UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMÀTICA, CIENCIAS DE LA COMPUTACIÒN E INNOVACIÒN TECNOLOGICA

CARRERA DE INGENIERIA EN SISTEMAS DE INFORMACIÓN

ANÁLISIS DE VULNERABILIDADES DEL SISTEMA DE INFORMACION DE LA EMPRESA PÚBLICA EMAPAL.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO **DE INGENIERO EN SISTEMAS DE INFORMACION**

AUTOR: JOSÉ MIGUEL IZURIETA LÓPEZ

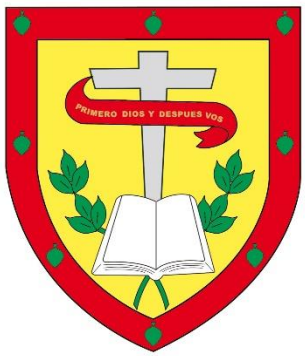
FRANCISCO JAVIER MONCAYO ORMAZA

DIRECTOR: ING. OLGER ANTONIO CAJAMARCA CRIOLLO, MGS

AZOGUES - ECUADOR

2023

DIOS, PATRIA, CULTURA Y DESARROLLO



UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMÀTICA, CIENCIAS DE LA COMPUTACIÒN E INNOVACIÒN TECNOLOGICA

CARRERA DE INGENIERIA EN SISTEMAS DE INFORMACIÓN

ANÁLISIS DE VULNERABILIDADES DEL SISTEMA DE INFORMACION DE LA EMPRESA PÚBLICA EMAPAL.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACION

AUTOR: JOSÉ MIGUEL IZURIETA LÓPEZ
FRANCISCO JAVIER MONCAYO ORMAZA

DIRECTOR: ING OLGER ANTONIO CAJAMARCA CRIOLLO, MGS

AZOGUES - ECUADOR

2023

DIOS, PATRIA, CULTURA Y DESARROLLO

Declaratoria de Autoría y Responsabilidad

Francisco Javier Moncayo Ormaza portador de la cédula de ciudadanía Nº **0302894167**. Declaro ser el autor de la obra: **"Análisis De Vulnerabilidades Del Sistema De Información De La Empresa Pública EMAPAL"**, sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católicade Cuenca de toda reclamación al respecto.

Azogues, **27 de marzo de 2023**

Francisco Javier Moncayo Ormaza

C.I. **0302894167**

Declaratoria de Autoría y Responsabilidad

José Miguel Izurieta López portador de la cédula de ciudadanía Nº **0301732723**. Declaro ser elautor de la obra: **"Análisis De Vulnerabilidades Del Sistema De Información De La Empresa Pública EMAPAL"**, sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sidoelaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área especifica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católicade Cuenca de toda reclamación al respecto.

Azogues, **27 de marzo de 2023**

.....

José Miguel Izurieta López

C.I. **0301732723**

Universidad Católica de Cuenca

Unidad Académica de Informática, Ciencias de la Computación, e Innovación Tecnológica

CARRERA DE SISTEMAS DE INFORMACIÓN

Azogues, 21 de marzo de 2023

Asunto: Aprobación trabajo de titulación.

Eco.
Nancy Peralta I
AUXILIAR DE SECRETARIA CARRERA DE SISTEMAS DE INFORMACIÓN

Su despacho. –

Por medio de la presente pongo en su conocimiento que he revisado el trabajo de titulación denominado: **"ANALISIS DE VULNERABILIDADES DEL SISTEMA DE INFORMACIÓN DE LA EMPRESA PÚBLICA EMAPAL"** de los estudiante FRANCISCO JAVIER MONCAYO ORMAZA, con cedula de identidad No 0302894167 y JOSÉ MIGUEL IZURIETA LÓPEZ, con cedula de identidad No 0301732723, los cuales cumplen con los requisitos establecidos por lo tanto se aprueba y recibe la nota 49/50 en el trabajo escrito de titulación.

Situación que informo para los fines pertinentes.

Atentamente,
DIOS, PATRIA, CULTURA Y DESARROLLO

Ing. Olger Antonio Cajamarca Criollo, Msc.
DOCENTE - TUTOR

AGRADECIMIENTO

Quiero expresar mi agradecimiento a Dios quien ha sido mi fortaleza y refugio en todo momento, gracias por haberme dado la oportunidad de culminar esta etapa en mi vida y por haberme dado la sabiduría y el conocimiento necesario para llevar a cabo este proyecto con éxito.

Le agradezco muy profundamente al personal de sistemas de EMAPAL y su paciencia, sin su colaboración e indicaciones precisas no hubiese podido lograr llegar a esta instancia tan anhelada. Gracias por su guía y todos sus consejos, los llevaré grabados para siempre en la memoria en mi futuro profesional.

Quiero expresar mi más sincero agradecimiento a mis amigos de la dirigencia estudiantil, quienes han sido un apoyo incondicional en mi camino hacia el éxito. Agradezco su dedicación, compromiso y trabajo incansable en la promoción de los valores estudiantiles, la representación de los intereses estudiantiles y la organización de eventos.

Además, quiero agradecer a mi compañero y amigo José Izurieta que ha sido una parte esencial en este proceso, merece mi más sincero agradecimiento por su amistad, dedicación, compromiso y apoyo constante. Reconozco que, sin su aporte y esfuerzo, nada de lo que he logrado hubiera sido posible.

Agradezco a nuestro tutor, Ing. Antonio Cajamarca por habernos apoyado en cada paso de este arduo proceso, por su guía y conocimientos, le agradezco mucho y le auguro muchos éxitos es su vida.

Por último, agradecer a la Universidad que me ha exigido tanto, pero al mismo tiempo me ha permitido obtener mi tan ansiado título. Agradezco a cada directivo por su trabajo y por su gestión, sin lo cual no estarían las bases ni las condiciones para aprender conocimientos

Gracias a todos y cada uno de los mencionados. ¡Este logro es también de ustedes!

Francisco Javier Moncayo Ormaza.

AGRADECIMIENTO

En primer lugar, quiero agradecer a Dios por su guía, protección y por brindarme la oportunidad de llevar a cabo este proyecto. Su amor y misericordia han sido mi fortaleza y me han dado la fuerza para superar los obstáculos en este camino

En segundo quiero agradecer a mi tutor de tesis, Antonio Cajamarca, por su orientación, paciencia y motivación constante durante todo el proceso de investigación. Sus consejos y conocimientos han sido fundamentales para el éxito de este trabajo.

También quiero agradecer a todos los profesores de la Unidad Académica De Informàtica, Ciencias De La Computaciòn E Innovaciòn Tecnologica, por su enseñanza y formación que han sido la base para la realización de este proyecto.

Agradezco a la empresa publica EMAPAL, especialmente a los ingenieros Morocho y Avila, pertenecientes al área de TI de la empresa, quienes generosamente ofrecieron su tiempo y colaboración para hacer posible esta investigación.

Agradezco a mis amigos Patricio y Paulo por su apoyo incondicional y motivación, sin ellos, este logro no habría sido posible, sin embargo, extiendo un agradecimiento especial a mi compañero y amigo Francisco Moncayo, ya que sin su apoyo durante una época difícil que sufri mientras cursaba la carrera no hubiese podido llegar a este punto. ¡Gracias Paco!

Finalmente, quiero agradecer a mi pareja Valeria Cabrera por estar a mi lado en todo momento, por su amor, paciencia y comprensión durante todos estos años, ya que sin la fortaleza que me ha brindado no hubiese podido obtener este logro.

A todos ellos, mi más sincero agradecimiento."

Jose Miguel Izurieta Lopez.

DEDICATORIA

Esta tesis es el resultado de años de esfuerzo, dedicación y perseverancia. Pero nada de esto habría sido posible sin el amor, el apoyo y el aliento incondicional de mi madre Ruth Moncayo quien han sido mi mayor apoyo, guía y ejemplo a seguir, gracias por haberme dado la vida y por haberme brindado su amor incondicional desde el primer día. Gracias por haberme enseñado los valores más importantes de la vida, como la perseverancia, el esfuerzo y la dedicación, y por haberme apoyado en cada uno de mis proyectos y metas. Este logro es un reflejo de su amor y su dedicación en mi vida, y sé que, sin su ayuda, no estaría aquí celebrando este importante logro en mi vida.

Asimismo, dedico este trabajo a mis hermanos Lucy, Juan Daniel e Israel, quienes han sido una presencia constante en mi vida y han sido un apoyo incondicional en cada etapa de mi camino. Ojalá algún día yo me convierta en se fuerza para que puedan seguir avanzando en su camino.

También les dedico este logro a mis abuelos Bertha y Gonzalo a pesar de no estar aquí me han enseñado a ser quien soy hoy. Gracias por por enseñarme el camino de la vida, gracias por sus consejos, por el amor que me han dado y por el apoyo incondicional en mi vida.

Esta tesis es, en parte, vuestra tesis también. Espero que, al leer estas líneas, sientan el orgullo que yo siento al haber llegado hasta aquí y al saber que ustedes han sido una pieza clave en este logro. Les dedico este trabajo con todo mi amor y agradecimiento por ser los mejores padres que alguien podría desear.

Gracias por todo.

Francisco Javier Moncayo Ormaza.

DEDICATORIA

A mi madre Eliana Lopez, por su amor incondicional, apoyo y motivación constante durante toda mi vida. Gracias por ser mi fortaleza y por creer en mí incluso cuando yo no lo hacía, por apoyarme en mis peores momentos y aunque a pesar que el dia de hoy ya no esta a mi lado siempre siento su presencia, se que me cuida y esta orgullosa de la persona en la que me he convertido.

Asi mismo a mi futura esposa Valeria Cabrera, por siempre haber confiado en mi, por amarme, por su comprensión y por acompañarme durante todos estos años, este logro también es tuyo.

Tambien quiero dedicar este logro a mi padre Patricio Izurieta, por las cosas buenas que logro inculcar en mi persona, sus enseñanzas y por sus gustos

Finalmente, a mi familia, en especial a mis abuelos, Jose Manuel Lopez Sacoto, Elba Victoria Vintimilla, mis hermanas Eliana Izurieta y Diana Avila, este trabajo va dedicado para ustedes con todo mi amor.

Jose Miguel Izurieta Lopez.

RESUMEN

La empresa pública EMAPAL, es responsable del suministro de agua y alcantarillado en el cantón Azogues. Actualmente cuenta con una infraestructura de tecnología de la información (TI) pero carece de un proceso distribuido para la gestión de riesgos de la información que ayude a la identificación de puntos críticos en el área, limitando la capacidad de tomar decisiones adecuadas para la implementación de medidas de seguridad. El objetivo de este estudio es analizar las vulnerabilidades y amenazas de los activos de TI en EMAPAL aplicando la Guía para la Gestión de Riesgos de la Seguridad de la Información como metodología, incluyendo la identificación de los activos de información, detección y valoración de amenazas y vulnerabilidades, y la recomendación de controles para reducir los niveles de riesgo. Con los resultados obtenidos se pudo identificar un total de 524 vulnerabilidades en 22 procesos, con un riesgo promedio de nivel medio. El estudio identificó también, múltiples vulnerabilidades y amenazas en la infraestructura de la empresa y ofreció soluciones en calidad de recomendación. Con la implementación de una guía de gestión de riesgos de la información permitiría a que EMAPAL mejore sus controles de seguridad y mantenga una protección continua, lo que les permitiría tomar decisiones más informadas y proteger sus activos de TI de una forma más efectiva.

Palabras clave: vulnerabilidades, amenazas, guía para la gestión de riesgos de la información, TI, activos de TI

ABSTRACT

Municipal Drinking Water and Sewerage Company EMAPAL (by its Spanish acronym) is responsible for water supply and sewerage in Azogues canton. It currently has an information technology (IT) infrastructure, but it does not have distributed process for information risk management to help identify critical points in the area, limiting the ability to make appropriate decisions to implement security measures. This study aims to analyze the vulnerabilities and threats of EMAPAL's IT assets by applying the Information Security Risk Management Guide as a methodology; this analysis includes identifying information assets, detecting and assessing threats and vulnerabilities, and recommending controls to reduce risk levels. According to the results, 524 vulnerabilities were identified in 22 processes with a medium risk level. The study also identified multiple vulnerabilities and threats in the company's infrastructure and recommended solutions. Implementing an information risk management guide would enable EMAPAL to improve its security controls and maintain continuous protection, allowing them to make more informed decisions and protect its IT assets more effectively.

Keywords: vulnerabilities, threats, information risk management guide, IT, IT assets

INDICE DE CONTENIDOS

INDICE DE TABLAS

ANEXOS

CAPITULO 1

1.1 INTRODUCCIÓN

En la actualidad, la tecnología ha avanzado de manera impresionante y ha intervenido prácticamente en todos los aspectos de nuestra vida, gracias al desarrollo constante de las Tecnologías de la Información y la Comunicación (TIC); sin embargo, este crecimiento constante también ha llevado a un aumento de la inseguridad, especialmente en el caso de las conexiones a Internet, donde es común encontrar diversas vulnerabilidades que pueden ser explotadas por personas malintencionadas para cometer delitos informáticos.

El análisis de vulnerabilidades se refiere a un proceso que tiene como finalidad la identificación y evaluación de los puntos débiles de un sistema, red, aplicación o dispositivo con el propósito de protegerlos de posibles ataques cibernéticos. En la actualidad, debido al avance tecnológico, este proceso se ha vuelto más crucial que nunca en aras de garantizar la seguridad de la información y la protección de datos confidenciales.

El análisis de vulnerabilidades implica un enfoque metódico y estructurado para identificar y evaluar las debilidades de una organización, con el objetivo de mejorar la seguridad y disminuir el riesgo de ataques cibernéticos. En general, se realiza en varias etapas, tales como; la identificación dos activos críticos, la evaluación de las vulnerabilidades, la priorización de los riesgos y la mitigación de las vulnerabilidades detectadas. Los resultados obtenidos del análisis de vulnerabilidades son de gran ayuda en la identificación y solución de los riesgos de seguridad en los sistemas y aplicaciones; además, también son útiles para asegurar el cumplimiento de las normas y regulaciones que se aplican en materia de seguridad de la información.

1.2 PLANTEAMIENTO DEL PROBLEMA

El impacto de las amenazas a los activos de información en las organizaciones puede ser devastador y en algunos casos, irreversible. La Empresa Pública Municipal de Agua Potable, Alcantarillado y Saneamiento Ambiental del Cantón Azogues (EMAPAL), es un claro ejemplo de ello, ya que, en enero de 2021, sufrió una intrusión en su sistema informático que afectó gravemente la base de datos. Este incidente pone en evidencia la

importancia de contar con una gestión de riesgos de la información eficaz que permita identificar, evaluar y tratar los riesgos que pueden afectar los activos de la información de la organización.

EMAPAL, al igual que muchas otras organizaciones, enfrenta la dificultad de establecer un proceso estructurado y metódico para la gestión de riesgos de la información que le permita evaluar y mejorar continuamente sus controles, con el fin de disminuir los riesgos a los que está expuesta. Esta situación ha impedido que la empresa pueda identificar los puntos críticos dentro del área de TI, lo que dificulta la toma de decisiones para la implementación de medidas de seguridad adecuadas.

Por lo tanto, es necesario que EMAPAL cuente con una guía de gestión de riesgos de la información que le permita establecer un proceso estructurado y metódico, con el fin de identificar, evaluar y tratar los riesgos de manera eficaz. La implementación de una guía de gestión de riesgos de la información, no solo permitiría a EMAPAL mejorar sus controles de seguridad, sino que también le permitiría una mejora continua, la protección de sus activos de información y la continuidad de sus operaciones en caso de futuras amenazas.

1.3 JUSTIFICACIÓN

La gestión de riesgos de la información es un proceso clave para cualquier organización, ya que permite identificar, evaluar y tratar los riesgos que pueden afectar los activos de la información. En el caso de EMAPAL, el reciente incidente de intrusión en su sistema informático y la afectación grave de su base de datos evidencia la necesidad de contar con un proceso estructurado y metódico para la gestión de riesgos de la información.

En la actualidad, EMAPAL enfrenta la dificultad de establecer un proceso efectivo de gestión de riesgos, lo que ha impedido la identificación de los puntos críticos dentro del área de TI y la toma de decisiones adecuadas para la implementación de medidas de seguridad. Por lo tanto, es necesario que EMAPAL cuente con una guía de gestión de riesgos de la información que le permita establecer un proceso estructurado y metódico, con el fin de identificar, evaluar y tratar los riesgos de manera eficaz.

La implementación de una guía de gestión de riesgos de la información, no solo permitiría a EMAPAL mejorar sus controles de seguridad, sino que también le permitiría una mejora continua, la protección de sus activos de información y la continuidad de sus operaciones en caso de futuras amenazas. En comparación con la implementación de un estándar de seguridad, la guía de gestión de riesgos de la información es una herramienta más flexible y adaptable a las necesidades específicas de la organización. Además, la implementación de un estándar puede ser costosa y requerir de recursos significativos, mientras que la implementación de una guía puede ser más sencilla y accesible para una empresa como EMAPAL que permita paliar los riesgos que se presenten.

En sintesis, la implementación de una guía de gestión de riesgos de la información es una necesidad para EMAPAL, ya que permitirá una gestión de riesgos efectiva, una mejora continua y una protección adecuada de sus activos de información.

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

Realizar un análisis de vulnerabilidades y amenazas del Departamento de TI en la EMAPAL (Empresa Municipal de Agua Potable y Alcantarillado), aplicando la Guía para la Gestión de Riesgos de la Seguridad de la Información

1.4.2 OBJETIVOS ESPECÍFICOS

1. Construir la fundamentación teórica relacionada a la sistémica de vulnerabilidades y estándares de seguridad informática.
2. Realizar un levantamiento de información de los activos de la informacion del departamento de TI de EMAPAL y terminales de los usuarios, a través de la observación, encuestas, entrevistas y documentación de la emprpesa.
3. Determinar las principales vulnerabilidades de los sistemas informáticos de la EMAPAL mediante la aplicación de la guía de gestión de riesgos de seguridad de la información
4. Recomendar soluciones a los riesgos encontrados a taves de una guía de gestión de riesgos de seguridad.

1.5 ALCANCE

Este trabajo de investigación consistirá en llevar a cabo un análisis de los activos de TI, terminales de los empleados, talento humano y el nivel organizacional del departamento de TI de la empresa EMAPAL, con el fin de identificar las vulnerabilidades, amenazas y controles, en cuanto a la seguridad de la información. Para llevar a cabo este análisis, se utilizará la Guía para la Gestión de Riesgos de la Seguridad de la Información del Ministerio de Telecomunicaciones y la Sociedad de la Información del Ecuador.

Cabe mencionar que debido a que no formamos parte de la organización y no tenemos acceso a toda la información, es posible que existan ciertos aspectos que no puedan ser incluidos en nuestro análisis, limitados información confidencial, procesos internos. No obstante, se presentarán sugerencias basadas en la guía para la gestión de riesgos de la información, con el objetivo de proponer medidas que permitan reducir los niveles de riesgo presentes en EMAPAL.

Ademas es pertinente aclarar que la investigación se circunscribe únicamente al edificio matriza de la empresa EMAPAL y escencialmente al departamento de TI, y los diferentes puntos de interés donde se halle infraestructura de TI.

1.6 METODOLOGÍA

Se empleará una investigación bibliográfica o documental, con el objetivo de adquirir información a través de páginas web, libros electrónicos, documentos, artículos e investigaciones similares al proyecto planteado. Estos serán de utilidad para la investigación debido a que abarca la observación, revisión de fuentes para recoger información investigación [10].

Dentro de esta investigación se empleará la Guia para la Gestion de Riesgos de la Informacion del Ministerio de Telecomunicaciones y de la Sociedad de la Informacion, la que nos permitirá determinar los activos de informacion existentes, detectar y valorar las amenazas, vulnerabilidades y controles existentes y finalmente recomendar controles a implementar para disminuir las puntuaciónes de riesgo de los activos.

Dentro de este trabajo de tesis se emplearán 3 tipos de investigación:

- La primera será investigación bibliográfica, a través de la cual, con artículos científicos, libros digitales, y cualquier tipo de información relacionada con nuestro tema nos permitirá tener una información organizada para realizar la investigación y el uso de herramientas.
- Investigación de Campo con el fin de conocer el funcionamiento de la empresa y su entorno de TI y de esta forma realizar los análisis necesarios de vulnerabilidad, su respectiva documentación y sus recomendaciones, todo esto dentro de la empresa de agua EMAPAL.

1.7 ESTADO DEL ARTE

En el año 2014, una investigación realizo "el análisis de riesgos informáticos y su incidencia en la seguridad e integridad de la información en la facultad de ingeniería civil y mecánica de la universidad técnica de Ambato". Los resultados que se obtuvieron en la investigación que casi un 80% de los equipos y sistemas sufrían fallas en la seguridad, ocasionando pérdidas de información. Sin embargo, el autor concluye que se debe realizar evaluaciones en los equipos y sistemas para el resguardo de información (Bedoya Reyes Donald Eduardo, 2014).

En una investigación del año 2015, se generó una "metodología para el análisis forense de datos e imágenes de acuerdo a las leyes del Ecuador". La autora concluye que las metodologías presentadas ayudaran a la investigación forense y proporciona guías bajo el marco legal ecuatoriano. Los resultados fueron satisfactorios puesto que se lograron alcanzar los objetivos de encontrar cual fue el provocador del delito, en este caso el software oculto (Granda Tonato Gabriela Estefanía, 2015).

En un estudio del 2017, se realizó un "análisis de vulnerabilidades y acciones correctivas sobre un sistema web". Los resultados del Pentesting realizo métodos de análisis de vulnerabilidades que identificaron que el sistema web de ventas y equipos físicos poseen varias fallas de seguridad. El autor concluye que las organizaciones hagan un poco más de conciencia sobre la importancia de la seguridad informática y no menospreciar loas análisis de vulnerabilidades para prevenir incidentes informáticos (Pinos Solano Danny Omar, 2017).

En otra investigación, se presentó un “Análisis de Vulnerabilidades de Seguridad Informática, del Sistema de Gestión Médica SISMEDICALEC, de la empresa Incomsis”. Los resultados indicados en la investigación son las soluciones más adecuadas para las vulnerabilidades informáticas en el sistema de la empresa Incomsis, para lo cual se identificó las funcionalidades del aplicativo web, también se analizó la seguridad de la información del mismo, mediante ataques informáticos (Quirola Valarezo Lisbeth Mariuxi, 2019).

En el año 2022, se realizó un Análisis de Cultura de Seguridad Informática. Caso de Estudio: León, Guanajuato, México. Los autores presentan resultados de desarrollo en un marco de referencia para establecer un plan de acción para crear una cultura de seguridad informática en las organizaciones Leonesas (Luis C. Villaverde Hidalgo, José L. Cabrera Guzmán, Jorge R. Parra Michel, Sandra A. Olivares Bautista, Alberto Ochoa Brust, Walter Mata, Leobardo A. Ceja Bravo, and Rafael Martínez Peláez, 2021).

La investigación de Triana Edwinson (2022), que tuvo como objetivo realizar un informe final con las competencias y destrezas adquiridas de los grupos Red Team para hallazgos de Vulnerabilidad y de los Blue Team para cierre de brechas de seguridad. El autor concluye que en toda organización debe existir la posibilidad de tener dos grupos de trabajo, unos que deben estar enfocados al ataque y descubrimiento de vulnerabilidades, y el otro grupo al hardening de equipos y protección de la red, y es por esto que dentro del contexto de este trabajo se logran identificar las diferentes fases que están compuestas para el desarrollo de pruebas de pentesting.

CAPÍTULO 2

En este capítulo abarcará los temas relacionados con la seguridad informática y sus vulnerabilidades, tomando en cuenta que su importancia radica en la prevención del robo de información en diferentes áreas, además permita identificar cualquier tipo de amenazas que puede sufrir las plataformas y equipos informáticos.

2.1 SEGURIDAD EN TÉRMINOS GENERALES

El término seguridad provine del latín seguritas, que es “estar sin cuidado”; es decir, sentirse a salvo, se emplea en un sentido muy similar: la ausencia de riesgos o peligros.

En términos generales, la seguridad se define como “el estado de bienestar que el ser humano percibe y disfruta”. Una definición dentro de las ciencias de la seguridad es ‘ciencia interdisciplinaria que está encargada de evaluar, estudiar y gestionar los riesgos a los que se encuentra sometida una persona, un bien o el ambiente’ [11].

2.2 CONCEPTO DE SEGURIDAD INFORMÁTICA

Es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora o circulante a través de las redes de computadoras [1].

Es por esto que esta disciplina del área de la informática encargada de la protección de la privacidad de datos dentro de los sistemas informáticos se ha convertido en una parte indispensable para los negocios y la operación de las empresas [2].

2.3 ¿QUÉ ES UNA AUDITORIA INFORMÁTICA?

Es el proceso llevado a cabo por profesionales específicamente capacitados para el efecto, que recoge, agrupa y evalúa evidencias para determinar si un Sistema de Información salvaguarda el activo empresarial, mantiene la integridad de los datos, precautelando los fines de la organización con el uso eficaz de los recursos, cumpliendo con las leyes y regulaciones establecidas [12]

Las auditorías informáticas son procedimientos que tienen como objetivo prevenir y evaluar la eficacia de los recursos tecnológicos de una organización. Éstas, establecen políticas para el mantenimiento de los sistemas, el cuidado preventivo de los equipos, el uso adecuado de los recursos por parte de los usuarios, el análisis de la red y la seguridad en línea. Además, pueden incluir la creación de un manual de procedimientos para actuar en caso de que se presenten problemas informáticos.

2.3.1 AUDITORIA INTERNA

Es aquella que se hace desde el ambiente interno de la empresa, es decir, sin empleados ajenos a la misma, ya sea por empleados que fueron directamente contratados o alguna subsidiaria a esta y la entidad tiene el poder de decisión sobre el proceso llevado a cabo para realizarla [13].

“Es una función que contribuye a una organización a lograr a alcanzar sus objetivos; para ello se apoya en un proceso sistemático para el análisis de los procesos del negocio, actividades y procedimientos relacionados con los retos de la organización”

La auditoría interna se encarga de verificar el cumplimiento de normas y políticas previamente establecidas por la alta dirección de la empresa. Sus funciones incluyen:

- Controlar los hechos para garantizar el cumplimiento de dichas normas y políticas,
- La verificación de los sistemas de control interno, establecido por la organización.
- Evaluar y verificar la información para evitar desvíos de los datos en los sistemas o procesos de la organización.
- Analizar los riesgos que tiene los sistemas informáticos dentro de la organización.
- Diseñar soluciones para los problemas encontrados.
- Presentar informes con resultados de cada auditoría realizada.

2.3.2 AUDITORIA EXTERNA

La auditoría es llevada a cabo por un tercero ajeno a la empresa. La principal tarea de la auditoría es estudiar los mecanismos de control existentes en una empresa u organización, evaluando si son apropiados y cumplen con los objetivos y estrategias establecidos, determinando qué cambios se deben hacer para alcanzar estos objetivos. La organización no tiene poder de decisión sobre el proceso de auditoría.

2.4 FASES DE LA AUDITORIA INFORMÁTICA

Existen 3 fases fundamentales en una auditoria informática que son:

- Planificación: En esta etapa se realiza una valoración de los procedimientos y sistemas, y se analizan los equipos informáticos y la evolución de los procesos de datos.
- Ejecución: Durante esta etapa, se recopila la mayor cantidad de información posible a través de entrevistas, encuestas y revisión de documentos de la empresa, para luego clasificarla y analizarla de manera adecuada.
- Finalización: En esta etapa, se realiza la presentación de informes que contienen los resultados de la auditoría, incluyendo los análisis realizados y las soluciones propuestas.

2.5 LOS MECANISMOS DE CONTROL EN EL ÁREA DE INFORMÁTICA

Se identifican: Directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

2.5.1 LOS OBJETIVOS DE LA AUDITORÍA INFORMÁTICA SON:

- El análisis de la eficiencia de los Sistemas Informáticos
- La verificación del cumplimiento de la Normativa en este ámbito
- La revisión de la eficaz gestión de los recursos informáticos.

2.5.2 TIPOS DE AUDITORÍA

Auditoría operacional: se refiere a la revisión de la operación de una empresa y juzga la eficiencia de la misma. La misma puede ser permisos de empleados o accesos a sistemas de gestión [14].

Auditoría administrativa: se refiere a la organización y eficiencia de la estructura del personal con la que cuenta el personal y los procesos administrativos en que actúa dicho personal [14].

Auditoría social: se refiere a la revisión del entorno social en que se ubica y desarrolla una empresa, con el fin de valorar aspectos externos e internos que interfieren en la productividad de la misma [14].

2.6 AUDITORÍA DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN

Una auditoría de seguridad informática se podría definir como la evaluación del nivel de madurez en seguridad de una organización, donde se analizan las políticas y procedimientos de seguridad definidos por la misma y se revisa su grado de cumplimiento. También, las medidas técnicas y organizativas implantadas para garantizar la seguridad [3].

2.6.1 ANÁLISIS DE RIESGO

Es el estudio de las causas de las posibles amenazas y probables eventos no deseados y los daños y consecuencias que éstas puedan producir [4].

La gestión del riesgo de la seguridad de la información debe ser una parte integral de todas las actividades de la gestión de la seguridad de la información y se deben aplicar tanto a la implementación como al funcionamiento continuo de un SGSI. La gestión del riesgo de la seguridad de la información debe ser un proceso continuo. Tal proceso debe establecer el contexto, evaluar los riesgos, tratar los riesgos utilizando un plan de tratamiento para implementar las recomendaciones y decisiones.

Las actividades para la gestión del riesgo de la seguridad de la información:

1. Establecimiento del contexto
2. Valoración del riesgo
3. Tratamiento del riesgo
4. Aceptación del riesgo
5. Comunicación del riesgo
6. Monitoreo y revisión del riesgo

2.7 CARACTERÍSTICAS DE UNA AUDITORIA INFORMÁTICA

- La información de la empresa y para la empresa, siempre importante, se ha convertido en un Activo Real de la misma, como su Stock o materias primas si las hay. Por ende, han de realizarse inversiones informáticas, materia de la que se ocupa la Auditoria de Inversión Informática [15].
- Del mismo modo, los Sistemas Informáticos han de protegerse de modo global y particular: a ello se debe la existencia de la Auditoría de Seguridad Informática en general, o a la auditoría de Seguridad de alguna de sus áreas, como pudieran ser Desarrollo o Técnica de Sistemas [15].
- Cuando se producen cambios estructurales en la Informática, se reorganiza de alguna forma su función: se está en el campo de la Auditoría de Organización Informática [15].
- Estos tres tipos de auditorías engloban a las actividades auditoras que se realizan en una auditoría parcial. De otra manera: cuando se realiza una auditoria del área de Desarrollo de Proyectos de la Informática de una empresa, es porque en ese desarrollo, existen además de ineficiencias, debilidades de organización, o de inversiones, o de seguridad, o alguna mezcla de ellas [15].

2.8 HERRAMIENTAS PARA UNA AUDITORIA INFORMÁTICA

Son recursos técnicos que permiten recopilar, analizar y procesar datos e información relacionados con los sistemas informáticos y de tecnología de una organización.
Algunas de las herramientas más comunes son:

- Backup y copias espejos de discos duros y medios removibles.
- Software de búsqueda de archivos.
- Google Desktop.
- Software de Recuperación de archivos borrados.
- Análisis de la memoria RAM.
- Análisis de la red.
- Actividad del equipo.

- Borrado definitivo
- Búsqueda de mails, historial de internet, chats.
- Otros: Encase Forensic, CondorLinux, Maltego, impresiones.

2.9 MECANISMOS DE PREVENCIÓN

Los mecanismos preventivos de seguridad se refieren a todas las medidas que se toman para evitar cualquier riesgo que pueda afectar la confidencialidad, integridad y disponibilidad de los componentes críticos del sistema**.**

Las 9 medidas básicas de seguridad informática, lo que asegurará la seguridad de la información de tu organización.

2.9.1 CONTROLES DE ACCESO A LOS DATOS MÁS ESTRICTOS

Una de las principales medidas de seguridad es limitar el acceso a la información. Cuantas menos personas accedan a una información, menor será el riesgo de comprometerla. Por lo tanto, es necesario implantar en nuestra empresa un sistema que impida dar acceso a datos innecesarios, a un usuario, cliente, etc. [16].

2.9.2 REALIZAR COPIAS DE SEGURIDAD

Poseer un sistema de copias de seguridad periódico permite que la empresa garantice que puede recuperar los datos ante una incidencia de carácter catastrófico, impidiendo la pérdida de los mismos y permitiendo la recuperación de la normalidad en el trabajo en apenas unos minutos [16].

2.9.3 UTILIZAR CONTRASEÑAS SEGURAS

El acceso a las distintas plataformas que utiliza la empresa (correo electrónico, servidor de copias de seguridad NAS, etc.) debe realizarse utilizando claves de seguridad (contraseñas) seguras, que impidan que puedan ser fácilmente descubiertas por piratas informáticos. El uso de contraseñas seguras es una de las medidas de seguridad informática más importantes en una empresa [16].

2.9.4 PROTEGER EL CORREO ELECTRÓNICO

Hoy en día, la mayoría de comunicaciones de nuestra empresa se realiza utilizando el correo electrónico. Por lo tanto, otra medida de seguridad es utilizar filtros antispam y sistemas de encriptado de mensajes, para asegurar la protección y privacidad de toda esa información [16].

2.9.5 CONTRATAR UN SOFTWARE INTEGRAL DE SEGURIDAD

¿Cómo proteger la información en internet? La mejor forma es contratando un paquete de seguridad integral que contenga antivirus, anti espías, antimalware, firewall, etc., y que permita proteger la información ante posibles ataques externos a través de internet [16].

2.9.6 UTILIZAR SOFTWARE DLP

Existen programas de prevención de pérdidas de datos (DLP) que pueden ser implementados como medida de seguridad en nuestra empresa para supervisar que ningún usuario esté copiando o compartiendo información o datos que no deberían [16].

2.9.7 TRABAJAR EN LA NUBE

Trabajar en la nube permite, entre otras ventajas, contar con los sistemas de seguridad de la información que posee el proveedor de servicios. Además, este proveedor será responsable de esa seguridad [16].

2.9.8 INVOLUCRAR A TODA LA EMPRESA EN LA SEGURIDAD

Para que las medidas de seguridad informática de una empresa funcionen, debe involucrar en su participación a todos los estamentos que participan en la misma, incluyendo a los agentes externos como puedan ser clientes, proveedores, etc. Muchas veces, nuestra empresa tiene implantados los sistemas correctos de seguridad, y la brecha en la misma, se produce al relacionarnos con un tercero que carece de estas medidas de seguridad [16].

2.9.9 MONITORIZACIÓN CONTINUA Y RESPUESTA INMEDIATA

Debe implantar en la empresa un sistema que permita monitorizar la gestión de los datos y detectar aquellos posibles fallos o actuaciones incorrectas. Este sistema de control permitirá actuar rápidamente para solventar cualquier incidencia y minimizar su repercusión [16].

2.10 CORRECCIÓN Y DETECCIÓN EN SEGURIDAD INFORMÁTICA

Una correcta corrección según el frente en el que se desea atajar, Es muy importante destacar las herramientas como los antimalware se encuentran más desarrolladas para los entornos que utilizan los usuarios no experimentados y por lo tanto son los vulnerables.

2.11 FORMAS DE DETECCIÓN DE VULNERABILIDADES

Antivirus: Es una herramienta clásica que pretende ser un escudo de defensa en tiempo real para evitar ejecuciones de archivos o accesos a web maliciosas.

Algunas de las variantes actuales que se puede encontrar son:

Antivirus de escritorio: instalado como una aplicación, permite el control antivirus en tiempo real o del sistema de archivos.

Antivirus en línea: cada vez se están desarrollando más aplicaciones web que permiten, mediante la instalación de plugins en el navegador, analizar nuestro sistema de archivos completo.

Análisis de ficheros en línea: servicio gratuito para análisis de ficheros sospechosos mediante el uso de múltiples motores antivirus, como complemento para comprobar si algún fichero sospechoso contiene o no algún tipo de código malicioso.

Antivirus portable: no requieren instalación en el sistema y consumen una pequeña cantidad de recursos.

Antivirus Live: arrancable y ejecutable desde una unidad extraíble USB, CD o DVD. Permite analizar nuestro disco duro en caso de no poder arrancar nuestro sistema operativo tras haber quedado inutilizable por algún efecto de malware.

Herramientas de bloqueo web: nos informan de la peligrosidad de los sitios web que visita, en algunos casos, nos informan de forma detallada, qué enlaces de esas páginas se consideran peligrosos y cuál es el motivo

2.12 AMENAZAS

Son circunstancias con la capacidad suficiente para llegar a causar daños o pérdidas a un sistema. Por ejemplo, un gusano informático es una de las amenazas que vive en un ordenador y se propaga en otros causando daños.

2.13 VULNERABILIDADES

Es el riesgo que una persona, sistema u objeto puede sufrir frente a peligros inminentes, sean ellos desastres naturales, desigualdades económicas, políticas, sociales o culturales. Las vulnerabilidades adoptan diferentes formas, dependiendo de la naturaleza del objeto de estudio, sus causas y consecuencias [5].

Las vulnerabilidades se pueden genera por:

- Errores de configuración.
- Errores en la gestión de recursos.
- Errores en los sistemas de validación.
- Errores que permiten el acceso a directorios.
- Errores en la gestión y asignación de permisos [6].

2.14 CLASIFICACIÓN DE VULNERABILIDADES

Phishing: Es una técnica de manipulación psicológica empleada por los ciberdelincuentes para obtener información confidencial de las personas, como contraseñas, números de

tarjetas de crédito y otra información personal. Esta estrategia se realiza a través de correos electrónicos, mensajes de texto, llamadas telefónicas y redes sociales, que parecen ser de empresas legítimas, pero en realidad son falsos. Los enlaces que se proporcionan en estos mensajes fraudulentos dirigen a sitios web falsificados que parecen ser de empresas u organizaciones de confianza, como bancos o proveedores de servicios en línea. Una vez en el sitio web falso, las personas pueden ser engañadas para ingresar su información personal o financiera, lo que es capturado por los ciberdelincuentes para cometer fraude.

Spam: es cualquier forma de comunicación no solicitada que se envía de forma masiva (correo electrónico masivo no solicitado, o UBE). Su forma más frecuente es un correo electrónico de publicidad enviado a un gran número de direcciones (correo electrónico de publicidad no solicitada, o UCE), pero el "spamming" también existe a través de menajes instantáneos, de texto (SMS), redes sociales o incluso mensajes de voz [17].

Botnets (Redes de robots): Una botnet o red zombi es un grupo de ordenadores o dispositivos que están bajo el control de un atacante, y que se usan para perpetrar actividades malintencionadas contra una víctima. El término botnet es una combinación de las palabras robot y network (red) para representar la naturaleza de un ciberataque realizado mediante una botnet [18].

