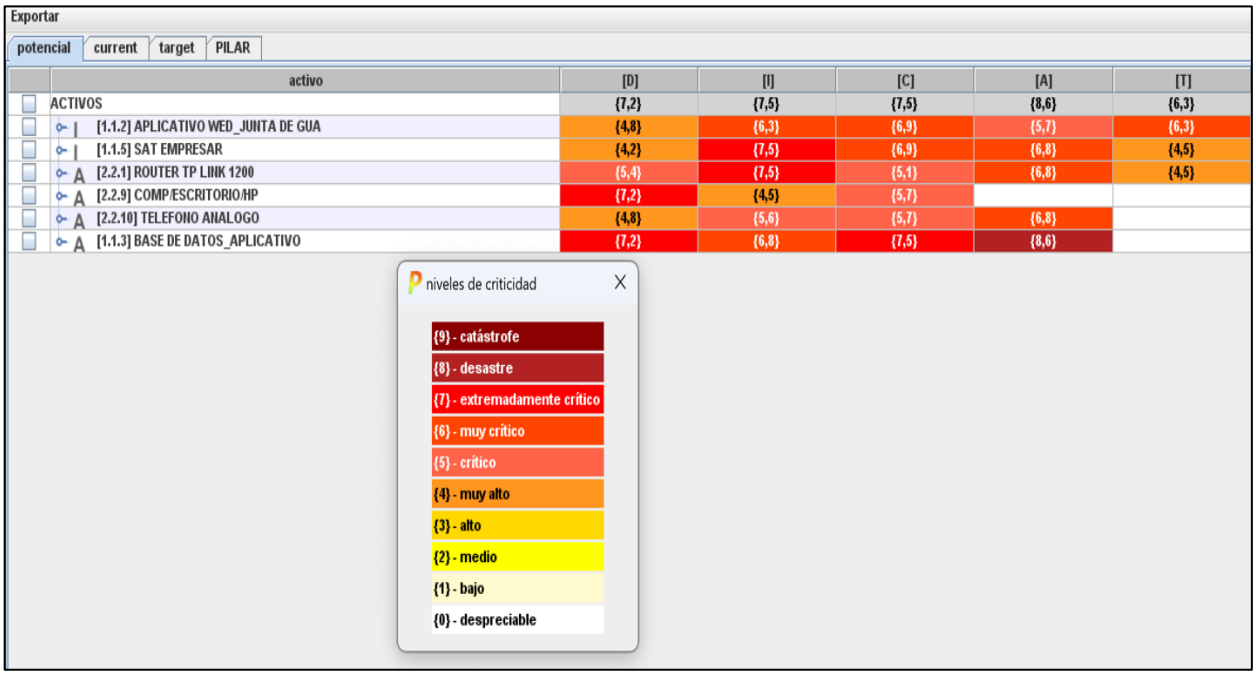
Resultados

Análisis de riesgos

Los activos encontrados y asignados al software arrojaron los sientes resultados de comprobación de afectación de riegos.

Figura 15

Resultado de activos en riesgos



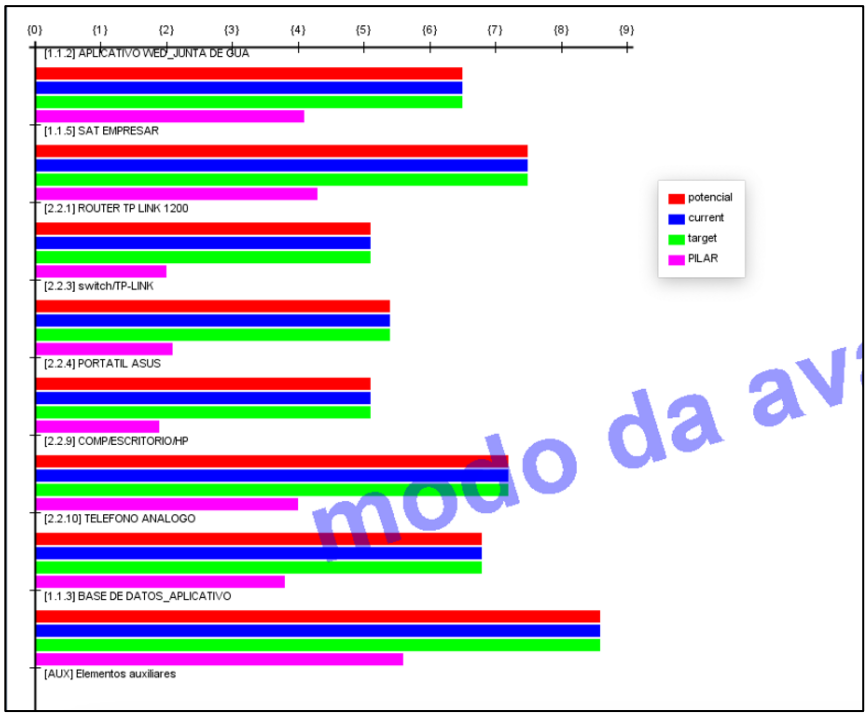
Nota. La imagen evidencia las valoraciones que están determinados por el software PILAR en relación con la amenaza por activo.

Identificación de Vulnerabilidades

El software PILAR luego de realizar el ingreso de la valoración para cada uno de los activos realiza un análisis automáticamente basado en las amenazas que incluyen el paquete del programa, para este proyecto se utiliza dos versiones (BASIC, INK) del software, para luego arrojarnos los siguientes resultados:

Figura 16

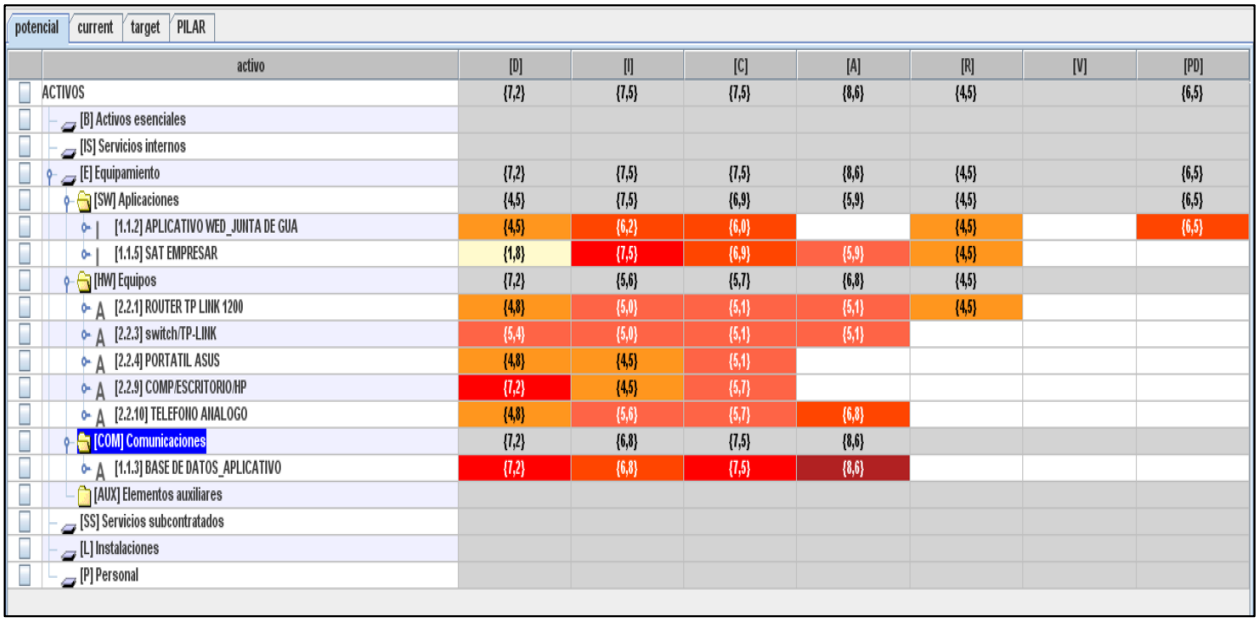
Riegos acumulado, evaluados por PILAR



Nota. La ilustración se puede evidenciar los resultados del análisis del riego para los activos JAMSA.