Trashing: Es una técnica de espionaje cibernético que implica buscar información sensible en la basura de empresas u organizaciones. Los atacantes buscan documentos impresos, discos duros antiguos, dispositivos de almacenamiento y otros materiales que puedan contener información importante. Una vez obtenida esta información, los atacantes pueden usarla para cometer fraudes o robo de identidad. Por lo tanto, es crucial que las empresas tengan políticas claras para la eliminación segura de información confidencial y la protección de sus residuos.

Malware: Es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas. El malware hostil, intrusivo e intencionadamente desagradable intenta invadir, dañar o deshabilitar ordenadores, sistemas informáticos, redes, tabletas y dispositivos móviles, a menudo asumiendo el control parcial de las operaciones de un dispositivo [19].

Inyección SQL injection: Es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos [20].

Ataques de contraseñas: Son un método utilizado por los delincuentes cibernéticos para descubrir las contraseñas y acceder a sistemas o cuentas que están protegidas. Hay diferentes formas de estos ataques, como el uso de software especializado para descifrar contraseñas, intentos repetidos de adivinar la contraseña o la interceptación de contraseñas mediante técnicas de hacking. Este tipo de ataque puede ser especialmente peligroso ya que puede permitir a los atacantes acceder a información confidencial o llevar a cabo actividades maliciosas en nombre del usuario legítimo.

Ataque DDoS: Un ataque DDoS, o ataque distribuido de denegación de servicio, es un tipo de ciberataque que intenta hacer que un sitio web o recurso de red no esté disponible colapsándolo con tráfico malintencionado para que no pueda funcionar correctamente [21].

En un ataque distribuido de denegación de servicio (DDoS), un atacante sobrecarga su objetivo con tráfico de Internet no deseado para que el tráfico normal no llegue a su destino previsto [21].

Configuración de seguridad incorrecta: Son fallos muy comunes, debido a que pueden encontrarse a nivel de la plataforma, el servidor web, el servidor de aplicaciones, la base de datos o, incluso, el código fuente del software [22].

2.15 SEGURIDAD FÍSICA Y LÓGICA EN INFORMÁTICA

SEGURIDAD FÍSICA

Son todas aquellas medidas que se pueden adoptar para proteger físicamente los dispositivos electrónicos que almacenan información. Esto engloba desde los ordenadores de la empresa hasta las memorias flash o los discos duros extraíbles [24].

Este es un aspecto que a menudo se pasa por alto cuando se trata de la seguridad informática en general. Muchas organizaciones a menudo toman medidas para prevenir o detectar el acceso no autorizado o la denegación de servicio, pero rara vez evitan que

los atacantes intenten acceder físicamente al lugar de operaciones donde se encuentren las impresiones del sistema [24].

SEGURIDAD LÓGICA INFORMÁTICA

La seguridad lógica informática es una referencia a la protección por el uso de software en una organización, e incluye identificación de usuarios y contraseñas de acceso, autenticación, derechos de acceso y niveles de autoridad. Estas medidas son para asegurar que sólo los usuarios autorizados son capaces de realizar acciones o acceder a información en una red o un equipo concreto [25].

2.16 SEGURIDAD ORGANIZACIÓN

La seguridad puede ayudar a las organizaciones a convivir y minimizar sus riesgos y no a eliminarnos, lo que es imposible (si no hay riesgo no hay negocio, por definición), por lo que, en realidad, y aplicada de la forma adecuada, se convierte en un elemento fundamental para colaborar en el desarrollo del negocio [23].

2.16.1 VALORACIÓN DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN

Un riesgo es una combinación de las consecuencias que se presentarían después de la ocurrencia de un evento indeseado y de su probabilidad de ocurrencia. La valoración del riesgo cuantifica o describe cualitativamente el riesgo y permite a los propietarios de los activos priorizar los riesgos de acuerdo con su gravedad percibida u otros criterios establecidos.

La valoración del riesgo consta de las siguientes actividades:

- Análisis del riesgo
- Identificación del riesgo
- Estimación del riesgo
- Evaluación del riesgo

2.16.2 IDENTIFICACIÓN DE AMENAZAS

Se deben identificar las amenazas y sus orígenes. Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas, por lo tanto, a las organizaciones.

2.16.3 IDENTIFICACIÓN DE VULNERABILIDADES

Se debe identificar las vulnerabilidades que pueden ser explotadas por las amenazas para causar daños a los activos o a la institución.

La sola presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que haya una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza correspondiente puede no requerir de la implementación de un control, pero es recomendable reconocerla y monitorearla para determinar los cambios.

2.16.4 IDENTIFICACIÓN DE EXISTENCIA DE CONTROLES

La identificación de los controles existentes para evitar trabajo o costos innecesarios, por ejemplo, en la duplicación de los controles. Además, mientras se identifican los controles existentes es recomendable hacer una verificación para garantizar que los controles funcionan correctamente – una referencia a los reportes de auditoría del SGSI**.**

2.16.5 EVALUACIÓN DEL RIESGO

Proceso de comparación del riesgo estimado contra un criterio de riesgo calculado dado para determinar la importancia del riesgo. El grado del riesgo es expresado numéricamente basado en las medidas del valor de los activos de información, el impacto de la amenaza y el alcance de la vulnerabilidad**.**

2.16.6 MONITOREO Y REVISIÓN DE LOS FACTORES DE RIESGO

Los riesgos no son estáticos. Las amenazas, las vulnerabilidades, la probabilidad o las consecuencias pueden cambiar abruptamente sin ninguna indicación. Por ende, es necesario el monitoreo constante para detectar estos cambios.

Las organizaciones deberían garantizar el monitoreo continuo de los siguientes aspectos:

- La gestión de riesgos, es decir, activos que ahora se consideran parte de la evaluación y mitigación de riesgos.
- La identificación de nuevas amenazas y la probabilidad de que se exploten vulnerabilidades existentes.
- También se menciona la importancia de identificar las vulnerabilidades que están expuestas a nuevas amenazas y el incremento en el impacto o consecuencias de las mismas.
- Se destaca la importancia de considerar los incidentes de seguridad de la información en la gestión del riesgo.

2.17 PROTECCIÓN DE INFORMACIÓN

Los tres principios de la seguridad informática son:

1 º principio de la seguridad informática

“El intruso al sistema utilizará cualquier artilugio que haga más fácil su acceso y posterior ataque” [26].

2º principio de la seguridad informática

“Los datos deben protegerse sólo hasta que pierdan su valor” [26].

3 º principio de la seguridad informática

“Las medidas de control se implementan para ser utilizadas de forma efectiva.

Deben ser eficientes, fáciles de usar y apropiadas al medio” [26].

2.18 POLÍTICAS DE SEGURIDAD

CONTROLES DE ACCESO

Los controles de acceso pueden implementarse a nivel de Sistema Operativo, de sistemas de información, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

IDENTIFICACIÓN Y AUTENTIFICACIÓN

Se constituye en la primera línea de defensa para la mayoría de los sistemas computarizados, al prevenir el ingreso de personas no autorizadas y es la base para casi todos los controles de acceso, además permite efectuar un seguimiento de las actividades de los usuarios.

LIMITACIONES A LOS SERVICIOS

Las limitaciones a los servicios son controles que se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o que han sido preestablecidos por el administrador del sistema.

2.19 HERRAMIENTAS DE EVALUACIÓN DE VULNERABILIDADES

Conocer qué herramienta se ajusta mejor a mis necesidades en cuanto a consumo de recursos, opciones de escaneo, y cantidad de malware encontrado en un diagnóstico.

Intruso	Es un escáner de vulnerabilidades proactivo que lo analiza tan pronto como se liberan nuevas vulnerabilidades. Además, cuenta con más de 10,000 controles de seguridad históricos, incluidos WannaCry, Heartbleed y SQL Injection.
AppTrana	E s un escáner de vulnerabilidades de aplicaciones web automatizado que detecta e informa vulnerabilidades según el top 10 de OWASP. CARACTERÍSTICAS • Rastreador de la nueva era para escanear aplicaciones de una sola página. • Función de pausa y reanudación

	• Pruebas de penetración manual adicionales y publicar el informe en el mismo panel • Solicitud de prueba de concepto para proporcionar evidencia de la vulnerabilidad informada y eliminar falsos positivos • Integración opcional con Indusface WAF para proporcionar parches virtuales instantáneos con cero falso positivo
SolarWinds	Proporciona detección de vulnerabilidades de red con su administrador de configuración de red. Sus capacidades de automatización de red implementarán rápidamente actualizaciones de firmware en dispositivos de red. Tiene funcionalidades para monitorear, administrar y proteger configuraciones de red. La herramienta simplificará y mejorará el cumplimiento de la red
Acunetix	Es un escáner de vulnerabilidades web totalmente automatizadas que detecta e informa sobre más de 4500 vulnerabilidades de aplicaciones web, incluidas todas las variantes de SQL Injection y XSS.
Netsparker	Es un escáner automatizado de precisión absoluta que identificará vulnerabilidades como la inyección SQL y la secuencia de comandos entre sitios en aplicaciones web y API web.
Tripwire IP360	Es su principal producto de gestión de vulnerabilidades. • Tripwire IP360 es la solución de evaluación de vulnerabilidades más importante del mundo que utilizan varias agencias y empresas para administrar sus riesgos de seguridad. • Utilizando los estándares abiertos, tripwire IP360 permite la integración de la gestión de riesgos y la vulnerabilidad en múltiples procesos del negocio. • Tripwire IP360 ofrece una solución de bajo ancho de banda, perfil de red sin perturbaciones y sin agentes • Al utilizar una vista amplia de las redes, tripwire IP360 detecta todas las vulnerabilidades, aplicaciones, configuraciones, hosts de red, etc.

Tabla 1. Herramientas de evaluación de vulnerabilidades

2.20 QUE ES UN SGSI (SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN)

Es un conjunto de políticas, procedimientos, controles y tecnologías diseñadas para proteger la información de una organización y minimizar los riesgos de seguridad de la información. El objetivo de un SGSI es establecer un marco de trabajo para la gestión de la seguridad de la información que permita a la organización identificar, evaluar y gestionar los riesgos de seguridad de la información.

2.21 GUÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE TECNOLOGIAS Y LA SOCIEDAD DE LA INFORMACION DEL ECUADOR.

Basada en la iso 27005 esta guia presenta un conjunto de y directrices para la gestión de riesgos de seguridad de la información en las organizaciones y tiene como objetivo ayudar a las organizaciones a identificar, evaluar y gestionar los riesgos de seguridad de la información que pueden enfrentar en su día a día.

La guía establece un marco de trabajo para la gestión de riesgos de seguridad de la información, que incluye los siguientes pasos:

1. Identificación de los activos de información: se trata de identificar todos los activos de información de la organización y su importancia para el negocio.
2. Análisis de riesgos: se analizan los riesgos a los que están expuestos los activos de información identificados en el paso anterior.
3. Evaluación de riesgos: se evalúan los riesgos identificados para determinar su probabilidad y su impacto en el negocio.
4. Tratamiento de riesgos: se definen las medidas necesarias para tratar los riesgos identificados. Estas medidas pueden ser la aceptación del riesgo, la transferencia del riesgo, la reducción del riesgo o la eliminación del riesgo.
5. Implementación de medidas de seguridad: se implementan las medidas de seguridad necesarias para reducir los riesgos identificados a un nivel aceptable.
6. Monitoreo y revisión: se monitorean continuamente los riesgos y las medidas de seguridad implementadas para asegurarse de que se mantengan actualizados y efectivos.

CAPÍTULO 3

APLICACION DE LA GUIA PARA LA GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACION

3.1 ESTABLECIMIENTO DEL CONTEXTO

3.1.1 ESTABLECER CRITERIOS BÁSICOS PARA LA GESTIÓN DE RIESGO

A través del uso de la guía para la gestión de riesgos de la información se establecen los siguientes criterios:

1. Identificación de amenazas
2. Identificación de vulnerabilidades
3. Probabilidad de ocurrencia de que la amenaza se cumpla
4. Probabilidad de ocurrencia de una vulnerabilidad pese a los controles existentes
5. Identificación de los controles existentes
6. Análisis de los riesgos residuales
7. Tratamiento del riesgo

3.1.2 DEFINIR ALCANCE Y LIMITES DE LA GESTIÓN DE RIESGO

El estudio se circunscribe en el edificio matriz de EMAPAL, se analizarán las áreas física, lógica y organizacional. El análisis se realizará de manera limitada dependiendo del nivel de acceso que nos otorgue la empresa, donde los parámetros a continuación presentados vienen dados por parte de la guía de para la gestión de riesgos de la información.

El análisis cubrirá:

- La Identificación de Activos de Información
- La valoración de dichos activos
- Las amenazas y vulnerabilidades
- Los controles existentes
- La evaluación de riesgos

En calidad de recomendación personal se incluirá:

- El tratamiento de riesgos
- Aceptación de riesgos

No se cubrirán en el análisis los siguientes aspectos; ya que dependen del manejo interno de la empresa, en función de la importancia y el costo que se les da a los activos, además se dará una copia de la guía al encargado del área de TI quien debería comunicar los riesgos a instancias más elevadas en la empresa y a su vez la monitorización y revisión dependerá del personal que labora en la empresa:

- Identificación y valoración de las consecuencias
- Valoración de incidentes
- Comunicación de riesgos
- Monitorización y revisión de riesgos

3.1.3 ESTABLECER UNA ORGANIZACIÓN PARA LA OPERACIÓN DE SGSI

La organización no cuenta con una estructura de operación para sgrsi, además al nosotros ser únicamente dos individuos que actúan fuera de la organización con acceso limitado tampoco se puede establecer una sgsi.

3.2 VALORACIÓN DEL RIESGO

3.2.1 IDENTIFICAR LOS ACTIVOS DE INFORMACIÓN

Se procede a realizar el levantamiento de información de los activos sus funciones y ubicación. Además, se pondera el valor del activo (VA) teniendo en cuenta el impacto de su perdida a través de criterios de confidencialidad, integridad y disponibilidad en una escala del 1 al 3, este calculo viene determinado por la guia de gestión de riesgos de la informacion.

$$\boldsymbol{VA = (C + I + D)/3}$$

CONFIDENCIALIDAD	CRITERIO
ALTO 3	La divulgación no autorizada de la información tiene un efecto crítico para la institución
MEDIO 2	La divulgación no autorizada de la información tiene un efecto limitado para la institución

BAJO 1	La divulgación de la información no tiene ningún efecto para la institución
INTEGRIDAD	**CRITERIO**
ALTO 3	La destrucción o modificación no autorizada de la información tiene un efecto severo para la institución
MEDIO 2	La destrucción o modificación no autorizada de la información tiene un efecto considerable para la institución
BAJO 1	La destrucción o modificación de la información tiene un efecto leve para la institución
DISPONIBILIDAD	**CRITERIO**
ALTO 3	La interrupción al acceso de la información o los sistemas tienen un efecto severo para la institución
MEDIO 2	La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la institución
BAJO 1	La interrupción al acceso de la información o los sistemas tienen un efecto mínimo para la institución

Tabla 2. Criterios de Valoracion de impacto del activo en base a la confidencialidad, integridad y disponibilidad

IDENTIFICACION DE ACTIVOS					VALORACIÓN DE IMPACTO			
N	Nombre	Descripción	Ubicación	Soporte	C: Confidencialidad I: Integridad D: Disponibilidad			
					C	I	D	VA
E1	Proliant Ml150 G6	GIS	Rack 1 Centro de datos 1	Logico y Fisico	3	3	2	2,67
E2	HP ML350 G8 V2	Active directory	Rack 1 Centro de datos 1	Logico y Fisico	3	2	1	2,00
E3	HP ML350 G8 V2	Documentacion Historica	Rack 1 Centro de datos 1	Logico y Fisico	2	2	1	1,67
E4	Proliant dl360 gen10	Bases de datos y gestion documental	Rack 1 Centro de datos 1	Logico y Fisico	3	3	3	3,00
E5	Proliant dl380 gen9	Aplicativo sistema ERP	Rack 1 Centro de datos 1	Logico y Fisico	1	2	3	2,00
E6	HP Compaq Pro 6300	Registro de asistencias	Departamento de TI	Logico y Fisico	2	1	1	1,33
E7	HP ML115 G1	Almacenamiento documental historico	Departamento de TI	Logico y Fisico	2	2	1	1,67

E8	Ubuntu 18.04	OS del Server	Proliant dl360 gen10	Logico	1	3	3	2,33
E9	Ubuntu 18.04	OS del Server	Proliant dl380 gen9	Logico	1	3	3	2,33
E10	Windows Server 2008	OS del Server	HP ML350 G8 V2	Logico	1	3	3	2,33
E11	Windows Server 2008	OS del Server	HP ML350 G8 V2	Logico	1	3	3	2,33
E12	Windows Server 2003	OS del Server	Proliant dl360 gen10	Logico	1	3	3	2,33
E13	Windows Server 2003	OS del Server	HP ML115 G1	Logico	1	3	3	2,33
E14	Windows 10	OS del Server	HP Compaq Pro 6300	Logico	1	3	3	2,33
E15	Postgis 2.2	Base de datos Geografica	Proliant Ml150 G6	Logico	3	3	2	2,67
E16	Postgresql 9.5	Base de datos	Proliant dl360 gen10	Logico	3	3	3	3,00
E17	SIIIM	Sistema ERP donde se desarrolla la actividad de la empreza	Proliant dl380 gen9	Logico	1	2	3	2,00
E18	SOPHOS SG 230 rev 1	Firewall	Rack 1 Centro de datos 1	Logico y Fisico	2	2	2	2,00
E19	HP MSR 900	Proveedor del servicio de internet	Rack 1 Centro de datos 1	Logico y Fisico	1	1	3	1,67
E20	HPE OfficeConect 1920S Series Switch	Administra la conexión de los servidores	Rack 1 Centro de datos 1	Logico y Fisico	1	1	3	1,67
E21	HPE OfficeConect 1920S Series Switch	Servicio de Internet Planta Baja	Rack 2 Centro de datos 1	Logico y Fisico	1	1	3	1,67
E22	HPE OfficeConect 1920S Series Switch	Servicio de Internet Planta Baja	Rack 2 Centro de datos 1	Logico y Fisico	1	1	3	1,67
E23	PE Aruba Instant On 1930 24G 4SFP/SFP	Usado en telefonia IP de la planta baja	Rack Centro de datos 2	Logico y Fisico	1	1	2	1,33

E24	HPE OfficeConect 1920S Series Switch	Conecta el servicio de internet con los pisos superiores y servicio a la planta baja	Rack Centro de datos 2	Logico y Fisico	1	1	3	1,67
E25	PE Aruba Instant On 1930 24G 4SFP/SFP	Usado en telefonia IP del piso 1	Rack Oficina Juridica	Logico y Fisico	1	1	2	1,33
E26	HPE OfficeConect 1920S Series Switch	Brinda servicio al piso 1	Rack Oficina Juridica	Logico y Fisico	1	1	3	1,67
E27	PE Aruba Instant On 1930 24G 4SFP/SFP	Usado en telefonia IP del piso 2	Rack Archivo	Logico y Fisico	1	1	2	1,33
E28	HPE OfficeConect 1920S Series Switch	Brinda servicio al piso 2	Rack Archivo	Logico y Fisico	1	1	3	1,67
E29	APX 530	Conectividad Inalambrica Departamento de Ti	Cieloraso departamento de TI	Logico y Fisico	1	1	2	1,33
E30	AP 55C	Conectividad Inalambrica	Cieloraso planta baja	Logico y Fisico	1	1	2	1,33
E31	AP 55C	Conectividad Inalambrica	Cieloraso piso 1	Logico y Fisico	1	1	2	1,33
E32	AP 55C	Conectividad Inalambrica	Cieloraso piso 2	Logico y Fisico	1	1	2	1,33
E33	Cableado Vertical Fibra Optica	Llevar internet desde el centro de datos a los switches de cada piso y la antena	Ducto	Logico y Fisico	1	1	3	1,67
E34	Cableado Horizontal UTP CAT 6/ 6A	Llevar internet desde el switch correspodiente de cada piso a	Edificio	Logico y Fisico	1	1	3	1,67

E35	VLANS	Agrupacion de dispositivos en subredes especificas	Entidad Logica de Red	Logico	3	1	3	2,33
E36	Redes Wireless	Redes WiFi	Puntos de Acceso Inalambrico	Logico	1	1	2	1,33
E37	Ubiquiti NanoStation M5 Loc0	Conecta con los puntos equidistantes de la empresa	Azotea	Logico y Fisico	1	1	2	1,33
E38	Panasonic KX-NS500	Sirve de centralita telefonica	Rack Centro de datos 2	Logico y Fisico	1	1	2	1,33
E39	Eaton 906 IIS	Sistemas de alimentacion ininterrumpida	Rack 1 Centro de datos 1	Fisico	1	1	1	1,00
E40	APC SRT2200XLA	Sistemas de alimentacion ininterrumpida	Centro de datos 1	Fisico	1	1	1	1,00
E41	APC SRT2200XLA	Sistemas de alimentacion ininterrumpida	Rack Centro de datos 2	Fisico	1	1	1	1,00
E42	Forza FDC-003K	Fuente de Poder ininterrumpible en caso de falla del suministro electrico	Departamento de TI	Fisico	1	1	1	1,00
E43	emapal.gob.ec/ 207.174.XXX. XXX/egob, edoc, etc	Funcionamiento a nivel de la Red y servicio a traves de una IP/Dominio unica	nic.ec	Logico	1	2	3	2,00
E44	www.emapal.gob.ec	Proporcionar informacion y/o servicios al publico	nic.ec	Logico	1	2	1	1,33

E45	Correo Masivo	Distribuir la emision de facturas o correos masivos	Tercerizada con Gmail	Logico	2	2	2	2,00
E46	Correo Corporativo	Uso de correo corporativo para empleados o areas de la empresa	nic.ec	Logico	2	2	2	2,00
E47	Consolas	Permiten el control de los diferentes activos de la empresa	Dispositivo o servicio respectivo	Logico	3	3	3	3,00
E48	Respaldo disco duro externo	Respaldo Acumulativo de la base de datos y del sistema ERP SIIM	Disco duro externo	Logico y Fisico	3	3	2	2,67
E49	Respaldo Telconet	Respaldo incremental de la base de datos y del sistema ERP SIIM	Telconet	Logico	3	3	2	2,67
E50	Kaspersky	Antivirus Institucional	Terminales de la empresa	Logico	1	1	1	1,00
E51	Biometrico	Registrar la asistencia de los empleados	Al lado de la puerta de acceso al centro de datos 1	Fisico y Logico	2	2	2	2,00
E52	Biotime 8.0	Registro de asistencia mediante biometria	HP Compaq Pro 6300	Logico	2	2	2	2,00
E53	Camaras de seguridad	Registrar la actividad en la empresa	Todo el edificio matriz	Fisico	1	1	1	1,00
E54	DVR modelo desconocido	Graba la actividad de las camaras de seguridad	Direccion administrativa	Fisico y Logico	2	2	1	1,67

E55	Rack 1 Centro de Datos 1	Alojamiento de equipos especializados	Centro de datos 1	Fisico	1	1	1	1,00
E56	Rack 2 Centro de datos 2	Alojamiento de equipos especializados	Centro de datos 1	Fisico	1	1	1	1,00
E57	Rack Centro de Datos 2	Alojamiento de equipos especializados	Centro de datos 2	Fisico	1	1	1	1,00
E58	Rack Piso 1	Alojamiento de equipos especializados	Oficina Juridica Piso 2	Fisico	1	1	1	1,00
E59	Rack Piso 2	Alojamiento de equipos especializados	Archivo Piso 3	Fisico	1	1	1	1,00
E60	Edificio Matriz	Edificio Matriz	Av Ernesto Che Guevara y Av 16 de Abril, Azogues	Fisico	1	3	3	2,33
E61	Centro de Datos 1	Alojamiento de equipos especializados	Edificio Matriz	Fisico	1	3	3	2,33
E62	Centro de Datos 2	Alojamiento de equipos especializados	Edificio Matriz	Fisico	1	3	3	2,33
E63	Oficina de Sistemas	Lugar donde laboran los empleados de Sistemas	Edificio Matriz	Fisico	1	2	2	1,67
E64	Terraza y soporte de la antena	Emplazamiento de la Antena	Edificio Matriz	Fisico	1	2	2	1,67
E65	Computadoras de escritorio	Computadoras de escritorio donde los empleados laboran	Edificio Matriz	Logico , Fisico y Organizacional	2	2	2	2,00

E66	Computadoras portatiles	Computadoras de portatiles donde los empleados laboran	Edificio Matriz	Logico , Fisico y Organizacional	2	2	2	2,00
E67	Funcionarios de Sistemas	Funcionarios de Sistemas	Edificio Matriz	Organizacional	3	2	2	2,33
E68	Funcionarios fuera del área de Sistemas	Funcionarios no concernientes a sistemas	Edificio Matriz	Organizacional	2	1	2	1,67
E69	TIC'S	Ubicación del departamento de sistemas a nivel organizacional	Organigrama Institucional	Organizacional	1	1	1	1,00

Tabla 3. Identificacion y valoracion de activos

3.2.2 IDENTIFICAR LAS AMENAZAS Y LAS VULNERABILIDADES

La guía para la gestión de riesgos de la información determina como vulnerabilidad un punto donde la infraestructura de TI o fallas humanas, y una amenaza la consecuencia de que una vulnerabilidad sea explotada

3.2.3 IDENTIFICAR LOS CONTROLES EXISTENTES

En este punto la guía para la gestión de riesgos de la información establece que se determinen los controles implementados por la empresa EMAPAL con sus activos de TI y en base a estos conocer evaluar en qué medida se mitigan las amenazas y vulnerabilidades las que han sido determinadas en base a entrevistas con el personal de TI y documentación limitada. (Para consultar los controles de manera detallada presentes en la tabla de Controles existenes revisar el Anexo 7)

3.3 IDENTIFICAR CONSECUENCIAS

Debido a la falta de información y acceso directo a los procesos de la empresa, no se pudo identificar las consecuencias reales de un incidente de seguridad de TI ya que dichas consecuencias dependen de como funcione la infraestructura de TI de la empresa.

3.4 VALORAR LAS CONSECUENCIAS

La valoración de las consecuencias es un aspecto importante en la evaluación de riesgos, sin embargo, debido a la falta de conocimiento sobre la situación económica de la empresa y el valor que se les da a los activos de TI, no se puede realizar una valoración precisa.

3.4.1 VALORAR LOS INCIDENTES

La identificación de incidentes es fundamental para realizar un análisis de riesgos, sin embargo, al trabajar únicamente con el departamento de TI y no tener una línea directa con la administración o dirección de la empresa, nose puede garantizar la identificación completa de los mismos.

3.4.2 DETERMINAR EL NIVEL DE ESTIMACION DEL RIESGO

En este punto se evaluarán los riesgos en base a la siguiente escala que viene dada por la propia guia para la gestión de riesgos de la informacion, nosotros al no pertenecer a la institución emplearemos la escala que se brinda en el documento

NIVEL DE AMENAZA	PROBABILIDAD	OCURRENCIA
ALTO 3	>50%	Bajo circunstancias normales
MEDIO 2	=50%	Errores, descuidos, accidentes
BAJO 1	>50%	En rara ocasión

Tabla 4. Calculo de Amenazas

NIVEL DE VULNERABILIDAD	CRITERIO
ALTO 3	No existen medidas de seguridad implementadas para prevenir la ocurrencia de la amenaza
MEDIO 2	Existen medidas de seguridad implementadas que no reducen la probabilidad de la amenaza a un nivel aceptable
BAJO 1	La medida de seguridad es adecuada

Tabla 5. Calculo de vulnerabilidades

3.4.3 EVALUAR EL RIESGO

Para evaluar el riesgo se realizará el siguiente cálculo que viene dado por la guia para la gestión de riesgos de la informacion:

$$Nivel\ de\ riesgo = VA * Nivel\ de\ Amenaza * Nivel\ de\ Vulnerabilidad$$

La guia para la gestión de riesgos de la informacion establece que el criterio de evaluación de riesgo se realizará en una puntuación de entre 1 y 27 a través de un semáforo donde los riesgos se segmentarán de la siguiente forma:

NIVEL DE RIESGO	
1 – 3,99	Riesgo BAJO
4 – 8,99	Riesgo MEDIO
9 – 27	Riesgo ALTO

Tabla 6. Nivel del Riesgo (Guia para la gestión de riesgos de la informacion)

Por efectos de presentación la tabla de Evaluacion del riesgo se presenta en un formato reducido (Para revisar la tabla de manera completa consultar el Anexo 8).

EVALUACION DEL RIESGO SEGÚN LOS PROCESOS Y CONTROLES EXISTENTES		
Proceso	**Calculo del riesgo**	**Nivel del riesgo**
Infraestructura	7,96	MEDIO
Sistemas Operativos	14,27	ALTO
Bases de Datos	17,68	ALTO
ERP	Indeterminado	Indeterminado
Firewall	2,00	BAJO
Redes	2,91	BAJO

Telefonia	3,34	MEDIO
Unit Power Suplies	3,50	MEDIO
Dominos/Subdominios	12,00	ALTO
Pagina Web	5,59	MEDIO
Correo Masivo	2,50	BAJO
Correo Corporativo	5,50	MEDIO
Consolas	4,00	MEDIO
Backups	5,34	MEDIO
Antivirus	1,00	BAJO
Asistencia	2,75	BAJO
Seguridad	7,75	MEDIO
Racks	1,79	BAJO
Ubicación Fisica	7,68	MEDIO
Terminales de los Empleados	11,24	ALTO
Talento Humano	9,23	ALTO
Estructura Organizacional	9,00	ALTO

Tabla 7. Evaluacion del riesgo según los procesos y controles existentes

3.5 TRATAMIENTO DEL RIESGO

3.5.1 SELECCIÓN DEL CONTROLES

Al no formar parte de la organización y no tener conocimiento pleno de la capacidad, financiera, operativa y administrativa, este punto del capítulo es de carácter sugestivo a partir, del conocimiento adquirido mediante documentación limitada, el levantamiento de información, entrevistas con el departamento de TI de la empresa y además de nuestro propio conocimiento.

La guia establece que los controles a implementarse, pueden ser Preventivos, para anticipar eventos no deseados y Correctivos para corregir eventos no deseados.

La implementación de controles permite la reducción en el nivel de amenaza, como de vulnerabilidades y por consiguiente intentar disminuir en uno el Nivel del riesgo.

Por efectos de presentación la tabla de Tratamiento de Riesgos se presenta a continuación en formato reducido (Para revisar la tabla de manera completa dirigirse al anexo 9).

EVALUACION DEL RIESGO SEGÚN LOS PROCESOS Y CONTROLES SUGERIDOS		
Proceso	**Calculo del riesgo**	**Nivel del riesgo**
Infraestructura	2,75	BAJO
Sistemas Operativos	2,62	BAJO
Bases de Datos	2,42	BAJO
ERP	Indeterminado	Indeterminado
Firewall	2,67	BAJO
Redes	1,76	BAJO
Telefonia	2,00	BAJO
Unit Power Suplies	1,13	BAJO
Dominos/Subdominios	1,00	BAJO
Pagina Web	1,73	BAJO
Correo Masivo	1,50	BAJO
Correo Corporativo	2,00	BAJO
Consolas	2,00	BAJO
Backups	2,77	BAJO
Antivirus	2,67	BAJO
Asistencia	2,04	BAJO
Seguridad	1,81	BAJO
Racks	1,07	BAJO

Ubicación Fisica	2,45	BAJO
Terminales de los Empleados	2,01	BAJO
Talento Humano	1,95	BAJO
Estructura Organizacional	1,34	BAJO

Tabla 8. Evaluacion del riesgo según los procesos y controles sugeridos

3.6 ACEPTACION DEL RIESGO

3.6.1 ACEPTAR EL RIESGO

En concordancia con lo dicho en el punto anterior al no pertenecer a la organización no se puede dar un criterio formal de aceptación de riesgos en base al impacto que puedan tener en los activos de TI, sin embargo, se optó por tratar los riesgos catalogados como ALTOS y MEDIOS y aceptar los de riesgos de nivel BAJO.

3.6.2 COMUNICACIÓN DEL RIESGO

Al tratar únicamente con el personal del área de TI como parte involucrada de la organización durante la realización de este estudio los resultados del análisis de los riesgos de los activos de TI serán comunicados únicamente a este nivel organizacional de la EMAPAL se comunicará el análisis de los riesgos de los activos de TI únicamente a este departamento, Se espera que se pueda proporcionar un panorama de las vulnerabilidades y amenazas que presenta la empresa, y que conjuntamente con los encargados de la toma de decisiones se mitigue en cierta medida los riesgos presentes.

3.6.3 MONITOREO Y REVISIÓN DEL RIESGO

El monitoreo del riesgo dependerá única y exclusivamente del personal de la empresa y las decisiones que tomen los encargados de la misma.

CONCLUSIONES Y RECOMENDACIONES

1. El conocimiento sistémico de vulnerabilidades es fundamental para proteger la información confidencial y garantizar la seguridad de los sistemas informáticos en el mundo actual. Es imprescindible tomar en cuenta los hallazgos al desarrollar cualquier tipo de sistema informático o estrategia de protección de datos, ya que una comprensión adecuada de estos conceptos puede marcar la diferencia entre un sistema seguro y uno vulnerable a amenazas cibernéticas. En consecuencia, se puede garantizar la integridad de los sistemas y la protección de la información confidencial en un entorno cada vez más conectado y digitalizado.
2. Se ha llevado a cabo el levantamiento de información del departamento de TI y de los activos de información de la empresa EMAPAL utilizando diversas técnicas, como encuestas, observación, entrevistas y documentación limitada. Sin embargo, debido a las restricciones propias de la empresa frente a terceros, especialmente en el área lógica y operativa, el levantamiento de información ha sido limitado. A pesar de ello, se ha logrado obtener la información necesaria que permitió analizar algunas amenazas y vulnerabilidades de dichos activos de manera efectiva, para recomendar acciones de mejora que el personal del departamento de TI y de la EMAPAL deberían acoger.
3. La implementación de la guía de gestión de riesgos de seguridad de la información ha permitido identificar múltiples vulnerabilidades y amenazas en la infraestructura de la empresa. Las principales de las que podemos hablar son:
   Los servidores presentan cierto grado de obsolescencia y utilizan software sin soporte oficial, lo que podría resultar en fallas en sus componentes. Además, los switches de los pisos 1 y 2 no están ubicados adecuadamente y las VLAN no están completamente configuradas, lo que representa un riesgo de seguridad. Las UPSs tienen una vida útil degradada y se han encontrado vulnerabilidades en los subdominios de EMAPAL. El manejo de las cámaras de seguridad y DVR representa un riesgo elevado debido a la falta de capacitación y el uso de direcciones IP públicas además de ser manejadas por el área Administrativa. La oficina de TI se encuentra en un lugar vulnerable y las terminales de los empleados pueden presentar fallos debido a su antigüedad y sistema operativo sin soporte. Se ha identificado que algunos comportamientos de los empleados comprometen la confidencialidad e integridad de la información de la empresa. Finalmente se determinó que los centros de datos no tienen seguridad ni la

infraestructura adecuada lo que puede llegar a comprometer los equipos que operan dentro de ellos.

4. En base a la guía para la gestión de riesgos de seguridad de la información, se han identificado varios riesgos en la infraestructura de la empresa y se han brindado diversas soluciones de manera general como la actualización de equipos y sistemas operativos, la configuración de las VLANs y la ocultación de las WLANS, el manejo adecuado de cámaras y DVR, el respaldo físico a través de un servidor y el uso de un generador para garantizar la operatividad plena de todas las áreas de la empresa. Se recomienda contratación de personal adicional para gestionar de manera adecuada las diferentes actividades de TI, además es importante implementar un plan de continuidad frente a la ausencia permanente del personal de TI indispensable, esto para garantizar la operatividad de la empresa. Todas estas recomendaciones buscan mitigar los riesgos y garantizar la seguridad de la información de la empresa. Para conocer de manera detallada los 524 controles correctivos recomendados revisar el Anexo 10, Tratamiento de Riesgos.

REFERENCIAS BIBLIOGRÁFICAS

[1]"Seguridad informática - Wikipedia, la enciclopedia libre", *Es.wikipedia.org*, 2022. [Online]. Disponible: https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica. [Consulta: 26-abr-2022].

[2]"¿Qué es la Seguridad Informática? | UNIR Ecuador", *Universidad Virtual. | UNIR Ecuador - Maestrías y Grados virtuales*, 2022. [En línea]. Disponible: https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/#:~:text=La%20seguridad%20inform%C3%A1tica%20%E2%80%94tambi%C3%A9n%20llamada,procesos%20por%20personas%20no%20autorizadas. [Consulta: 26-abr-2022].

[3]"Auditoría de seguridad informática, ¿en qué consiste?", *UNIR*, 2022. [En línea]. Disponible: https://www.unir.net/ingenieria/revista/auditoria-seguridad-informatica/. [Consulta: 26-abr-2022].

[4]"Análisis de riesgo - Wikipedia, la enciclopedia libre", *Es.wikipedia.org*, 2022. [Online]. Disponible: https://es.wikipedia.org/wiki/An%C3%A1lisis_de_riesgo. [Consulta: 26-abr-2022].

[5]"Significado de Vulnerabilidad", *Significados* , 2022. [En línea]. Disponible: https://www.significados.com/vulnerabilidad/. [Consulta: 26-abr-2022].

[6]A. TEAM, "Tipos de Vulnerabilidades y Amenazas informáticas", *Ambit-bst.com* , 2022. [Online]. Disponible: https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas. [Consulta: 26-abr-2022].

[7]S. Figueiras, "¿Qué es el Pentesting?", *Ceupe.mx* , 2022. [En línea]. Disponible: https://www.ceupe.mx/blog/que-es-el-pentesting.html. [Consulta: 26-abr-2022].

[8] "Definición de guía - Qué es, Significado y Concepto." [Online]. Available: ttps://definicion.de/guia/. [Accessed: 08-Feb-2023].

*[*9] S. D. Diaz, "Pruebas de seguridad en aplicaciones web como imperativo en la calidad de desarrollo del software,"

[10] L. Reyes-Ruiz and F. Carmona Alvarado, "La investigación documental para la comprensión ontológica del objeto de estudio," *Ediciones Universidad Simón Bolívar*, Barranquilla, Oct. 2020.

[11] "Seguridad", Wikipedia, 29 de septiembre de 2020. https://es.wikipedia.org/wiki/Seguridad

[12] Colaboradores de los proyectos Wikipedia, "tipo de auditoría para sistemas de información," Wikipedia.org, 03 de febrero de 2007. https://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica

[13] Colaboradores de los proyectos Wikipedia, "tipo de auditoría para sistemas de información," Wikipedia.org, 03 de febrero de 2007. https://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica

[14] Colaboradores de los proyectos Wikipedia, "tipo de auditoría para sistemas de información," *Wikipedia.org*, Feb. 03, 2007. https://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica (accessed Feb. 07, 2023).