Figura 17

Estado de afectación de riegos por activo



potencial | current | target | PILAR

activo	[D]	[I]	[C]	[A]	[R]	[V]	[PD]
ACTIVOS	{7,2}	{7,5}	{7,5}	{8,6}	{4,5}		{6,5}
[B] Activos esenciales							
[IS] Servicios internos							
[E] Equipamiento	{7,2}	{7,5}	{7,5}	{8,6}	{4,5}		{6,5}
[SW] Aplicaciones	{4,5}	{7,5}	{6,9}	{5,9}	{4,5}		{6,5}
[1.1.2] APLICATIVO WED_JUNTA DE GUA	{4,5}	{6,2}	{6,0}		{4,5}		{6,5}
[1.1.5] SAT EMPRESAR	{1,8}	{7,5}	{6,9}	{5,9}	{4,5}		
[HW] Equipos	{7,2}	{5,6}	{5,7}	{6,8}	{4,5}		
[2.2.1] ROUTER TP LINK 1200	{4,8}	{5,0}	{5,1}	{5,1}	{4,5}		
[2.2.3] switch/TP-LINK	{5,4}	{5,0}	{5,1}	{5,1}			
[2.2.4] PORTATIL ASUS	{4,8}	{4,5}	{5,1}				
[2.2.9] COMP/ESCRITORIO HP	{7,2}	{4,5}	{5,7}				
[2.2.10] TELEFONO ANALOGO	{4,8}	{5,6}	{5,7}	{6,8}			
[COM] Comunicaciones	{7,2}	{6,8}	{7,5}	{8,6}			
[1.1.3] BASE DE DATOS_APLICATIVO	{7,2}	{6,8}	{7,5}	{8,6}			
[AUX] Elementos auxiliares							
[SS] Servicios subcontratados							
[L] Instalaciones							
[P] Personal							

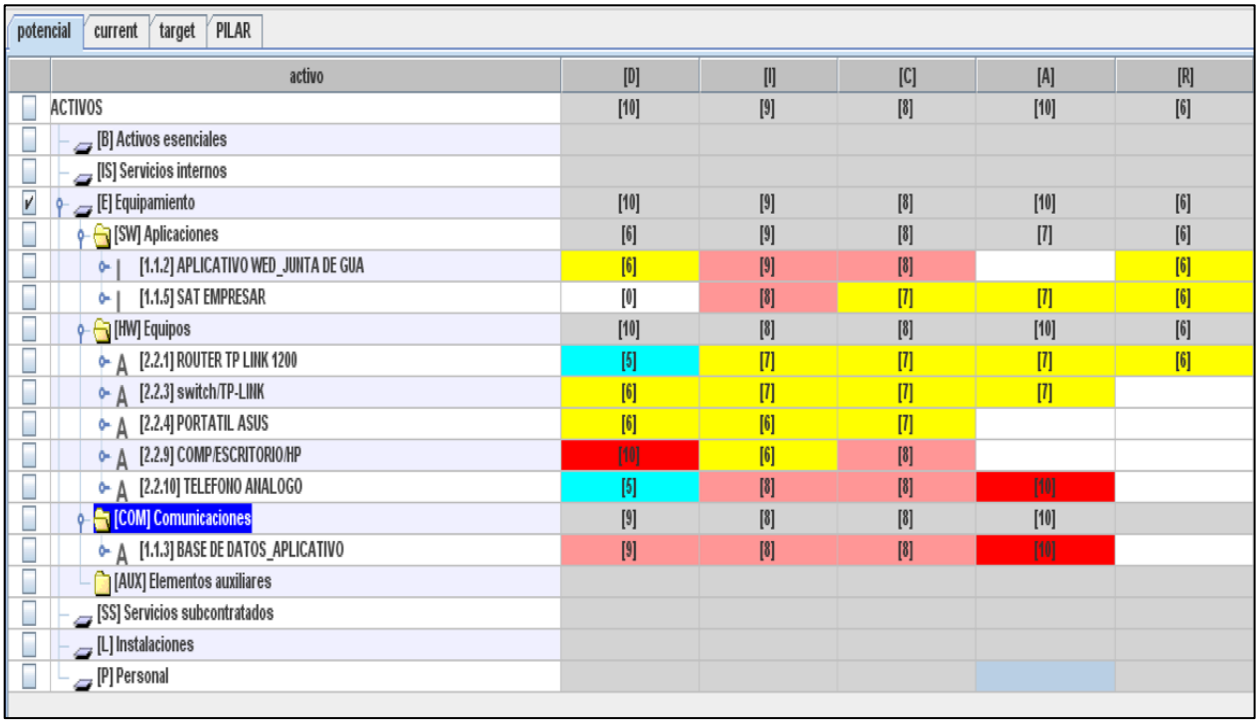
Nota. La ilustración se puede evidenciar los resultados del análisis del riesgo para cada uno de los activos del JAMSA.

Impacto de Riesgos

Cada uno de los activos son evaluados con sus colores respectivos y su impacto para cada amenaza, siendo los activos de software los de mayor vulnerabilidad para el sistema informático del JAMSA.

Figura 18

Valoración de impacto de los riegos de los activos de JAMSA



potencial | current | target | PILAR

activo	[D]	[I]	[C]	[A]	[R]
ACTIVOS	[10]	[9]	[8]	[10]	[6]
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento	[10]	[9]	[8]	[10]	[6]
[SW] Aplicaciones	[6]	[9]	[8]	[7]	[6]
[1.1.2] APLICATIVO WED_JUNTA DE GUA	[6]	[9]	[8]		[6]
[1.1.5] SAT EMPRESAR	[0]	[8]	[7]	[7]	[6]
[HW] Equipos	[10]	[8]	[8]	[10]	[6]
[2.2.1] ROUTER TP LINK 1200	[5]	[7]	[7]	[7]	[6]
[2.2.3] switch/TP-LINK	[6]	[7]	[7]	[7]	
[2.2.4] PORTATIL ASUS	[6]	[6]	[7]		
[2.2.9] COMP/ESCRITORIO/HP	[10]	[6]	[8]		
[2.2.10] TELEFONO ANALOGO	[5]	[8]	[8]	[10]	
[COM] Comunicaciones	[9]	[8]	[8]	[10]	
[1.1.3] BASE DE DATOS_APLICATIVO	[9]	[8]	[8]	[10]	
[AUX] Elementos auxiliares					
[SS] Servicios subcontratados					
[L] Instalaciones					
[P] Personal					

Nota. La imagen muestra el impacto de los riegos, para los activos del JAMSA.