[15] "Área Académica: Sistemas Computacionales Tema: Auditoría Informática Profesor(a):Academia de Administración y Sociales."

[16] “Las 9 Medidas De Seguridad Informática Básicas Para Proteger La Empresa.” [Online]. Available: https://www.datos101.com/blog/medidas-de-seguridad-informatica/. [Accessed: 11-Feb-2023].

[17] “¿Qué es el spam? Definición y cómo protegerte | ESET.” [Online]. Available: https://www.eset.com/es/caracteristicas/spam/. [Accessed: 11-Feb-2023].

[18] “¿Qué es botnet? - Definición y cómo funciona | Proofpoint ES.” [Online]. Available: https://www.proofpoint.com/es/threat-reference/botnet. [Accessed: 11-Feb-2023].

[19] “¿Qué es el malware? Definición y cómo saber si está infectado | Malwarebytes.” [Online]. Available: https://es.malwarebytes.com/malware/. [Accessed: 11-Feb-2023].

[20] “Inyección SQL - Wikipedia, la enciclopedia libre.” [Online]. Available: https://es.wikipedia.org/wiki/Inyección_SQL. [Accessed: 11-Feb-2023].

[21] “¿Qué es un ataque DDoS? | Akamai.” [Online]. Available: https://www.akamai.com/es/our-thinking/ddos. [Accessed: 11-Feb-2023].

[22] “¿Qué es la configuración de seguridad incorrecta?” [Online]. Available: https://keepcoding.io/blog/que-es-la-configuracion-de-seguridad-incorrecta/. [Accessed: 11-Feb-2023].

[23] “Seguridad organizacional - Seguritecnia.” [Online]. Available: https://www.seguritecnia.es/tecnologias-y-servicios/seguridad-organizacional_20160910.html. [Accessed: 08-Feb-2023].

[24] “Seguridad física informática, ¿una asignatura pendiente? | VIU.” [Online]. Available: https://www.universidadviu.com/es/actualidad/nuestros-

expertos/seguridad-fisica-informatica-una-asignatura-pendiente. [Accessed: 08-Feb-2023].

[25] “Conceptos sobre seguridad lógica informática | VIU.” [Online]. Available: https://www.universidadviu.com/es/actualidad/nuestros-expertos/conceptos-sobre-seguridad-logica-informatica. [Accessed: 08-Feb-2023].

[26] L. I. Rosalba, C. Meza, and P. 41, “UNIDAD IV SEGURIDAD LÓGICA 4.1 INTRODUCCIÓN A LA SEGURIDAD LÓGICA.”

ANEXOS

ANEXO 1: ENCUESTA AL PERSONAL DE TI

Seguridad física.

Este cuestionario verifica la seguridad física de las instalaciones que utiliza el área de sistemas, ya que de esto depende la continuidad de los servicios que presta el área a la organización, en cuanto a necesidades de información.

1. ¿Se han adoptado medidas de seguridad en el departamento de sistemas de información?
SI ( ) NO ( )
2. ¿Existen una persona responsable de la seguridad?
SI ( ) NO ( )
3. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?
SI ( ) NO ( )
4. ¿Existe personal de vigilancia en la institución?
SI ( ) NO ( )
5. ¿La vigilancia se contrata?
a) Directamente ( )
b) Por medio de empresas que venden ese servicio ( )
6. ¿Existe una clara definición de funciones entre los puestos clave?
SI ( ) NO ( )
7. ¿Se investiga a los vigilantes cuando son contratados directamente?
SI ( ) NO ( )
8. ¿Se controla el trabajo fuera de horario?
SI ( ) NO ( )
9. ¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas?
SI ( ) NO ( )
10. ¿Existe vigilancia en el departamento de cómputo las 24 horas?
SI ( ) NO ( )

SI ( ) NO ( )
11. ¿Existe vigilancia a la entrada del departamento de cómputo las 24horas?
a) ¿Vigilante? ( )
b) ¿Recepcionista? ( )
c) ¿Tarjeta de control de acceso? ( )
d) ¿Nadie? ( )
12. ¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?
SI ( ) NO ( )
13. Se ha instruido a estas personas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización?
SI ( ) NO ( )
14. El edificio donde se encuentra la computadora está situado a salvo de:
a) ¿Inundación? ( )
b) ¿Terremoto? ( )
c) ¿Fuego? ( )
d) ¿Sabotaje? ( )
15. El centro de cómputo tiene salida al exterior al exterior?
SI ( ) NO ( )

23. ¿Existe alarma para detectar condiciones anormales del ambiente?
A) En el departamento de cómputo? ( )
b) En el cuarto frio? ( )
c) En otros lados ( )
24. ¿La alarma es perfectamente audible?
SI ( ) NO ( )
25. ¿Esta alarma también está conectada)
a)Al puesto de guardias? ( )
b) A la estación de Bomberos? ( )
c) A ningún otro lado? ( )
Otro_____
26. Existen extintores de fuego
a) Manuales? ( )
b) Automáticos? ( )
c) No existen ( )
27. ¿Se ha adiestrado el personal en el manejo de los extintores?
SI ( ) NO ( )
28. ¿Los extintores, manuales o automáticos a base de
TIPO SI NO
a) Agua, ( ) ( )

c) No existen ( )
27. ¿Se ha adiestrado el personal en el manejo de los extintores?
SI ( ) NO ( )
28. ¿Los extintores, manuales o automáticos a base de
TIPO SI NO
a) Agua, ( ) ( )

b) Gas? ( ) ( )
c) Otros ( ) ( )
29. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores?
SI ( ) NO ( )
30. ¿Si es que existen extintores automáticos son activador por detectores automáticos de fuego?
SI ( ) NO ( )
31. ¿Si los extintores automáticos son a base de agua ¿Se han tomado medidas para evitar que el agua cause más daño que el fuego?
SI ( ) NO ( )

32. ¿Si los extintores automáticos son a base de gas, ¿Se ha tomado medidas para evitar que el gas cause más daño que el fuego?
SI ( ) NO ( )
33. ¿Existe un lapso de tiempo suficiente, antes de que funcionen los extintores automáticos para que el personal
a) Corte la acción de los extintores por tratarse de falsas alarmas? SI ( ) NO ( )
b) Pueda cortar la energía Eléctrica SI ( ) NO ( )
c) Pueda abandonar el local sin peligro de intoxicación SI ( ) NO ( )
d) Es inmediata su acción? SI ( ) NO ( )
34. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?
SI ( ) NO ( )
35. ¿Saben que hacer los operadores del departamento de cómputo, en caso de que ocurra una emergencia ocasionado por fuego?
SI ( ) NO ( )
36. ¿El personal ajeno a operación sabe qué hacer en el caso de una emergencia (incendio)?
SI ( ) NO ( )
37. ¿Existe salida de emergencia?
SI ( ) NO ( )
38. ¿Esta puerta solo es posible abrirla:
a) Desde el interior ? ( )
b) Desde el exterior? ( )
c) Ambos Lados ( )

39. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen?
SI ( ) NO ( )
40. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?
SI ( ) NO ( )
41. ¿Se ha tomado medidas para minimizar la posibilidad de fuego:
a) Evitando artículos inflamables en el departamento de cómputo? ( )
b) Prohibiendo fumar a los operadores en el interior? ( )
c) Vigilando y manteniendo el sistema eléctrico? ( )
d) No se ha previsto ( )
42. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo?
SI ( ) NO ( )
43. ¿Se limpia con frecuencia el polvo acumulado debajo del piso falso si existe?
SI ( ) NO ( )
44. ¿Se controla el acceso y préstamo en:
a) Cuarto de Servidores? ( )
b) Área de Desarrollo de Aplicaciones? ( )
45. Explique la forma como se ha clasificado la información vital, esencial, no esencial, etc.

46 Se Cuenta con copias de los archivos en lugar distinto al de la computadora?
SI ( ) NO ( )
47. Explique la forma en que están protegidas físicamente estas copias (bóveda, cajas de seguridad etc.) que garantice su integridad en caso de incendio, inundación, terremotos, etc.
48. ¿Se tienen establecidos procedimientos de actualización a estas copias?
SI ( ) NO ( )
49. Indique el número de copias que se mantienen, de acuerdo con la forma en que se clasifique la información: 0 1 2 3

50 Existe departamento de auditoría interna en la institución?
SI ( ) NO ( )
51. ¿Este departamento de auditoría interna conoce todos los aspectos delos sistemas?
SI ( ) NO ( )
52. ¿Qué tipos de controles ha propuesto?
53. ¿Se cumplen?
SI ( ) NO ( )
54. ¿Se auditan los sistemas en operación?
SI ( ) NO ( )
55. ¿Con que frecuencia?
a) Cada seis meses ( )
b) Cada año ( )
c) Otra (especifique) ( )

56. ¿Cuándo se efectúan modificaciones a los programas, a iniciativa de quién es?

a) Usuario ( )

b) Director de informática ( )

c) Jefe de análisis y programación ( )

d) Programador ( )

e) Otras (especifique) _____

57. ¿La solicitud de modificaciones a los programas se hacen en forma?

a) Oral? ( )

b) Escrita? ( )

En caso de ser escrita solicite formatos.

58. Una vez efectuadas las modificaciones, ¿se presentan las pruebas a los interesados?

SI ( ) NO ( )

59 Existe control estricto en las modificaciones?

SI ( ) NO ( )

60. ¿Existen controles y medidas de seguridad sobre las siguientes operaciones?

¿Cuáles son?

( ) Recepción de documentos_____

( ) Información Confidencial_____

( ) Captación de documentos_____

( ) Cómputo Electrónico_____

( ) Programas_____

( ) Documentos de Salida_____

( ) Archivos Magnéticos_____

( ) Operación del equipo de computación_____

( ) En cuanto al acceso de personal_____

( ) Identificación del personal_____

( ) Policía_____

( ) Seguros contra robo e incendio_____

( ) Cajas de seguridad_____

( ) Otras (especifique)_____

61. ¿Se revisa que tengan la fecha de las modificaciones cuando se hayan efectuado?

SI ( ) NO ( )

62 Si se tienen terminales conectadas, ¿se ha establecido procedimientos de operación?

SI ( ) NO ( )

63. Se verifica identificación:
a) De la terminal ( )
b) Del Usuario ( )
c) No se pide identificación ( )
64. ¿Se ha establecido que información puede ser acezada y por qué persona?
SI ( ) NO ( )
65. ¿Se ha establecido un número máximo de violaciones en sucesión para que la computadora cierre esa terminal y se de aviso al responsable de ella?
SI ( ) NO ( )
66. ¿Se registra cada violación a los procedimientos con el fin de llevar estadísticas y frenar las tendencias mayores?
SI ( ) NO ( )
67. Usted consume alimentos en su lugar de trabajo
Si ( )
No ( )
68. Usted consume bebidas en su lugar de trabajo como: (jugo, agua, energizante, etc.)
Si ( )
No ( )
69. La seguridad del centro de cómputo es automatizado como: (alarma, cámara, etc.)
SI ( )
NO ( )

ANEXO 2: ENCUESTA AL PERSONAL DE LA EMPRESA

ENCUESTA A PERSONAL DE LA EMPRESA EMAPAL EP ACERCA DE SEGURIDAD INFORMATICA RELACIONADA CON LA SEGURIDAD ORGANIZACIONAL

SELECCIONE EL AREA EN LA QUE TRABAJA

- Administrativo
- Comercial
- Financiero
- Gerencial
- Jurídico
- Planificación
- Técnico

¿PARA SUS LABORES DIARIOS DENTRO DE LA EMPRESA USTED UTILIZA LA COMPUTADORA QUE LE HA SIDO PROVEIDA POR EMAPAL?

- Si
- No
- A veces

¿SE REQUIERE UNA CONTRASEÑA PARA INGRESAR A LA COMPUTADORA DONDE USTED TRABAJA?

- Si
- No
- No lo se

¿LA CONTRASEÑA PARA INGRESAR A LA COMPUTADORA DONDE USTED TRABAJA?

- Conoce la contraseña de memoria
- La contraseña esta anotada en su lugar o cerca de su lugar de trabajo (por ejemplo, en una nota, un cuaderno, una agenda, etc.)
- La contraseña esta anotada, pero la lleva con su persona (por ejemplo, en su billetera, una agenda o cuaderno que ande a llevar con usted, etc.)
- La tiene anotada en su teléfono celular
- Mi computadora de trabajo no necesita contraseña para su ingreso

¿NECESITA UN USUARIO PARA ACCEDER A LA PLATAFORMA DE TRABAJO (ACCEDER AL SISTEMA)?

- Si
- No
- No lo se

¿SU USUARIO PARA INGRESAR A LA PLATAFORMA DE TRABAJO (ACCEDER AL SISTEMA) ?:

- El usuario lo conoce de memoria
- El usuario esta anotado en su lugar de trabajo (notas cuadernos agendas etc.)
- El usuario esta anotado, pero lo lleva con su persona (por ejemplo, billetera, una agenda o cuaderno que lleve con usted, etc.)
- Lo tiene anotado en su teléfono celular

- Mi plataforma de trabajo no necesita de un usuario para su ingreso
- Tiene el inicio de sesión ya guardado (se necesita el usuario, pero no es necesario introducirlo porque esta guardada en el inicio de sesión)

¿NECESITA CONTRASEÑA PARA ACCEDER A LA PLATAFORMA DE TRABAJO (ACCEDER AL SISTEMA)?

- Si
- No
- No lo se

¿LA CONTRASEÑA PARA INGRESAR A LA PLATAFORMA DE TRABAJO (ACCEDER AL SISTEMA) ?:

- Conoce la contraseña de memoria
- La contraseña esta anotada en su lugar de trabajo (notas cuadernos agendas etc.)
- La contraseña esta anotada, pero la lleva con su persona (por ejemplo, billetera, una agenda o cuaderno que lleve con usted, etc.)
- La tiene anotada en su teléfono celular
- Mi plataforma de trabajo no necesita contraseña para su ingreso
- Tiene el inicio de sesión ya guardado (usa contraseña, pero no es necesario introducirla porque esta guardada en el inicio de sesión)

¿QUIENES CONOCEN SU CONTRASEÑA PARA EL INGRESO A LA COMPUTADORA DONDE TRABAJA?

- Solo yo
- Compañero/as de trabajo (No cuenta el personal de sistemas para esta respuesta)
- Amigo/as fuera de la empresa
- Pareja
- Familiares
- No se necesita de usuario para ingresar al sistema

¿QUIENES CONOCEN SU USUARIO PARA EL INGRESO A LA PLATAFORMA DE TRABAJO? (AL SISTEMA DE TRABAJO)

- Solo yo
- Compañero/as de trabajo (No cuenta el personal de sistemas para esta respuesta)
- Amigo/as fuera de la empresa
- Pareja
- Familiares
- No se necesita de usuario para ingresar al sistema

¿QUIENES CONOCEN SU CONTRASEÑA PARA EL INGRESO A LA PLATAFORMA DE TRABAJO? (AL SISTEMA DE TRABAJO)

- Solo yo
- Compañero/as de trabajo (No cuenta el personal de sistemas para esta respuesta)
- Amigo/as fuera de la empresa
- Pareja
- Familiares

- No se necesita de usuario para ingresar al sistema

¿USTED COMPARTE SU COMPUTADORA DE TRABAJO EN LA EMPRESA CON ALGUN OTRO COMPAÑERO DE TRABAJO POR MOTIVOS DE TRABAJO?

- Si
- No

¿CONOCE SI ALGUN COMPAÑERO DE TRABAJO TIENE ACCESO A SU COMPUTADORA? (LOS EMPLEADOS DEL AREA DE SISTEMAS NO CUENTAN PARA LA RESPUESTA)

- Si
- No

¿SI USTED DESEA PUEDE TRAER SU PROPIA COMPUTADORA PARA REALIZAR EL TRABAJO EN LA EMPRESA?

- Si
- No

¿ALGUNA VES A TENIDO QUE TRABAJAR, FUERA DEL HORARIO O HA TENIDO QUE HACER HORAS EXTRA?

- Si
- No

¿SI A TENIDO QUE REALIZAR TRABAJO FUERA DE HORARIO HA HECHO HORAS EXTRA LO HA HECHO?:

- Dentro de la empresa
- Desde un lugar externo a la empresa
- No he tenido que trabajar fuera de horario

¿TIENE RELACIONES FAMILIARES PERSONAL DE LA EMPRESA?

- Si
- No

¿HA TENIDO ALGUNA RELACION SENTIMENTAL/AFECTIVA CON ALGUIEN PERSONAL DE LA EMPRESA?

- Si
- No
- Prefiero no responder

¿DE UN NUMERO DEL 1 – 5 DONDE 1 ES MALO Y 5 ES EXCELENTE COMO CONSIDERA SU AMBIENTE LABORAL?

1. 2. 3. 4. 5.

¿ALGUNA VES A TENIDO ALGUN ALTERCADO CON ALGUN COMPAÑERO DE TRABAJO?

- Si
- No

SELECCIONE LOS DISPOSITIVOS DE SU PROPIEDAD QUE TRAE A LA EMPRESA Y LOS USA A TRAVES DE CONECCION WIFI DENTRO DE LA MISMA

- Teléfono celular
- Computadora portátil
- Tablets/tabletas
- Ninguno

EN SU COMPUTADORA DE TRABAJO EN LA EMPRESA SE LE PERMITE CONECTAR ALGUNO DE LOS SIGUIENTES DISPOSITIVOS DE SU PROPIEDAD

- Memorias USB
- Teléfono celular
- Tableta/tablet
- Cd/s
- Discos duros/solidos
- Ninguno

¿CUANDO FINALIZA SU HORARIO LABORAL SU TERMINAL (COMPUTADORA/PORTATIL) USTED GENERALMENTE LA DEJA EN QUE ESTADO?

- Apagada
- Suspendida
- Hibernando
- Encendida
- Cierra sesión

¿CUANDO SE AUSENTA EN HORARIO LABORAL (ALMUERZO, REUNIONES, OTROS) SU TERMINAL (COMPUTADORA/PORTATIL) USTED GENERALMENTE EN QUE ESTADO LO DEJA?

- Apagada
- Suspendida
- Hibernando
- Encendida
- Cierra sesión

¿EL ACCESO A SU AREA DE TRABAJO ES A TRAVES DE?:

- Tarjeta de acceso
- Código de acceso
- Biometría
- Llaves
- Libre acceso

¿ES USTED EL/LA UNICA PERSONA CON EL ACCESO A SU AREA DE TRABAJO ADEMAS DE SUS COMPAÑEROS DE AREA?

- Si
- No
- No se
- Es de libre acceso

USTED CONSUME ALIMENTOS EN SU LUGAR DE TRABAJO

- Si
- No

USTED CONSUME BEBIDAS EN SU LUGAR DE TRABAJO COMO: (JUGO, AGUA, ENERGIZANTE, ETC.)

- Si
- No

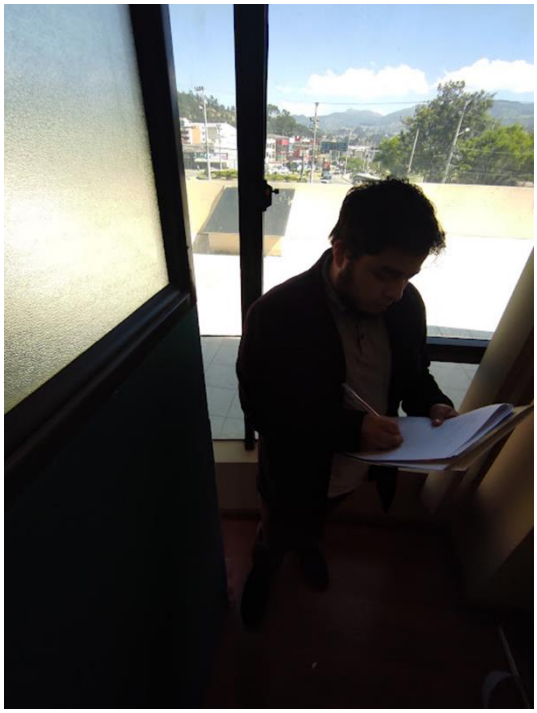
¿ALGUNA VEZ A LLEVADO SU COMPUTADOR/PORTATIL PERSONAL AL TRABAJO PARA PODER HACER SUS LABORES?

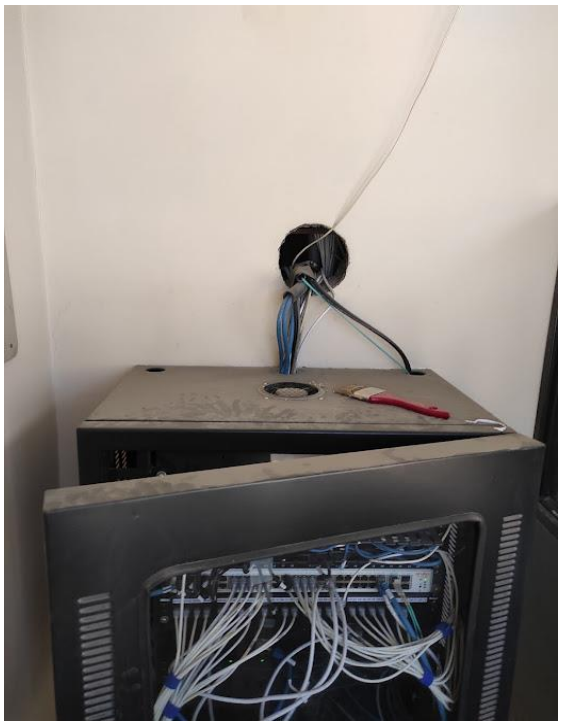
- Si
- No

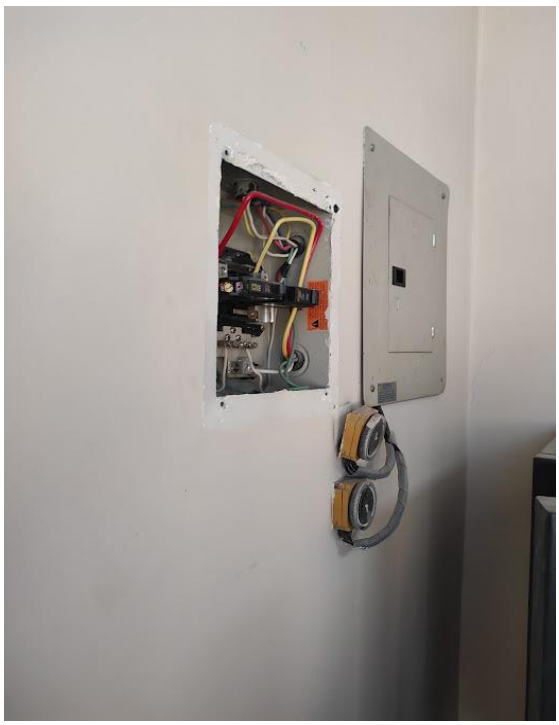
¿ALGUNA VES HA LLEVADO UN EQUIPO DEL TRABAJO A SU DOMICILIO PARA REALIZAR LABORES PENDIENTES?

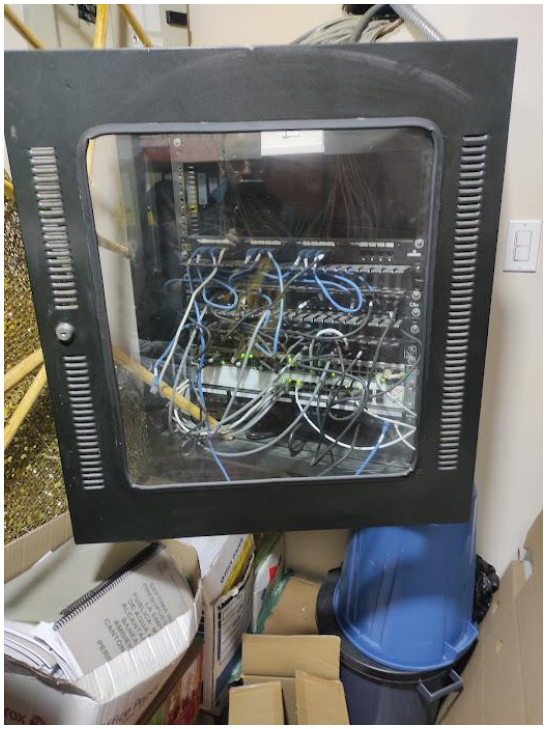
- Si
- No

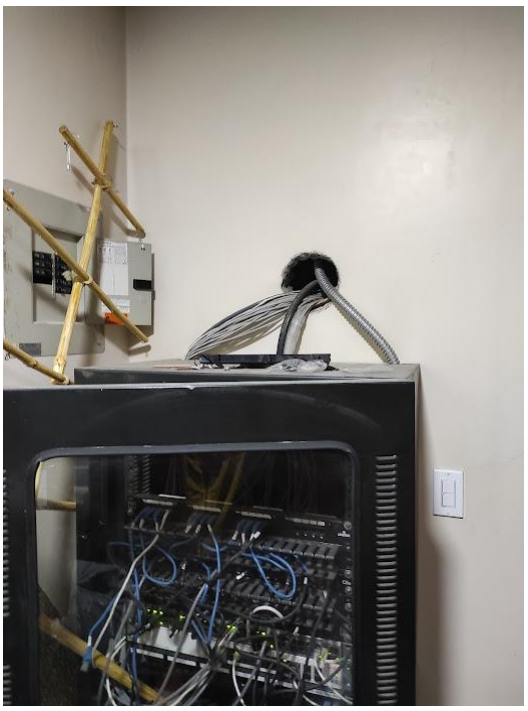
ANEXO 3: ANÁLISIS DE LOS EQUIPOS DE EMAPAL

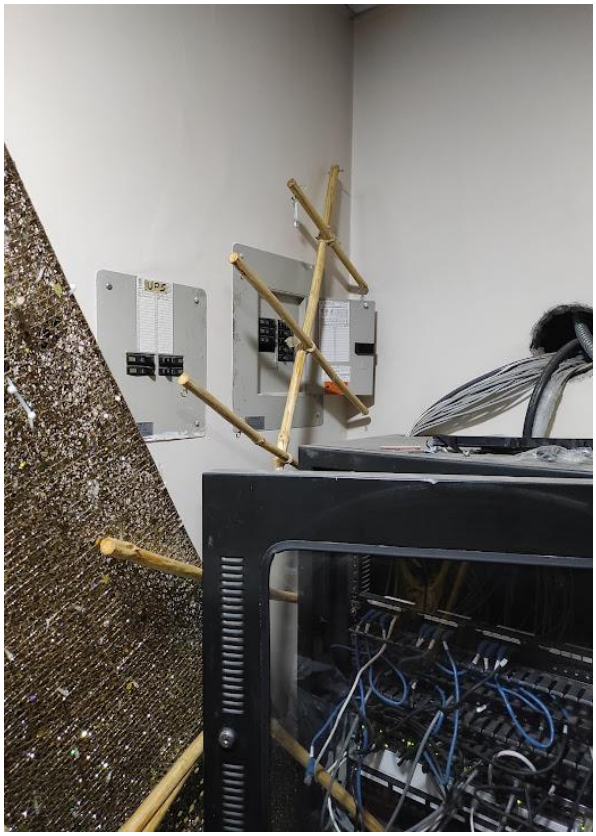


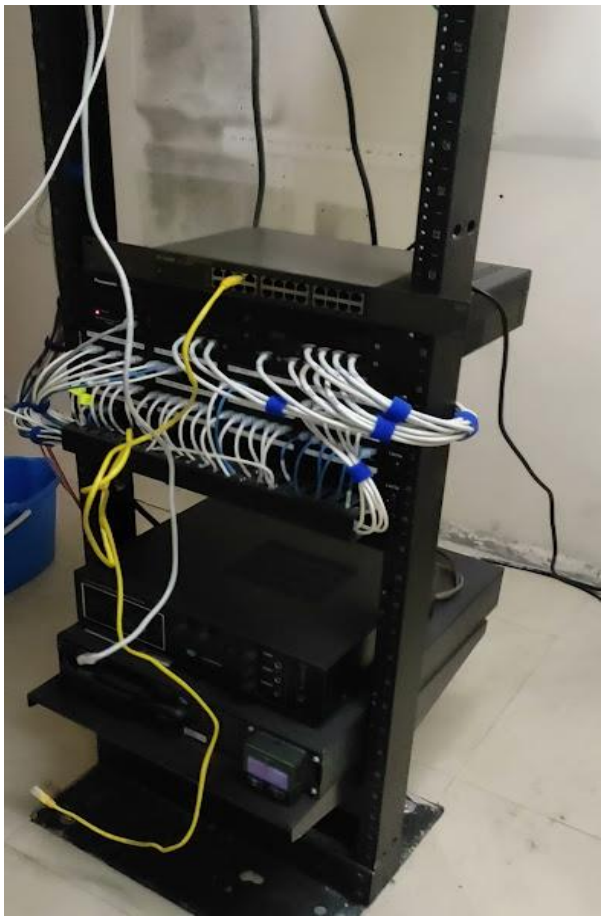


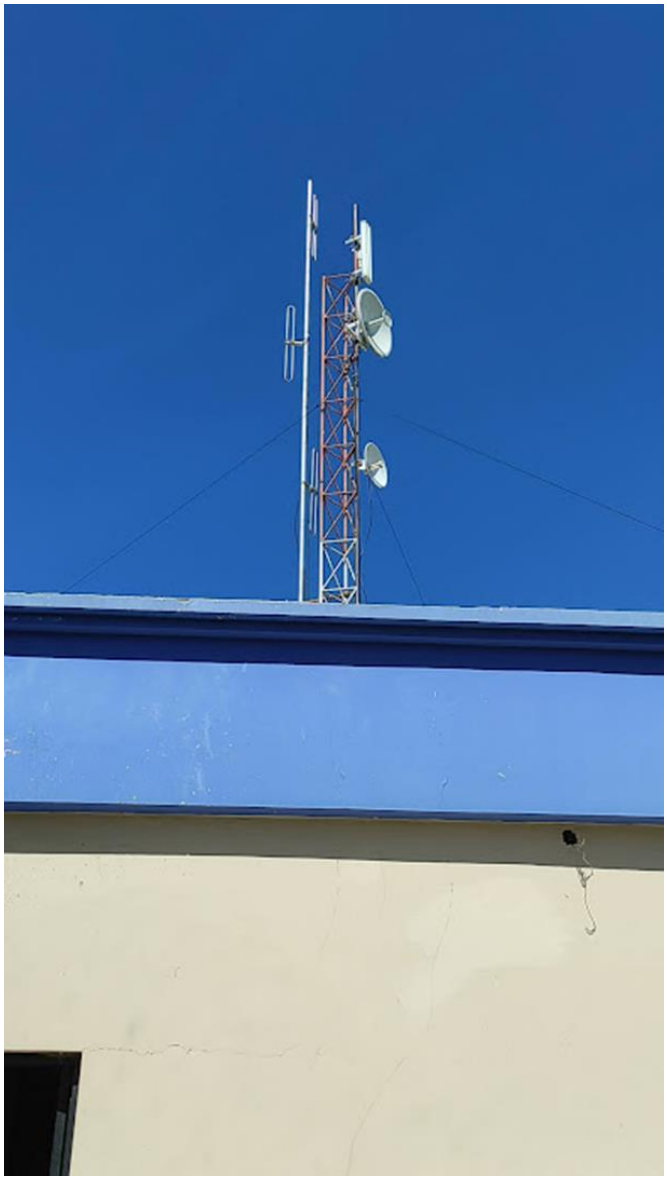






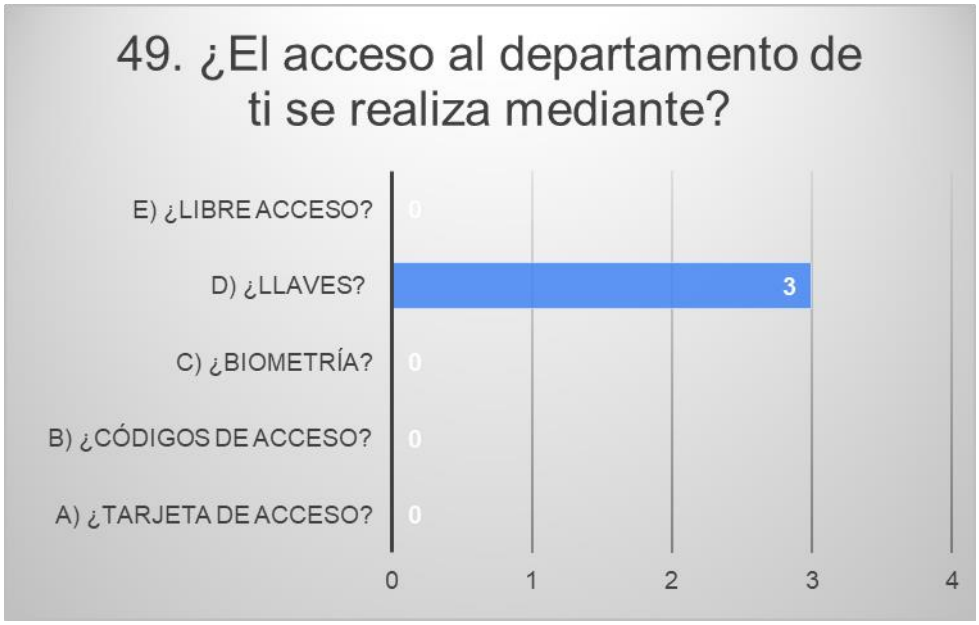

UPS



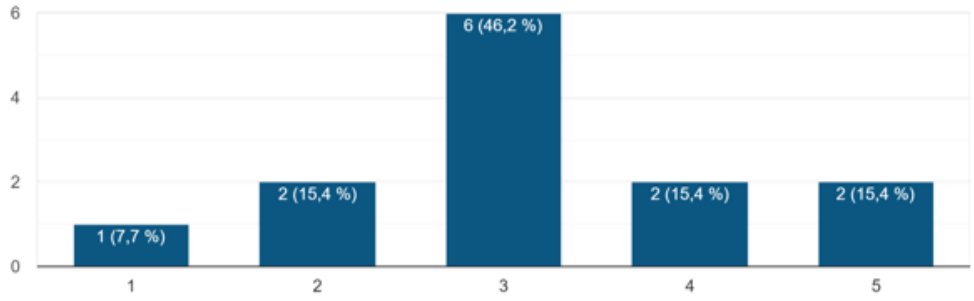


ANEXO 4: ENCUESTAS

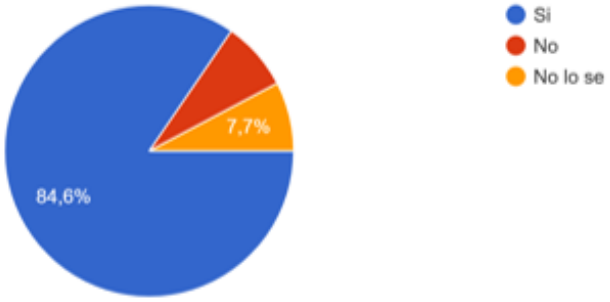

47. ¿Qué vigilancia existe dentro del departamento de ti?
D) ¿NINGUNA?
3
C) ¿SENSORES DE MOVIMIENTO?
0
B) ¿CÁMARA DE VIDEO CON AUDIO?
0
A) ¿CÁMARA DE VIDEO SIN AUDIO?
0
0
1
2
3
4


49. ¿El acceso al departamento de ti se realiza mediante?
E) ¿LIBRE ACCESO?
0
D) ¿LLAVES?
3
C) ¿BIOMETRÍA?
0
B) ¿CÓDIGOS DE ACCESO?
0
A) ¿TARJETA DE ACCESO?
0
0
1
2
3
4

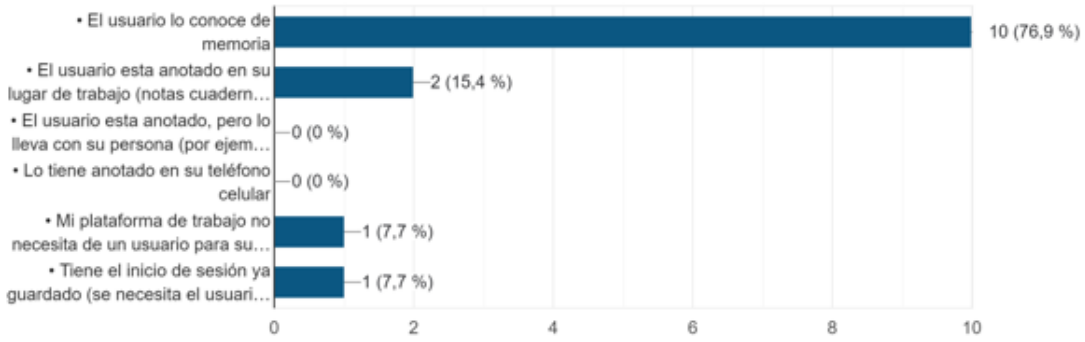
¿DE UN NUMERO DEL 1 – 5 DONDE 1 ES MALO Y 5 ES EXCELENTE COMO CONSIDERA SU AMBIENTE LABORAL?



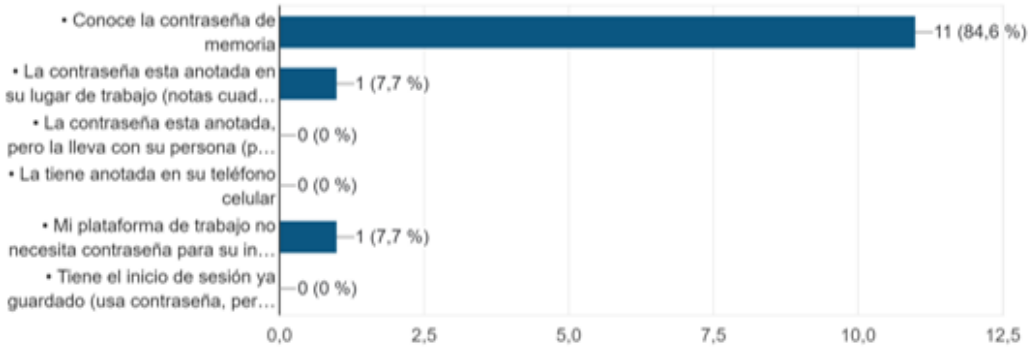
¿NECESITA UN USUARIO PARA ACCEDER A LA PLATAFORMA DE TRABAJO (ACCEDER AL SISTEMA)?



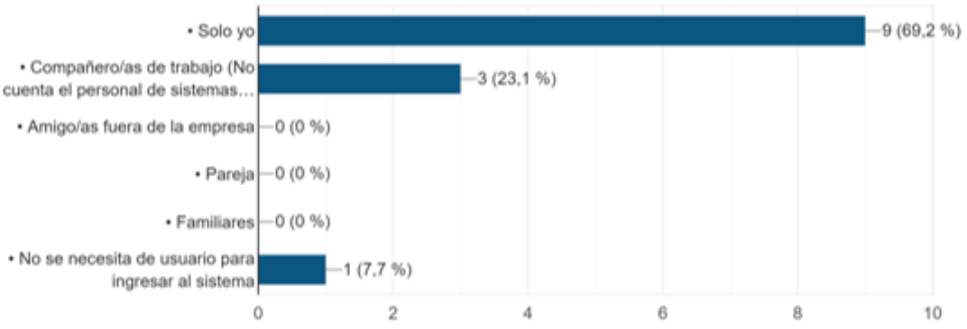
¿SU USUARIO PARA INGRESAR A LA PLATAFORMA DE TRABAJO (ACCEDER AL SISTEMA)



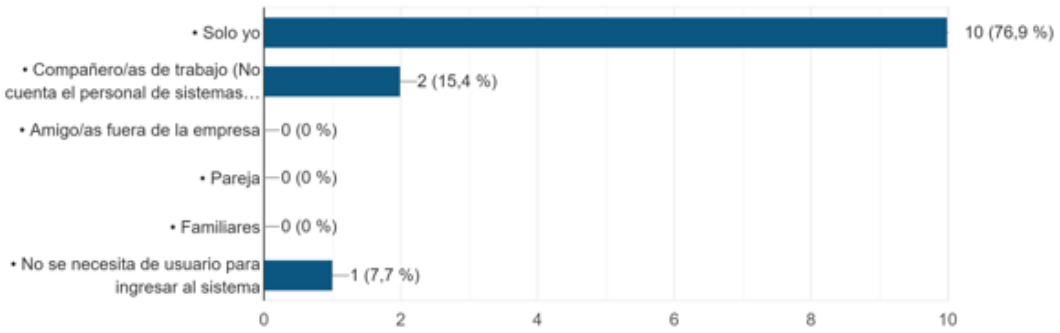
¿LA CONTRASEÑA PARA INGRESAR A LA PLATAFORMA DE TRABAJO (ACCEDER AL SISTEMA)?



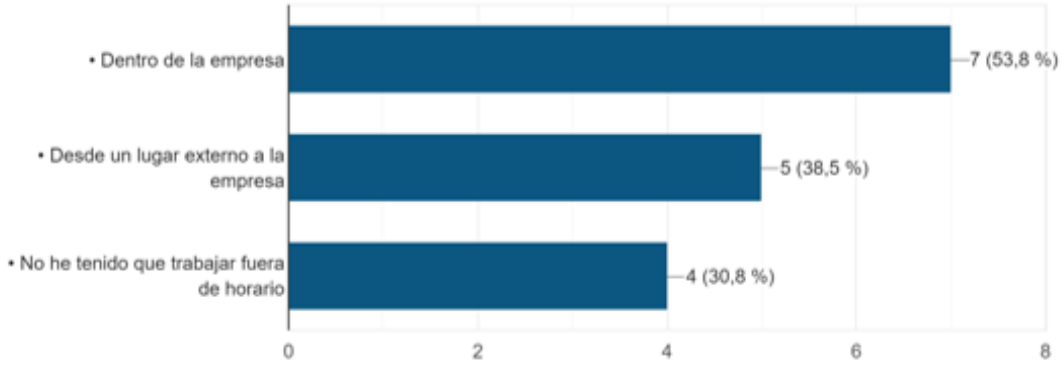
¿QUIENES CONOCEN SU CONTRASEÑA PARA EL INGRESO A LA COMPUTADORA DONDE TRABAJA?



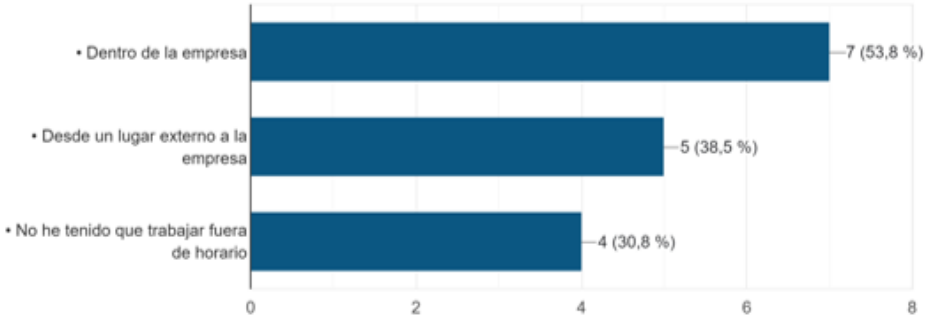
¿QUIENES CONOCEN SU USUARIO PARA EL INGRESO A LA PLATAFORMA DE TRABAJO? (AL SISTEMA DE TRABAJO)



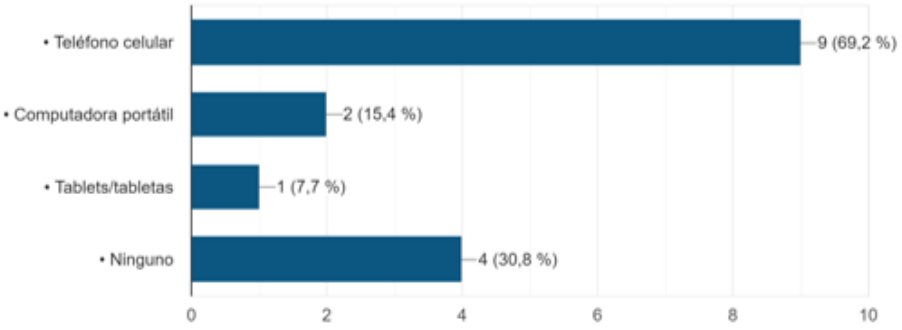
¿SI Ha TENIDO QUE REALIZAR TRABAJO FUERA DE HORARIO HA HECHO HORAS EXTRA LO HA HECHO?



¿SI Ha TENIDO QUE REALIZAR TRABAJO FUERA DE HORARIO HA HECHO HORAS EXTRA LO HA HECHO?



SELECCIONE LOS DISPOSITIVOS DE SU PROPIEDAD QUE TRAE A LA EMPRESA Y LOS USA A TRAVES DE CONECCION WIFI DENTRO DE LA MISMA



ANEXO 5: TABLA VALORACIÓN DE ACTIVOS

IDENTIFICACION DE ACTIVOS					Valoracion de Impacto			
N	**Nombre**	**Descripción**	**Ubicación**	**Soporte**	C: Confidencialidad I:Integridad D: Disponibilidad			
					C	I	D	VA
E1	Proliant Ml150 G6	GIS	Rack 1 Centro de datos 1	Logico y Fisico	3	3	2	2,67
E2	HP ML350 G8 V2	Active directory	Rack 1 Centro de datos 1	Logico y Fisico	3	2	1	2,00
E3	HP ML350 G8 V2	Documentacion Historica	Rack 1 Centro de datos 1	Logico y Fisico	2	2	1	1,67

E4	Proliant dl360 gen10	Bases de datos y gestion documental	Rack 1 Centro de datos 1	Logico y Fisico	3	3	3	3,00
E5	Proliant dl380 gen9	Aplicativo sistema ERP	Rack 1 Centro de datos 1	Logico y Fisico	1	2	3	2,00
E6	HP Compaq Pro 6300	Registro de asistencias	Departamento de TI	Logico y Fisico	2	1	1	1,33
E7	HP ML115 G1	Almacenamiento documental historico	Departamento de TI	Logico y Fisico	2	2	1	1,67
E8	Ubuntu 18.04	OS del Server	Proliant dl360 gen10	Logico	1	3	3	2,33
E9	Ubuntu 18.04	OS del Server	Proliant dl380 gen9	Logico	1	3	3	2,33
E10	Windows Server 2008	OS del Server	HP ML350 G8 V2	Logico	1	3	3	2,33
E11	Windows Server 2008	OS del Server	HP ML350 G8 V2	Logico	1	3	3	2,33
E12	Windows Server 2003	OS del Server	Proliant dl360 gen10	Logico	1	3	3	2,33
E13	Windows Server 2003	OS del Server	HP ML115 G1	Logico	1	3	3	2,33
E14	Windows 10	OS del Server	HP Compaq Pro 6300	Logico	1	3	3	2,33
E15	Postgis 2.2	Base de datos Geografica	Proliant Ml150 G6	Logico	3	3	2	2,67
E16	Postgresql 9.5	Base de datos	Proliant dl360 gen10	Logico	3	3	3	3,00
E17	SIIIM	Sistema ERP donde se desarrolla la actividad de la empreza	Proliant dl380 gen9	Logico	1	2	3	2,00
E18	SOPHOS SG 230 rev 1	Firewall	Rack 1 Centro de datos 1	Logico y Fisico	2	2	2	2,00
E19	HP MSR 900	Proveedor del servicio de internet	Rack 1 Centro de datos 1	Logico y Fisico	1	1	3	1,67
E20	HPE OfficeConect 1920S Series Switch	Administra la conexión de los servidores	Rack 1 Centro de datos 1	Logico y Fisico	1	1	3	1,67

E21	HPE OfficeConect 1920S Series Switch	Servicio de Internet Planta Baja	Rack 2 Centro de datos 1	Logico y Fisico	1	1	3	1,67
E22	HPE OfficeConect 1920S Series Switch	Servicio de Internet Planta Baja	Rack 2 Centro de datos 1	Logico y Fisico	1	1	3	1,67
E23	PE Aruba Instant On 1930 24G 4SFP/SFP	Usado en telefonia IP de la planta baja	Rack Centro de datos 2	Logico y Fisico	1	1	2	1,33
E24	HPE OfficeConect 1920S Series Switch	Conecta el servicio de internet con los pisos superiores y servicio a la planta baja	Rack Centro de datos 2	Logico y Fisico	1	1	3	1,67
E25	PE Aruba Instant On 1930 24G 4SFP/SFP	Usado en telefonia IP del piso 1	Rack Oficina Juridica	Logico y Fisico	1	1	2	1,33
E26	HPE OfficeConect 1920S Series Switch	Brinda servicio al piso 1	Rack Oficina Juridica	Logico y Fisico	1	1	3	1,67
E27	PE Aruba Instant On 1930 24G 4SFP/SFP	Usado en telefonia IP del piso 2	Rack Archivo	Logico y Fisico	1	1	2	1,33
E28	HPE OfficeConect 1920S Series Switch	Brinda servicio al piso 2	Rack Archivo	Logico y Fisico	1	1	3	1,67
E29	APX 530	Conectividad Inalambrica Departamento de Ti	Cieloraso departamento de TI	Logico y Fisico	1	1	2	1,33
E30	AP 55C	Conectividad Inalambrica	Cieloraso planta baja	Logico y Fisico	1	1	2	1,33
E31	AP 55C	Conectividad Inalambrica	Cieloraso piso 1	Logico y Fisico	1	1	2	1,33
E32	AP 55C	Conectividad Inalambrica	Cieloraso piso 2	Logico y Fisico	1	1	2	1,33

E33	Cableado Vertical Fibra Optica	Llevar internet desde el centro de datos a los switches de cada piso y la antena	Ducto	Logico y Fisico	1	1	3	1,67
E34	Cableado Horizontal UTP CAT 6/ 6A	Llevar internet desde el switch correspodiente de cada piso a	Edificio	Logico y Fisico	1	1	3	1,67
E35	VLANS	Agrupacion de dispositivos en subredes especificas	Entidad Logica de Red	Logico	3	1	3	2,33
E36	Redes Wireless	Redes WiFi	Puntos de Acceso Inalambrico	Logico	1	1	2	1,33
E37	Ubiquiti NanoStation M5 Loc0	Conecta con los puntos equidistantes de la empresa	Azotea	Logico y Fisico	1	1	2	1,33
E38	Panasonic KX-NS500	Sirve de centralita telefonica	Rack Centro de datos 2	Logico y Fisico	1	1	2	1,33
E39	Eaton 906 IIS	Sistemas de alimentacion ininterrumpida	Rack 1 Centro de datos 1	Fisico	1	1	1	1,00
E40	APC SRT2200XLA	Sistemas de alimentacion ininterrumpida	Centro de datos 1	Fisico	1	1	1	1,00
E41	APC SRT2200XLA	Sistemas de alimentacion ininterrumpida	Rack Centro de datos 2	Fisico	1	1	1	1,00

E42	Forza FDC-003K	Fuente de Poder ininterrumpible en caso de falla del suministro electrico	Departamento de TI	Fisico	1	1	1	1,00
E43	emapal.gob.ec/207.174.XXX.XXX/egob, edoc, etc	Funcionamiento a nivel de la Red y servicio a traves de una IP/Dominio unica	nic.ec	Logico	1	2	3	2,00
E44	www.emapal.gob.ec	Proporcionar informacion y/o servicios al publico	nic.ec	Logico	1	2	1	1,33
E45	Correo Masivo	Distribuir la emision de facturas o correos masivos	Tercerizada con Gmail	Logico	2	2	2	2,00
E46	Correo Corporativo	Uso de correo corporativo para empleados o areas de la empresa	nic.ec	Logico	2	2	2	2,00
E47	Consolas	Permiten el control de los diferentes activos de la empresa	Dispositivo o servicio respectivo	Logico	3	3	3	3,00
E48	Respaldo disco duro externo	Respaldo Acumulativo de la base de datos y del sistema ERP SIIM	Disco duro externo	Logico y Fisico	3	3	2	2,67

E49	Respaldo Telconet	Respaldo incremental de la base de datos y del sistema ERP SIIM	Telconet	Logico	3	3	2	2,67
E50	Kaspersky	Antivirus Institucional	Terminales de la empresa	Logico	1	1	1	1,00
E51	Biometrico	Registrar la asistencia de los empleados	Al lado de la puerta de acceso al centro de datos 1	Fisico y Logico	2	2	2	2,00
E52	Biotime 8.0	Registro de asistencia mediante biometria	HP Compaq Pro 6300	Logico	2	2	2	2,00
E53	Camaras de seguridad	Registrar la actividad en la empresa	Todo el edificio matriz	Fisico	1	1	1	1,00
E54	DVR modelo desconocido	Graba la actividad de las camaras de seguridad	Direccion administrativa	Fisico y Logico	2	2	1	1,67
E55	Rack 1 Centro de Datos 1	Alojamiento de equipos especializados	Centro de datos 1	Fisico	1	1	1	1,00
E56	Rack 2 Centro de datos 2	Alojamiento de equipos especializados	Centro de datos 1	Fisico	1	1	1	1,00
E57	Rack Centro de Datos 2	Alojamiento de equipos especializados	Centro de datos 2	Fisico	1	1	1	1,00
E58	Rack Piso 1	Alojamiento de equipos especializados	Oficina Juridica Piso 2	Fisico	1	1	1	1,00
E59	Rack Piso 2	Alojamiento de equipos especializados	Archivo Piso 3	Fisico	1	1	1	1,00

E60	Edificio Matriz	Edificio Matriz	Av Ernesto Che Guevara y Av 16 de Abril, Azogues	Fisico	1	3	3	2,33
E61	Centro de Datos 1	Alojamiento de equipos especializados	Edificio Matriz	Fisico	1	3	3	2,33
E62	Centro de Datos 2	Alojamiento de equipos especializados	Edificio Matriz	Fisico	1	3	3	2,33
E63	Oficina de Sistemas	Lugar donde laboran los empleados de Sistemas	Edificio Matriz	Fisico	1	2	2	1,67
E64	Terraza y soporte de la antena	Emplazamiento de la Antena	Edificio Matriz	Fisico	1	2	2	1,67
E65	Computadoras de escritorio	Computadoras de escritorio donde los empleados laboran	Edificio Matriz	Logico , Fisico y Organizacional	2	2	2	2,00
E66	Computadoras portatiles	Computadoras de portatiles donde los empleados laboran	Edificio Matriz	Logico , Fisico y Organizacional	2	2	2	2,00
E67	Funcionarios de Sistemas	Funcionarios de Sistemas	Edificio Matriz	Organizacional	3	2	2	2,33
E68	Talento Humano	Funcionarios no concernientes a sistemas	Edificio Matriz	Organizacional	2	1	2	1,67
E69	TIC'S	Ubicación del departamento de sistemas a nivel organizacional	Organigrama Institucional	Organizacional	1	1	1	1,00

ANEXO 6: TABLA AMENAZAS Y VULNERABILIDADES

ANALISIS DE RIESGOS				
N	**Proceso**	**Nombre**	**Amenazas**	**Vulnerabilidades**
E1	Infraestructura	Proliant dl360 gen10	Fallos en los componentes	Antigüedad del servidor de mas de 10 años
			Problemas de rendimiento	
			Problemas de capacidad de almacenamiento	
			Compatibilidad con Software Obsoleto	
			Problemas de escalabilidad	
			Hurto	Seguridad inadecuada para acceder al centro de datos
			Perdida total de la Informacion	Falta de respaldos del servidor
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada
			Subidas o bajadas de tension	Fallo en la red electrica
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño
E2		HP ML350 G8 V2	Fallos en los componentes	Antigüedad del servidor de 10 años
			Problemas de rendimiento	
			Problemas de capacidad de almacenamiento	
			Compatibilidad con Software Obsoleto	
			Problemas de escalabilidad	
			Hurto	Seguridad inadecuada para acceder al centro de datos
			Perdida total de la Informacion	Falta de respaldos del servidor
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada
			Subidas o bajadas de tension	Fallo en la red electrica
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño
E3		HP ML350 G8 V2	Fallos en los componentes	Antigüedad del servidor de 10 años
			Problemas de rendimiento	
			Problemas de capacidad de almacenamiento	
			Compatibilidad con Software Obsoleto	
			Problemas de escalabilidad	
			Hurto	Seguridad inadecuada para acceder al centro de datos
			Perdida total de la Informacion	Falta de respaldos del servidor
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire

			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada
			Subidas o bajadas de tension	Fallo en la red electrica
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño
E4		Proliant dl360 gen10	Hurto	Seguridad inadecuada para acceder al centro de datos
			Perdida total de la Informacion	Falta de respaldos del servidor
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada
			Subidas o bajadas de tension	Fallo en la red electrica
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño
E5		Proliant dl380 gen9	Fallos en los componentes	Antigüedad del servidor de 9 años
			Problemas de rendimiento	
			Problemas de capacidad de almacenamiento	
			Compatibilidad con Software Obsoleto	
			Problemas de escalabilidad	
			Hurto	Seguridad inadecuada para acceder al centro de datos
			Perdida total de la Informacion	Falta de respaldos del servidor
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada
			Subidas o bajadas de tension	Fallo en la red electrica
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño
E6		HP Compaq Pro 6300	Fallo del equipo	Hardware no dedicado para ejercer como servidor
			Fallos en los componentes	Antigüedad del equipo de 10 años estimados
			Problemas de rendimiento	
			Problemas de capacidad de almacenamiento	
			Compatibilidad con Software Obsoleto	
			Problemas de escalabilidad	
			Hurto	Seguridad inadecuada para acceder a la oficina de TI
			Perdida total de la Informacion	Falta de respaldos del servidor
			Recalentamiento del equipo	Ubicado en el departamento de TI
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicado en el departamento de TI
			Subidas o bajadas de tension	Fallo en la red electrica
E7		HP ML115 G1	Fallos en los componentes	Antigüedad del servidor de mas de 10 años
			Problemas de rendimiento	
			Problemas de capacidad de almacenamiento	
			Compatibilidad con Software Obsoleto	
			Problemas de escalabilidad	

			Hurto	Seguridad inadecuada para acceder a la oficina de TI
			Perdida total de la Informacion	Falta de respaldos del servidor
			Recalentamiento del equipo	Ubicado en el departamento de TI
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicado en el departamento de TI
			Subidas o bajadas de tension	Fallo en la red electrica
E8	OS	Ubuntu 18	Fallas de seguridad, estabilidad y rendimiento	Configuracion Inadecuada
			Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Soporte proximo a finalizar en abril del 2023
E9		Ubuntu 18	Fallas de seguridad, estabilidad y rendimiento	Configuracion Inadecuada
			Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Soporte proximo a finalizar en abril del 2023
E10		Windows Server 2008	Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Sistema Operativo sin soporte
			Vulnerabilidades detectadas	Sistema Operativo sin las ultimas actualizaciones
E11		Windows Server 2008	Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Sistema Operativo sin soporte
			Vulnerabilidades detectadas	Sistema Operativo sin las ultimas actualizaciones
E12		Windows Server 2003	Fallos y vulnerabilidad a amenazas	Sistema Operativo sin soporte
			Vulnerabilidades detectadas	Sistema Operativo sin las ultimas actualizaciones
E13		Windows Server 2003	Fallos y vulnerabilidad a amenazas	Sistema Operativo sin soporte
			Explotacion de vulnerabilidades detectadas	Sistema Operativo sin las ultimas actualizaciones
E14		Windows 10	Ataques de malware	Sin soporte como servidor
			Bajas del rendimiento	Sin soporte como servidor
			Intrusiones	Seguridad inadecuada para uso como servidor
			Hackeos	Seguridad inadecuada para uso como servidor
E15	Bases de Datos	Postgis 2.2	Explotaciones de amenazas conocidas	Version antigua del software
			Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Software sin soporte
E16		Postgresql 9.5	Explotaciones de amenazas conocidas	Version antigua del software
			Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Software sin soporte
E17	ERP	SIIIM	INFORMACION RESERVADA	INFORMACION RESERVADA
E18	FIREWALL	SOPHOS SG 230 rev 1	Trafico indeseado	Configuracion inadecuada
			Intrusiones no autorizadas	Puertos abiertos no autorizados
			Vulnerabilidades detectadas	Firmware desactualizado
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño
E19	RED	HP MSR 900	Fallos y explotacion de vulnerabilidades	Firmware desactualizado
			Acceso no autorizado	Contraseñas por defecto
			Acceso no autorizado	Contraseñas filtradas
			Hurto	Seguridad inadecuada para acceder al centro de datos
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire

			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada
			Subidas o bajadas de tension	Fallo en la red electrica
			Corte del servicio de internet	Fallo del proveedor del servicio
				Fallos del hardware
				Configuracion inadecuada del dispositivos
E20		HPE OfficeConect 1920S Series Switch	Fallos y explotacion de vulnerabilidades	Firmware desactualizado
			Hurto	Seguridad inadecuada para acceder al centro de datos
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada
			Subidas o bajadas de tension	Fallo en la red electrica
			Desconeccion entre los servidores y la intranet de la empresa	Fallos del hardware
				Configuracion inadecuada del dispositivos
			Mayor latencia de datos	Cableado desordenado
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar
E21		HPE OfficeConect 1920S Series Switch	Fallos y explotacion de vulnerabilidades	Firmware desactualizado
			Hurto	Seguridad inadecuada para acceder al centro de datos
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada
			Subidas o bajadas de tension	Fallo en la red electrica
			Desconeccion del servicio de red en la planta baja	Fallos del hardware
				Configuracion inadecuada del dispositivos
			Mayor latencia de datos	Cableado desordenado
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar
E22		HPE OfficeConect 1920S Series Switch	Fallos y explotacion de vulnerabilidades	Firmware desactualizado
			Hurto	Seguridad inadecuada para acceder al centro de datos
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada
			Subidas o bajadas de tension	Fallo en la red electrica
			Desconeccion del servicio de red en la planta baja	Fallos del hardware
				Configuracion inadecuada del dispositivos
			Mayor latencia de datos	Cableado desordenado
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar

			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar
E23		PE Aruba Instant On 1930 24G 4SFP/SFP	Fallos y explotacion de vulnerabilidades	Firmware desactualizado
			Hurto	Seguridad inadecuada para acceder al centro de datos
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada
			Subidas o bajadas de tension	Fallo en la red electrica
			Desconeccion del servicio de telefonia IP en la planta baja	Fallos del hardware
				Configuracion inadecuada del dispositivos
			Interferencias electromagneticas	Cableado desordenado
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar
E24		HPE OfficeConect 1920S Series Switch	Fallos y explotacion de vulnerabilidades	Firmware desactualizado
			Hurto	Seguridad inadecuada para acceder al centro de datos
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada
			Subidas o bajadas de tension	Fallo en la red electrica
			Desconeccion del servicio de red en los pisos superiores	Fallos del hardware
				Configuracion inadecuada del dispositivos
			Mayor latencia de datos	Cableado desordenado
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar
E25		PE Aruba Instant On 1930 24G 4SFP/SFP	Fallos y explotacion de vulnerabilidades	Firmware desactualizado
			Manejo inadecuado por personal no capacitado	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza
			Hurto	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza
			Subidas o bajadas de tension	Fallo en la red electrica
			Desconeccion del servicio de telefonia IP en el piso 1	Fallos del hardware
				Configuracion inadecuada del dispositivos
			Interferencias electromagneticas	Cableado desordenado
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar
E26			Fallos y explotacion de vulnerabilidades	Firmware desactualizado

		HPE OfficeConect 1920S Series Switch	Manejo inadecuado por personal no capacitado	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza
			Hurto	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza
			Subidas o bajadas de tension	Fallo en la red electrica
			Desconeccion del servicio de red en el piso 1	Fallos del hardware
				Configuracion inadecuada del dispositivos
			Mayor latencia de datos	Cableado desordenado
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar
E27		PE Aruba Instant On 1930 24G 4SFP/SFP	Fallos y explotacion de vulnerabilidades	Firmware desactualizado
			Manejo inadecuado por personal no capacitado	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza
			Hurto	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza
			Subidas o bajadas de tension	Fallo en la red electrica
			Desconeccion del servicio de telefonia IP en el piso 2	Fallos del hardware
				Configuracion inadecuada del dispositivos
			Interferencias electromagneticas	Cableado desordenado
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar
E28		HPE OfficeConect 1920S Series Switch	Fallos y explotacion de vulnerabilidades	Firmware desactualizado
			Manejo inadecuado por personal no capacitado	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza
			Hurto	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada
			Subidas o bajadas de tension	Fallo en la red electrica
			Desconeccion del servicio de red en el piso 2	Fallos del hardware
				Configuracion inadecuada del dispositivos
			Mayor latencia de datos	Cableado desordenado
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar
E29		APX 530	Hurto	Entrada de personas no autorizadas
			Daños Fisicos	Maltrato/ Caida

			Alta latencia	Interferencia electromagnetica
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicacion elevada
			Subidas o bajadas de tension	Fallo en la red electrica
			Indisponibilidad del servicio	Fallos en los componentes
			Indisponibilidad del servicio	Configuracion inadecuada
			Fallos y explotacion de vulnerabilidades	Firmware desactualizado
			Alta latencia	Trafico de red exesivo
E30		AP 55C	Hurto	Acceso libre al dispositivo
			Daños Fisicos	Maltrato/ Caida
			Alta latencia	Interferencia electromagnetica
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicacion elevada
			Subidas o bajadas de tension	Fallo en la red electrica
			Indisponibilidad del servicio	Fallos en los componentes
			Indisponibilidad del servicio	Configuracion inadecuada
			Fallos y explotacion de vulnerabilidades	Firmware desactualizado
			Alta latencia	Trafico de red exesivo
E31		AP 55C	Hurto	Acceso libre al dispositivo
			Daños Fisicos	Maltrato/ Caida
			Alta latencia	Interferencia electromagnetica
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicacion elevada
			Subidas o bajadas de tension	Fallo en la red electrica
			Indisponibilidad del servicio	Fallos en los componentes
			Indisponibilidad del servicio	Configuracion inadecuada
			Fallos y explotacion de vulnerabilidades	Firmware desactualizado
			Alta latencia	Trafico de red exesivo
E32		AP 55C	Hurto	Acceso libre al dispositivo
			Daños Fisicos	Maltrato/ Caida
			Alta latencia	Interferencia electromagnetica
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicacion elevada
			Subidas o bajadas de tension	Fallo en la red electrica
			Indisponibilidad del servicio	Fallos en los componentes
			Indisponibilidad del servicio	Configuracion inadecuada
			Fallos y explotacion de vulnerabilidades	Firmware desactualizado
			Alta latencia	Trafico de red exesivo
E33		Cableado Vertical Fibra Optica	Destrucion	Daño fisico/Rotura/Cortes
			Alta latencia	Interferencia electromagnetica
E34		Cableado Horizontal UTP CAT 6/ 6A	Destrucion	Daño fisico/Rotura/Cortes
			Alta latencia	Interferencia electromagnetica
E35			Accesos no autorizados	Configuracion incompleta

		Redes VLAN	Conflicto de direcciones IP	
			Dificultad par reconfigurar las VLANS	
			Bajo rendimiento de la red	
			Ataque de snooping	Filtracion de la tabla de subredes
			Accesos no autorizados a subredes	Filtracion de la tabla de subredes
			Interrupcion de servicios	Filtracion de la tabla de subredes
E36		Redes Wireless	Accesos a redes con permisos superirores	Filtracion de contraseñas
			Accesos no autorizados	Contraseñas debiles
			Ataques de fuerza bruta y diccionarios de contraseñas	Contraseñas debiles
			Intercepcion de trafico de red	Cifrado de red debil
			Inyeccion de paquetes	Cifrado de red debil
			Menor privacidad, seguridad y control	Redes wifi visibles
E37		Antena Ubiquiti Nanostation M5 LOC0	Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Exposicion al aire libre
			Desgaste por el clima	Exposicion al aire libre
			Sobrecarga electrica	Rayos
			Caidas/ Vibraciones exesivas	Instalacion incorrecta
			Daño fisico	Mantenimiento inadecuado
E38	TELEFONIA	Panasonic KX-NS500	Fallos y explotacion de vulnerabilidades	Firmware desactualizado
			Hurto	Seguridad inadecuada para acceder al centro de datos
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada
			Subidas o bajadas de tension	Fallo en la red electrica
			Fallo del servicio de telefonia IP	Fallos del hardware
				Configuracion inadecuada del dispositivos
E39	UPS	Eaton 906 IIS	Fallas de la bateria y daños en la electronica	Tiempo de vida de uso prolongado
				Sobrecargas, descargas electricas
				Degradacion natural
				Mala estimacion de la carga
E40		APC SRT2200XLA		Tiempo de vida de uso prolongado
				Sobrecargas, descargas electricas
				Degradacion natural
				Mala estimacion de la carga
E41		APC SRT2200XLA		Tiempo de vida de uso prolongado
				Sobrecargas, descargas electricas
				Degradacion natural
				Mala estimacion de la carga
E42		Forza FDC-003K		Tiempo de vida de uso prolongado
				Sobrecargas, descargas electricas
				Degradacion natural
				Mala estimacion de la carga
E43	Dominio/IP	emapal.gob.ec/2	Explotacion de vulnerabilidades relacionadas con Open SSH 7.4	Vulnerabilidades en el puerto 22 y 2222 relacionadas al uso de Open SSH 7.4

	Y Subdominios	07.174.XXX.XXX/egob, edoc, etc	Panel de logeo a CPANEL publica, ingreso no autorizado a traves de fuerza bruta, diccionarios, pishing,ingenieria social.	Acceso publico al puerto 2082 y 2083
			Panel de logeo a WebHostManager publica, ingreso no autorizado a traves de fuerza bruta, diccionarios, pishing,ingenieria social.	Acceso publico al puerto 2086 y 2087
E44	Pagina Web	www.emapal.gob.ec	Informacion erronea	Web desactualizada
			Falta de informacion	Web desactualizada
			Explotacion de vulnerabilidades propias de la plataforma/servicio	Puerto y subdominio visible en el servicio de recursos humanos
			Ataques de fuerza bruta	Puerto y subdominio visible en el servicio de recursos humanos
			Informacion sensible de la estructura de la plataforma vuelta publica	Puerto y subdominio visible en el servicio de recursos humanos
E45	Servicio de Correo Masivo	Correo Masivo	Desconeccion con el servicio	Problemas tecnicos
			Desconeccion con el servicio	Desconeccion de la intranet de la empresa con internet
			Perdida del control de datos	No ser dueños del servicio
			Ataques de fuerza bruta o de diccionarios	Contraseñas inadecuadas
E46	Servicio de Correo Corporatico	Correo Corporativo	Desconeccion con el servicio	Problemas tecnicos
			Desconeccion con el servicio	Desconeccion de la intranet de la empresa con internet
			Perdida del control de datos	No ser dueños del servicio
			Filtracion de informacion	Uso de correo institucional para servicios externos
			Descargas de malware	Uso de correo institucional para servicios externos
			Filtracion de credenciales y/o informacion persona o de la empresa	Correos con Pishing
			Infeccion de la red/ terminal	Correos infectados de malware
			Ataques de fuerza bruta o de diccionarios	Contraseñas inadecuadas
E47	Software	Consolas	Ataques de fuerza bruta o de diccionarios	Contraseñas inadecuadas
			Codigo malicioso	Exploits de software
			Codigo malicioso	Inyeccion de codigo
E48	BACK UPS	Respaldo disco duro externo	Perdida	Objeto transportable y accesible
			Destruccion	Sensible a agentes fisicos, caidas, golpes
			Hurto	Objeto transportable y accesible
			Perdida de datos	Daño mecanico, caidas golpes, agentes fisicos
			Robo de datos	Falta de contraseña/encriptacion
E49		Respaldo Telconet	Robo/Alteracion de la informacion	Acceso no autorizado
			Corrupcion/Perdida de datos	Error humano
			Corrupcion/Perdida de datos	Fallos en el hardware donde se almacena
			Destruccion del hardware donde se almacena el respaldo	Desastres naturales
			Destruccion del hardware donde se almacena el respaldo	Amenazas ambientales
E50	ANTI VIRUS	Kaspersky	Malware	Antivirus desactualizado
E51			Registro erroneo	Fecha y hora incorrectas
			Registro erroneo	Identificacion erronea

	ASISTENCIA	MB360 ZKTECO	Daño	Daño mecanico, caidas golpes, agentes fisicos
			Destruccion	Daño mecanico, caidas golpes, agentes fisicos
E52		Biotime 8.0	Explotacion de vulnerabilidades	Firmware desactualizado
			Ataques de fuerza bruta o de diccionarios	Contraseñas inadecuadas
			Robo de informacion biometrica	Firmware desactualizado
			Robo de informacion biometrica	Contraseñas inadecuadas
E53	SEGURIDAD	Camaras de seguridad	Vandalismo o robo	Activos en lugares accesibles
			Daño	Daño mecanico, caidas golpes, agentes fisicos
			Destruccion	Daño mecanico, caidas golpes, agentes fisicos
			Fallos en el funcionamiento, baja resolucion de las imágenes	Camaras antiguas
			Puntos ciegos ubicados en los lugares donde las camaras no funcionan	Camaras sin funcionamiento
			Acceso no autorizado , intrusiones	Asignacion de una ip publicas a traves del dominio para que esten disponibles para el director administrativo desde su dispositivo movil
			Inyeccion de codigo malicioso y/o spyware	Asignacion de una ip publicas a traves del dominio para que esten disponibles para el director administrativo desde su dispositivo movil
E54		DVR modelo desconocido	Intrusiones por credenciales debiles/nulas	Sistema de camaras a cargo de la direccion administrativa
			Intruciones a puertos abiertos	Sistema de camaras a cargo de la direccion administrativa
			Explotacion de vulnerabilidades por software desactualizado	Sistema de camaras a cargo de la direccion administrativa
			Infecciones de malware	Sistema de camaras a cargo de la direccion administrativa
			Fallos debido a configuracion inadecuada	Sistema de camaras a cargo de la direccion administrativa
			Hurto	Seguridad inadecuada
			Destruccion del equipo	Manipulacion del dispositivo
			Recalentamiento del equipo	Ubicación inadecuada
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicación inadecuada
			Subidas o bajadas de tension	Fallo en la red electrica
E55	RACKS	Rack 1 Centro de Datos 1	Daño por fallas mecánicas	Derrame de líquidos
			Daño por fallas mecánicas	Humedad y corrosión
			Daño por fallas mecánicas	Vibración excesiva
			Daño por fallas mecánicas	Sobrecarga de peso
			Daño por fallas mecánicas	Fallas en los soportes
E56		Rack 2 Centro de datos 2	Daño por fallas mecánicas	Derrame de líquidos
			Daño por fallas mecánicas	Humedad y corrosión
			Daño por fallas mecánicas	Vibración excesiva
			Daño por fallas mecánicas	Sobrecarga de peso
			Daño por fallas mecánicas	Fallas en los soportes
E57		Rack Centro	Daño por fallas mecánicas	Derrame de líquidos
			Daño por fallas mecánicas	Sol, Humedad Corrosión

		de Datos 2	Daño por fallas mecánicas	Vibración excesiva
			Daño por fallas mecánicas	Sobrecarga de peso
			Daño por fallas mecánicas	Fallas en los soportes
E58		Rack Piso 1	Daño por fallas mecánicas	Sol Humedad , Corrosión
			Daño por fallas mecánicas	Vibración excesiva
			Daño por fallas mecánicas	Sobrecarga de peso
			Daño por fallas mecánicas	Fallas en los soportes
			Incendios/Desastres ambientales	Rack abierto
			Daño en los equipos al momento de mitigar un incendio	Falta de extintores de CO2
E59		Rack Piso 2	Daño por fallas mecánicas	Humedad y corrosión
			Daño por fallas mecánicas	Vibración excesiva
			Daño por fallas mecánicas	Sobrecarga de peso
			Daño por fallas mecánicas	Fallas en los soportes
			Incendios/Desastres ambientales/Hurto	Rack abierto
			Incendio/Acumulacion de polvo	Almacenamiento de documentacion fisica cercana
			Daño en los equipos al momento de mitigar un incendio	Falta de extintores de CO2
E60	UBICACIÓN FISICA	Edificio Matriz	Robo, Vandalismo	Seguridad Fisica Inadecuada
			Inundacion	Desborde del rio
			Destruccion del edificio	Incendios
			Daños	Daño por agentes medioambientales, climatologicos
E61		Centro de Datos 1	Sobrecalentamiento/Acumulacion de polvo	Ventilacion y climatizacion inadecuada
			Intrusiones/Hurto/Destruccion de equipos	Poca seguridad para el ingreso al centro de datos
			Intrusiones/Hurto/Destruccion de equipos	Ventana que da al exterior
			Inundacion	Colinda con un baño
			Inundacion	Ubicado en la primera planta
			Incendios/Desastres ambientales/Polvo	Piso flotante
			Incendios/Desastres ambientales	Racks abiertos
			Acumulacion de polvo	Almacenamiento de equipos en desuso
			Daño en los equipos al momento de mitigar un incendio	Falta de extintores de CO2
			Intrusiones/Hurto/Destruccion de equipos	Falta de monitoreo de seguridad
			Cambios ambientales	Falta de monitoreo ambiental
			Subidas , bajadas de tension o cortes electricos	Falta de monitoreo electrico
			Ingresos no autorizados	Registro de ingreso
E62		Centro de Datos 2	Sobrecalentamiento/Acumulacion de polvo	Ventilacion y climatizacion inadecuada
			Intrusiones/Hurto/Destruccion de equipos	Poca seguridad para el ingreso al centro de datos
			Inundacion	Colinda con un baño
			Inundacion	Ubicado en la primera planta
			Acumulacion de polvo, incendios	Almacenamiento de equipos en desuso y cajas
			Daño en los equipos al momento de mitigar un incendio	Falta de extintores de CO2
			Intrusiones/Hurto/Destruccion de equipos	Falta de monitoreo de seguridad
			Cambios ambientales	Falta de monitoreo ambiental