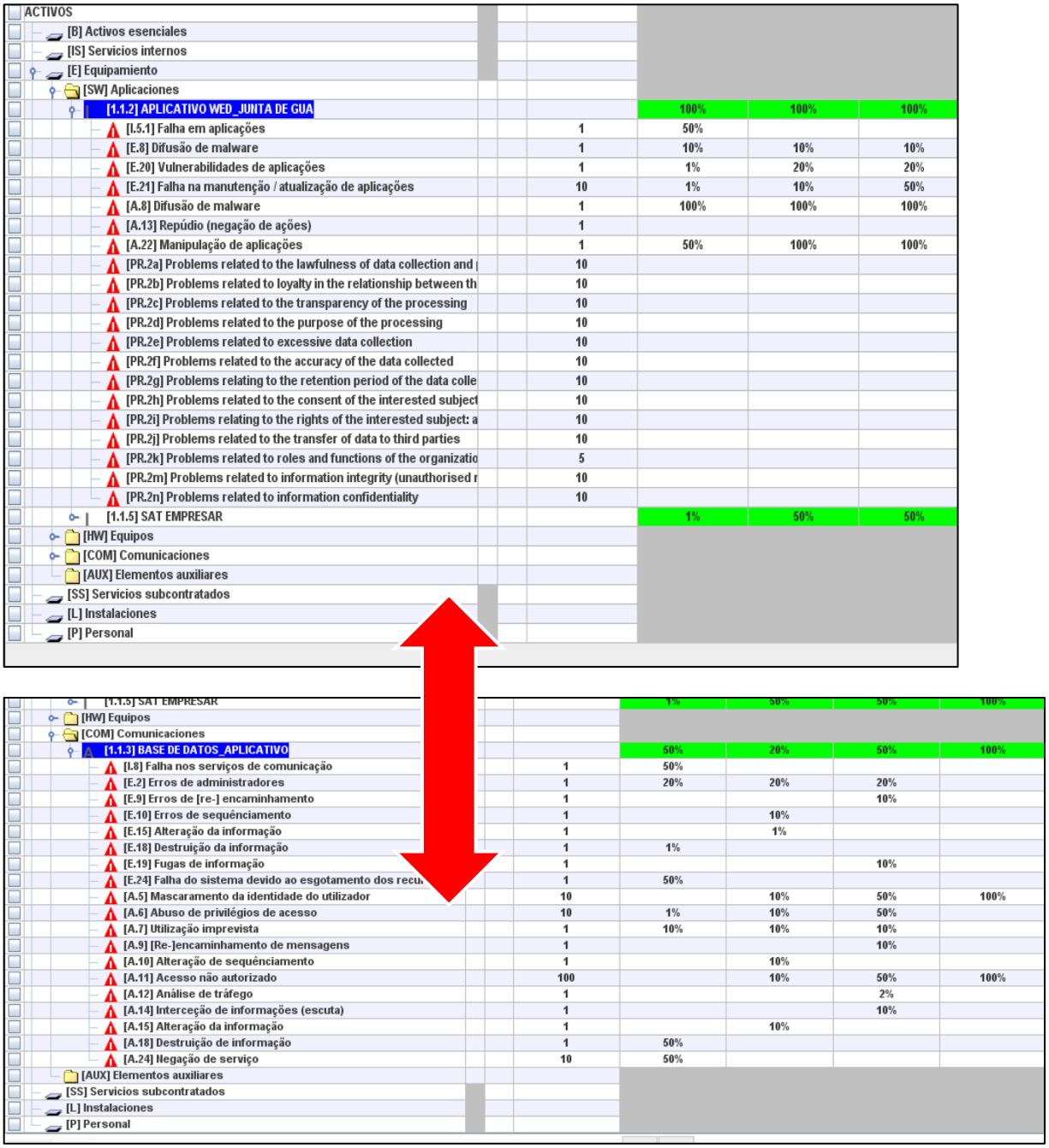
Tratamiento de riesgos de la Información

La valoración de riesgos implica contrastar el nivel de riesgo identificado durante el procedimiento de análisis con los estándares de riesgo predefinidos.

Reconocer las prácticas de gestión, sistemas técnicos y procedimientos ya establecidos para el control de riesgos (Plan de contingencia), y analizar sus puntos fuertes y debilidades de los eventos que se podrían presentarse, tal como se puede evidenciar a continuación:

Figura 19

Valoración de vulnerabilidad por eventos



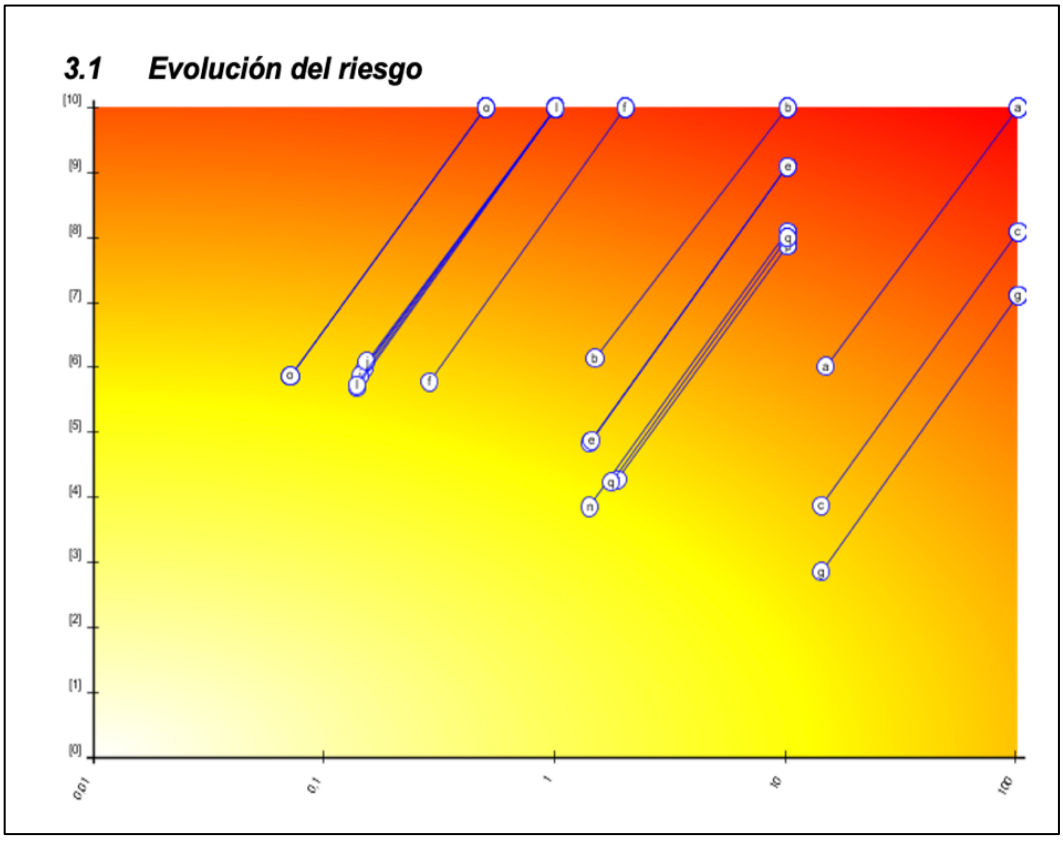
Nota. La imagen muestra la valoración por evento en cada uno de los activos del JAMSA.