			Subidas , bajadas de tension o cortes electricos	Falta de monitoreo electrico
			Ingresos no autorizados	Falta de registro de ingreso
E63		Oficina de Sistemas	Sobrecalentamiento/Acumulacion de polvo	Ventilacion y climatizacion inadecuada
			Intrusiones/Hurto/Destruccion de equipos	Poca seguridad para el ingreso a la oficina
			Inundacion	Ubicado en la primera planta
			Acumulacion de polvo	Falta de limpieza
			Daño en los equipos al momento de mitigar un incendio	Falta de extintores de CO2
			Intrusiones/Hurto/Destruccion de equipos	Ventanas con acceso al exterior
			Destruccion o daño de los equipos	Subidas , bajadas de tension o cortes electricos
			Ingresos no autorizados	Ausencia de registro de ingreso
			Destruccion o daño	Incendios/Desastres ambientales/Polvo
E64		Terraza y soporte de la antena	Intrusiones/Hurto/Destruccion de equipos	Acceso no autorizado
			Degradacion por agentes ambientales	Falta de mantenimiento y limpieza
E65	TERMINALES DE LOS EMPLEADOS	Computadoras de escritorio	Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Terminales con OS WINDOWS 7(sin soporte)
			Vulnerabilidades detectadas	Terminales desactualizadas
			Fallos en los componentes	Terminales con una antigüedad estimada en 17 años
			Problemas de rendimiento	
			Problemas de capacidad de almacenamiento	
			Compatibilidad con Software Obsoleto	
			Problemas de escalabilidad	
			Fallos en los componentes	Terminales con una antigüedad estimada en 11 años
			Problemas de rendimiento	
			Problemas de capacidad de almacenamiento	
			Compatibilidad con Software Obsoleto	
			Problemas de escalabilidad	
			Fallos en los componentes	Terminales con una antigüedad estimada en 7 años
			Problemas de rendimiento	
			Problemas de capacidad de almacenamiento	
			Compatibilidad con Software Obsoleto	
			Problemas de escalabilidad	
			Rendimiento probre	Terminales con procesadores viejos y de poca capacidad
			Sobrecalentamiento	
			Pantallasos azules	
			Reinicios Inesperados	
			Corrupcion/Perdida de datos	
			Aplicaciones que no responden	Terminales con 2 - 3 GB de RAM
			Bajo rendimiento	
			Reinicios Inesperados	
			Corrupcion/Perdida de datos	
			Aplicaciones que no responden	Terminales con 4 GB de RAM
			Bajo rendimiento	
			Conflicto de tareas	Terminales compartidas entre empleados
			Filtracion de datos	

			Desorganizacion de archivos e informacion	
			Uso ineficiente del terminal	
			Infeccion de malware	Conexión de dispositivos personales a terminales de la empreza
			Robo de datos	
			Conflictos en la politica de seguridad	
			Accesos no autorizados	Contraseñas debiles para acceso al terminal
			Accesos no autorizados	Terminales sin contraseña
			Accesos no autorizados	Terminales sin usuario
			Llevarse los terminales de forma no autorizada fuera de la empresa	Poco control fisico de los terminales
			Subidas o bajadas de tension	Fallo en la red electrica
			Destruccion por inundacion	Aumento del caudal del rio/ lluvia
			Daños fisicos	Golpes o caidas
E66		Computadoras portatiles	Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Terminales con OS WINDOWS 7(sin soporte)
			Vulnerabilidades detectadas	Terminales desactualizadas
			Fallos en los componentes	Terminales con una antigüedad estimada en 15 años
			Problemas de rendimiento	
			Problemas de capacidad de almacenamiento	
			Compatibilidad con Software Obsoleto	
			Problemas de escalabilidad	
			Fallos en los componentes	Terminales con una antigüedad estimada entre 9 - 11 años
			Problemas de rendimiento	
			Problemas de capacidad de almacenamiento	
			Compatibilidad con Software Obsoleto	
			Problemas de escalabilidad	
			Fallos en los componentes	Terminales con una antigüedad estimada en 7 años
			Problemas de rendimiento	
			Problemas de capacidad de almacenamiento	
			Compatibilidad con Software Obsoleto	
			Problemas de escalabilidad	
			Rendimiento probre	Terminales con procesadores viejos y de poca capacidad
			Sobrecalentamiento	
			Pantallasos azules	
			Reinicios Inesperados	
			Corrupcion/Perdida de datos	
			Aplicaciones que no responden	Terminales con 2 - 3 GB de RAM
			Bajo rendimiento	
			Reinicios Inesperados	
			Corrupcion/Perdida de datos	
			Aplicaciones que no responden	Terminales con 4 GB de RAM
			Bajo rendimiento	
			Conflicto de tareas	Terminales compartidas entre empleados
			Filtracion de datos	
			Desorganizacion de archivos e informacion	
			Uso ineficiente del terminal	
			Infeccion de malware	

			Robo de datos	Conexión de dispositivos personales a terminales de la empreza
			Conflictos en la politica de seguridad	
			Accesos no autorizados	Contraseñas debiles para acceso al terminal
			Accesos no autorizados	Terminales sin contraseña
			Accesos no autorizados	Terminales sin usuario
			Hurto	Poco control fisico de los terminales y portailidad de los mismos
			Llevarse los terminales de forma no autorizada fuera de la empresa	Poco control fisico de los terminales y portailidad de los mismos
			Perdida	Poco control fisico de los terminales y portailidad de los mismos
			Daños fisicos	Golpes o caidas
E67	TALENTO HUMANO	Personal del Area de Sistemas	Falta de supervisión y mantenimiento de los sistemas y equipos, lo que puede llevar a fallos técnicos y aumentar la probabilidad de i ataques.	Falta de personal
			Dificultad para responder a emergencias y resolver problemas técnicos de manera eficiente.	
			Problemas para llevar a cabo las tareas diarias y garantizar la disponibilidad y continuidad del servicio.	
			Gasto de tiempo en la capacitacion de nuevo personal por contrato que tiende a rotar cada ciclo a la alcaldia de Azogues	
			Carga de trabajo exesiva	
			Falta de documentacion	Personal unico e indispensable
			Conocimiento tecnico especifico de la infraestructura de TI para el personal nuevo	
			Falta de conocimiento frente a sistemas personalizados para el personal nuevo	
			Ausencia de un plan de continuidad frente a la ausencia permanente del personal	
E68		Funcionarios de la empresa no pertenecientes al area de Sistemas	Acceso no autorizado a traves de diversos metodos	Contraseñas debiles
			Olvidos/Contraseñas expuestas y accesos no autorizados	Mal manejo de las contraseñas de ingreso al terminal
				Desconocimiento de credenciales de ingreso a la terminal
				Mal manejo de las contraseñas de ingreso a la plataforma de trabajo
				Desconocimiento de credenciales de ingreso a la terminal
			Contraseñas expuestas/Accesos no autorizados/Alteracion de la informacion	Conocimiento de terceros de la contraseña de ingreso al terminal
			Credenciales expuestas/Accesos no autorizados/Alteracion de la informacion	Conocimiento de terceros de las credenciales personales para el ingreso a la plataforma de trabajo
			Accesos no autorizados/Alteracion de la informacion	Acceso a la terminal de trabajo por terceros en la empresa
			Proteccion limitada del equipo frente a malware	Uso de terminales personales para laborar en el trabajo
			Perdida de confidencialidad de la informacion	
			Problemas de compatiibilidad	
			Incumplimiento de normativas	
			Hurto	Horas extras en la empresa
			Perdida de la confidencialidad de la informacion	Horas extras desde fuera de la empresa

			Proteccion limitada del equipo frente a malware	Horas extras desde fuera de la empresa
			Perdida de la integridad de la informacion debido a falta de imparcialidad y/o conflicto de intereses	Relaciones familiares en la empresa
			Perdida de la integridad de la informacion debido a falta de imparcialidad y/o conflicto de intereses	Relaciones sentimentales/afectivas en la empresa
			Sabotajes/Alteracion de la informacion	Ambiente laboral malo en la empresa
			Sabotajes/Alteracion de la informacion	Altercados entre empleados de la empresa
			Contaminacion de la red con malware	Uso de la red wifi de la empresa en dispositivos personales
			Accesos no autorizados/Alteracion de la informacion	Terminales activas por parte de los empleados al ausentarse por momentos(almuerzo,reunion,etc)
			Accesos no autorizados/Alteracion de la informacion	Terminales activas por parte de los empleados al finalizar con la jornada laboral
			Hurto/perdida de confidencialidad	Llevarse terminales de la empresa al hogar para realizar labores
			Pishing	Uso inadecuado del correo insitucional
E69	INSTITUCIONAL	Departamento de TI	Accionar a nivel de apoyo unicamente	Nivel incorrecto dentro del organigrama
			Reformas a planes operativos	Depende de la direccion administrativa
			Cambios en la planeacion prevista	Depende de la direccion administrativa
			Falta de autonomia, y operatividad	No cuenta con una estructura propia con sus propio departamentos y procesos
			Falta de actualizacion y/o adquisicion de software y hardware	Excesiva burocratizacion para la adquisicion o renovacion de activos de TI

ANEXO 7: TABLA CONTROLES EXISTENTES

ANALISIS DE RIESGOS					**Controles Implementados**
N	**Proceso**	**Nombre**	**Amenazas**	**Vulnerabilidades**	
E1	Infraestructura	Proliant dl360 gen10	Fallos en los componentes	Antigüedad del servidor de más de 10 años	Mantenimiento Local
			Problemas de rendimiento		Mantenimiento Local
			Problemas de capacidad de almacenamiento		Mantenimiento Local
			Compatibilidad con Software Obsoleto		Mantenimiento Local
			Problemas de escalabilidad		Mantenimiento Local
			Hurto	Seguridad inadecuada para acceder al centro de datos	Cerrado bajo llave
			Perdida total de la Informacion	Falta de respaldos del servidor	Sin control
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada	Ventanas abiertas con mallas

				ventilacion/filtracion de aire	
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	Sin control
			Subidas o bajadas de tension	Fallo en la red electrica	Uso de UPS
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño	Sin control
E2		HP ML350 G8 V2	Fallos en los componentes	Antigüedad del servidor de 10 años	Mantenimiento Local
			Problemas de rendimiento		Mantenimiento Local
			Problemas de capacidad de almacenamiento		Mantenimiento Local
			Compatibilidad con Software Obsoleto		Mantenimiento Local
			Problemas de escalabilidad		Mantenimiento Local
			Hurto	Seguridad inadecuada para acceder al centro de datos	Cerrado bajo llave
			Perdida total de la Informacion	Falta de respaldos del servidor	Sin control
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	Ventanas abiertas con mallas
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	Sin control
			Subidas o bajadas de tension	Fallo en la red electrica	Uso de UPS
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño	Sin control
E3		HP ML350 G8 V2	Fallos en los componentes	Antigüedad del servidor de 10 años	Uso no permanente/Mantenimiento Local
			Problemas de rendimiento		Uso no permanente/Mantenimiento Local
			Problemas de capacidad de almacenamiento		Uso no permanente/Mantenimiento Local
			Compatibilidad con Software Obsoleto		Uso no permanente/Mantenimiento Local
			Problemas de escalabilidad		Uso no permanente/Mantenimiento Local
			Hurto	Seguridad inadecuada para acceder al centro de datos	Cerrado bajo llave

			Perdida total de la Informacion	Falta de respaldos del servidor	Sin control
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	Ventanas abiertas con mallas
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	Sin control
			Subidas o bajadas de tension	Fallo en la red electrica	Uso de UPS
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño	Sin control
E4		Proliant dl360 gen10	Hurto	Seguridad inadecuada para acceder al centro de datos	Cerrado bajo llave
			Perdida total de la Informacion	Falta de respaldos del servidor	Informacion respaldada por el proveedor de internet y de forma fisica
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	Ventanas abiertas con mallas
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	Sin control
			Subidas o bajadas de tension	Fallo en la red electrica	Uso de UPS
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño	Sin control
E5		Proliant dl380 gen9	Fallos en los componentes	Antigüedad del servidor de 9 años	Mantenimiento Local
			Problemas de rendimiento		Mantenimiento Local
			Problemas de capacidad de almacenamiento		Mantenimiento Local
			Compatibilidad con Software Obsoleto		Mantenimiento Local
			Problemas de escalabilidad		Mantenimiento Local
			Hurto	Seguridad inadecuada para acceder al centro de datos	Cerrado bajo llave
			Perdida total de la Informacion	Falta de respaldos del servidor	Informacion respaldada por el proveedor de internet y de forma fisica
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada	Ventanas abiertas con mallas

				ventilacion/filtracion de aire	
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	Sin control
			Subidas o bajadas de tension	Fallo en la red electrica	Uso de UPS
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño	Sin control
E6		HP Compaq Pro 6300	Fallo del equipo	Hardware no dedicado para ejercer como servidor	Mantenimiento Local
			Fallos en los componentes	Antigüedad del equipo de 10 años estimados	Mantenimiento Local
			Problemas de rendimiento		Mantenimiento Local
			Problemas de capacidad de almacenamiento		Mantenimiento Local
			Compatibilidad con Software Obsoleto		Mantenimiento Local
			Problemas de escalabilidad		Mantenimiento Local
			Hurto	Seguridad inadecuada para acceder a la oficina de TI	Cerrado bajo llave
			Perdida total de la Informacion	Falta de respaldos del servidor	Sin control
			Recalentamiento del equipo	Ubicado en el departamento de TI	Mantenimiento Local
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicado en el departamento de TI	Mantenimiento local
			Subidas o bajadas de tension	Fallo en la red electrica	Uso de UPS
E7		HP ML115 G1	Fallos en los componentes	Antigüedad del servidor de mas de 10 años	Uso no permanente/Mantenimiento Local
			Problemas de rendimiento		Uso no permanente/Mantenimiento Local
			Problemas de capacidad de almacenamiento		Uso no permanente/Mantenimiento Local
			Compatibilidad con Software Obsoleto		Uso no permanente/Mantenimiento Local
			Problemas de escalabilidad		Uso no permanente/Mantenimiento Local
			Hurto	Seguridad inadecuada para acceder a la oficina de TI	Cerrado bajo llave
			Perdida total de la Informacion	Falta de respaldos del servidor	Sin control
			Recalentamiento del equipo	Ubicado en el departamento de TI	Sin control
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicado en el departamento de TI	Sin control
			Subidas o bajadas de tension	Fallo en la red electrica	Uso de UPS

E8	OS	Ubuntu 18	Fallas de seguridad, estabilidad y rendimiento	Configuracion Inadecuada	Mantenimiento local
			Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Soporte proximo a finalizar en abril del 2023	Mantenimiento local
E9		Ubuntu 18	Fallas de seguridad, estabilidad y rendimiento	Configuracion Inadecuada	Mantenimiento local
			Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Soporte proximo a finalizar en abril del 2023	Mantenimiento local
E10		Windows Server 2008	Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Sistema Operativo sin soporte	Software en su ultima version
			Vulnerabilidades detectadas	Sistema Operativo sin las ultimas actualizaciones	Software en su ultima version
E11		Windows Server 2008	Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Sistema Operativo sin soporte	Software en su ultima version
			Vulnerabilidades detectadas	Sistema Operativo sin las ultimas actualizaciones	Software en su ultima version
E12		Windows Server 2003	Fallos y vulnerabilidad a amenazas	Sistema Operativo sin soporte	Software en su ultima version
			Vulnerabilidades detectadas	Sistema Operativo sin las ultimas actualizaciones	Software en su ultima version
E13		Windows Server 2003	Fallos y vulnerabilidad a amenazas	Sistema Operativo sin soporte	Software en su ultima version
			Explotacion de vulnerabilidades detectadas	Sistema Operativo sin las ultimas actualizaciones	Software en su ultima version
E14		Windows 10	Ataques de malware	Sin soporte como servidor	Mantenimiento local
			Bajas del rendimiento	Sin soporte como servidor	Mantenimiento local
			Intrusiones	Seguridad inadecuada para uso como servidor	Mantenimiento local
			Hackeos	Seguridad inadecuada para uso como servidor	Mantenimiento local
E15	Bases de Datos	Postgis 2.2	Explotaciones de amenazas conocidas	Version antigua del software	Software en su ultima version
			Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Software sin soporte	Software en su ultima version
E16		Postgresql 9.5	Explotaciones de amenazas conocidas	Version antigua del software	Software en su ultima version
			Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Software sin soporte	Software en su ultima version
E17	ERP	SIIIM	INFORMACION RESERVADA	INFORMACION RESERVADA	RESERVADO
E18	FIREWALL	SOPHOS SG 230 rev 1	Trafico indeseado	Configuracion inadecuada	Soporte contratado
			Intrusiones no autorizadas	Puertos abiertos no autorizados	Soporte contratado

			Vulnerabilidades detectadas	Firmware desactualizado	Soporte contratado
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño	Sin control
E19	RED	HP MSR 900	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	Firmware actualizado
			Acceso no autorizado	Contraseñas por defecto	Control tercerisado
			Acceso no autorizado	Contraseñas filtradas	Control tercerisado
			Hurto	Seguridad inadecuada para acceder al centro de datos	Cerrado bajo llave
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	Sin control
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	Sin control
			Subidas o bajadas de tension	Fallo en la red electrica	Uso de UPS
			Corte del servicio de internet	Fallo del proveedor del servicio	Control tercerisado
				Fallos del hardware	Control tercerisado
				Configuracion inadecuada del dispositivos	Control tercerisado
E20		HPE OfficeConect 1920S Series Switch	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	Firmware actualizado
			Hurto	Seguridad inadecuada para acceder al centro de datos	Cerrado bajo llave
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	Ventanas abiertas con mallas
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	Sin control
			Subidas o bajadas de tension	Fallo en la red electrica	Uso de UPS
			Desconeccion entre los servidores y la intranet de la empresa	Fallos del hardware	Mantenimiento local
				Configuracion inadecuada del dispositivos	Mantenimiento local
			Mayor latencia de datos	Cableado desordenado	Mantenimiento local
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	Cableado etiquetado

			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	Cableado etiquetado
E21		HPE OfficeConect 1920S Series Switch	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	Firmware actualizado
			Hurto	Seguridad inadecuada para acceder al centro de datos	Cerrado bajo llave
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	Ventanas abiertas con mallas
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	Sin control
			Subidas o bajadas de tension	Fallo en la red electrica	Uso de UPS
			Desconeccion del servicio de red en la planta baja	Fallos del hardware	Mantenimiento local
				Configuracion inadecuada del dispositivos	Mantenimiento local
			Mayor latencia de datos	Cableado desordenado	Mantenimiento local
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	Cableado etiquetado
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	Cableado etiquetado
E22		HPE OfficeConect 1920S Series Switch	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	Firmware actualizado
			Hurto	Seguridad inadecuada para acceder al centro de datos	Cerrado bajo llave
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	Ventanas abiertas con mallas
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	Sin control
			Subidas o bajadas de tension	Fallo en la red electrica	Uso de UPS
			Desconeccion del servicio de red en la planta baja	Fallos del hardware	Mantenimiento local
				Configuracion inadecuada del dispositivos	Mantenimiento local
			Mayor latencia de datos	Cableado desordenado	Mantenimiento local
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	Cableado etiquetado
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	Cableado etiquetado
E23		PE Aruba Instant On	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	Firmware actualizado

		1930 24G 4SFP/SFP	Hurto	Seguridad inadecuada para acceder al centro de datos	Cerrado bajo llave
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	Ventilacion a traves de la ventana abierta hacia el centro de datos
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	Sin control
			Subidas o bajadas de tension	Fallo en la red electrica	Uso de UPS
			Desconeccion del servicio de telefonia IP en la planta baja	Fallos del hardware	Mantenimiento local
				Configuracion inadecuada del dispositivos	Mantenimiento local
			Interferencias electromagneticas	Cableado desordenado	Mantenimiento local
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	Cableado etiquetado
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	Cableado etiquetado
E24		HPE OfficeConect 1920S Series Switch	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	Firmware actualizado
			Hurto	Seguridad inadecuada para acceder al centro de datos	Cerrado bajo llave
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	Ventilacion a traves de la ventana abierta hacia el centro de datos
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	Sin control
			Subidas o bajadas de tension	Fallo en la red electrica	Uso de UPS
			Desconeccion del servicio de red en los pisos superiores	Fallos del hardware	Mantenimiento local
				Configuracion inadecuada del dispositivos	Mantenimiento local
			Mayor latencia de datos	Cableado desordenado	Mantenimiento local
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	Cableado etiquetado
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	Cableado etiquetado
E25		PE Aruba Instant On 1930 24G 4SFP/SFP	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	Firmware actualizado
			Manejo inadecuado por personal no capacitado	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	Sin control

			Hurto	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	Sin control
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	Sin control
			Subidas o bajadas de tension	Fallo en la red electrica	Sin control
			Desconeccion del servicio de telefonia IP en el piso 1	Fallos del hardware	Mantenimiento local
				Configuracion inadecuada del dispositivos	Mantenimiento local
			Interferencias electromagneticas	Cableado desordenado	Mantenimiento local
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	Cableado etiquetado
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	Cableado etiquetado
E26		HPE OfficeConect 1920S Series Switch	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	Firmware actualizado
			Manejo inadecuado por personal no capacitado	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	Sin control
			Hurto	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	Sin control
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	Sin control
			Subidas o bajadas de tension	Fallo en la red electrica	Sin control
			Desconeccion del servicio de red en el piso 1	Fallos del hardware	Mantenimiento local
				Configuracion inadecuada del dispositivos	Mantenimiento local
			Mayor latencia de datos	Cableado desordenado	Mantenimiento local
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	Cableado etiquetado
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	Cableado etiquetado
E27		PE Aruba Instant On 1930 24G 4SFP/SFP	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	Firmware actualizado
			Manejo inadecuado por personal no capacitado	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	Sin control
			Hurto	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	Sin control
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicación inadecuada con acceso limitado a	Sin control

				personal no autorizado de la empreza	
			Subidas o bajadas de tension	Fallo en la red electrica	Sin control
			Desconeccion del servicio de telefonia IP en el piso 2	Fallos del hardware	Mantenimiento local
				Configuracion inadecuada del dispositivos	Mantenimiento local
			Interferencias electromagneticas	Cableado desordenado	Mantenimiento local
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	Cableado etiquetado
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	Cableado etiquetado
E28		HPE OfficeConect 1920S Series Switch	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	Firmware actualizado
			Manejo inadecuado por personal no capacitado	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	Sin control
			Hurto	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	Sin control
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	Sin control
			Subidas o bajadas de tension	Fallo en la red electrica	Sin control
			Desconeccion del servicio de red en el piso 2	Fallos del hardware	Mantenimiento local
				Configuracion inadecuada del dispositivos	Mantenimiento local
			Mayor latencia de datos	Cableado desordenado	Mantenimiento local
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	Cableado etiquetado
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	Cableado etiquetado
E29		APX 530	Hurto	Entrada de personas no autorizadas	Camaras/ Guardias
			Daños Fisicos	Maltrato/ Caida	Mantenimiento local
			Alta latencia	Interferencia electromagnetica	Mantenimiento local
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicacion elevada	Mantenimiento local
			Subidas o bajadas de tension	Fallo en la red electrica	Sin control
			Indisponibilidad del servicio	Fallos en los componentes	Mantenimiento local
			Indisponibilidad del servicio	Configuracion inadecuada	Mantenimiento local
			Fallos y explotacion de vulnerabilidades	Firmware desactualizado	Mantenimiento local
			Alta latencia	Trafico de red exesivo	Mantenimiento local
E30		AP 55C	Hurto	Acceso libre al dispositivo	Camaras/ Guardias

			Daños Fisicos	Maltrato/ Caida	Mantenimiento local
			Alta latencia	Interferencia electromagnetica	Mantenimiento local
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicacion elevada	Mantenimiento local
			Subidas o bajadas de tension	Fallo en la red electrica	Sin control
			Indisponibilidad del servicio	Fallos en los componentes	Mantenimiento local
			Indisponibilidad del servicio	Configuracion inadecuada	Mantenimiento local
			Fallos y explotacion de vulnerabilidades	Firmware desactualizado	Mantenimiento local
			Alta latencia	Trafico de red exesivo	Mantenimiento local
E31		AP 55C	Hurto	Acceso libre al dispositivo	Camaras/ Guardias
			Daños Fisicos	Maltrato/ Caida	Mantenimiento local
			Alta latencia	Interferencia electromagnetica	Mantenimiento local
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicacion elevada	Mantenimiento local
			Subidas o bajadas de tension	Fallo en la red electrica	Sin control
			Indisponibilidad del servicio	Fallos en los componentes	Mantenimiento local
			Indisponibilidad del servicio	Configuracion inadecuada	Mantenimiento local
			Fallos y explotacion de vulnerabilidades	Firmware desactualizado	Mantenimiento local
			Alta latencia	Trafico de red exesivo	Mantenimiento local
E32		AP 55C	Hurto	Acceso libre al dispositivo	Camaras/ Guardias
			Daños Fisicos	Maltrato/ Caida	Mantenimiento local
			Alta latencia	Interferencia electromagnetica	Mantenimiento local
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicacion elevada	Mantenimiento local
			Subidas o bajadas de tension	Fallo en la red electrica	Sin control
			Indisponibilidad del servicio	Fallos en los componentes	Mantenimiento local
			Indisponibilidad del servicio	Configuracion inadecuada	Mantenimiento local
			Fallos y explotacion de vulnerabilidades	Firmware desactualizado	Mantenimiento local
			Alta latencia	Trafico de red exesivo	Mantenimiento local
E33		Cableado Vertical Fibra Optica	Destrucion	Daño fisico/Rotura/Cortes	Mantenimiento local
			Alta latencia	Interferencia electromagnetica	Mantenimiento local
E34		Cableado Horizontal UTP CAT 6/ 6A	Destrucion	Daño fisico/Rotura/Cortes	Mantenimiento local
			Alta latencia	Interferencia electromagnetica	Mantenimiento local
E35		Redes VLAN	Accesos no autorizados	Configuracion incompleta	Mantenimiento local
			Conflicto de direcciones IP		Mantenimiento local

			Dificultad par reconfigurar las VLANS		Mantenimiento local
			Bajo rendimiento de la red		Mantenimiento local
			Ataque de snooping	Filtracion de la tabla de subredes	Direccionamiento confidencial
			Accesos no autorizados a subredes	Filtracion de la tabla de subredes	Direccionamiento confidencial
			Interrupcion de servicios	Filtracion de la tabla de subredes	Direccionamiento confidencial
E36		Redes Wireless	Accesos a redes con permisos superirores	Filtracion de contraseñas	Sin control
			Accesos no autorizados	Contraseñas debiles	Politica de contraseñas
			Ataques de fuerza bruta y diccionarios de contraseñas	Contraseñas debiles	Politica de contraseñas
			Intercepcion de trafico de red	Cifrado de red debil	WPA2 PSK
			Inyeccion de paquetes	Cifrado de red debil	WPA2 PSK
			Menor privacidad, seguridad y control	Redes wifi visibles	Sin control
E37		Antena Ubiquiti Nanostation M5 LOC0	Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Exposicion al aire libre	Mantenimiento local
			Desgaste por el clima	Exposicion al aire libre	Mantenimiento local
			Sobrecarga electrica	Rayos	Sin control
			Caidas/ Vibraciones exesivas	Instalacion incorrecta	Mantenimiento local
			Daño fisico	Mantenimiento inadecuado	Mantenimiento ocacional
E38	TELEFONIA	Panasonic KX-NS500	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	Firmware actualizado
			Hurto	Seguridad inadecuada para acceder al centro de datos	Cerrado bajo llave
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	Ventilacion hacia el centro de datos 1 a traves de una ventana
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	Sin control
			Subidas o bajadas de tension	Fallo en la red electrica	Uso de UPS
			Fallo del servicio de telefonia IP	Fallos del hardware	Mantenimiento local
				Configuracion inadecuada del dispositivos	Mantenimiento local
E39	UPS	Eaton 906 IIS	Fallas de la bateria y daños en la electronica	Tiempo de vida de uso prolongado	Mantenimiento local
				Sobrecargas, descargas electricas	Mantenimiento local
				Degradacion natural	Mantenimiento local
				Mala estimacion de la carga	Mantenimiento local
E40		APC SRT2200XLA		Tiempo de vida de uso prolongado	Mantenimiento local

				Sobrecargas, descargas electricas	Mantenimiento local
				Degradacion natural	Mantenimiento local
				Mala estimacion de la carga	Mantenimiento local
E41		APC SRT2200XLA		Tiempo de vida de uso prolongado	Mantenimiento local
				Sobrecargas, descargas electricas	Mantenimiento local
				Degradacion natural	Mantenimiento local
				Mala estimacion de la carga	Mantenimiento local
E42		Forza FDC-003K		Tiempo de vida de uso prolongado	Mantenimiento local
				Sobrecargas, descargas electricas	Mantenimiento local
				Degradacion natural	Mantenimiento local
				Mala estimacion de la carga	Mantenimiento local
E43	Dominio/IP Y Subdominios	emapal.gob.ec/ 207.174.XXX.XXX/egob, edoc, etc	Explotacion de vulnerabilidades relacionadas con Open SSH 7.4	Vulnerabilidades en el puerto 22 y 2222 relacionadas al uso de Open SSH 7.4	Sin control
			Panel de logeo a CPANEL publica, ingreso no autorizado a traves de fuerza bruta, diccionarios, pishing,ingenieria social.	Acceso publico al puerto 2082 y 2083	Sin control
			Panel de logeo a WebHostManager publica, ingreso no autorizado a traves de fuerza bruta, diccionarios, pishing,ingenieria social.	Acceso publico al puerto 2086 y 2087	Sin control
E44	Pagina Web	www.emapal.gob.ec	Informacion erronea	Web desactualizada	Mantenimiento local
			Falta de informacion	Web desactualizada	Mantenimiento local
			Explotacion de vulnerabilidades propias de la plataforma/servicio	Puerto y subdominio visible en el servicio de recursos humanos	Mantenimiento local
			Ataques de fuerza bruta	Puerto y subdominio visible en el servicio de recursos humanos	Mantenimiento local
			Informacion sensible de la estructura de la plataforma vuelta publica	Puerto y subdominio visible en el servicio de recursos humanos	Mantenimiento local
E45	Servicio de Correo Masivo	Correo Masivo	Desconeccion con el servicio	Problemas tecnicos	Control tercerisado
			Desconeccion con el servicio	Desconeccion de la intranet de la empresa con internet	Control tercerisado
			Perdida del control de datos	No ser dueños del servicio	Control tercerisado
			Ataques de fuerza bruta o de diccionarios	Contraseñas inadecuadas	Politica de contraseñas
E46	Servicio de Correo Corporatico	Correo Corporativo	Desconeccion con el servicio	Problemas tecnicos	Control tercerisado
			Desconeccion con el servicio	Desconeccion de la intranet de la empresa con internet	Control tercerisado

			Perdida del control de datos	No ser dueños del servicio	Control tercerisado
			Filtracion de informacion	Uso de correo institucional para servicios externos	Politicas de uso de correos
			Descargas de malware	Uso de correo institucional para servicios externos	Politicas de uso de correos
			Filtracion de credenciales y/o informacion persona o de la empresa	Correos con Pishing	Sin control
			Infeccion de la red/ terminal	Correos infectados de malware	Firewall / Antivirus
			Ataques de fuerza bruta o de diccionarios	Contraseñas inadecuadas	Politica de contraseñas
E47	Software	Consolas	Ataques de fuerza bruta o de diccionarios	Contraseñas inadecuadas	Politica de contraseñas
			Codigo malicioso	Exploits de software	Software actualizado
			Codigo malicioso	Inyeccion de codigo	Software actualizado
E48	BACKUPS	Respaldo disco duro externo	Perdida	Objeto transportable y accesible	Almacenamiento bajo llave
			Destruccion	Sensible a agentes fisicos, caidas, golpes	Almacenamiento bajo llave
			Hurto	Objeto transportable y accesible	Almacenamiento bajo llave
			Perdida de datos	Daño mecanico, caidas golpes, agentes fisicos	Manejo adecuado
			Robo de datos	Falta de contraseña/encriptacion	Disco duro cifrado
E49		Respaldo Telconet	Robo/Alteracion de la informacion	Acceso no autorizado	Control tercerisado
			Corrupcion/Perdida de datos	Error humano	Control tercerisado
			Corrupcion/Perdida de datos	Fallos en el hardware donde se almacena	Control tercerisado
			Destruccion del hardware donde se almacena el respaldo	Desastres naturales	Control tercerisado
			Destruccion del hardware donde se almacena el respaldo	Amenazas ambientales	Control tercerisado
E50	ANTIVIRUS	Kaspersky	Malware	Antivirus desactualizado	Antivirus actualizado
E51	ASISTENCIA	MB360 ZKTECO	Registro erroneo	Fecha y hora incorrectas	Mantenimiento local
			Registro erroneo	Identificacion erronea	Mantenimiento local
			Daño	Daño mecanico, caidas golpes, agentes fisicos	Mantenimiento local
			Destruccion	Daño mecanico, caidas golpes, agentes fisicos	Mantenimiento local
E52		Biotime 8.0	Explotacion de vulnerabilidades	Firmware desactualizado	Mantenimiento local
			Ataques de fuerza bruta o de diccionarios	Contraseñas inadecuadas	Politica de contraseñas
			Robo de informacion biometrica	Firmware desactualizado	Firmware actualizado

			Robo de informacion biometrica	Contraseñas inadecuadas	Politica de contraseñas
E53	SEGURIDAD	Camaras de seguridad	Vandalismo o robo	Activos en lugares accesibles	Camaras/Guardias de seguridad
			Daño	Daño mecanico, caidas golpes, agentes fisicos	Sin control
			Destruccion	Daño mecanico, caidas golpes, agentes fisicos	Sin control
			Fallos en el funcionamiento, baja resolucion de las imágenes	Camaras antiguas	Sin control
			Puntos ciegos ubicados en los lugares donde las camaras no funcionan	Camaras sin funcionamiento	Sin control
			Acceso no autorizado , intrusiones	Asignacion de una ip publicas a traves del dominio para que esten disponibles para el director administrativo desde su dispositivo movil	Sin control
			Inyeccion de codigo malicioso y/o spyware	Asignacion de una ip publicas a traves del dominio para que esten disponibles para el director administrativo desde su dispositivo movil	Sin control
E54		DVR modelo desconocido	Intrusiones por credenciales debiles/nulas	Sistema de camaras a cargo de la direccion administrativa	Sin control
			Intruciones a puertos abiertos	Sistema de camaras a cargo de la direccion administrativa	Sin control
			Explotacion de vulnerabilidades por software desactualizado	Sistema de camaras a cargo de la direccion administrativa	Sin control
			Infecciones de malware	Sistema de camaras a cargo de la direccion administrativa	Sin control
			Fallos debido a configuracion inadecuada	Sistema de camaras a cargo de la direccion administrativa	Sin control
			Hurto	Seguridad inadecuada	Sin control
			Destruccion del equipo	Manipulacion del dispositivo	Sin control
			Recalentamiento del equipo	Ubicación inadecuada	Sin control
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicación inadecuada	Sin control
			Subidas o bajadas de tension	Fallo en la red electrica	Sin control
E55	RACKS	Rack 1 Centro de Datos 1	Daño por fallas mecánicas	Derrame de líquidos	Mantenimiento Local
			Daño por fallas mecánicas	Humedad y corrosión	Mantenimiento Local
			Daño por fallas mecánicas	Vibración excesiva	Mantenimiento Local
			Daño por fallas mecánicas	Sobrecarga de peso	Mantenimiento Local
			Daño por fallas mecánicas	Fallas en los soportes	Mantenimiento Local

E56		Rack 2 Centro de datos 2	Daño por fallas mecánicas	Derrame de líquidos	Mantenimiento Local
			Daño por fallas mecánicas	Humedad y corrosión	Mantenimiento Local
			Daño por fallas mecánicas	Vibración excesiva	Mantenimiento Local
			Daño por fallas mecánicas	Sobrecarga de peso	Mantenimiento Local
			Daño por fallas mecánicas	Fallas en los soportes	Mantenimiento Local
E57		Rack Centro de Datos 2	Daño por fallas mecánicas	Derrame de líquidos	Mantenimiento Local
			Daño por fallas mecánicas	Sol, Humedad Corrosión	Mantenimiento Local
			Daño por fallas mecánicas	Vibración excesiva	Mantenimiento Local
			Daño por fallas mecánicas	Sobrecarga de peso	Mantenimiento Local
			Daño por fallas mecánicas	Fallas en los soportes	Mantenimiento Local
E58		Rack Piso 1	Daño por fallas mecánicas	Sol Humedad , Corrosión	Mantenimiento Local
			Daño por fallas mecánicas	Vibración excesiva	Mantenimiento Local
			Daño por fallas mecánicas	Sobrecarga de peso	Mantenimiento Local
			Daño por fallas mecánicas	Fallas en los soportes	Mantenimiento Local
			Incendios/Desastres ambientales	Rack abierto	Sin control
			Daño en los equipos al momento de mitigar un incendio	Falta de extintores de CO2	Extintores tradicionales
E59		Rack Piso 2	Daño por fallas mecánicas	Humedad y corrosión	Mantenimiento Local
			Daño por fallas mecánicas	Vibración excesiva	Mantenimiento Local
			Daño por fallas mecánicas	Sobrecarga de peso	Mantenimiento Local
			Daño por fallas mecánicas	Fallas en los soportes	Mantenimiento Local
			Incendios/Desastres ambientales/Hurto	Rack abierto	Sin control
			Incendio/Acumulacion de polvo	Almacenamiento de documentacion fisica cercana	Sin control
			Daño en los equipos al momento de mitigar un incendio	Falta de extintores de CO2	Extintores tradicionales
E60	UBICACIÓN FISICA	Edificio Matriz	Robo, Vandalismo	Seguridad Fisica Inadecuada	Camaras / Seguridad privada
			Inundacion	Desborde del rio	Sin control
			Destruccion del edificio	Incendios	Extintores
			Daños	Daño por agentes medioambientales, climatologicos	Mantenimiento
E61		Centro de Datos 1	Sobrecalentamiento/Acumulacion de polvo	Ventilacion y climatizacion inadecuada	Ventilacion natural a traves de dos ventanas enrejadas
			Intrusiones/Hurto/Destruccion de equipos	Poca seguridad para el ingreso al centro de datos	Entrada bajo llave
			Intrusiones/Hurto/Destruccion de equipos	Ventana que da al exterior	Camaras/ Guardias
			Inundacion	Colinda con un baño	Sin control
			Inundacion	Ubicado en la primera planta	Sin control
			Incendios/Desastres ambientales/Polvo	Piso flotante	Sin control
			Incendios/Desastres ambientales	Racks abiertos	Sin control
			Acumulacion de polvo	Almacenamiento de equipos en desuso	Equipos en desuso acomodados en una esquina

			Daño en los equipos al momento de mitigar un incendio	Falta de extintores de CO2	Sin control
			Intrusiones/Hurto/Destruccion de equipos	Falta de monitoreo de seguridad	Sin control
			Cambios ambientales	Falta de monitoreo ambiental	Sin control
			Subidas , bajadas de tension o cortes electricos	Falta de monitoreo electrico	Sin control
			Ingresos no autorizados	Registro de ingreso	Sin control
E62		Centro de Datos 2	Sobrecalentamiento/Acumulacion de polvo	Ventilacion y climatizacion inadecuada	Ventana abierta hacia el centro de datos 1
			Intrusiones/Hurto/Destruccion de equipos	Poca seguridad para el ingreso al centro de datos	Entrada bajo llave
			Inundacion	Colinda con un baño	Sin control
			Inundacion	Ubicado en la primera planta	Sin control
			Acumulacion de polvo, incendios	Almacenamiento de equipos en desuso y cajas	Limpieza ocacional
			Daño en los equipos al momento de mitigar un incendio	Falta de extintores de CO2	Sin control
			Intrusiones/Hurto/Destruccion de equipos	Falta de monitoreo de seguridad	Sin control
			Cambios ambientales	Falta de monitoreo ambiental	Sin control
			Subidas , bajadas de tension o cortes electricos	Falta de monitoreo electrico	Sin control
			Ingresos no autorizados	Falta de registro de ingreso	Sin control
E63		Oficina de Sistemas	Sobrecalentamiento/Acumulacion de polvo	Ventilacion y climatizacion inadecuada	Abrir ventanas/ Limpieza
			Intrusiones/Hurto/Destruccion de equipos	Poca seguridad para el ingreso a la oficina	Entrada bajo llave
			Inundacion	Ubicado en la primera planta	Sin control
			Acumulacion de polvo	Falta de limpieza	Limpieza
			Daño en los equipos al momento de mitigar un incendio	Falta de extintores de CO2	Sin control
			Intrusiones/Hurto/Destruccion de equipos	Ventanas con acceso al exterior	Camaras
			Destruccion o daño de los equipos	Subidas , bajadas de tension o cortes electricos	Sin control
			Ingresos no autorizados	Ausencia de registro de ingreso	Sin control
			Destruccion o daño	Incendios/Desastres ambientales/Polvo	Sin control
E64		Terraza y soporte de la antena	Intrusiones/Hurto/Destruccion de equipos	Acceso no autorizado	Acceso limitado
			Degradacion por agentes ambientales	Falta de mantenimiento y limpieza	Mantenimiento ocacional
E65	TERMINALES DE LOS	Computadoras de escritorio	Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Terminales con OS WINDOWS 7(sin soporte)	Equipos actualizados a la ultima version

	EMPLEADOS		Vulnerabilidades detectadas	Terminales desactualizadas	Mantenimiento Local
			Fallos en los componentes	Terminales con una antigüedad estimada en 17 años	Mantenimiento Local
			Problemas de rendimiento		Mantenimiento Local
			Problemas de capacidad de almacenamiento		Mantenimiento Local
			Compatibilidad con Software Obsoleto		Mantenimiento Local
			Problemas de escalabilidad		Mantenimiento Local
			Fallos en los componentes	Terminales con una antigüedad estimada en 11 años	Mantenimiento Local
			Problemas de rendimiento		Mantenimiento Local
			Problemas de capacidad de almacenamiento		Mantenimiento Local
			Compatibilidad con Software Obsoleto		Mantenimiento Local
			Problemas de escalabilidad		Mantenimiento Local
			Fallos en los componentes	Terminales con una antigüedad estimada en 7 años	Mantenimiento Local
			Problemas de rendimiento		Mantenimiento Local
			Problemas de capacidad de almacenamiento		Mantenimiento Local
			Compatibilidad con Software Obsoleto		Mantenimiento Local
			Problemas de escalabilidad		Mantenimiento Local
			Rendimiento probre	Terminales con procesadores viejos y de poca capacidad	Mantenimiento Local
			Sobrecalentamiento		Mantenimiento Local
			Pantallasos azules		Mantenimiento Local
			Reinicios Inesperados		Mantenimiento Local
			Corrupcion/Perdida de datos		Mantenimiento Local
			Aplicaciones que no responden	Terminales con 2 - 3 GB de RAM	Mantenimiento Local
			Bajo rendimiento		Mantenimiento Local
			Reinicios Inesperados		Mantenimiento Local
			Corrupcion/Perdida de datos		Mantenimiento Local
			Aplicaciones que no responden	Terminales con 4 GB de RAM	Mantenimiento Local
			Bajo rendimiento		Mantenimiento Local
			Conflicto de tareas	Terminales compartidas entre empleados	Cuentas de usuario
			Filtracion de datos		Cuentas de usuario
			Desorganizacion de archivos e informacion		Cuentas de usuario
			Uso ineficiente del terminal		Cuentas de usuario
			Infeccion de malware	Conexión de dispositivos personales a terminales de la empreza	Registro de actividades del terminal
			Robo de datos		Registro de actividades del terminal
			Conflictos en la politica de seguridad		Registro de actividades del terminal
			Accesos no autorizados	Contraseñas debiles para acceso al terminal	Politica de contraseñas
			Accesos no autorizados	Terminales sin contraseña	Sin control
			Accesos no autorizados	Terminales sin usuario	Sin control
			Llevarse los terminales de forma no autorizada fuera de la empresa	Poco control fisico de los terminales	Sin control

			Subidas o bajadas de tension	Fallo en la red electrica	Sin control
			Destruccion por inundacion	Aumento del caudal del rio/ lluvia	Sin control
			Daños fisicos	Golpes o caidas	Sin control
E66		Computadoras portatiles	Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Terminales con OS WINDOWS 7(sin soporte)	Equipos actualizados a la ultima version
			Vulnerabilidades detectadas	Terminales desactualizadas	Mantenimiento Local
			Fallos en los componentes	Terminales con una antigüedad estimada en 15 años	Mantenimiento Local
			Problemas de rendimiento		Mantenimiento Local
			Problemas de capacidad de almacenamiento		Mantenimiento Local
			Compatibilidad con Software Obsoleto		Mantenimiento Local
			Problemas de escalabilidad		Mantenimiento Local
			Fallos en los componentes	Terminales con una antigüedad estimada entre 9 - 11 años	Mantenimiento Local
			Problemas de rendimiento		Mantenimiento Local
			Problemas de capacidad de almacenamiento		Mantenimiento Local
			Compatibilidad con Software Obsoleto		Mantenimiento Local
			Problemas de escalabilidad		Mantenimiento Local
			Fallos en los componentes	Terminales con una antigüedad estimada en 7 años	Mantenimiento Local
			Problemas de rendimiento		Mantenimiento Local
			Problemas de capacidad de almacenamiento		Mantenimiento Local
			Compatibilidad con Software Obsoleto		Mantenimiento Local
			Problemas de escalabilidad		Mantenimiento Local
			Rendimiento probre	Terminales con procesadores viejos y de poca capacidad	Mantenimiento Local
			Sobrecalentamiento		Mantenimiento Local
			Pantallasos azules		Mantenimiento Local
			Reinicios Inesperados		Mantenimiento Local
			Corrupcion/Perdida de datos		Mantenimiento Local
			Aplicaciones que no responden	Terminales con 2 - 3 GB de RAM	Mantenimiento Local
			Bajo rendimiento		Mantenimiento Local
			Reinicios Inesperados		Mantenimiento Local
			Corrupcion/Perdida de datos		Mantenimiento Local
			Aplicaciones que no responden	Terminales con 4 GB de RAM	Mantenimiento Local
			Bajo rendimiento		Mantenimiento Local
			Conflicto de tareas	Terminales compartidas entre empleados	Cuentas de usuario
			Filtracion de datos		Cuentas de usuario
			Desorganizacion de archivos e informacion		Cuentas de usuario
			Uso ineficiente del terminal		Cuentas de usuario
			Infeccion de malware	Conexión de dispositivos personales a	Registro de actividades del terminal
			Robo de datos		Registro de actividades del terminal

			Conflictos en la politica de seguridad	terminales de la empreza	Registro de actividades del terminal
			Accesos no autorizados	Contraseñas debiles para acceso al terminal	Politica de contraseñas
			Accesos no autorizados	Terminales sin contraseña	Sin control
			Accesos no autorizados	Terminales sin usuario	Sin control
			Hurto	Poco control fisico de los terminales y portailidad de los mismos	Sin control
			Llevarse los terminales de forma no autorizada fuera de la empresa	Poco control fisico de los terminales y portailidad de los mismos	Sin control
			Perdida	Poco control fisico de los terminales y portailidad de los mismos	Sin control
			Daños fisicos	Golpes o caidas	Sin control
E67	TALENTO HUMANO	Personal del Area de Sistemas	Falta de supervisión y mantenimiento de los sistemas y equipos, lo que puede llevar a fallos técnicos y aumentar la probabilidad de i ataques.	Falta de personal	Division de tareas entre los empleados
			Dificultad para responder a emergencias y resolver problemas técnicos de manera eficiente.		Division de tareas entre los empleados
			Problemas para llevar a cabo las tareas diarias y garantizar la disponibilidad y continuidad del servicio.		Division de tareas entre los empleados
			Gasto de tiempo en la capacitacion de nuevo personal por contrato que tiende a rotar cada ciclo a la alcaldia de Azogues		Division de tareas entre los empleados
			Carga de trabajo exesiva		Division de tareas entre los empleados
			Falta de documentacion	Personal unico e indispensable	Sin control
			Conocimiento tecnico especifico de la infraestructura de TI para el personal nuevo		Sin control
			Falta de conocimiento frente a sistemas personalizados para el personal nuevo		Sin control
			Ausencia de un plan de continuidad frente a la ausencia permanente del personal		Sin control
E68		Funcionarios de la empresa no pertenecientes al area de Sistemas	Acceso no autorizado a traves de diversos metodos	Contraseñas debiles	Politica de formato de contraseñas
			Olvidos/Contraseñas expuestas y accesos no autorizados	Mal manejo de las contraseñas de ingreso al terminal	Sin control
				Desconocimiento de credenciales de ingreso a la terminal	Sin control

				Mal manejo de las contraseñas de ingreso a la plataforma de trabajo	Sin control
				Desconocimiento de credenciales de ingreso a la terminal	Sin control
			Contraseñas expuestas/Accesos no autorizados/Alteracion de la informacion	Conocimiento de terceros de la contraseña de ingreso al terminal	Sin control
			Credenciales expuestas/Accesos no autorizados/Alteracion de la informacion	Conocimiento de terceros de las credenciales personales para el ingreso a la plataforma de trabajo	Sin control
			Accesos no autorizados/Alteracion de la informacion	Acceso a la terminal de trabajo por terceros en la empresa	Sin control
			Proteccion limitada del equipo frente a malware	Uso de terminales personales para laborar en el trabajo	Politica de no uso de dispositivos personales para laborar en la empresa
			Perdida de confidencialidad de la informacion		Politica de no uso de dispositivos personales para laborar en la empresa
			Problemas de compatiibilidad		Politica de no uso de dispositivos personales para laborar en la empresa
			Incumplimiento de normativas		Politica de no uso de dispositivos personales para laborar en la empresa
			Hurto	Horas extras en la empresa	Camaras / Registro de actividad de los terminales
			Perdida de la confidencialidad de la informacion	Horas extras desde fuera de la empresa	Sin control
			Proteccion limitada del equipo frente a malware	Horas extras desde fuera de la empresa	Sin control
			Perdida de la integridad de la informacion debido a falta de imparcialidad y/o conflicto de intereses	Relaciones familiares en la empresa	Gestion de RRHH
			Perdida de la integridad de la informacion debido a falta de imparcialidad y/o conflicto de intereses	Relaciones sentimentales/afectivas en la empresa	Gestion de RRHH
			Sabotajes/Alteracion de la informacion	Ambiente laboral malo en la empresa	Gestion de RRHH
			Sabotajes/Alteracion de la informacion	Altercados entre empleados de la empresa	Gestion de RRHH
			Contaminacion de la red con malware	Uso de la red wifi de la empresa en dispositivos personales	Segmentacion de la red y firewall
			Accesos no autorizados/Alteracion de la informacion	Terminales activas por parte de los empleados al ausentarse por	Politicas de uso de terminales

				momentos(almuerzo,reunion,etc)	
			Accesos no autorizados/Alteracion de la informacion	Terminales activas por parte de los empleados al finalizar con la jornada laboral	Politicas de uso de terminales
			Hurto/perdida de confidencialidad	Llevarse terminales de la empresa al hogar para realizar labores	Politicas de uso de terminales
			Pishing	Uso inadecuado del correo insitucional	Politicas de uso del correo
E69	INSTITUCIONAL	Departamento de TI	Accionar a nivel de apoyo unicamente	Nivel incorrecto dentro del organigrama	Sin control
			Reformas a planes operativos	Depende de la direccion administrativa	Sin control
			Cambios en la planeacion prevista	Depende de la direccion administrativa	Sin control
			Falta de autonomia, y operatividad	No cuenta con una estructura propia con sus propio departamentos y procesos	Division de tareas entre los empleados
			Falta de actualizacion y/o adquisicion de software y hardware	Excesiva burocratizacion para la adquisicion o renovacion de activos de TI	Solicitudes respectivas

ANEXO 8: TABLA EVALUACIÓN DE RIESGOS

ANALISIS DE RIESGOS					EVALUACION DE RIESGOS					
					Impacto	Probabilidad				
N	**Proceso**	**Nombre**	**Amenazas**	**Vulnerabilidades**	**VA**	**Nivel de amenaza**	**Nivel de Vulnerabilidad**	**Controles Implementados**	**Calculo de evaluacion de Riesgo**	**Nivel del riesgo**
E1	Infraestructura	Proliant dl360 gen10	Fallos en los componentes	Antigüedad del servidor de mas de 10 años	2,67	2	3	Mantenimiento Local	16,02	ALTO
			Problemas de rendimiento		2,67	2	3	Mantenimiento Local	16,02	ALTO
			Problemas de capacidad de almacenamiento		2,67	2	3	Mantenimiento Local	16,02	ALTO
			Compatibilidad con Software Obsoleto		2,67	2	3	Mantenimiento Local	16,02	ALTO
			Problemas de escalabilidad		2,67	2	3	Mantenimiento Local	16,02	ALTO
			Hurto	Seguridad inadecuada para acceder al centro de datos	2,67	1	2	Cerrado bajo llave	5,34	MEDIO
			Perdida total de la Informacion	Falta de respaldos del servidor	2,67	2	3	Sin control	16,02	ALTO

			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	2,67	2	2	Ventanas abiertas con mallas	10,68	ALTO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	2,67	2	3	Sin control	16,02	ALTO
			Subidas o bajadas de tension	Fallo en la red electrica	2,67	1	1	Uso de UPS	2,67	BAJO
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño	2,67	1	2	Sin control	5,34	MEDIO
E2		HP ML350 G8 V2	Fallos en los componentes	Antigüedad del servidor de 10 años	2,00	2	3	Mantenimiento Local	12	ALTO
			Problemas de rendimiento		2,00	2	3	Mantenimiento Local	12	ALTO
			Problemas de capacidad de almacenamiento		2,00	2	3	Mantenimiento Local	12	ALTO
			Compatibilidad con Software Obsoleto		2,00	2	3	Mantenimiento Local	12	ALTO
			Problemas de escalabilidad		2,00	2	3	Mantenimiento Local	12	ALTO
			Hurto	Seguridad inadecuada para acceder al centro de datos	2,00	1	2	Cerrado bajo llave	4	MEDIO
			Perdida total de la Informacion	Falta de respaldos del servidor	2,00	2	3	Sin control	12	ALTO
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	2,00	2	2	Ventanas abiertas con mallas	8	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	2,00	2	3	Sin control	12	ALTO
			Subidas o bajadas de tension	Fallo en la red electrica	2,00	1	1	Uso de UPS	2	BAJO
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño	2,00	1	2	Sin control	4	MEDIO
E3		HP ML350 G8 V2	Fallos en los componentes	Antigüedad del servidor de 10 años	1,67	2	3	Uso no permanente/ Mantenimiento Local	10,02	ALTO
			Problemas de rendimiento		1,67	2	3	Uso no permanente/ Mantenimiento Local	10,02	ALTO
			Problemas de capacidad de almacenamiento		1,67	2	3	Uso no permanente/ Mantenimiento Local	10,02	ALTO

			Compatibilidad con Software Obsoleto		1,67	2	3	Uso no permanente/ Mantenimiento Local	10,02	ALTO
			Problemas de escalabilidad		1,67	2	3	Uso no permanente/ Mantenimiento Local	10,02	ALTO
			Hurto	Seguridad inadecuada para acceder al centro de datos	1,67	1	2	Cerrado bajo llave	3,34	MEDIO
			Perdida total de la Informacion	Falta de respaldos del servidor	1,67	2	3	Sin control	10,02	ALTO
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	1,67	2	2	Ventanas abiertas con mallas	6,68	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	1,67	2	3	Sin control	10,02	ALTO
			Subidas o bajadas de tension	Fallo en la red electrica	1,67	1	1	Uso de UPS	1,67	BAJO
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño	1,67	1	2	Sin control	3,34	MEDIO
E4		Proliant dl360 gen10	Hurto	Seguridad inadecuada para acceder al centro de datos	3,00	1	2	Cerrado bajo llave	6	MEDIO
			Perdida total de la Informacion	Falta de respaldos del servidor	3,00	1	2	Informacion respaldada por el proveedor de internet y de forma fisica	6	MEDIO
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	3,00	2	2	Ventanas abiertas con mallas	12	ALTO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	3,00	2	3	Sin control	18	ALTO
			Subidas o bajadas de tension	Fallo en la red electrica	3,00	1	1	Uso de UPS	3	BAJO
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño	3,00	1	2	Sin control	6	MEDIO
E5		Proliant dl380 gen9	Fallos en los componentes	Antigüedad del servidor de 9 años	2,00	2	2	Mantenimiento Local	8	MEDIO
			Problemas de rendimiento		2,00	2	2	Mantenimiento Local	8	MEDIO

			Problemas de capacidad de almacenamiento		2,00	2	2	Mantenimiento Local	8	MEDIO
			Compatibilidad con Software Obsoleto		2,00	2	2	Mantenimiento Local	8	MEDIO
			Problemas de escalabilidad		2,00	2	2	Mantenimiento Local	8	MEDIO
			Hurto	Seguridad inadecuada para acceder al centro de datos	2,00	1	2	Cerrado bajo llave	4	MEDIO
			Perdida total de la Informacion	Falta de respaldos del servidor	2,00	1	2	Informacion respaldada por el proveedor de internet y de forma fisica	4	MEDIO
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	2,00	2	2	Ventanas abiertas con mallas	8	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	2,00	2	3	Sin control	12	ALTO
			Subidas o bajadas de tension	Fallo en la red electrica	2,00	1	1	Uso de UPS	2	BAJO
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño	2,00	1	2	Sin control	4	MEDIO
E6		HP Compaq Pro 6300	Fallo del equipo	Hardware no dedicado para ejercer como servidor	1,33	2	2	Mantenimiento Local	5,32	MEDIO
			Fallos en los componentes	Antigüedad del equipo de 10 años estimados	1,33	2	2	Mantenimiento Local	5,32	MEDIO
			Problemas de rendimiento		1,33	2	2	Mantenimiento Local	5,32	MEDIO
			Problemas de capacidad de almacenamiento		1,33	2	2	Mantenimiento Local	5,32	MEDIO
			Compatibilidad con Software Obsoleto		1,33	2	2	Mantenimiento Local	5,32	MEDIO
			Problemas de escalabilidad		1,33	2	2	Mantenimiento Local	5,32	MEDIO
			Hurto	Seguridad inadecuada para acceder a la oficina de TI	1,33	2	2	Cerrado bajo llave	5,32	MEDIO
			Perdida total de la Informacion	Falta de respaldos del servidor	1,33	2	2	Sin control	5,32	MEDIO
			Recalentamiento del equipo	Ubicado en el departamento de TI	1,33	1	3	Mantenimiento Local	3,99	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicado en el departamento de TI	1,33	2	2	Mantenimiento local	5,32	MEDIO
			Subidas o bajadas de tension	Fallo en la red electrica	1,33	1	1	Uso de UPS	1,33	BAJO
E7			Fallos en los componentes		1,67	2	2	Uso no permanente/	6,68	MEDIO

								Mantenimiento Local		
			Problemas de rendimiento	Antigüedad del servidor de mas de 10 años	1,67	2	2	Uso no permanente/ Mantenimiento Local	6,68	MEDIO
			Problemas de capacidad de almacenamiento		1,67	2	2	Uso no permanente/ Mantenimiento Local	6,68	MEDIO
			Compatibilidad con Software Obsoleto		1,67	2	2	Uso no permanente/ Mantenimiento Local	6,68	MEDIO
		HP ML115 G1	Problemas de escalabilidad		1,67	2	2	Uso no permanente/ Mantenimiento Local	6,68	MEDIO
			Hurto	Seguridad inadecuada para acceder a la oficina de TI	1,67	2	2	Cerrado bajo llave	6,68	MEDIO
			Perdida total de la Informacion	Falta de respaldos del servidor	1,67	1	3	Sin control	5,01	MEDIO
			Recalentamiento del equipo	Ubicado en el departamento de TI	1,67	2	3	Sin control	10,02	ALTO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicado en el departamento de TI	1,67	2	2	Sin control	6,68	MEDIO
			Subidas o bajadas de tension	Fallo en la red electrica	1,67	1	1	Uso de UPS	1,67	BAJO
E8	OS	Ubuntu 18	Fallas de seguridad, estabilidad y rendimiento	Configuracion Inadecuada	2,33	1	1	Mantenimiento local	2,33	BAJO
			Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Soporte proximo a finalizar en abril del 2023	2,33	2	3	Mantenimiento local	13,98	ALTO
E9		Ubuntu 18	Fallas de seguridad, estabilidad y rendimiento	Configuracion Inadecuada	2,33	1	1	Mantenimiento local	2,33	BAJO
			Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Soporte proximo a finalizar en abril del 2023	2,33	2	3	Mantenimiento local	13,98	ALTO
E10		Windows Server 2008	Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Sistema Operativo sin soporte	2,33	3	3	Software en su ultima version	20,97	ALTO
			Vulnerabilidades detectadas	Sistema Operativo sin las ultimas actualizaciones	2,33	3	3	Software en su ultima version	20,97	ALTO
E11		Windows Server 2008	Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Sistema Operativo sin soporte	2,33	3	3	Software en su ultima version	20,97	ALTO
			Vulnerabilidades detectadas	Sistema Operativo sin las ultimas actualizaciones	2,33	3	3	Software en su ultima version	20,97	ALTO
E12		Windows Server 2003	Fallos y vulnerabilidad a amenazas	Sistema Operativo sin soporte	2,33	3	3	Software en su ultima version	20,97	ALTO
			Vulnerabilidades detectadas	Sistema Operativo sin las ultimas actualizaciones	2,33	3	3	Software en su ultima version	20,97	ALTO

E13		Windows Server 2003	Fallos y vulnerabilidad a amenazas	Sistema Operativo sin soporte	2,33	3	3	Software en su ultima version	20,97	ALTO
			Explotacion de vulnerabilidades detectadas	Sistema Operativo sin las ultimas actualizaciones	2,33	3	3	Software en su ultima version	20,97	ALTO
E14		Windows 10	Ataques de malware	Sin soporte como servidor	2,33	1	3	Mantenimiento local	6,99	MEDIO
			Bajas del rendimiento	Sin soporte como servidor	2,33	1	3	Mantenimiento local	6,99	MEDIO
			Intrusiones	Seguridad inadecuada para uso como servidor	2,33	1	3	Mantenimiento local	6,99	MEDIO
			Hackeos	Seguridad inadecuada para uso como servidor	2,33	1	3	Mantenimiento local	6,99	MEDIO
E15	Bases de Datos	Postgis 2.2	Explotaciones de amenazas conocidas	Version antigua del software	2,67	2	2	Software en su ultima version	10,68	ALTO
			Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Software sin soporte	2,67	3	3	Software en su ultima version	24,03	ALTO
E16		Postgre sql 9.5	Explotaciones de amenazas conocidas	Version antigua del software	3,00	2	3	Software en su ultima version	18	ALTO
			Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Software sin soporte	3,00	2	3	Software en su ultima version	18	ALTO
E17	ERP	SIIIM	INFORMACION RESERVADA	INFORMACION RESERVADA	2,00	RESERVADO	RESEVADO	RESERVADO	RESERVADO	RESERVADO
E18	FIREWALL	SOPHOS SG 230 rev 1	Trafico indeseado	Configuracion inadecuada	2,00	1	1	Soporte contratado	2	BAJO
			Intrusiones no autorizadas	Puertos abiertos no autorizados	2,00	1	1	Soporte contratado	2	BAJO
			Vulnerabilidades detectadas	Firmware desactualizado	2,00	1	1	Soporte contratado	2	BAJO
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño	2,00	1	1	Sin control	2	BAJO
E19	RED	HP MSR 900	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,67	1	1	Firmware actualizado	1,67	BAJO
			Acceso no autorizado	Contraseñas por defecto	1,67	1	1	Control tercerisado	1,67	BAJO
			Acceso no autorizado	Contraseñas filtradas	1,67	1	1	Control tercerisado	1,67	BAJO
			Hurto	Seguridad inadecuada para acceder al centro de datos	1,67	1	2	Cerrado bajo llave	3,34	MEDIO
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	1,67	2	2	Sin control	6,68	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	1,67	2	2	Sin control	6,68	MEDIO
			Subidas o bajadas de tension	Fallo en la red electrica	1,67	1	1	Uso de UPS	1,67	BAJO

			Corte del servicio de internet	Fallo del proveedor del servicio	1,67	1	1	Control tercerisado	1,67	BAJO
				Fallos del hardware	1,67	1	1	Control tercerisado	1,67	BAJO
				Configuracion inadecuada del dispositivos	1,67	1	1	Control tercerisado	1,67	BAJO
E20		HPE Office Conect 1920S Series Switch	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,67	1	1	Firmware actualizado	1,67	BAJO
			Hurto	Seguridad inadecuada para acceder al centro de datos	1,67	1	2	Cerrado bajo llave	3,34	MEDIO
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	1,67	2	2	Ventanas abiertas con mallas	6,68	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	1,67	2	2	Sin control	6,68	MEDIO
			Subidas o bajadas de tension	Fallo en la red electrica	1,67	1	3	Uso de UPS	5,01	MEDIO
			Desconeccion entre los servidores y la intranet de la empresa	Fallos del hardware	1,67	1	1	Mantenimiento local	1,67	BAJO
				Configuracion inadecuada del dispositivos	1,67	1	1	Mantenimiento local	1,67	BAJO
			Mayor latencia de datos	Cableado desordenado	1,67	1	1	Mantenimiento local	1,67	BAJO
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO
E21		HPE Office Conect 1920S Series Switch	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,67	1	1	Firmware actualizado	1,67	BAJO
			Hurto	Seguridad inadecuada para acceder al centro de datos	1,67	1	2	Cerrado bajo llave	3,34	MEDIO
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	1,67	2	2	Ventanas abiertas con mallas	6,68	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	1,67	2	2	Sin control	6,68	MEDIO
			Subidas o bajadas de tension	Fallo en la red electrica	1,67	1	3	Uso de UPS	5,01	MEDIO
			Desconeccion del servicio de red en la planta baja	Fallos del hardware	1,67	1	1	Mantenimiento local	1,67	BAJO
				Configuracion inadecuada del dispositivos	1,67	1	1	Mantenimiento local	1,67	BAJO

			Mayor latencia de datos	Cableado desordenado	1,67	1	1	Mantenimiento to local	1,67	BAJO
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO
E22		HPE Office Conect 1920S Series Switch	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,67	1	1	Firmware actualizado	1,67	BAJO
			Hurto	Seguridad inadecuada para acceder al centro de datos	1,67	1	2	Cerrado bajo llave	3,34	MEDIO
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	1,67	2	2	Ventanas abiertas con mallas	6,68	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	1,67	2	2	Sin control	6,68	MEDIO
			Subidas o bajadas de tension	Fallo en la red electrica	1,67	1	3	Uso de UPS	5,01	MEDIO
			Desconeccion del servicio de red en la planta baja	Fallos del hardware	1,67	1	1	Mantenimiento to local	1,67	BAJO
				Configuracion inadecuada del dispositivos	1,67	1	1	Mantenimiento to local	1,67	BAJO
			Mayor latencia de datos	Cableado desordenado	1,67	1	1	Mantenimiento to local	1,67	BAJO
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO
E23		PE Aruba Instant On 1930 24G 4SFP/SFP	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,33	1	1	Firmware actualizado	1,33	BAJO
			Hurto	Seguridad inadecuada para acceder al centro de datos	1,33	1	2	Cerrado bajo llave	2,66	BAJO
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	1,33	2	2	Ventilacion a traves de la ventana abierta hacia el centro de datos	5,32	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	1,33	2	2	Sin control	5,32	MEDIO
			Subidas o bajadas de tension	Fallo en la red electrica	1,33	1	3	Uso de UPS	3,99	MEDIO
				Fallos del hardware	1,33	1	1	Mantenimiento to local	1,33	BAJO

			Desconeccion del servicio de telefonia IP en la planta baja	Configuracion inadecuada del dispositivos	1,33	1	1	Mantenimiento local	1,33	BAJO
			Interferencias electromagneticas	Cableado desordenado	1,33	1	1	Mantenimiento local	1,33	BAJO
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	1,33	1	1	Cableado etiquetado	1,33	BAJO
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	1,33	1	1	Cableado etiquetado	1,33	BAJO
E24		HPE Office Conect 1920S Series Switch	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,67	1	1	Firmware actualizado	1,67	BAJO
			Hurto	Seguridad inadecuada para acceder al centro de datos	1,67	1	2	Cerrado bajo llave	3,34	MEDIO
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	1,67	2	2	Ventilacion a traves de la ventana abierta hacia el centro de datos	6,68	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	1,67	2	2	Sin control	6,68	MEDIO
			Subidas o bajadas de tension	Fallo en la red electrica	1,67	1	3	Uso de UPS	5,01	MEDIO
			Desconeccion del servicio de red en los pisos superiores	Fallos del hardware	1,67	1	1	Mantenimiento local	1,67	BAJO
				Configuracion inadecuada del dispositivos	1,67	1	1	Mantenimiento local	1,67	BAJO
			Mayor latencia de datos	Cableado desordenado	1,67	1	1	Mantenimiento local	1,67	BAJO
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO
E25		PE Aruba Instant On 1930 24G 4SFP/SFP	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,33	1	1	Firmware actualizado	1,33	BAJO
			Manejo inadecuado por personal no capacitado	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	1,33	1	3	Sin control	3,99	MEDIO
			Hurto	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	1,33	2	2	Sin control	5,32	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicación inadecuada con acceso limitado a personal no	1,33	2	2	Sin control	5,32	MEDIO

				autorizado de la empreza						
			Subidas o bajadas de tension	Fallo en la red electrica	1,33	1	3	Sin control	3,99	MEDIO
			Desconeccion del servicio de telefonia IP en el piso 1	Fallos del hardware	1,33	1	1	Mantenimiento local	1,33	BAJO
				Configuracion inadecuada del dispositivos	1,33	1	1	Mantenimiento local	1,33	BAJO
			Interferencias electromagneticas	Cableado desordenado	1,33	1	2	Mantenimiento local	2,66	BAJO
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	1,33	1	1	Cableado etiquetado	1,33	BAJO
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	1,33	1	1	Cableado etiquetado	1,33	BAJO
E26		HPE Office Conect 1920S Series Switch	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,67	1	1	Firmware actualizado	1,67	BAJO
			Manejo inadecuado por personal no capacitado	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	1,67	1	3	Sin control	5,01	MEDIO
			Hurto	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	1,67	2	2	Sin control	6,68	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	1,67	2	2	Sin control	6,68	MEDIO
			Subidas o bajadas de tension	Fallo en la red electrica	1,67	1	3	Sin control	5,01	MEDIO
			Desconeccion del servicio de red en el piso 1	Fallos del hardware	1,67	1	1	Mantenimiento local	1,67	BAJO
				Configuracion inadecuada del dispositivos	1,67	1	1	Mantenimiento local	1,67	BAJO
			Mayor latencia de datos	Cableado desordenado	1,67	1	2	Mantenimiento local	3,34	MEDIO
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO
E27		PE Aruba Instant On 1930 24G 4SFP/SFP	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,33	1	1	Firmware actualizado	1,33	BAJO
			Manejo inadecuado por personal no capacitado	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	1,33	2	3	Sin control	7,98	MEDIO

			Hurto	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	1,33	2	2	Sin control	5,32	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	1,33	2	3	Sin control	7,98	MEDIO
			Subidas o bajadas de tension	Fallo en la red electrica	1,33	1	3	Sin control	3,99	MEDIO
			Desconeccion del servicio de telefonia IP en el piso 2	Fallos del hardware	1,33	1	1	Mantenimiento local	1,33	BAJO
				Configuracion inadecuada del dispositivos	1,33	1	1	Mantenimiento local	1,33	BAJO
			Interferencias electromagneticas	Cableado desordenado	1,33	1	2	Mantenimiento local	2,66	BAJO
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	1,33	1	1	Cableado etiquetado	1,33	BAJO
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	1,33	1	1	Cableado etiquetado	1,33	BAJO
E28		HPE Office Conect 1920S Series Switch	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,67	1	1	Firmware actualizado	1,67	BAJO
			Manejo inadecuado por personal no capacitado	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	1,67	2	3	Sin control	10,02	ALTO
			Hurto	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	1,67	2	2	Sin control	6,68	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	1,67	2	3	Sin control	10,02	ALTO
			Subidas o bajadas de tension	Fallo en la red electrica	1,67	1	3	Sin control	5,01	MEDIO
			Desconeccion del servicio de red en el piso 2	Fallos del hardware	1,67	1	1	Mantenimiento local	1,67	BAJO
				Configuracion inadecuada del dispositivos	1,67	1	1	Mantenimiento local	1,67	BAJO
			Mayor latencia de datos	Cableado desordenado	1,67	1	2	Mantenimiento local	3,34	MEDIO
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO
E29		APX 530	Hurto	Entrada de personas no autorizadas	1,33	1	1	Camaras/ Guardias	1,33	BAJO

			Daños Fisicos	Maltrato/ Caida	1,33	1	1	Mantenimiento local	1,33	BAJO
			Alta latencia	Interferencia electromagnetica	1,33	1	1	Mantenimiento local	1,33	BAJO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicacion elevada	1,33	1	1	Mantenimiento local	1,33	BAJO
			Subidas o bajadas de tension	Fallo en la red electrica	1,33	1	3	Sin control	3,99	MEDIO
			Indisponibilidad del servicio	Fallos en los componentes	1,33	1	1	Mantenimiento local	1,33	BAJO
			Indisponibilidad del servicio	Configuracion inadecuada	1,33	1	1	Mantenimiento local	1,33	BAJO
			Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,33	1	1	Mantenimiento local	1,33	BAJO
			Alta latencia	Trafico de red exesivo	1,33	1	2	Mantenimiento local	2,66	BAJO
E30		AP 55C	Hurto	Acceso libre al dispositivo	1,33	1	1	Camaras/ Guardias	1,33	BAJO
			Daños Fisicos	Maltrato/ Caida	1,33	1	1	Mantenimiento local	1,33	BAJO
			Alta latencia	Interferencia electromagnetica	1,33	1	1	Mantenimiento local	1,33	BAJO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicacion elevada	1,33	1	1	Mantenimiento local	1,33	BAJO
			Subidas o bajadas de tension	Fallo en la red electrica	1,33	1	3	Sin control	3,99	MEDIO
			Indisponibilidad del servicio	Fallos en los componentes	1,33	1	1	Mantenimiento local	1,33	BAJO
			Indisponibilidad del servicio	Configuracion inadecuada	1,33	1	1	Mantenimiento local	1,33	BAJO
			Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,33	1	1	Mantenimiento local	1,33	BAJO
			Alta latencia	Trafico de red exesivo	1,33	1	2	Mantenimiento local	2,66	BAJO
E31		AP 55C	Hurto	Acceso libre al dispositivo	1,33	1	1	Camaras/ Guardias	1,33	BAJO
			Daños Fisicos	Maltrato/ Caida	1,33	1	1	Mantenimiento local	1,33	BAJO
			Alta latencia	Interferencia electromagnetica	1,33	1	1	Mantenimiento local	1,33	BAJO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicacion elevada	1,33	1	1	Mantenimiento local	1,33	BAJO
			Subidas o bajadas de tension	Fallo en la red electrica	1,33	1	3	Sin control	3,99	MEDIO
			Indisponibilidad del servicio	Fallos en los componentes	1,33	1	1	Mantenimiento local	1,33	BAJO
			Indisponibilidad del servicio	Configuracion inadecuada	1,33	1	1	Mantenimiento local	1,33	BAJO
			Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,33	1	1	Mantenimiento local	1,33	BAJO
			Alta latencia	Trafico de red exesivo	1,33	1	2	Mantenimiento local	2,66	BAJO
E32		AP 55C	Hurto	Acceso libre al dispositivo	1,33	1	1	Camaras/ Guardias	1,33	BAJO
			Daños Fisicos	Maltrato/ Caida	1,33	1	1	Mantenimiento local	1,33	BAJO
			Alta latencia	Interferencia electromagnetica	1,33	1	1	Mantenimiento local	1,33	BAJO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicacion elevada	1,33	1	1	Mantenimiento local	1,33	BAJO