El plan de contingencia ya operativo, cumple con los objetivos dispuestos a este proyecto y se realiza la entrega del mismo al vicepresidente de la Junta de agua, quien remite una carta de constancia de elaboración y aplicación de esta propuesta.

Se adjunta las diferentes pruebas fotográficas, así como el informe del software, además cada señalar que el análisis de los activos arrojo los siguientes resultados, que podrían usarse para mejoras futuras en el sistema informático, basándose en que el riesgo esta determinado directamente por el impacto de una amenaza al activarse la contingencia.

Figura 20

Resulatdo final de la evolución del riegos



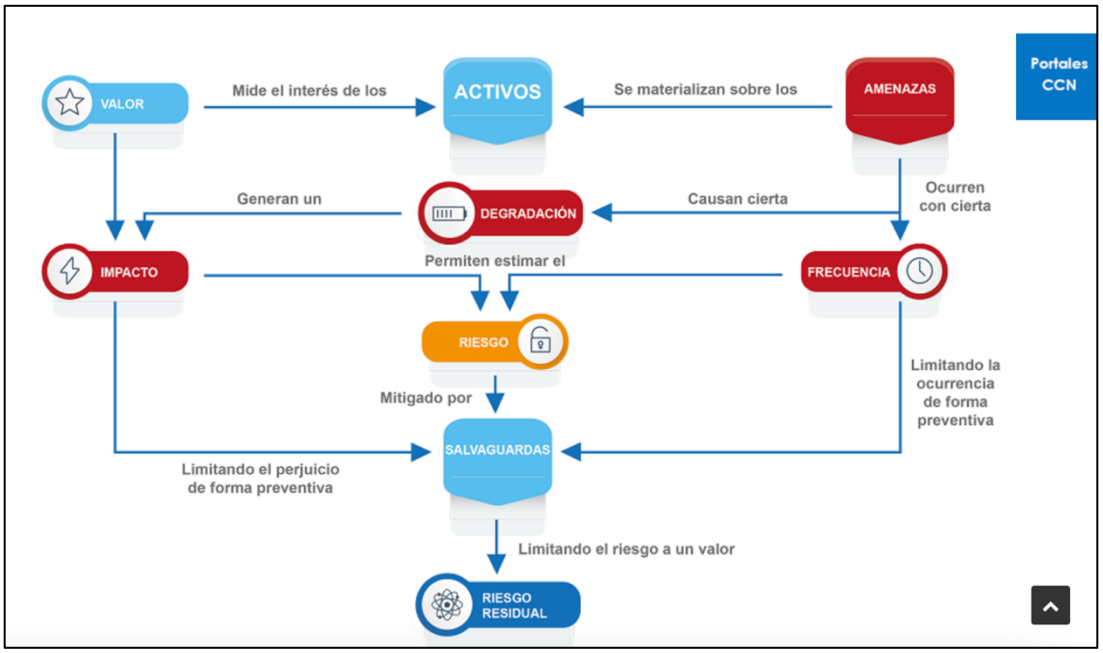
Nota. La imagen muestra el avance de riesgo con relación a los activos y las amenazas posibles.

Los riesgos presentan una alta probabilidad y podrían tener un impacto significativo. En este caso, la recomendación es abordarlos de inmediato para eliminarlos de esta categoría.

El software Pilar (AER), cumple el siguiente proceso para el procesamiento del análisis de riegos:

Figura 21

Procesos de ejecución del PILAR



Nota. La imagen muestra el proceso que realiza Pilar mediante Magerit para su ejecución de análisis de riegos, Tomado del (Centro Criptológico Nacional, 2023).

Capítulo IV

Plan de contingencia para la Junta de Agua

“Miño san Antonio”

1922
ECUADOR
ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

REDES Y
TELECOMUNICACIONES

Introducción

El plan de contingencia creado para la Junta de Agua “Miño San Antonio”, es una propuesta que podrá ser ejecutado por cualquier ente admirativo o a su vez por los miembros de la comunidad con conocimientos básicos en ofimático, claramente con la supervisión de los dirigentes.

La siguiente propuesta estará disponible para el JAMSA siempre que el personal lo necesite y también es preciso mencionar que podría ser aplicado a las juntas vecinas.

El plan de contingencia mitiga tres escenarios posibles el antes de suputarse el evento, al momento del suceso la planificación futura.

Objetivo

Mitigar los eventos que amenazan con interrumpir el servicio que brindan los bienes tecnológicos, y con la continuidad de las actividades cotidianas de todos los socios del JAMSA.

Alcance

El plan de contingencia esta creado para suplir las necesidades del JAMSA, para su sistema tecnológico con la información brindada por la entidad y los datos procesados en PILAR(EAR).

Metodología

Para la elaboración del Plan de Contingencia, nos sustentaremos en las normas y la metodología con la que trabaja el software elegido para este proyecto:

- ISO/IEC 27001:2013.
- ISO/IEC 31000:
- MAGERIT

Teniendo en cuenta que los servicios no solo deben estar funcionales, si no determinar una calidad de los mismo nos respaldamos en la norma:

- ISO/IEC 9001.

Desarrollo de procesos

Contingentes:

- Eventos naturales como incendios, inundaciones, terremotos y erupción volcánica.
- Mal funciones en componentes de hardware y software.
- Acceso a la información por parte de individuos no autorizados.
- Corte de servicios internet/energía eléctrica

Objetivo:

Determinar los pasos que se deben seguir cuando se den lugar las amenazas, en contra del sistema informático, los procesos a realizar antes del suceso (Respaldo), durante el mismo y después (Plan de contingencia), con fin de poder restablecer el servicio en el menor tiempo posible.

Alcance:

El plan de contingencia se enfocará a mitigar los eventos que podrían provocar pérdidas totales de toda la infraestructura tecnológica y afectación a los miembros de la Junta.

Dentro del plan se incluirá el tratamiento que se deberá realizar a los datos para su resguardo y recuperación, en caso de ser necesario al desarrollo del evento y después del mismo. A continuación, se presenta el plan de contingencia que contara con los procesos:

- Plan preventivo
- Plan en emergencia
- Plan restauración

Tabla 5

Plan de contingencia para desastres naturales

<table>
<tr><td>Plan # 01

Versión 1.0</td><td>Contingencia:
Eventos naturales como incendios, inundaciones, terremotos y erupción volcánica.</td><td>  </td></tr>
<tr><td>Páginas:5</td><td></td><td>Fecha: DD/MM/AA</td></tr>
<tr><td colspan="3">1.Plan de preventivo</td></tr>
<tr><td colspan="3">1.1 Eventualidad

Un incendio es una forma de desastre originada por un fuego no regulado, capaz de causar perjuicios tanto en términos de estructuras como de impactos físicos.

Las inundaciones, clasificadas como fenómenos naturales, presentan una amenaza continua en prácticamente cualquier área donde se registren precipitaciones, aunque cabe señalar que la lluvia no es la única causa desencadenante de este suceso. En su mayoría, las inundaciones tienen lugar en un período de horas o días, lo que brinda la oportunidad de evacuar áreas propensas a sufrir afectaciones.

Definimos sismos como los movimientos vibratorios, veloces y contundentes de la superficie terrestre, también conocidos como temblores o terremotos. Estos eventos se originan debido a perturbaciones en el interior de la Tierra, en particular, por el choque entre placas tectónicas. La distinción entre temblores y terremotos radica en la magnitud del movimiento sísmico, siendo este último el más peligroso debido a su capacidad destructiva, que puede tener consecuencias fatales.</td></tr>
</table>

Las **erupciones volcánicas** representan algunos de los fenómenos naturales más impactantes de nuestro mundo y una asombrosa manifestación del poder de la Tierra. Una erupción volcánica es un evento geológico que ocurre cuando el magma y otros componentes alojados en el interior de un volcán emergen hacia la superficie terrestre.

Son incidentes de naturaleza y no están sujetos a control humano. Los recursos susceptibles de ser impactados durante esta situación son:

- Documentos
- Equipos informáticos
- Bienes pertenecientes al JAMSA.
- Personal que forma parte de la comunidad.

1.2 Objetivo

Reestablecer de manera efectiva el funcionamiento en el menor lapso viable y proseguir con las operaciones cotidianas de la Junta y la comunidad.

1.3 Entorno

Este evento, afectara a toda la oficina del JAMSA

1.4 Encargados

Los principales representes de la Junta y la persona externa encargada y creador del software de operación en la Junta de agua “Miño San Antonio”, aseguraran que se de cumplimiento de todas las medidas preventivas establecidas en el plan de contingencia, respaldadas por la comunidad.

1.5 Actividades de Mitigación

- Elaborar un plan de evacuación que será compartido con todos los dirigentes y la comunidad.
- Colocar señalizaciones indicativas de las vías de evacuación dentro de las instalaciones de la facultad.
- Realizar simulacros de evacuación semestrales con la participación de todo el personal de la institución.
- Marcar las rutas seguras con señalizaciones claras.
- Establecer puntos de encuentro seguros para el personal.
- Mantener un registro actualizado del personal del JAMSA.
- Realizar inspecciones anuales o mensuales de la infraestructura.

2.Plan en Emergencia

2.1 Activación del plan

El plan se inicializa cuando el evento se de por terminado, según el desastre natural y que la comunidad ya se encuentre fuera de peligro.

2.2 Actividades para la contingencia

Durante la evacuación, se llevará a cabo conforme a lo delineado en los simulacros, con individuos designados para dirigir a todo el personal hacia áreas seguras, siguiendo las indicaciones proporcionadas por la señalización dispuesta en la institución.

- Además, el personal se debe encontrar fuera de peligro.

2.3 Proceso de mitigación

Una vez confirmada la finalización de la contingencia y confirmada la evacuación del lugar, se procederá a evaluar los daños y determinar su nivel de gravedad.

Se tomarán las siguientes medidas:

Las actividades del JAMSA se suspenderán por el tiempo que los dirigentes crean conveniente.

Esto se hará considerando la posibilidad de volver a experimentar otro o le mismo desastre natural y daños adicionales en la infraestructura.

Se realizará una revisión detallada de las instalaciones, incluyendo conexiones eléctricas y equipos.

Se procederá a evaluar y documentar los daños ocasionados, y si es requerido, se creará un inventario de los mismos.

3.Plan restauración

3.1 Personal responsable

Los principales representes de la Junta y la persona externa encargada y creador del software de operación en la Junta de agua" Miño San Antonio", aseguraran que el servicio se encuentre operativo en el menor tiempo posible.

3.2 Actividades

Una vez completada la revisión de los informes, se iniciará el proceso de reemplazo y recuperación de todos los recursos del JAMSA en la medida que sea posible.

Se procederá a examinar la información que haya sido perdida y se buscará en las copias de seguridad almacenadas en la Junta de agua.

3.3 Recomendaciones

se estima que al terminar el suceso se deben reunir las autoridades principales para evaluar los daños tanto en el sistema tecnológico como y de los bienes inmuebles

para reanudar su operación de toda la comunidad y que se recupere el suministro de agua y se retome todo lo referente a lo administrativo. Una vez terminado todo el proceso se debe realizar una revisión de que todos los puntos, se encuentren ya aplicados y que el plan de contingencia se archive para otra ocasión.

Nota. La tabla muestra del plan de contingencia para eventos naturales como incendios, inundaciones, terremotos y erupción volcánica.

Tabla 6

Plan de contingencia para mal funciones en componentes de hardware y software

<table>
<tr><td>Plan # 02

Versión 2.0</td><td>Contingencia:
Mal funciones en componentes de hardware y software.</td><td>  </td></tr>
<tr><td>Páginas: 3</td><td></td><td>Fecha: DD/MM/AA</td></tr>
<tr><td colspan="3">1.Plan de preventivo</td></tr>
<tr><td colspan="3">1.1 Eventualidad

La emergencia se activa cuando el equipamiento tecnológico del JAMSA, suscita un daño permanente o que necesite un mantenimiento correctivo para continuar con su operación y seguir brindando el servicio dentro de la Junta, dada por manipulación de los mismos o daños del equipamiento por el uso y terminación de garantías, afectando a:

• Activos software
• Activos hardware
• Activos comunicación
• Sistemas operativos
• Programas de operación en el JAMSA

1.2 Objetivo

Reestablecer de manera efectiva el funcionamiento del equipamiento tecnológico en el menor lapso viable y proseguir con las operaciones cotidianas de la Junta de agua.

Garantizar la privacidad, completitud y accesibilidad de estos datos es crucial para el JAMSA.</td></tr>
</table>

1.3 Entorno

Este evento, afectara a toda la oficina del JAMSA

1.4 Encargados

Los principales representes de la Junta y la persona externa encargada y creador del software de operación en la Junta de agua" Miño San Antonio", aseguraran que se de cumplimiento de todas las medidas preventivas establecidas en el plan de contingencia.

1.5 Actividades de Mitigación

- Contar con Backus diarios y respaldo de información relevante para la institución.
- Revisar de manera periódica el estado del Software de todos los equipos.
- Mantener los equipos actualizados.
- Todos los computadores deben tener antivirus actualizados.
- Realizar un evaluó del físico de los activos.
- Realizar mantenimientos preventivos.

2.Plan en Emergencia

2.1 Activación del plan

El plan se inicializa cuando los activos tecnológicos se encentren sin la probabilidad de dar servicio o que prácticamente no se puede acceder a los mismos.

2.2 Actividades para la contingencia

- Identificar el posible origen del deterioro de los activos.
- Confirmar si varios dispositivos están experimentando la misma dificultad.
- Rastrear el camino del archivo infectado, si es relevante.