			Subidas o bajadas de tension	Fallo en la red electrica	1,33	1	3	Sin control	3,99	MEDIO
			Indisponibilidad del servicio	Fallos en los componentes	1,33	1	1	Mantenimiento local	1,33	BAJO
			Indisponibilidad del servicio	Configuracion inadecuada	1,33	1	1	Mantenimiento local	1,33	BAJO
			Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,33	1	1	Mantenimiento local	1,33	BAJO
			Alta latencia	Trafico de red exesivo	1,33	1	2	Mantenimiento local	2,66	BAJO
E33		Cableado Vertical Fibra Optica	Destrucion	Daño fisico/Rotura/Cortes	1,67	1	1	Mantenimiento local	1,67	BAJO
			Alta latencia	Interferencia electromagnetica	1,67	1	1	Mantenimiento local	1,67	BAJO
E34		Cableado Horizontal UTP CAT 6/ 6A	Destrucion	Daño fisico/Rotura/Cortes	1,67	1	1	Mantenimiento local	1,67	BAJO
			Alta latencia	Interferencia electromagnetica	1,67	1	1	Mantenimiento local	1,67	BAJO
E35		Redes VLAN	Accesos no autorizados	Configuracion incompleta	2,33	1	2	Mantenimiento local	4,66	MEDIO
			Conflicto de direcciones IP		2,33	2	2	Mantenimiento local	9,32	ALTO
			Dificultad par reconfigurar las VLANS		2,33	1	2	Mantenimiento local	4,66	MEDIO
			Bajo rendimiento de la red		2,33	1	2	Mantenimiento local	4,66	MEDIO
			Ataque de snooping	Filtracion de la tabla de subredes	2,33	1	1	Direccionamiento confidencial	2,33	BAJO
			Accesos no autorizados a subredes	Filtracion de la tabla de subredes	2,33	1	1	Direccionamiento confidencial	2,33	BAJO
			Interrupcion de servicios	Filtracion de la tabla de subredes	2,33	1	1	Direccionamiento confidencial	2,33	BAJO
E36		Redes Wireless	Accesos a redes con permisos superirores	Filtracion de contraseñas	1,33	2	3	Sin control	7,98	MEDIO
			Accesos no autorizados	Contraseñas debiles	1,33	1	2	Politica de contraseñas	2,66	BAJO
			Ataques de fuerza bruta y diccionarios de contraseñas	Contraseñas debiles	1,33	1	2	Politica de contraseñas	2,66	BAJO
			Intercepcion de trafico de red	Cifrado de red debil	1,33	1	1	WPA2 PSK	1,33	BAJO
			Inyeccion de paquetes	Cifrado de red debil	1,33	1	1	WPA2 PSK	1,33	BAJO
			Menor privacidad, seguridad y control	Redes wifi visibles	1,33	2	3	Sin control	7,98	MEDIO
E37		Antena Ubiquiti Nanostation M5 LOC0	Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Exposicion al aire libre	1,33	1	1	Mantenimiento local	1,33	BAJO
			Desgaste por el clima	Exposicion al aire libre	1,33	1	1	Mantenimiento local	1,33	BAJO
			Sobrecarga electrica	Rayos	1,33	2	2	Sin control	5,32	MEDIO
			Caidas/ Vibraciones exesivas	Instalacion incorrecta	1,33	1	1	Mantenimiento local	1,33	BAJO
			Daño fisico	Mantenimiento inadecuado	1,33	1	3	Mantenimiento ocacional	3,99	MEDIO
E38	TELEFONIA	Panasonic	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,67	1	1	Firmware actualizado	1,67	BAJO

		KX-NS500	Hurto	Seguridad inadecuada para acceder al centro de datos	1,67	1	2	Cerrado bajo llave	3,34	MEDIO
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	1,67	2	2	Ventilacion hacia el centro de datos 1 a traves de una ventana	6,68	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	1,67	2	2	Sin control	6,68	MEDIO
			Subidas o bajadas de tension	Fallo en la red electrica	1,67	1	1	Uso de UPS	1,67	BAJO
			Fallo del servicio de telefonia IP	Fallos del hardware	1,67	1	1	Mantenimiento local	1,67	BAJO
				Configuracion inadecuada del dispositivos	1,67	1	1	Mantenimiento local	1,67	BAJO
E39	UPS	Eaton 906 IIS	Fallas de la bateria y daños en la electronica	Tiempo de vida de uso prolongado	1,00	2	3	Mantenimiento local	6	MEDIO
				Sobrecargas, descargas electricas	1,00	1	1	Mantenimiento local	1	BAJO
				Degradacion natural	1,00	2	3	Mantenimiento local	6	MEDIO
				Mala estimacion de la carga	1,00	1	1	Mantenimiento local	1	BAJO
E40		APC SRT2200XLA		Tiempo de vida de uso prolongado	1,00	2	3	Mantenimiento local	6	MEDIO
				Sobrecargas, descargas electricas	1,00	1	1	Mantenimiento local	1	BAJO
				Degradacion natural	1,00	2	3	Mantenimiento local	6	MEDIO
				Mala estimacion de la carga	1,00	1	1	Mantenimiento local	1	BAJO
E41		APC SRT2200XLA		Tiempo de vida de uso prolongado	1,00	2	3	Mantenimiento local	6	MEDIO
				Sobrecargas, descargas electricas	1,00	1	1	Mantenimiento local	1	BAJO
				Degradacion natural	1,00	2	3	Mantenimiento local	6	MEDIO
				Mala estimacion de la carga	1,00	1	1	Mantenimiento local	1	BAJO
E42		Forza FDC-003K		Tiempo de vida de uso prolongado	1,00	2	3	Mantenimiento local	6	MEDIO
				Sobrecargas, descargas electricas	1,00	1	1	Mantenimiento local	1	BAJO
				Degradacion natural	1,00	2	3	Mantenimiento local	6	MEDIO
				Mala estimacion de la carga	1,00	1	1	Mantenimiento local	1	BAJO
E43	Dominio/IP Y Subdominios	emapal.gob.ec/207.174.XXX.XXX/e	Explotacion de vulnerabilidades relacionadas con Open SSH 7.4	Vulnerabilidades en el puerto 22 y 2222 relacionadas al uso de Open SSH 7.4	2,00	2	3	Sin control	12	ALTO

		gob, edoc, etc	Panel de logeo a CPANEL publica, ingreso no autorizado a traves de fuerza bruta, diccionarios, pishing,ingenieria social.	Acceso publico al puerto 2082 y 2083	2,00	2	3	Sin control	12	ALTO
			Panel de logeo a WebHostManager publica, ingreso no autorizado a traves de fuerza bruta, diccionarios, pishing,ingenieria social.	Acceso publico al puerto 2086 y 2087	2,00	2	3	Sin control	12	ALTO
E44	Pagina Web	www.emapal.gob.ec	Informacion erronea	Web desactualizada	1,33	3	2	Mantenimiento local	7,98	MEDIO
			Falta de informacion	Web desactualizada	1,33	3	2	Mantenimiento local	7,98	MEDIO
			Explotacion de vulnerabilidades propias de la plataforma/servicio	Puerto y subdominio visible en el servicio de recursos humanos	1,33	1	3	Mantenimiento local	3,99	MEDIO
			Ataques de fuerza bruta	Puerto y subdominio visible en el servicio de recursos humanos	1,33	1	3	Mantenimiento local	3,99	MEDIO
			Informacion sensible de la estructura de la plataforma vuelta publica	Puerto y subdominio visible en el servicio de recursos humanos	1,33	1	3	Mantenimiento local	3,99	MEDIO
E45	Servicio de Correo Masivo	Correo Masivo	Desconeccion con el servicio	Problemas tecnicos	2,00	1	1	Control tercerisado	2	BAJO
			Desconeccion con el servicio	Desconeccion de la intranet de la empresa con internet	2,00	1	1	Control tercerisado	2	BAJO
			Perdida del control de datos	No ser dueños del servicio	2,00	1	1	Control tercerisado	2	BAJO
			Ataques de fuerza bruta o de diccionarios	Contraseñas inadecuadas	2,00	2	1	Politica de contraseñas	4	MEDIO
E46	Servicio de Correo Corporatico	Correo Corporativo	Desconeccion con el servicio	Problemas tecnicos	2,00	1	1	Control tercerisado	2	BAJO
			Desconeccion con el servicio	Desconeccion de la intranet de la empresa con internet	2,00	1	1	Control tercerisado	2	BAJO
			Perdida del control de datos	No ser dueños del servicio	2,00	1	1	Control tercerisado	2	BAJO
			Filtracion de informacion	Uso de correo institucional para servicios externos	2,00	2	2	Politicas de uso de correos	8	MEDIO
			Descargas de malware	Uso de correo institucional para servicios externos	2,00	2	2	Politicas de uso de correos	8	MEDIO
			Filtracion de credenciales y/o informacion persona o de la empresa	Correos con Pishing	2,00	2	3	Sin control	12	ALTO
			Infeccion de la red/ terminal	Correos infectados de malware	2,00	2	1	Firewall / Antivirus	4	MEDIO
			Ataques de fuerza bruta o de diccionarios	Contraseñas inadecuadas	2,00	1	3	Politica de contraseñas	6	MEDIO

E47	Software	Consolas	Ataques de fuerza bruta o de diccionarios	Contraseñas inadecuadas	3,00	2	1	Politica de contraseñas	6	MEDIO
			Codigo malicioso	Exploits de software	3,00	1	1	Software actualizado	3	BAJO
			Codigo malicioso	Inyeccion de codigo	3,00	1	1	Software actualizado	3	BAJO
E48	BACKUPS	Respaldo disco duro externo	Perdida	Objeto transportable y accesible	2,67	2	2	Almacenamiento bajo llave	10,68	ALTO
			Destruccion	Sensible a agentes fisicos, caidas, golpes	2,67	2	2	Almacenamiento bajo llave	10,68	ALTO
			Hurto	Objeto transportable y accesible	2,67	2	2	Almacenamiento bajo llave	10,68	ALTO
			Perdida de datos	Daño mecanico, caidas golpes, agentes fisicos	2,67	1	2	Manejo adecuado	5,34	MEDIO
			Robo de datos	Falta de contraseña/encriptacion	2,67	1	1	Disco duro cifrado	2,67	BAJO
E49		Respaldo Telconet	Robo/Alteracion de la informacion	Acceso no autorizado	2,67	1	1	Control tercerisado	2,67	BAJO
			Corrupcion/Perdida de datos	Error humano	2,67	1	1	Control tercerisado	2,67	BAJO
			Corrupcion/Perdida de datos	Fallos en el hardware donde se almacena	2,67	1	1	Control tercerisado	2,67	BAJO
			Destruccion del hardware donde se almacena el respaldo	Desastres naturales	2,67	1	1	Control tercerisado	2,67	BAJO
			Destruccion del hardware donde se almacena el respaldo	Amenazas ambientales	2,67	1	1	Control tercerisado	2,67	BAJO
E50	ANTIVIRUS	Kaspersky	Malware	Antivirus desactualizado	1,00	1	1	Antivirus actualizado	1	BAJO
E51	ASISTENCIA	MB360 ZKTECO	Registro erroneo	Fecha y hora incorrectas	2,00	1	1	Mantenimiento local	2	BAJO
			Registro erroneo	Identificacion erronea	2,00	1	1	Mantenimiento local	2	BAJO
			Daño	Daño mecanico, caidas golpes, agentes fisicos	2,00	1	1	Mantenimiento local	2	BAJO
			Destruccion	Daño mecanico, caidas golpes, agentes fisicos	2,00	1	1	Mantenimiento local	2	BAJO
E52		Biotime 8.0	Explotacion de vulnerabilidades	Firmware desactualizado	2,00	1	1	Mantenimiento local	2	BAJO
			Ataques de fuerza bruta o de diccionarios	Contraseñas inadecuadas	2,00	2	2	Politica de contraseñas	8	MEDIO
			Robo de informacion biometrica	Firmware desactualizado	2,00	1	1	Firmware actualizado	2	BAJO
			Robo de informacion biometrica	Contraseñas inadecuadas	2,00	1	1	Politica de contraseñas	2	BAJO
E53	SEGURIDAD	Camaras de seguridad	Vandalismo o robo	Activos en lugares accesibles	1,00	2	1	Camaras/Guardias de seguridad	2	BAJO
			Daño	Daño mecanico, caidas golpes, agentes fisicos	1,00	3	3	Sin control	9	ALTO
			Destruccion	Daño mecanico, caidas golpes, agentes fisicos	1,00	3	3	Sin control	9	ALTO

			Fallos en el funcionamiento, baja resolucion de las imágenes	Camaras antiguas	1,00	3	3	Sin control	9	ALTO
			Puntos ciegos ubicados en los lugares donde las camaras no funcionan	Camaras sin funcionamiento	1,00	3	3	Sin control	9	ALTO
			Acceso no autorizado , intrusiones	Asignacion de una ip publicas a traves del dominio para que esten disponibles para el director administrativo desde su dispositivo movil	1,00	2	3	Sin control	6	MEDIO
			Inyeccion de codigo malicioso y/o spyware	Asignacion de una ip publicas a traves del dominio para que esten disponibles para el director administrativo desde su dispositivo movil	1,00	2	3	Sin control	6	MEDIO
E54		DVR modelo desconocido	Intrusiones por credenciales debiles/nulas	Sistema de camaras a cargo de la direccion administrativa	1,67	2	3	Sin control	10,02	ALTO
			Intruciones a puertos abiertos	Sistema de camaras a cargo de la direccion administrativa	1,67	2	3	Sin control	10,02	ALTO
			Explotacion de vulnerabilidades por software desactualizado	Sistema de camaras a cargo de la direccion administrativa	1,67	2	3	Sin control	10,02	ALTO
			Infecciones de malware	Sistema de camaras a cargo de la direccion administrativa	1,67	2	3	Sin control	10,02	ALTO
			Fallos debido a configuracion inadecuada	Sistema de camaras a cargo de la direccion administrativa	1,67	2	3	Sin control	10,02	ALTO
			Hurto	Seguridad inadecuada	1,67	2	2	Sin control	6,68	MEDIO
			Destruccion del equipo	Manipulacion del dispositivo	1,67	1	2	Sin control	3,34	MEDIO
			Recalentamiento del equipo	Ubicación inadecuada	1,67	2	3	Sin control	10,02	ALTO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicación inadecuada	1,67	2	2	Sin control	6,68	MEDIO
			Subidas o bajadas de tension	Fallo en la red electrica	1,67	1	3	Sin control	5,01	MEDIO
E55	RACKS	Rack 1 Centro de Datos 1	Daño por fallas mecánicas	Derrame de líquidos	1,00	1	1	Mantenimiento Local	1	BAJO
			Daño por fallas mecánicas	Humedad y corrosión	1,00	1	1	Mantenimiento Local	1	BAJO
			Daño por fallas mecánicas	Vibración excesiva	1,00	1	1	Mantenimiento Local	1	BAJO
			Daño por fallas mecánicas	Sobrecarga de peso	1,00	1	1	Mantenimiento Local	1	BAJO

			Daño por fallas mecánicas	Fallas en los soportes	1,00	1	1	Mantenimiento Local	1	BAJO
E56		Rack 2 Centro de datos 2	Daño por fallas mecánicas	Derrame de líquidos	1,00	1	1	Mantenimiento Local	1	BAJO
			Daño por fallas mecánicas	Humedad y corrosión	1,00	1	1	Mantenimiento Local	1	BAJO
			Daño por fallas mecánicas	Vibración excesiva	1,00	1	1	Mantenimiento Local	1	BAJO
			Daño por fallas mecánicas	Sobrecarga de peso	1,00	1	1	Mantenimiento Local	1	BAJO
			Daño por fallas mecánicas	Fallas en los soportes	1,00	1	1	Mantenimiento Local	1	BAJO
E57		Rack Centro de Datos 2	Daño por fallas mecánicas	Derrame de líquidos	1,00	1	1	Mantenimiento Local	1	BAJO
			Daño por fallas mecánicas	Sol, Humedad Corrosión	1,00	1	1	Mantenimiento Local	1	BAJO
			Daño por fallas mecánicas	Vibración excesiva	1,00	1	1	Mantenimiento Local	1	BAJO
			Daño por fallas mecánicas	Sobrecarga de peso	1,00	1	1	Mantenimiento Local	1	BAJO
			Daño por fallas mecánicas	Fallas en los soportes	1,00	1	1	Mantenimiento Local	1	BAJO
E58		Rack Piso 1	Daño por fallas mecánicas	Sol Humedad , Corrosión	1,00	2	2	Mantenimiento Local	4	MEDIO
			Daño por fallas mecánicas	Vibración excesiva	1,00	1	1	Mantenimiento Local	1	BAJO
			Daño por fallas mecánicas	Sobrecarga de peso	1,00	1	1	Mantenimiento Local	1	BAJO
			Daño por fallas mecánicas	Fallas en los soportes	1,00	1	1	Mantenimiento Local	1	BAJO
			Incendios/Desastres ambientales	Rack abierto	1,00	2	3	Sin control	6	MEDIO
			Daño en los equipos al momento de mitigar un incendio	Falta de extintores de CO2	1,00	1	3	Extintores tradicionales	3	BAJO
E59		Rack Piso 2	Daño por fallas mecánicas	Humedad y corrosión	1,00	2	2	Mantenimiento Local	4	MEDIO
			Daño por fallas mecánicas	Vibración excesiva	1,00	1	1	Mantenimiento Local	1	BAJO
			Daño por fallas mecánicas	Sobrecarga de peso	1,00	1	1	Mantenimiento Local	1	BAJO
			Daño por fallas mecánicas	Fallas en los soportes	1,00	1	1	Mantenimiento Local	1	BAJO
			Incendios/Desastres ambientales/Hurto	Rack abierto	1,00	2	3	Sin control	6	MEDIO
			Incendio/Acumulacion de polvo	Almacenamiento de documentacion fisica cercana	1,00	1	3	Sin control	3	BAJO
			Daño en los equipos al momento de mitigar un incendio	Falta de extintores de CO2	1,00	1	3	Extintores tradicionales	3	BAJO
E60	UBICACIÓN FISICA	Edificio Matriz	Robo, Vandalismo	Seguridad Fisica Inadecuada	2,33	1	2	Camaras / Seguridad privada	4,66	MEDIO
			Inundacion	Desborde del rio	2,33	1	1	Sin control	2,33	BAJO
			Destruccion del edificio	Incendios	2,33	1	3	Extintores	6,99	MEDIO
			Daños	Daño por agentes medioambientales, climatologicos	2,33	1	1	Mantenimiento	2,33	BAJO
E61		Centro de Datos 1	Sobrecalentamiento/ Acumulacion de polvo	Ventilacion y climatizacion inadecuada	2,33	2	3	Ventilacion natural a traves de dos ventanas enrejadas	13,98	ALTO

			Intrusiones/Hurto/Destruccion de equipos	Poca seguridad para el ingreso al centro de datos	2,33	2	2	Entrada bajo llave	9,32	ALTO
			Intrusiones/Hurto/Destruccion de equipos	Ventana que da al exterior	2,33	1	3	Camaras/ Guardias	6,99	MEDIO
			Inundacion	Colinda con un baño	2,33	1	3	Sin control	6,99	MEDIO
			Inundacion	Ubicado en la primera planta	2,33	1	3	Sin control	6,99	MEDIO
			Incendios/Desastres ambientales/Polvo	Piso flotante	2,33	2	3	Sin control	13,98	ALTO
			Incendios/Desastres ambientales	Racks abiertos	2,33	2	3	Sin control	13,98	ALTO
			Acumulacion de polvo	Almacenamiento de equipos en desuso	2,33	2	3	Equipos en desuso acomodados en una esquina	13,98	ALTO
			Daño en los equipos al momento de mitigar un incendio	Falta de extintores de CO2	2,33	3	3	Sin control	20,97	ALTO
			Intrusiones/Hurto/Destruccion de equipos	Falta de monitoreo de seguridad	2,33	1	3	Sin control	6,99	MEDIO
			Cambios ambientales	Falta de monitoreo ambiental	2,33	2	3	Sin control	13,98	ALTO
			Subidas , bajadas de tension o cortes electricos	Falta de monitoreo electrico	2,33	1	2	Sin control	4,66	MEDIO
			Ingresos no autorizados	Registro de ingreso	2,33	1	2	Sin control	4,66	MEDIO
E62		Centro de Datos 2	Sobrecalentamiento/ Acumulacion de polvo	Ventilacion y climatizacion inadecuada	2,33	2	3	Ventana abierta hacia el centro de datos 1	13,98	ALTO
			Intrusiones/Hurto/Destruccion de equipos	Poca seguridad para el ingreso al centro de datos	2,33	1	2	Entrada bajo llave	4,66	MEDIO
			Inundacion	Colinda con un baño	2,33	1	1	Sin control	2,33	BAJO
			Inundacion	Ubicado en la primera planta	2,33	1	1	Sin control	2,33	BAJO
			Acumulacion de polvo, incendios	Almacenamiento de equipos en desuso y cajas	2,33	2	2	Limpieza ocacional	9,32	ALTO
			Daño en los equipos al momento de mitigar un incendio	Falta de extintores de CO2	2,33	3	3	Sin control	20,97	ALTO
			Intrusiones/Hurto/Destruccion de equipos	Falta de monitoreo de seguridad	2,33	1	3	Sin control	6,99	MEDIO
			Cambios ambientales	Falta de monitoreo ambiental	2,33	2	3	Sin control	13,98	ALTO
			Subidas , bajadas de tension o cortes electricos	Falta de monitoreo electrico	2,33	1	3	Sin control	6,99	MEDIO
			Ingresos no autorizados	Falta de registro de ingreso	2,33	1	2	Sin control	4,66	MEDIO
E63		Oficina de Sistemas	Sobrecalentamiento/ Acumulacion de polvo	Ventilacion y climatizacion inadecuada	1,67	1	1	Abrir ventanas/ Limpieza	1,67	BAJO
			Intrusiones/Hurto/Destruccion de equipos	Poca seguridad para el ingreso a la oficina	1,67	1	2	Entrada bajo llave	3,34	MEDIO
			Inundacion	Ubicado en la primera planta	1,67	1	1	Sin control	1,67	BAJO
			Acumulacion de polvo	Falta de limpieza	1,67	1	1	Limpieza	1,67	BAJO

			Daño en los equipos al momento de mitigar un incendio	Falta de extintores de CO2	1,67	3	3	Sin control	15,03	ALTO
			Intrusiones/Hurto/Destruccion de equipos	Ventanas con acceso al exterior	1,67	2	2	Camaras	6,68	MEDIO
			Destruccion o daño de los equipos	Subidas , bajadas de tension o cortes electricos	1,67	1	2	Sin control	3,34	MEDIO
			Ingresos no autorizados	Ausencia de registro de ingreso	1,67	1	3	Sin control	5,01	MEDIO
			Destruccion o daño	Incendios/Desastres ambientales/Polvo	1,67	1	2	Sin control	3,34	MEDIO
E64		Terraza y soporte de la antena	Intrusiones/Hurto/Destruccion de equipos	Acceso no autorizado	1,67	1	2	Acceso limitado	3,34	MEDIO
			Degradacion por agentes ambientales	Falta de mantenimiento y limpieza	1,67	2	2	Mantenimiento ocacional	6,68	MEDIO
E65	TERMINALES DE LOS EMPLEADOS	Computadoras de escritorio	Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Terminales con OS WINDOWS 7(sin soporte)	2,00	3	3	Equipos actualizados a la ultima version	18	ALTO
			Vulnerabilidades detectadas	Terminales desactualizadas	2,00	2	2	Mantenimiento Local	8	MEDIO
			Fallos en los componentes	Terminales con una antigüedad estimada en 17 años	2,00	3	3	Mantenimiento Local	18	ALTO
			Problemas de rendimiento		2,00	3	3	Mantenimiento Local	18	ALTO
			Problemas de capacidad de almacenamiento		2,00	3	3	Mantenimiento Local	18	ALTO
			Compatibilidad con Software Obsoleto		2,00	3	3	Mantenimiento Local	18	ALTO
			Problemas de escalabilidad		2,00	3	3	Mantenimiento Local	18	ALTO
			Fallos en los componentes	Terminales con una antigüedad estimada en 11 años	2,00	2	3	Mantenimiento Local	12	ALTO
			Problemas de rendimiento		2,00	2	3	Mantenimiento Local	12	ALTO
			Problemas de capacidad de almacenamiento		2,00	2	3	Mantenimiento Local	12	ALTO
			Compatibilidad con Software Obsoleto		2,00	2	3	Mantenimiento Local	12	ALTO
			Problemas de escalabilidad		2,00	2	3	Mantenimiento Local	12	ALTO
			Fallos en los componentes	Terminales con una antigüedad estimada en 7 años	2,00	1	2	Mantenimiento Local	4	MEDIO
			Problemas de rendimiento		2,00	1	2	Mantenimiento Local	4	MEDIO
			Problemas de capacidad de almacenamiento		2,00	1	2	Mantenimiento Local	4	MEDIO
			Compatibilidad con Software Obsoleto		2,00	1	2	Mantenimiento Local	4	MEDIO
			Problemas de escalabilidad		2,00	1	2	Mantenimiento Local	4	MEDIO
			Rendimiento probre	Terminales con procesadores viejos y de poca capacidad	2,00	3	3	Mantenimiento Local	18	ALTO
			Sobrecalentamiento		2,00	3	3	Mantenimiento Local	18	ALTO
			Pantallasos azules		2,00	3	3	Mantenimiento Local	18	ALTO
			Reinicios Inesperados		2,00	3	3	Mantenimiento Local	18	ALTO

			Corrupcion/Perdida de datos		2,00	3	3	Mantenimiento Local	18	ALTO
			Aplicaciones que no responden	Terminales con 2 - 3 GB de RAM	2,00	2	3	Mantenimiento Local	12	ALTO
			Bajo rendimiento		2,00	2	3	Mantenimiento Local	12	ALTO
			Reinicios Inesperados		2,00	2	3	Mantenimiento Local	12	ALTO
			Corrupcion/Perdida de datos		2,00	2	3	Mantenimiento Local	12	ALTO
			Aplicaciones que no responden	Terminales con 4 GB de RAM	2,00	2	2	Mantenimiento Local	8	MEDIO
			Bajo rendimiento		2,00	2	2	Mantenimiento Local	8	MEDIO
			Conflicto de tareas	Terminales compartidas entre empleados	2,00	2	2	Cuentas de usuario	8	MEDIO
			Filtracion de datos		2,00	1	2	Cuentas de usuario	4	MEDIO
			Desorganizacion de archivos e informacion		2,00	2	2	Cuentas de usuario	8	MEDIO
			Uso ineficiente del terminal		2,00	1	2	Cuentas de usuario	4	MEDIO
			Infeccion de malware	Conexión de dispositivos personales a terminales de la empreza	2,00	2	2	Registro de actividades del terminal	8	MEDIO
			Robo de datos		2,00	2	2	Registro de actividades del terminal	8	MEDIO
			Conflictos en la politica de seguridad		2,00	3	2	Registro de actividades del terminal	12	ALTO
			Accesos no autorizados	Contraseñas debiles para acceso al terminal	2,00	1	3	Politica de contraseñas	6	MEDIO
			Accesos no autorizados	Terminales sin contraseña	2,00	1	3	Sin control	6	MEDIO
			Accesos no autorizados	Terminales sin usuario	2,00	1	3	Sin control	6	MEDIO
			Llevarse los terminales de forma no autorizada fuera de la empresa	Poco control fisico de los terminales	2,00	1	3	Sin control	6	MEDIO
			Subidas o bajadas de tension	Fallo en la red electrica	2,00	1	3	Sin control	6	MEDIO
			Destruccion por inundacion	Aumento del caudal del rio/ lluvia	2,00	1	1	Sin control	2	BAJO
			Daños fisicos	Golpes o caidas	2,00	1	3	Sin control	6	MEDIO
E66		Computadoras portatiles	Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Terminales con OS WINDOWS 7(sin soporte)	2,00	3	3	Equipos actualizados a la ultima version	18	ALTO
			Vulnerabilidades detectadas	Terminales desactualizadas	2,00	3	3	Mantenimiento Local	18	ALTO
			Fallos en los componentes	Terminales con una antigüedad estimada en 15 años	2,00	3	3	Mantenimiento Local	18	ALTO
			Problemas de rendimiento		2,00	3	3	Mantenimiento Local	18	ALTO
			Problemas de capacidad de almacenamiento		2,00	3	3	Mantenimiento Local	18	ALTO
			Compatibilidad con Software Obsoleto		2,00	3	3	Mantenimiento Local	18	ALTO

			Problemas de escalabilidad		2,00	3	3	Mantenimiento Local	18	ALTO
			Fallos en los componentes	Terminales con una antigüedad estimada entre 9 - 11 años	2,00	2	3	Mantenimiento Local	12	ALTO
			Problemas de rendimiento		2,00	2	3	Mantenimiento Local	12	ALTO
			Problemas de capacidad de almacenamiento		2,00	2	3	Mantenimiento Local	12	ALTO
			Compatibilidad con Software Obsoleto		2,00	2	3	Mantenimiento Local	12	ALTO
			Problemas de escalabilidad		2,00	2	3	Mantenimiento Local	12	ALTO
			Fallos en los componentes	Terminales con una antigüedad estimada en 7 años	2,00	2	2	Mantenimiento Local	8	MEDIO
			Problemas de rendimiento		2,00	2	2	Mantenimiento Local	8	MEDIO
			Problemas de capacidad de almacenamiento		2,00	2	2	Mantenimiento Local	8	MEDIO
			Compatibilidad con Software Obsoleto		2,00	2	2	Mantenimiento Local	8	MEDIO
			Problemas de escalabilidad		2,00	2	2	Mantenimiento Local	8	MEDIO
			Rendimiento probre	Terminales con procesadores viejos y de poca capacidad	2,00	3	3	Mantenimiento Local	18	ALTO
			Sobrecalentamiento		2,00	3	3	Mantenimiento Local	18	ALTO
			Pantallasos azules		2,00	3	3	Mantenimiento Local	18	ALTO
			Reinicios Inesperados		2,00	3	3	Mantenimiento Local	18	ALTO
			Corrupcion/Perdida de datos		2,00	3	3	Mantenimiento Local	18	ALTO
			Aplicaciones que no responden	Terminales con 2 - 3 GB de RAM	2,00	2	3	Mantenimiento Local	12	ALTO
			Bajo rendimiento		2,00	2	3	Mantenimiento Local	12	ALTO
			Reinicios Inesperados		2,00	2	3	Mantenimiento Local	12	ALTO
			Corrupcion/Perdida de datos		2,00	2	3	Mantenimiento Local	12	ALTO
			Aplicaciones que no responden	Terminales con 4 GB de RAM	2,00	2	2	Mantenimiento Local	8	MEDIO
			Bajo rendimiento		2,00	2	2	Mantenimiento Local	8	MEDIO
			Conflicto de tareas	Terminales compartidas entre empleados	2,00	2	2	Cuentas de usuario	8	MEDIO
			Filtracion de datos		2,00	1	2	Cuentas de usuario	4	MEDIO
			Desorganizacion de archivos e informacion		2,00	2	2	Cuentas de usuario	8	MEDIO
			Uso ineficiente del terminal		2,00	1	2	Cuentas de usuario	4	MEDIO
			Infeccion de malware	Conexión de dispositivos personales a terminales de la empreza	2,00	2	2	Registro de actividades del terminal	8	MEDIO
			Robo de datos		2,00	2	2	Registro de actividades del terminal	8	MEDIO
			Conflictos en la politica de seguridad		2,00	3	2	Registro de actividades del terminal	12	ALTO

			Accesos no autorizados	Contraseñas debiles para acceso al terminal	2,00	1	3	Politica de contraseñas	6	MEDIO
			Accesos no autorizados	Terminales sin contraseña	2,00	1	3	Sin control	6	MEDIO
			Accesos no autorizados	Terminales sin usuario	2,00	1	3	Sin control	6	MEDIO
			Hurto	Poco control fisico de los terminales y portailidad de los mismos	2,00	2	3	Sin control	12	ALTO
			Llevarse los terminales de forma no autorizada fuera de la empresa	Poco control fisico de los terminales y portailidad de los mismos	2,00	3	3	Sin control	18	ALTO
			Perdida	Poco control fisico de los terminales y portailidad de los mismos	2,00	2	3	Sin control	12	ALTO
			Daños fisicos	Golpes o caidas	2,00	2	3	Sin control	12	ALTO
E67	TALENTO HUMANO	Personal del Area de Sistemas	Falta de supervisión y mantenimiento de los sistemas y equipos, lo que puede llevar a fallos técnicos y aumentar la probabilidad de i ataques.	Falta de personal	2,00	2	3	Division de tareas entre los empleados	12	ALTO
			Dificultad para responder a emergencias y resolver problemas técnicos de manera eficiente.		2,00	2	3	Division de tareas entre los empleados	12	ALTO
			Problemas para llevar a cabo las tareas diarias y garantizar la disponibilidad y continuidad del servicio.		2,00	2	3	Division de tareas entre los empleados	12	ALTO
			Gasto de tiempo en la capacitacion de nuevo personal por contrato que tiende a rotar cada ciclo a la alcaldia de Azogues		2,00	2	3	Division de tareas entre los empleados	12	ALTO
			Carga de trabajo exesiva		2,00	3	3	Division de tareas entre los empleados	18	ALTO
			Falta de documentacion	Personal unico e indispensable	2,33	2	3	Sin control	13,98	ALTO
			Conocimiento tecnico especifico de la infraestructura de TI para el personal nuevo		2,33	2	3	Sin control	13,98	ALTO
			Falta de conocimiento frente a sistemas personalizados para el personal nuevo		2,33	3	3	Sin control	20,97	ALTO
			Ausencia de un plan de continuidad frente a la ausencia		2,33	3	3	Sin control	20,97	ALTO

			permanente del personal							
E68		Funcionarios de la empresa no pertenecientes al area de Sistemas	Acceso no autorizado a traves de diversos metodos	Contraseñas debiles	1,67	3	2	Politica de formato de contraseñas	10,02	ALTO
			Olvidos/Contraseñas expuestas y accesos no autorizados	Mal manejo de las contraseñas de ingreso al terminal	1,67	2	2	Sin control	6,68	MEDIO
				Desconocimiento de credenciales de ingreso a la terminal	1,67	1	2	Sin control	3,34	MEDIO
				Mal manejo de las contraseñas de ingreso a la plataforma de trabajo	1,67	2	2	Sin control	6,68	MEDIO
				Desconocimiento de credenciales de ingreso a la terminal	1,67	1	2	Sin control	3,34	MEDIO
			Contraseñas expuestas/Accesos no autorizados/Alteracion de la informacion	Conocimiento de terceros de la contraseña de ingreso al terminal	1,67	2	2	Sin control	6,68	MEDIO
			Credenciales expuestas/Accesos no autorizados/Alteracion de la informacion	Conocimiento de terceros de las credenciales personales para el ingreso a la plataforma de trabajo	1,67	2	2	Sin control	6,68	MEDIO
			Accesos no autorizados/Alteracion de la informacion	Acceso a la terminal de trabajo por terceros en la empresa	1,67	2	2	Sin control	6,68	MEDIO
			Proteccion limitada del equipo frente a malware	Uso de terminales personales para laborar en el trabajo	1,67	3	3	Politica de no uso de dispositivos personales para laborar en la empresa	15,03	ALTO
			Perdida de confidencialidad de la informacion		1,67	3	3	Politica de no uso de dispositivos personales para laborar en la empresa	15,03	ALTO
			Problemas de compatiibilidad		1,67	2	3	Politica de no uso de dispositivos personales para laborar en la empresa	10,02	ALTO
			Incumplimiento de normativas		1,67	3	3	Politica de no uso de dispositivos personales para laborar en la empresa	15,03	ALTO
			Hurto	Horas extras en la empresa	1,67	1	3	Camaras / Registro de actividad de los terminales	5,01	MEDIO

			Perdida de la confidencialidad de la informacion	Horas extras desde fuera de la empresa	1,67	2	2	Sin control	6,68	MEDIO
			Proteccion limitada del equipo frente a malware	Horas extras desde fuera de la empresa	1,67	2	2	Sin control	6,68	MEDIO
			Perdida de la integridad de la informacion debido a falta de imparcialidad y/o conflicto de intereses	Relaciones familiares en la empresa	1,67	1	2	Gestion de RRHH	3,34	MEDIO
			Perdida de la integridad de la informacion debido a falta de imparcialidad y/o conflicto de intereses	Relaciones sentimentales/afectivas en la empresa	1,67	1	2	Gestion de RRHH	3,34	MEDIO
			Sabotajes/Alteracion de la informacion	Ambiente laboral malo en la empresa	1,67	1	2	Gestion de RRHH	3,34	MEDIO
			Sabotajes/Alteracion de la informacion	Altercados entre empleados de la empresa	1,67	1	2	Gestion de RRHH	3,34	MEDIO
			Contaminacion de la red con malware	Uso de la red wifi de la empresa en dispositivos personales	1,67	1	1	Segmentacion de la red y firewall	1,67	BAJO
			Accesos no autorizados/Alteracion de la informacion	Terminales activas por parte de los empleados al ausentarse por momentos(almuerzo,reunion,etc)	1,67	2	3	Politicas de uso de terminales	10,02	ALTO
			Accesos no autorizados/Alteracion de la informacion	Terminales activas por parte de los empleados al finalizar con la jornada laboral	1,67	1	3	Politicas de uso de terminales	5,01	MEDIO
			Hurto/perdida de confidencialidad	Llevarse terminales de la empresa al hogar para realizar labores	1,67	2	3	Politicas de uso de terminales	10,02	ALTO
			Pishing	Uso inadecuado del correo insitucional	1,67	1	3	Politicas de uso del correo	5,01	MEDIO
E69	Estructura Organizacional	Departamento de TI	Accionar a nivel de apoyo unicamente	Nivel incorrecto dentro del organigrama	1,00	3	3	Sin control	9	ALTO
			Reformas a planes operativos	Depende de la direccion administrativa	1,00	3	3	Sin control	9	ALTO
			Cambios en la planeacion prevista	Depende de la direccion administrativa	1,00	3	3	Sin control	9	ALTO
			Falta de autonomia, y operatividad	No cuenta con una estructura propia con sus propio departamentos y procesos	1,00	3	3	Division de tareas entre los empleados	9	ALTO
			Falta de actualizacion y/o adquisicion de software y hardware	Excesiva burocratizacion para la adquisicion o renovacion de activos de TI	1,00	3	3	Solicitudes respectivas	9	ALTO

ANEXO 9: TRATAMIENTO DE RIESGOS

ANALISIS DE RIESGOS					EVALUACION DE RIESGOS						TRATAMIENTO DE RIESGOS						
					Impacto	Probabilidad		Controles Implementados	Calculo de evaluacion de Riesgo	Nivel del riesgo	Metodo de tratamiento	Tipo de control	Controles a implementar	Nivel de amenaza	Nivel de vulnerabilidad	Calculo de evaluacion del riesgo con el control implementado	Nivel del riesgo con el control implementado
N	Proceso	Nombre	Amenazas	Vulnerabilidades	VA	Nivel de amenaza	Nivel de Vulnerabilidad										
E1	Infraestructura	Proliant dl360 gen10	Fallos en los componentes	Antigüedad del servidor de mas de 10 años	2,67	2	3	Mantenimiento Local	16,02	ALTO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	2,67	BAJO
			Problemas de rendimiento		2,67	2	3	Mantenimiento Local	16,02	ALTO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	2,67	BAJO
			Problemas de capacidad de almacenamiento		2,67	2	3	Mantenimiento Local	16,02	ALTO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	2,67	BAJO
			Compatibilidad con Software Obsoleto		2,67	2	3	Mantenimiento Local	16,02	ALTO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	2,67	BAJO
			Problemas de escalabilidad		2,67	2	3	Mantenimiento Local	16,02	ALTO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	2,67	BAJO
			Hurto	Seguridad inadecuada para acceder al centro de datos	2,67	1	2	Cerrado bajo llave	5,34	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Camaras/Ingreso con tarjetas de identificacion	1	1	2,67	BAJO