• Realizar pruebas en los activos. • Si es preciso, realizar un formateo del dispositivo. • Posteriormente, llevar a cabo pruebas que verifiquen el correcto funcionamiento del equipo. **2.3 Proceso de mitigación** • Realizar mantenimientos preventivos cada 6 meses de uso en el JAMSA. • Comprar equipos con garantías. • Trabajar con licenciamientos. • Realizar limpieza física de los equipos.
3.Plan restauración
3.1 Personal responsable Los principales representes de la Junta y la persona externa encargada y creador del software de operación en la Junta de agua" Miño San Antonio", aseguraran que el servicio se encuentre operativo en el menor tiempo posible. **3.3 Recomendaciones** se estima que al terminar el suceso se deben reunir las autoridades principales para evaluar los daños tanto en el sistema tecnológico para reanudar su operación en el JAMSA Una vez terminado todo el proceso se debe realizar una revisión de que todos los puntos, se encuentren ya aplicados y que el plan de contingencia se archive para otra ocasión.

Nota. La tabla muestra el plan de contingencia para la denegación de servicio u operación por parte de los activos.

Tabla 7

Plan de contingencia para acceso a la información por individuos no autorizados

<table>
<tr><td>Plan # 03

Versión 3.0</td><td rowspan="2">Contingencia:

Acceso a la información por parte de individuos no autorizados</td><td>  </td></tr>
<tr><td>Páginas: 4</td><td>Fecha: DD/MM/AA</td></tr>
<tr><td colspan="3">1.Plan de preventivo</td></tr>
<tr><td colspan="3">1.1 Eventualidad

Cuando se presenta una vulnerabilidad en la información por parte de personal que no se encuentra autorizado a ingresar a los bienes tecnológicos o los bienes documentales.

1.2 Objetivo

Reestablecer de manera efectiva el funcionamiento del equipamiento tecnológico en el menor lapso viable y proseguir con las operaciones cotidianas de la Junta de agua.

Garantizar la privacidad, completitud y accesibilidad de estos datos es crucial para el JAMSA.

1.3 Entorno

Este evento, afectara a toda la oficina del JAMSA</td></tr>
</table>

1.4 Encargados

Los principales representes de la Junta y la persona externa encargada y creador del software de operación en la Junta de agua" Miño San Antonio", asegurarán que se de cumplimiento de todas las medidas preventivas establecidas en el plan de contingencia, respaldadas por la comunidad.

1.5 Actividades de Mitigación

- En el contexto de los registros digitales, resulta de suma importancia establecer contraseñas robustas, evitando aquellas que sean fáciles de adivinar, y cambiarlas cada seis meses.
- Para los registros físicos, es esencial limitar el acceso a personal autorizado; si es factible, implementar sistemas de autenticación biométrica o el uso de tarjetas para la revisión de información.
- Garantizar que los programas antivirus estén en constante operación y brinden una protección efectiva de la información.
- Prevenir la recepción de correos electrónicos no autorizados.
- Evitar la descarga no autorizada de contenido en dispositivos institucionales.
- Mantener respaldos actualizados, preferiblemente almacenados en la nube (utilizando OneDrive o de pago).

2.Plan en Emergencia

2.1 Activación del plan

El plan se activa cuando el personal administrativo de la junta evidencie que la información que se maneja siempre no se encuentre en su lugar o que prácticamente se haya realizado un borrado.

2.2 Actividades para la contingencia

Evaluar el alcance de los daños causados por el robo o la pérdida de información validando los siguientes puntos:

- Identificar qué información falta y su importancia.
- Verificar la integridad de las copias de seguridad.
- Intentar recuperar la documentación en caso de ser factible.
- Realizar un cambio completo de todas las contraseñas del sistema.
- Emplear herramientas para identificar y analizar posibles malware, así como el tipo de malware que ha afectado al sistema de información, si corresponde.
- Reforzar la seguridad de los datos, promoviendo el uso de contraseñas seguras o la autenticación de usuarios.
- En caso de ser posible, consultar a un especialista en seguridad informática para abordar la situación.

2.3 Proceso de mitigación

- Actualización de contraseñas.
- Implementación de autenticación de usuarios.
- Restauración de datos desde las copias de seguridad.

3.Plan restauración
3.1 Personal responsable Los principales representes de la Junta y la persona externa encargada y creador del software de operación en la Junta de agua” Miño San Antonio”, asegurarán que el servicio se encuentre operativo en el menor tiempo posible. **3.2 Actividades** Una vez completada la revisión de los informes, se iniciará el proceso de reemplazo y recuperación de todos los recursos del JAMSA en la medida que sea posible. Se procederá a examinar la información que haya sido perdida y se buscará en las copias de seguridad almacenadas en la Junta de agua. **3.3 Recomendaciones** se estima que al terminar el suceso se deben reunir las autoridades principales para evaluar los daños tanto en el sistema tecnológico para reanudar su operación en el JAMSA Una vez terminado todo el proceso se debe realizar una revisión de que todos los puntos, se encuentren ya aplicados y que el plan de contingencia se archive para otra ocasión.

Nota. La tabla muestra el plan de contingencia para la contingencia de acceso a la información por parte de individuos no autorizados.

Tabla 8

Plan de contingencia para cortes de servicios

<table>
<tr><td>Plan # 04

Versión 4.0</td><td rowspan="2">Contingencia:

Corte de servicios internet/energía eléctrica</td><td>  </td></tr>
<tr><td>Páginas: 4</td><td>Fecha: DD/MM/AA</td></tr>
<tr><td colspan="3">1.Plan de preventivo</td></tr>
<tr><td colspan="3">1.1 Eventualidad

Este incidente ocurre cuando hay una interrupción en el suministro de electricidad o la conexión a internet, situación que puede derivar de un evento catastrófico o una interrupción en las actividades planificadas, afectando a:

• Activos software
• Activos hardware
• Activos comunicación
• Sistemas operativos
• Programas de operación en el JAMSA

1.2 Objetivo

Reestablecer de manera efectiva el funcionamiento del equipamiento tecnológico en el menor tiempo posible y proseguir con las operaciones cotidianas de la Junta de agua.</td></tr>
</table>

1.3 Entorno

Este evento, afectara a toda la oficina del JAMSA

1.4 Encargados

Los principales representes de la Junta y la persona externa encargada y creador del software de operación en la Junta de agua “Miño San Antonio”, asegurarán que se de cumplimiento de todas las medidas preventivas establecidas en el plan de contingencia, respaldadas por la comunidad.

1.5 Actividades de Mitigación

- Verificar los dispositivos de resguardo de información.
- Llevar a cabo inspecciones del suministro de energía y las infraestructuras eléctricas.
- Resguardar los dispositivos del JAMSA mediante sistemas de respaldo UPS o reguladores de voltaje, con el propósito de garantizar el flujo ininterrumpido de energía eléctrica.
- Asegurarse de poseer un servicio de internet estable y que nos permita realizar las actividades sin interrupciones.

2.Plan en Emergencia

2.1 Activación del plan

El plan se inicializa cuando se verifique la falta de servicio, energía eléctrica o internet.

2.2 Actividades para la contingencia

- Notificar la interrupción del suministro eléctrico a la compañía y coordinar una resolución pronta.
- Informar a la proveedora de servicios de internet sobre la falla y llevar a cabo la gestión correspondiente para su solución.
- Detener temporalmente las tareas que requieran energía eléctrica de manera esencial.
- Realizar el proceso adecuado de apagado y desconexión de los dispositivos en caso de que la reanudación del servicio no sea inmediata.

2.3 Proceso de mitigación

Encender los dispositivos y verificar si los datos en proceso no se han visto perjudicados, reanudar de forma inmediata las tareas que hubieran sido interrumpidas.

3.Plan restauración

3.1 Personal responsable

Los principales representes de la Junta y la persona externa encargada y creador del software de operación en la Junta de agua “Miño San Antonio”, asegurarán que el servicio se encuentre operativo en el menor tiempo posible.

3.2 Actividades

Una vez completada la revisión de los informes, se iniciará el proceso de reemplazo y recuperación de todos los recursos del JAMSA en la medida que sea posible.

Se procederá a examinar la información que haya sido perdida y se buscará en las copias de seguridad almacenadas en la Junta de agua.

3.3 Recomendaciones

- Evitar hacer conexiones en enchufes múltiples
- Es conveniente desconectar los equipos después de usarlos.
- Tener mucho cuidado con el cableado de red y eléctrico.

Nota. La tabla muestra el plan de contingencia en caso de suscitarse cortes de servicios, internet y energía eléctrica.

Adquisición de software

Para culminar es preciso que en caso de que se desea realizar un análisis más detallado, y dependiendo de la infraestructura tecnológica a aplicar se podría adquirir el licenciamiento que nos da acceso a la herramienta por completo.

Figura 22

Costo de adquisición de sofware Pilar(AER)

Nota. La imagen muestra la página web del software Pilar/AER donde está documentada todo sobre su uso, Tomado del (Centro Criptológico Nacional, 2023).

Durante el tiempo de desarrollo del proyecto pude evidenciar que la página web que era de uso privado y comprada no posee una base de datos tan sólida que ayude a la JAMSA a respaldar información, por lo que se brindó una mano para que el dueño del software lo realice en el lanzamiento de las versiones futuras.

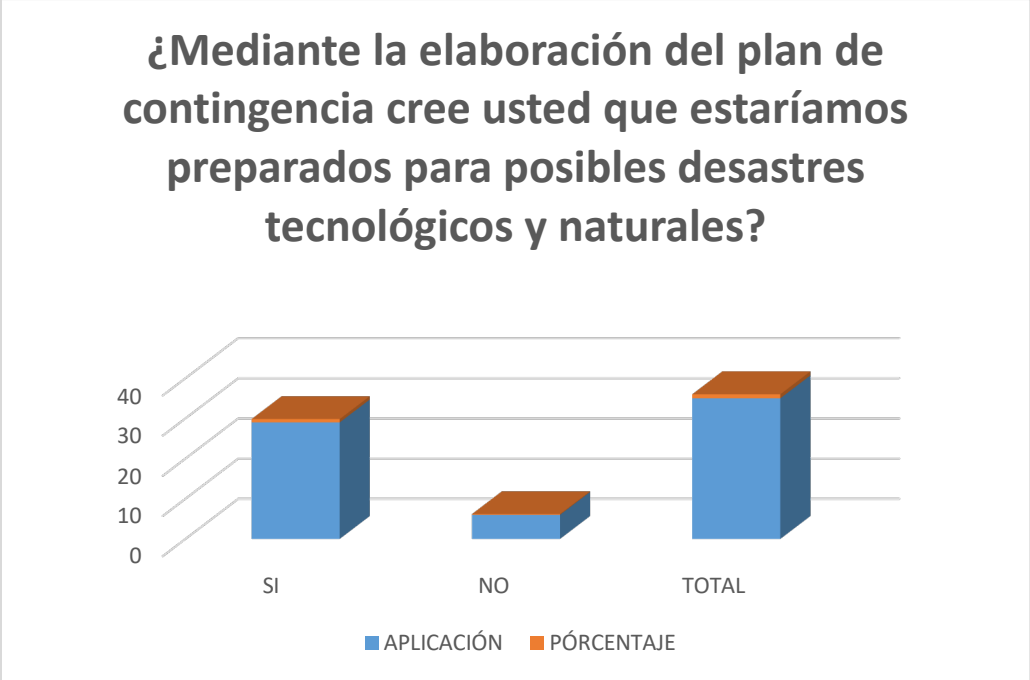
Procesamiento de encuestas a los miembros del JAMSA

Con el propósito de validar la factibilidad de la propuesta, se procedió a aplicar una encuesta a los miembros posibles del JAMSA, como se muestra a continuación:

Figura 23

Procesamiento de encuesta

VALORACIÓN	APLICACIÓN	PÓRCENTAJE
SI	29	83%
NO	6	17%
TOTAL	35	100%



Nota. La imagen muestra el porcentaje de aceptación del proyecto por algunos miembros que quisieron formar parte de la encuesta.

Capítulo V

Conclusiones y Recomendaciones

Conclusiones

Los planes de contingencia para servicios informáticos se enfocan en la creación de medidas que prevengan o reduzcan el efecto de una situación imprevista y permitan la recuperación de los servicios informáticos y/o tecnológicos afectados por dicha contingencia.

Cabe destacar, que el ser una zona de riesgo debido al volcán Cotopaxi, se ha previsto y recomendado que los respaldos se hagan de manera física y de manera digital (almacenamiento en la nube), y se recupere cualquier pérdida del sistema informático relacionado con la facturación a los socios de la Junta, que es de punto más crítico de la entidad.

Para llevar a cabo la implementación del plan, se llevarán a cabo las recomendaciones y los procedimientos previamente definidos en el análisis de riesgos, junto con las políticas y estrategias adecuadas, con el objetivo de disminuir el efecto de las posibles amenazas y, por consiguiente, el riesgo identificado en el análisis correspondiente.

La metodología que se aplicará consta de dos componentes principales: la metodología técnica utilizada para el análisis de riesgos, y la metodología empleada para validar la propuesta. La primera se basa en el método Magerit, mientras que la segunda implica la aplicación de encuestas. Ambos métodos permitirán determinar la viabilidad de implementar la propuesta en el JAMSA.

Los encuestados coinciden en que el plan de contingencia puede ser de gran ayuda para la Junta, permitiéndole preservar su información y operatividad en caso de sucesos tecnológicos y/o naturales.

Recomendaciones

Basándonos en lo previamente mencionado, se sugiere la implementación inmediata de medidas para gestionar los riesgos, establecer planes de respaldo y contingencia que incluyan diversas estrategias para ser aplicadas antes, durante y después de un incidente.

El objetivo principal de estas acciones es proteger la información que se maneja a través del sistema contable del JAMSA.

Además, se sugiere que, dado que la propuesta presentada es aplicable sin problemas en otras Juntas Administradoras de Agua Potable, se considere su implementación inmediata en estas instituciones.

Según lo mencionado anteriormente, se sugiere la implementación inmediata de un plan de gestión de riesgos, así como de un plan de respaldo y contingencia que incluya diversas estrategias antes, durante y después de una posible infiltración o catástrofe. El propósito principal de estas medidas es proteger la información manejada por el sistema contable de la Junta Administradora de Agua Potable “Miño San Antonio”

Bibliografía

El Minnesota de Hoy. (septiembre de 2022). Obtenido de https://www.elminnesotadehoy.com/investigan-masivo-ataque-cibernetico-a-distrito-escolar-de-los-angeles/?utm_source=rss&utm_medium=rss&utm_campaign=investigan-masivo-ataque-cibernetico-a-distrito-escolar-de-los-angeles

Fernández, J. I. (octubre de 2015). Obtenido de https://e-archivo.uc3m.es/bitstream/handle/10016/22424/PFC_Jose_Ignacio_Verdu_Fernandez.pdf?sequence=1&isAllowed=y#:~:text=El%20plan%20de%20contingencia%20es,operando%20aunque%20sea%20al%20m%C3%ADnimo.

Ortega, D. (13 de enero de 2011). Obtenido de http://calidadtic.blogspot.com/2011/01/como-hacer-un-plan-de-contingencia.html

Universidad Simón Bolívar. (2009). *Scielo.* Obtenido de http://ve.scielo.org/scielo.php?script=sci_abstract&pid=S1690-75152009000100004&lng=es&nrm=iso

Gobierno del encuentro. (2013). Obtenido de https://www.gestionderiesgos.gob.ec/wp-content/uploads/downloads/2012/07/Plan_de_Emergencia_Institucional.pdf

Sordo, A. I. (s.f.). *Hubspot.* Obtenido de https://blog.hubspot.es/marketing/sistema-informacion

Guglieri, J. (24 de enero de 1999). Obtenido de https://www.computerworld.es/archive/reingenieria-y-seguridad-en-el-ciberespacio

Isaca. (s.f.). Obtenido de https://www.isaca.org/About-ISACA/Press-room/News-Releases/Spanish/Pages/ISACA-Launches-Risk-IT-Framework-to-Help-Organizations-Balance-Risk-with-Profit-Spanish.aspx

M. A. (octubre de 2012). Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Bsi. (s.f.). Obtenido de https://www.bsigroup.com/es-ES/ISO-31000-Gestion-de-Riesgos/

Palacios Pacheco, R. A. (2013). *RRAE.* Obtenido de https://rraae.cedia.edu.ec/Record/ESPAM_8aa23ffce738803f34b96ea4d5897031

Welington, C. G. (2020). Obtenido de file:///C:/Users/usuario%201/Downloads/MUTC-000732.pdf

PMOinformatica.com. (s.f.). La oficina de proyectos de informática.

MAGERIT. (2012). Metodología de Análisis y Gestión.

Areitio Bertolín, J. (2008). s*eguridad de la información. Redes, informática y sistemas de información.* Paraninfo, SA.

León, R. d. (Julio de 2023). Obtenido de https://cursosonlineweb.com/informacion.html

Tramullas, J. (2020). Temas y métodos de investigación en Ciencia de la Información, 2000-2019. Revisión bibliográfica. *Profesional de la Información*.

Bernal, M., & Rodriguez, D. (2020). Las tecnologías de la información y omunicación como factor de innovación. *Scientia et Technica Año XXIV,*. Obtenido de https://www.redalyc.org/journal/849/84959429009/84959429009.pdf

Zarzet, V. (2020). IMPACTOS DE LA DIGITALIZACIÓN EN LOS SISTEMAS DE INFORMACIÓN DE GESTIÓN Y COSTOS. *Revista Del Instituto Internacional De Costos,* .

Peñafiel, K. (2021). Factores que determinan la Vulneración Informática y el Desarrollo de una aplicación móvil para concientizar sobre. *Fides et Ratio - Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia*. Obtenido de http://scielo.org.bo/scielo.php?script=sci_arttext&pid=s2071-081x2021000100009

Navas, N. (2021). Modelo de seguridad informática para riesgos de robo de información por el uso de las redes sociales. *Universidad Salesiana*.

Sanchez, P. (2021). Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia. *Información Técnologica* . doi:http://dx.doi.org/10.4067/S0718-07642021000500121

Agudeo, D. (2023). Plan de Seguridad Informática. *Universidad de Antioquia*.

Castillo, D. (2020). Plan de seguridad informática basado en la norma iso 27001, para proteger la información y activos de la empresa privada Megaprofer S.A. *Universidad Técnica de Ambato*. Obtenido de http://repositorio.uta.edu.ec/handle/123456789/30690

Izquierdo, J. (2020). Indicadores de compromiso (IOC) para detección de amenazas en la seguridad informática con enfoque en el código malicioso. *Universidad Salesiana*.

Pazmiño, C. (2022). Las Tics como herramienta para la gestión de riesgos. *Revista Científica de la Investigación y el Conocimiento*.

More, A. (2022). Evaluación de técnicas de Ethical hacking para el diagnóstico de vulnerabilidades de la seguridad informática en una empresa prestadora de servicios. *Universidad Señor Sipan*.

Villaseca, I. (2023). Diseño de una propuesta de ciberseguridad para la detección de fuga de información a través de dispositivos IoT en el área de TI de una empresa embotelladora y distribuidora de bebidas en Arequipa – 2021.

Olmedo, M. (2020). Seguridad de la información en plataformas e-learning en tiempos de pandemia COVID-19. *Revista UNIDA Científica,*.

Garcia, S. (2021). Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú. *Enfoque UTE*. doi:https://doi.org/10.29019/enfoqueute.743

Amate, F. (2020). Método para realizar copias de seguridad de imágenes médicas basado en tareas automatizadas. *Universidad Santiago de Chile* .

Cando, M. (2020). Prevención en ciberseguridad. *3 c TIC: cuadernos de desarrollo aplicados a las TIC,*.

León, D. d. (2021). Procedimiento para el cálculo y la mejora de la capacidad tecnológica en organizaciones empresariales. *Revista Universidad y Sociedad*.

Loyola, F. (2022). Control y contabilización de activos fijos y su incidencia en la toma de decisiones administrativas. *Universidad de Guayaquil*.

Cartuche, J. (2022). SEGURIDAD IOT: PRINCIPALES AMENAZAS EN UNA TAXONOMÍA DE ACTIVOS. *Revista Científica de las universidades de Aldas Peruanas*.

Ayudaley. (2020). Obtenido de https://ayudaleyprotecciondatos.es/2018/03/19/contingencia-continuidad-negocio/

Martínez, J. A. (2016). *Guía para la aplicación de ISO 9001 2015.* Alpha.

Junta administradora de agua “Miño San Antonio”. (s.f.). Gobierno Autónomo Descentralizado Parroquía rural San Juan de Pastocalle.

Gobierno Autónomo Descentralizado Parroquía rural San Juan de Pastocalle. (s.f.). Gobierno Autónomo Descentralizado Parroquía rural San Juan de Pastocalle.

Centro Criptológico Nacional. (2023). *PILAR*. Obtenido de PILAR: https://pilar.ccn-cert.cni.es/index.php/metodologia/implementacion

Anexos