			Perdida total de la Informacion	Falta de respaldos del servidor	2,67	2	3	Sin control	16,02	ALTO	Mitigar/Evitar/Transferir	Preventivo	Respaldos en la nube/Adquirir un servidor para respaldar la informacion	1	1	2,67	BAJO
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	2,67	2	2	Ventanas abiertas con mallas	10,68	ALTO	Mitigar/Evitar/Transferir	Preventivo	Uso de aire acondicionado	1	2	5,34	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	2,67	2	3	Sin control	16,02	ALTO	Mitigar/Evitar/Transferir	Preventivo	Limpieza constante y Mantenimiento local	2	2	10,68	ALTO
			Subidas o bajadas de tension	Fallo en la red electrica	2,67	1	1	Uso de UPS	2,67	BAJO	Aceptar	Preventivo	Compra de un generador para el edifico	1	1	2,67	BAJO
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño	2,67	1	2	Sin control	5,34	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Llevar el centro de datos a una planta superior/Clausurar el baño colindante	1	1	2,67	BAJO
E2		HP ML350 G8 V2	Fallos en los componentes	Antigüedad del servidor de 10 años	2,00	2	3	Mantenimiento Local	12	ALTO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	2	BAJO
			Problemas de rendimiento		2,00	2	3	Mantenimiento Local	12	ALTO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	2	BAJO

			Problemas de capacidad de almacenamiento		2,00	2	3	Mantenimiento Local	12	ALTO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	2	BAJO
			Compatibilidad con Software Obsoleto		2,00	2	3	Mantenimiento Local	12	ALTO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	2	BAJO
			Problemas de escalabilidad		2,00	2	3	Mantenimiento Local	12	ALTO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	2	BAJO
			Hurto	Seguridad inadecuada para acceder al centro de datos	2,00	1	2	Cerrado bajo llave	4	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Camaras/Ingreso con tarjetas de identificacion	1	1	2	BAJO
			Perdida total de la Informacion	Falta de respaldos del servidor	2,00	2	3	Sin control	12	ALTO	Mitigar/Evitar/Transferir	Preventivo	Respaldos en la nube/Adquirir un servidor para respaldar la informacion	1	1	2	BAJO
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	2,00	2	2	Ventanas abiertas con mallas	8	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Uso de aire acondicionado	1	2	4	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	2,00	2	3	Sin control	12	ALTO	Mitigar/Evitar/Transferir	Preventivo	Limpieza constante y Mantenimiento local	2	2	8	MEDIO

			Subidas o bajadas de tension	Fallo en la red electrica	2,00	1	1	Uso de UPS	2	BAJO	Aceptar	Preventivo	Compra de un generador para el edifico	1	1	2	BAJO
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño	2,00	1	2	Sin control	4	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Llevar el centro de datos a una planta superior/Clausurar el baño colindante	1	1	2	BAJO
E3		HP ML350 G8 V2	Fallos en los componentes	Antigüedad del servidor de 10 años	1,67	2	3	Uso no permanente/Mantenimiento Local	10,02	ALTO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	1,67	BAJO
			Problemas de rendimiento		1,67	2	3	Uso no permanente/Mantenimiento Local	10,02	ALTO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	1,67	BAJO
			Problemas de capacidad de almacenamiento		1,67	2	3	Uso no permanente/Mantenimiento Local	10,02	ALTO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	1,67	BAJO
			Compatibilidad con Software Obsoleto		1,67	2	3	Uso no permanente/Mantenimiento Local	10,02	ALTO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	1,67	BAJO
			Problemas de escalabilidad		1,67	2	3	Uso no permanente/Mantenimiento Local	10,02	ALTO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	1,67	BAJO
			Hurto	Seguridad inadecuada para acceder al centro de datos	1,67	1	2	Cerrado bajo llave	3,34	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Camaras/Ingreso con tarjetas de identificacion	1	1	1,67	BAJO

			Perdida total de la Informacion	Falta de respaldos del servidor	1,67	2	3	Sin control	10,02	ALTO	Mitigar/Evitar/Transferir	Preventivo	Respaldos en la nube/Adquirir un servidor para respaldar la informacion	1	1	1,67	BAJO
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	1,67	2	2	Ventanas abiertas con mallas	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Uso de aire acondicionado	1	2	3,34	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	1,67	2	3	Sin control	10,02	ALTO	Mitigar/Evitar/Transferir	Preventivo	Limpieza constante y Mantenimiento local	2	2	6,68	MEDIO
			Subidas o bajadas de tension	Fallo en la red electrica	1,67	1	1	Uso de UPS	1,67	BAJO	Aceptar	Preventivo	Compra de un generador para el edifico	1	1	1,67	BAJO
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño	1,67	1	2	Sin control	3,34	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Llevar el centro de datos a una planta superior/Clausurar el baño colindante	1	1	1,67	BAJO
E4		Proliant dl360 gen10	Hurto	Seguridad inadecuada para acceder al centro de datos	3,00	1	2	Cerrado bajo llave	6	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Camaras/Ingreso con tarjetas de identificacion	1	1	3	BAJO
			Perdida total de la	Falta de respaldos del servidor	3,00	1	2	Informacion respaldada por el proveedor de	6	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Respaldos en la nube/Adquirir un servidor para	1	1	3	BAJO

			Informacion					internet y de forma fisica					respaldar la informacion				
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	3,00	2	2	Ventanas abiertas con mallas	12	ALTO	Mitigar/Evitar/Transferir	Preventivo	Uso de aire acondicionado	1	2	6	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	3,00	2	3	Sin control	18	ALTO	Mitigar/Evitar/Transferir	Preventivo	Limpieza constante y Mantenimiento local	2	2	12	ALTO
			Subidas o bajadas de tension	Fallo en la red electrica	3,00	1	1	Uso de UPS	3	BAJO	Aceptar	Preventivo	Compra de un generador para el edifico	1	1	3	BAJO
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño	3,00	1	2	Sin control	6	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Llevar el centro de datos a una planta superior/Clausurar el baño colindante	1	1	3	BAJO
E5		Proliant dl380 gen9	Fallos en los componentes	Antigüedad del servidor de 9 años	2,00	2	2	Mantenimiento Local	8	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	2	BAJO
			Problemas de rendimiento		2,00	2	2	Mantenimiento Local	8	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	2	BAJO

			Problemas de capacidad de almacenamiento		2,00	2	2	Mantenimiento Local	8	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	2	BAJO
			Compatibilidad con Software Obsoleto		2,00	2	2	Mantenimiento Local	8	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	2	BAJO
			Problemas de escalabilidad		2,00	2	2	Mantenimiento Local	8	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	2	BAJO
			Hurto	Seguridad inadecuada para acceder al centro de datos	2,00	1	2	Cerrado bajo llave	4	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Camaras/Ingreso con tarjetas de identificacion	1	1	2	BAJO
			Perdida total de la Informacion	Falta de respaldos del servidor	2,00	1	2	Informacion respaldada por el proveedor de internet y de forma fisica	4	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Respaldos en la nube/Adquirir un servidor para respaldar la informacion	1	1	2	BAJO
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	2,00	2	2	Ventanas abiertas con mallas	8	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Uso de aire acondicionado	1	2	4	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	2,00	2	3	Sin control	12	ALTO	Mitigar/Evitar/Transferir	Preventivo	Limpieza constante y Mantenimiento local	2	2	8	MEDIO

			Subidas o bajadas de tension	Fallo en la red electrica	2,00	1	1	Uso de UPS	2	BAJO	Aceptar	Preventivo	Compra de un generador para el edifico	1	1	2	BAJO
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño	2,00	1	2	Sin control	4	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Llevar el centro de datos a una planta superior/Clausurar el baño colindante	1	1	2	BAJO
E6		HP Compaq Pro 6300	Fallo del equipo	Hardware no dedicado para ejercer como servidor	1,33	2	2	Mantenimiento Local	5,32	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Uso de un servidor de la empresa/Migracion a Cloud	1	1	1,33	BAJO
			Fallos en los componentes	Antigüedad del equipo de 10 años estimados	1,33	2	2	Mantenimiento Local	5,32	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Uso de un servidor de la empresa/Migracion a Cloud	1	1	1,33	BAJO
			Problemas de rendimiento		1,33	2	2	Mantenimiento Local	5,32	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Uso de un servidor de la empresa/Migracion a Cloud	1	1	1,33	BAJO
			Problemas de capacidad de almacenamiento		1,33	2	2	Mantenimiento Local	5,32	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Uso de un servidor de la empresa/Migracion a Cloud	1	1	1,33	BAJO
			Compatibilidad con Software Obsoleto		1,33	2	2	Mantenimiento Local	5,32	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Uso de un servidor de la empresa/Migracion a Cloud	1	1	1,33	BAJO
			Problemas de escalabilidad		1,33	2	2	Mantenimiento Local	5,32	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Uso de un servidor de la empresa/Migracion a Cloud	1	1	1,33	BAJO

			Hurto	Seguridad inadecuada para acceder a la oficina de TI	1,33	2	2	Cerrado bajo llave	5,32	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Llevar el dispositivo al centro de datos	1	2	2,66	BAJO
			Perdida total de la Informacion	Falta de respaldos del servidor	1,33	2	2	Sin control	5,32	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Respaldos en la nube/Adquirir un servidor para respaldar la informacion	1	1	1,33	BAJO
			Recalentamiento del equipo	Ubicado en el departamento de TI	1,33	1	3	Mantenimiento Local	3,99	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Llevar el dispositivo al centro de datos	1	2	2,66	BAJO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicado en el departamento de TI	1,33	2	2	Mantenimiento local	5,32	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Limpieza constante y Mantenimiento local	1	2	2,66	BAJO
			Subidas o bajadas de tension	Fallo en la red electrica	1,33	1	1	Uso de UPS	1,33	BAJO	Aceptar	Preventivo	Compra de un generador para el edifico	1	1	1,33	BAJO
E7		HP ML115 G1	Fallos en los componentes	Antigüedad del servidor de mas de 10 años	1,67	2	2	Uso no permanente/Mantenimiento Local	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	1,67	BAJO
			Problemas de rendimiento		1,67	2	2	Uso no permanente/Mantenimiento Local	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	1,67	BAJO
			Problemas de capacidad de almacenamiento		1,67	2	2	Uso no permanente/Mantenimiento Local	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	1,67	BAJO

			Compatibilidad con Software Obsoleto		1,67	2	2	Uso no permanente/Mantenimiento Local	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	1,67	BAJO
			Problemas de escalabilidad		1,67	2	2	Uso no permanente/Mantenimiento Local	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Migracion a Cloud/Compra de un nuevo servidor	1	1	1,67	BAJO
			Hurto	Seguridad inadecuada para acceder a la oficina de TI	1,67	2	2	Cerrado bajo llave	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Llevar el dispositivo al centro de datos	1	2	3,34	MEDIO
			Perdida total de la Informacion	Falta de respaldos del servidor	1,67	1	3	Sin control	5,01	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Respaldos en la nube/Adquirir un servidor para respaldar la informacion	1	1	1,67	BAJO
			Recalentamiento del equipo	Ubicado en el departamento de TI	1,67	2	3	Sin control	10,02	ALTO	Mitigar/Evitar/Transferir	Preventivo	Llevar el dispositivo al centro de datos	2	2	6,68	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicado en el departamento de TI	1,67	2	2	Sin control	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Limpieza constante y Mantenimiento local	1	2	3,34	MEDIO
			Subidas o bajadas de tension	Fallo en la red electrica	1,67	1	1	Uso de UPS	1,67	BAJO	Aceptar	Preventivo	Compra de un generador para el edifico	1	1	1,67	BAJO
E8	OS	Ubuntu 18	Fallas de seguridad, estabilidad y rendimiento	Configuracion Inadecuada	2,33	1	1	Mantenimiento local	2,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	2,33	BAJO

			Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Soporte proximo a finalizar en abril del 2023	2,33	2	3	Mantenimiento local	13,98	ALTO	Mitigar/Evitar/Transferir	Preventivo	Cambiar de version a una con soporte	1	1	2,33	BAJO
E9		Ubuntu 18	Fallas de seguridad, estabilidad y rendimiento	Configuracion Inadecuada	2,33	1	1	Mantenimiento local	2,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	2,33	BAJO
			Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Soporte proximo a finalizar en abril del 2023	2,33	2	3	Mantenimiento local	13,98	ALTO	Mitigar/Evitar/Transferir	Preventivo	Cambiar de version a una con soporte	1	1	2,33	BAJO
E10		Windows Server 2008	Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Sistema Operativo sin soporte	2,33	3	3	Software en su ultima version	20,97	ALTO	Mitigar/Evitar/Transferir	Preventivo	Cambiar de version a una con soporte	1	1	2,33	BAJO
			Vulnerabilidades detectadas	Sistema Operativo sin las ultimas actualizaciones	2,33	3	3	Software en su ultima version	20,97	ALTO	Mitigar/Evitar/Transferir	Preventivo	Cambiar de version a una con soporte	1	1	2,33	BAJO

E11		Windows Server 2008	Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Sistema Operativo sin soporte	2,33	3	3	Software en su ultima version	20,97	ALTO	Mitigar/Evitar/Transferir	Preventivo	Cambiar de version a una con soporte	1	1	2,33	BAJO
			Vulnerabilidades detectadas	Sistema Operativo sin las ultimas actualizaciones	2,33	3	3	Software en su ultima version	20,97	ALTO	Mitigar/Evitar/Transferir	Preventivo	Cambiar de version a una con soporte	1	1	2,33	BAJO
E12		Windows Server 2003	Fallos y vulnerabilidad a amenazas	Sistema Operativo sin soporte	2,33	3	3	Software en su ultima version	20,97	ALTO	Mitigar/Evitar/Transferir	Preventivo	Cambiar de version a una con soporte	1	1	2,33	BAJO
			Vulnerabilidades detectadas	Sistema Operativo sin las ultimas actualizaciones	2,33	3	3	Software en su ultima version	20,97	ALTO	Mitigar/Evitar/Transferir	Preventivo	Cambiar de version a una con soporte	1	1	2,33	BAJO
E13		Windows Server 2003	Fallos y vulnerabilidad a amenazas	Sistema Operativo sin soporte	2,33	3	3	Software en su ultima version	20,97	ALTO	Mitigar/Evitar/Transferir	Preventivo	Cambiar de version a una con soporte	1	1	2,33	BAJO
			Explotacion de vulnerabilidades detectadas	Sistema Operativo sin las ultimas actualizaciones	2,33	3	3	Software en su ultima version	20,97	ALTO	Mitigar/Evitar/Transferir	Preventivo	Cambiar de version a una con soporte	1	1	2,33	BAJO
E14		Windows 10	Ataques de malware	Sin soporte como servidor	2,33	1	3	Mantenimiento local	6,99	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Cambiar a un SO dedicado a servidores con soporte	1	1	2,33	BAJO
			Bajas del rendimiento	Sin soporte como servidor	2,33	1	3	Mantenimiento local	6,99	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Cambiar a un SO dedicado a servidores con soporte	1	1	2,33	BAJO

			Intrusiones	Seguridad inadecuada para uso como servidor	2,33	1	3	Mantenimiento local	6,99	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Cambiar a un SO dedicado a servidores con soporte	1	1	2,33	BAJO
			Hackeos	Seguridad inadecuada para uso como servidor	2,33	1	3	Mantenimiento local	6,99	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Cambiar a un SO dedicado a servidores con soporte	1	1	2,33	BAJO
E15	Bases de Datos	Postgis 2.2	Explotaciones de amenazas conocidas	Version antigua del software	2,67	2	2	Software en su ultima version	10,68	ALTO	Mitigar/Evitar/Transferir	Preventivo	Cambiar de version a una con soporte	1	1	2,67	BAJO
			Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Software sin soporte	2,67	3	3	Software en su ultima version	24,03	ALTO	Mitigar/Evitar/Transferir	Preventivo	Cambiar de version a una con soporte	1	1	2,67	BAJO
E16		Postgresql 9.5	Explotaciones de amenazas conocidas	Version antigua del software	3,00	2	3	Software en su ultima version	18	ALTO	Mitigar/Evitar/Transferir	Preventivo	Cambiar de version a una con soporte	1	1	3	BAJO
			Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Software sin soporte	3,00	2	3	Software en su ultima version	18	ALTO	Mitigar/Evitar/Transferir	Preventivo	Cambiar de version a una con soporte	1	1	3	BAJO
E17	ERP	SIIIM	INFORMACION RESERVADA	INFORMACION RESERVADA	2,00	RESERVADO	RESERVADO	RESERVADO	RESERVADO	RESERVADO	RESERVADO	Preventivo	RESERVADO	RESERVADO	RESERVADO	RESERVADO	RESERVADO

E18	FIREWALL	SOPHOS SG 230 rev 1	Trafico indeseado	Configuracion inadecuada	2,00	1	1	Soporte contratado	2	BAJO	Aceptar	Preventivo	Soporte Contratado	1	1	2	BAJO
			Intrusiones no autorizadas	Puertos abiertos no autorizados	2,00	1	1	Soporte contratado	2	BAJO	Aceptar	Preventivo	Soporte Contratado	1	1	2	BAJO
			Vulnerabilidades detectadas	Firmware desactualizado	2,00	1	1	Soporte contratado	2	BAJO	Aceptar	Preventivo	Soporte Contratado	1	1	2	BAJO
			Destruccion por inundacion	Aumento del caudal del rio/ Centro de datos colindante con un baño	2,00	1	1	Sin control	2	BAJO	Aceptar	Preventivo	Soporte Contratado	1	1	2	BAJO
E19	RED	HP MSR 900	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,67	1	1	Firmware actualizado	1,67	BAJO	Aceptar	Preventivo				0	BAJO
			Acceso no autorizado	Contraseñas por defecto	1,67	1	1	Control tercerisado	1,67	BAJO	Aceptar	Preventivo				0	BAJO
			Acceso no autorizado	Contraseñas filtradas	1,67	1	1	Control tercerisado	1,67	BAJO	Aceptar	Preventivo				0	BAJO
			Hurto	Seguridad inadecuada para acceder al centro de datos	1,67	1	2	Cerrado bajo llave	3,34	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Camaras/Ingreso con tarjetas de identificacion	1	1	1,67	BAJO
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	1,67	2	2	Sin control	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Uso de aire acondicionado	1	2	3,34	MEDIO

			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	1,67	2	2	Sin control	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Limpieza constante y Mantenimiento local	2	2	6,68	MEDIO
			Subidas o bajadas de tension	Fallo en la red electrica	1,67	1	1	Uso de UPS	1,67	BAJO	Aceptar	Preventivo	Compra de un generador para el edifico	1	1	1,67	BAJO
			Corte del servicio de internet	Fallo del proveedor del servicio	1,67	1	1	Control tercerisado	1,67	BAJO	Aceptar	Preventivo	Control de terceros	1	1	1,67	BAJO
				Fallos del hardware	1,67	1	1	Control tercerisado	1,67	BAJO	Aceptar	Preventivo	Control de terceros	1	1	1,67	BAJO
				Configuracion inadecuada del dispositivos	1,67	1	1	Control tercerisado	1,67	BAJO	Aceptar	Preventivo	Control de terceros	1	1	1,67	BAJO
E20		HPE OfficeConect 1920S Series Switch	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,67	1	1	Firmware actualizado	1,67	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,67	BAJO
			Hurto	Seguridad inadecuada para acceder al centro de datos	1,67	1	2	Cerrado bajo llave	3,34	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Camaras/Ingreso con tarjetas de identificacion	1	1	1,67	BAJO
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	1,67	2	2	Ventanas abiertas con mallas	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Uso de aire acondicionado	1	2	3,34	MEDIO

			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	1,67	2	2	Sin control	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Limpieza constante y Mantenimiento local	2	2	6,68	MEDIO
			Subidas o bajadas de tension	Fallo en la red electrica	1,67	1	3	Uso de UPS	5,01	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	1	1	1,67	BAJO
			Desconeccion entre los servidores y la intranet de la empresa	Fallos del hardware	1,67	1	1	Mantenimiento local	1,67	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,67	BAJO
				Configuracion inadecuada del dispositivos	1,67	1	1	Mantenimiento local	1,67	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,67	BAJO
			Mayor latencia de datos	Cableado desordenado	1,67	1	1	Mantenimiento local	1,67	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,67	BAJO
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,67	BAJO
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,67	BAJO
E21		HPE OfficeConect 1920S	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,67	1	1	Firmware actualizado	1,67	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,67	BAJO

		Series Switch	Hurto	Seguridad inadecuada para acceder al centro de datos	1,67	1	2	Cerrado bajo llave	3,34	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Camaras/Ingreso con tarjetas de identificacion	1	1	1,67	BAJO
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	1,67	2	2	Ventanas abiertas con mallas	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Uso de aire acondicionado	1	2	3,34	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	1,67	2	2	Sin control	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Limpieza constante y Mantenimiento local	2	2	6,68	MEDIO
			Subidas o bajadas de tension	Fallo en la red electrica	1,67	1	3	Uso de UPS	5,01	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	1	1	1,67	BAJO
			Desconeccion del servicio de red en la planta baja	Fallos del hardware	1,67	1	1	Mantenimiento local	1,67	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,67	BAJO
				Configuracion inadecuada del dispositivos	1,67	1	1	Mantenimiento local	1,67	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,67	BAJO
			Mayor latencia de datos	Cableado desordenado	1,67	1	1	Mantenimiento local	1,67	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,67	BAJO

			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,67	BAJO
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,67	BAJO
E22		HPE OfficeConnect 1920S Series Switch	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,67	1	1	Firmware actualizado	1,67	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,67	BAJO
			Hurto	Seguridad inadecuada para acceder al centro de datos	1,67	1	2	Cerrado bajo llave	3,34	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Camaras/Ingreso con tarjetas de identificacion	1	1	1,67	BAJO
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	1,67	2	2	Ventanas abiertas con mallas	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Uso de aire acondicionado	1	2	3,34	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	1,67	2	2	Sin control	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Limpieza constante y Mantenimiento local	2	2	6,68	MEDIO

			Subidas o bajadas de tension	Fallo en la red electrica	1,67	1	3	Uso de UPS	5,01	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	1	1	1,67	BAJO
			Desconeccion del servicio de red en la planta baja	Fallos del hardware	1,67	1	1	Mantenimiento local	1,67	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,67	BAJO
				Configuracion inadecuada del dispositivos	1,67	1	1	Mantenimiento local	1,67	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,67	BAJO
			Mayor latencia de datos	Cableado desordenado	1,67	1	1	Mantenimiento local	1,67	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,67	BAJO
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,67	BAJO
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,67	BAJO
E23		PE Aruba Instant On 1930 24G 4SFP/SFP	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,33	1	1	Firmware actualizado	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Hurto	Seguridad inadecuada para acceder al centro de datos	1,33	1	2	Cerrado bajo llave	2,66	BAJO	Aceptar	Preventivo	Camaras/Ingreso con tarjetas de identificacion	1	1	1,33	BAJO

			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	1,33	2	2	Ventilacion a traves de la ventana abierta hacia el centro de datos	5,32	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Uso de aire acondicionado	1	2	2,66	BAJO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	1,33	2	2	Sin control	5,32	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Limpieza constante y Mantenimiento local	2	2	5,32	MEDIO
			Subidas o bajadas de tension	Fallo en la red electrica	1,33	1	3	Uso de UPS	3,99	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	1	1	1,33	BAJO
			Desconeccion del servicio de telefonia IP en la planta baja	Fallos del hardware	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
				Configuracion inadecuada del dispositivos	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Interferencias electromagneticas	Cableado desordenado	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,33	BAJO
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	1,33	1	1	Cableado etiquetado	1,33	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,33	BAJO

			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	1,33	1	1	Cableado etiquetado	1,33	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,33	BAJO
E24		HPE OfficeConnect 1920S Series Switch	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,67	1	1	Firmware actualizado	1,67	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,67	BAJO
			Hurto	Seguridad inadecuada para acceder al centro de datos	1,67	1	2	Cerrado bajo llave	3,34	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Camaras/Ingreso con tarjetas de identificacion	1	1	1,67	BAJO
			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	1,67	2	2	Ventilacion a traves de la ventana abierta hacia el centro de datos	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Uso de aire acondicionado	1	2	3,34	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	1,67	2	2	Sin control	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Limpieza constante y Mantenimiento local	2	2	6,68	MEDIO
			Subidas o bajadas de tension	Fallo en la red electrica	1,67	1	3	Uso de UPS	5,01	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	1	1	1,67	BAJO
			Desconeccion del servicio de red en los	Fallos del hardware	1,67	1	1	Mantenimiento local	1,67	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,67	BAJO
				Configuracion inadecuada	1,67	1	1	Mantenimiento local	1,67	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,67	BAJO

			pisos superiores	del dispositivos													
			Mayor latencia de datos	Cableado desordenado	1,67	1	1	Mantenimiento local	1,67	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,67	BAJO
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,67	BAJO
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,67	BAJO
E25		PE Aruba Instant On 1930 24G 4SFP/SFP	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,33	1	1	Firmware actualizado	1,33	BAJO	Aceptar	Preventivo	Firmware actualizado	1	1	1,33	BAJO
			Manejo inadecuado por personal no capacitado	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	1,33	1	3	Sin control	3,99	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Cerrar el rack	1	1	1,33	BAJO
			Hurto	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	1,33	2	2	Sin control	5,32	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Cerrar el rack	1	1	1,33	BAJO

			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	1,33	2	2	Sin control	5,32	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Mantenimiento local, limpieza y cerrar el rack	1	1	1,33	BAJO
			Subidas o bajadas de tension	Fallo en la red electrica	1,33	1	3	Sin control	3,99	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	1	1	1,33	BAJO
			Desconeccion del servicio de telefonia IP en el piso 1	Fallos del hardware	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
				Configuracion inadecuada del dispositivos	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Interferencias electromagneticas	Cableado desordenado	1,33	1	2	Mantenimiento local	2,66	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,33	BAJO
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	1,33	1	1	Cableado etiquetado	1,33	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,33	BAJO
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	1,33	1	1	Cableado etiquetado	1,33	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,33	BAJO
E26		HPE OfficeConect 1920S	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,67	1	1	Firmware actualizado	1,67	BAJO	Aceptar	Preventivo	Firmware actualizado	1	1	1,67	BAJO

		Series Switch	Manejo inadecuado por personal no capacitado	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	1,67	1	3	Sin control	5,01	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Cerrar el rack	1	1	1,67	BAJO
			Hurto	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	1,67	2	2	Sin control	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Cerrar el rack	1	1	1,67	BAJO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	1,67	2	2	Sin control	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Mantenimiento local, limpieza y cerrar el rack	1	1	1,67	BAJO
			Subidas o bajadas de tension	Fallo en la red electrica	1,67	1	3	Sin control	5,01	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	1	1	1,67	BAJO
			Desconeccion del servicio de red en el piso 1	Fallos del hardware	1,67	1	1	Mantenimiento local	1,67	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,67	BAJO
				Configuracion inadecuada del dispositivos	1,67	1	1	Mantenimiento local	1,67	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,67	BAJO
			Mayor latencia de datos	Cableado desordenado	1,67	1	2	Mantenimiento local	3,34	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Cableado etiquetado y organizado	1	1	1,67	BAJO

			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,67	BAJO
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,67	BAJO
E27		PE Aruba Instant On 1930 24G 4SFP/SFP	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,33	1	1	Firmware actualizado	1,33	BAJO	Aceptar	Preventivo	Firmware actualizado	1	1	1,33	BAJO
			Manejo inadecuado por personal no capacitado	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	1,33	2	3	Sin control	7,98	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Cerrar el rack	1	1	1,33	BAJO
			Hurto	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	1,33	2	2	Sin control	5,32	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Cerrar el rack	1	1	1,33	BAJO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	1,33	2	3	Sin control	7,98	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Mantenimiento local, limpieza y cerrar el rack	1	1	1,33	BAJO

			Subidas o bajadas de tension	Fallo en la red electrica	1,33	1	3	Sin control	3,99	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	1	1	1,33	BAJO
			Desconeccion del servicio de telefonia IP en el piso 2	Fallos del hardware	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
				Configuracion inadecuada del dispositivos	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Interferencias electromagneticas	Cableado desordenado	1,33	1	2	Mantenimiento local	2,66	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,33	BAJO
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	1,33	1	1	Cableado etiquetado	1,33	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,33	BAJO
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	1,33	1	1	Cableado etiquetado	1,33	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,33	BAJO
E28		HPE OfficeConect 1920S Series Switch	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,67	1	1	Firmware actualizado	1,67	BAJO	Aceptar	Preventivo	Firmware actualizado	1	1	1,67	BAJO
			Manejo inadecuado por personal no capacitado	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	1,67	2	3	Sin control	10,02	ALTO	Mitigar/Evitar/Transferir	Preventivo	Cerrar el rack	1	1	1,67	BAJO

			Hurto	Ubicación inadecuada con acceso limitado a personal no autorizado de la empreza	1,67	2	2	Sin control	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Cerrar el rack	1	1	1,67	BAJO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	1,67	2	3	Sin control	10,02	ALTO	Mitigar/Evitar/Transferir	Preventivo	Mantenimiento local, limpieza y cerrar el rack	1	1	1,67	BAJO
			Subidas o bajadas de tension	Fallo en la red electrica	1,67	1	3	Sin control	5,01	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	1	1	1,67	BAJO
			Desconeccion del servicio de red en el piso 2	Fallos del hardware	1,67	1	1	Mantenimiento local	1,67	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,67	BAJO
				Configuracion inadecuada del dispositivos	1,67	1	1	Mantenimiento local	1,67	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,67	BAJO
			Mayor latencia de datos	Cableado desordenado	1,67	1	2	Mantenimiento local	3,34	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Cableado etiquetado y organizado	1	1	1,67	BAJO
			Menor eficiencia para resolver problemas relacionados al cableado	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,67	BAJO
			Dificultad para realizar mantenimiento	Cableado desordenado y/o sin etiquetar	1,67	1	1	Cableado etiquetado	1,67	BAJO	Aceptar	Preventivo	Cableado etiquetado y organizado	1	1	1,67	BAJO

E29		APX 530	Hurto	Entrada de personas no autorizadas	1,33	1	1	Camaras/ Guardias	1,33	BAJO	Aceptar	Preventivo	Camaras/ Guardias	1	1	1,33	BAJO
			Daños Fisicos	Maltrato/ Caida	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Alta latencia	Interferencia electromagnetica	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicacion elevada	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Subidas o bajadas de tension	Fallo en la red electrica	1,33	1	3	Sin control	3,99	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	1	1	1,33	BAJO
			Indisponibilidad del servicio	Fallos en los componentes	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Indisponibilidad del servicio	Configuracion inadecuada	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Alta latencia	Trafico de red exesivo	1,33	1	2	Mantenimiento local	2,66	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
E30		AP 55C	Hurto	Acceso libre al dispositivo	1,33	1	1	Camaras/ Guardias	1,33	BAJO	Aceptar	Preventivo	Camaras/ Guardias	1	1	1,33	BAJO
			Daños Fisicos	Maltrato/ Caida	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO

			Alta latencia	Interferencia electromagnetica	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicacion elevada	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Subidas o bajadas de tension	Fallo en la red electrica	1,33	1	3	Sin control	3,99	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	1	1	1,33	BAJO
			Indisponibilidad del servicio	Fallos en los componentes	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Indisponibilidad del servicio	Configuracion inadecuada	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Alta latencia	Trafico de red exesivo	1,33	1	2	Mantenimiento local	2,66	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
E31		AP 55C	Hurto	Acceso libre al dispositivo	1,33	1	1	Camaras/ Guardias	1,33	BAJO	Aceptar	Preventivo	Camaras/ Guardias	1	1	1,33	BAJO
			Daños Fisicos	Maltrato/ Caida	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Alta latencia	Interferencia electromagnetica	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO

			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicacion elevada	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Subidas o bajadas de tension	Fallo en la red electrica	1,33	1	3	Sin control	3,99	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	1	1	1,33	BAJO
			Indisponibilidad del servicio	Fallos en los componentes	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Indisponibilidad del servicio	Configuracion inadecuada	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Alta latencia	Trafico de red exesivo	1,33	1	2	Mantenimiento local	2,66	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
E32		AP 55C	Hurto	Acceso libre al dispositivo	1,33	1	1	Camaras/ Guardias	1,33	BAJO	Aceptar	Preventivo	Camaras/ Guardias	1	1	1,33	BAJO
			Daños Fisicos	Maltrato/ Caida	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Alta latencia	Interferencia electromagnetica	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicacion elevada	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO

			Subidas o bajadas de tension	Fallo en la red electrica	1,33	1	3	Sin control	3,99	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	1	1	1,33	BAJO
			Indisponibilidad del servicio	Fallos en los componentes	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Indisponibilidad del servicio	Configuracion inadecuada	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Alta latencia	Trafico de red exesivo	1,33	1	2	Mantenimiento local	2,66	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
E33		Cableado Vertical Fibra Optica	Destrucion	Daño fisico/Rotura/ Cortes	1,67	1	1	Mantenimiento local	1,67	BAJO	Aceptar	Preventivo	Mantenimiento	1	1	1,67	BAJO
			Alta latencia	Interferencia electromagnetica	1,67	1	1	Mantenimiento local	1,67	BAJO	Aceptar	Preventivo	Mantenimiento	1	1	1,67	BAJO
E34		Cableado Horizontal UTP CAT 6/ 6A	Destrucion	Daño fisico/Rotura/ Cortes	1,67	1	1	Mantenimiento local	1,67	BAJO	Aceptar	Preventivo	Mantenimiento	1	1	1,67	BAJO
			Alta latencia	Interferencia electromagnetica	1,67	1	1	Mantenimiento local	1,67	BAJO	Aceptar	Preventivo	Mantenimiento	1	1	1,67	BAJO
E35		Redes VLAN	Accesos no autorizados	Configuracion incompleta	2,33	1	2	Mantenimiento local	4,66	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Finalizar la configuracion de las VLANS	1	1	2,33	BAJO
			Conflicto de direcciones IP		2,33	2	2	Mantenimiento local	9,32	ALTO	Mitigar/Evitar/Transferir	Correctivo	Finalizar la configuracion de las VLANS	1	1	2,33	BAJO

			Dificultad par reconfigurar las VLANS		2,33	1	2	Mantenimiento local	4,66	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Finalizar la configuracion de las VLANS	1	1	2,33	BAJO
			Bajo rendimiento de la red		2,33	1	2	Mantenimiento local	4,66	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Finalizar la configuracion de las VLANS	1	1	2,33	BAJO
			Ataque de snooping	Filtracion de la tabla de subredes	2,33	1	1	Direccionamiento confidencial	2,33	BAJO	Aceptar	Preventivo	Direccionamiento confidencial	1	1	2,33	BAJO
			Accesos no autorizados a subredes	Filtracion de la tabla de subredes	2,33	1	1	Direccionamiento confidencial	2,33	BAJO	Aceptar	Preventivo	Direccionamiento confidencial	1	1	2,33	BAJO
			Interrupcion de servicios	Filtracion de la tabla de subredes	2,33	1	1	Direccionamiento confidencial	2,33	BAJO	Aceptar	Preventivo	Direccionamiento confidencial	1	1	2,33	BAJO
E36		Redes Wireless	Accesos a redes con permisos superirores	Filtracion de contraseñas	1,33	2	3	Sin control	7,98	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Cambio de contraseñas cada 2 semanas	1	1	1,33	BAJO
			Accesos no autorizados	Contraseñas debiles	1,33	1	2	Politica de contraseñas	2,66	BAJO	Aceptar	Correctivo	Politica de contraseñas	1	1	1,33	BAJO
			Ataques de fuerza bruta y diccionarios de contraseñas	Contraseñas debiles	1,33	1	2	Politica de contraseñas	2,66	BAJO	Aceptar	Correctivo	Politica de contraseñas	1	1	1,33	BAJO
			Intercepcion de trafico de red	Cifrado de red debil	1,33	1	1	WPA2 PSK	1,33	BAJO	Aceptar	Preventivo	WPA2 PSK	1	1	1,33	BAJO
			Inyeccion de paquetes	Cifrado de red debil	1,33	1	1	WPA2 PSK	1,33	BAJO	Aceptar	Preventivo	WPA2 PSK	1	1	1,33	BAJO

			Menor privacidad, seguridad y control	Redes wifi visibles	1,33	2	3	Sin control	7,98	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Ocultacion de las redes	1	1	1,33	BAJO
E37		Antena Ubiquiti Nanostation M5 LOC0	Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Exposicion al aire libre	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Desgaste por el clima	Exposicion al aire libre	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Sobrecarga electrica	Rayos	1,33	2	2	Sin control	5,32	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Uso de un pararrayos / Protector de sobretencion, y asegurar una coneccion a tierra adecuada	1	1	1,33	BAJO
			Caidas/ Vibraciones exesivas	Instalacion incorrecta	1,33	1	1	Mantenimiento local	1,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,33	BAJO
			Daño fisico	Mantenimiento inadecuado	1,33	1	3	Mantenimiento ocacional	3,99	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Mantenimiento local y limpieza	1	1	1,33	BAJO
E38	TELEFONIA	Panasonic KX-NS500	Fallos y explotacion de vulnerabilidades	Firmware desactualizado	1,67	1	1	Firmware actualizado	1,67	BAJO	Aceptar	Preventivo	Firmware actualizado	1	1	1,67	BAJO
			Hurto	Seguridad inadecuada para acceder al centro de datos	1,67	1	2	Cerrado bajo llave	3,34	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Camaras y acceso con credenciales	1	1	1,67	BAJO

			Recalentamiento del equipo	Infraestructura inadecuada del centro de datos, referida a que no existe una adecuada ventilacion/filtracion de aire	1,67	2	2	Ventilacion hacia el centro de datos 1 a traves de una ventana	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Aire acondicionado	1	2	3,34	MEDIO
			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Centro de datos con infraestructura inadecuada	1,67	2	2	Sin control	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Limpieza constante y Mantenimiento local	1	2	3,34	MEDIO
			Subidas o bajadas de tension	Fallo en la red electrica	1,67	1	1	Uso de UPS	1,67	BAJO	Aceptar	Preventivo	Compra de un generador para el edifico	1	1	1,67	BAJO
			Fallo del servicio de telefonia IP	Fallos del hardware	1,67	1	1	Mantenimiento local	1,67	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,67	BAJO
				Configuracion inadecuada del dispositivos	1,67	1	1	Mantenimiento local	1,67	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1,67	BAJO
E39	UPS	Eaton 906 IIS	Fallas de la bateria y daños en la electronica	Tiempo de vida de uso prolongado	1,00	2	3	Mantenimiento local	6	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	1	1	1	BAJO
				Sobrecargas, descargas electricas	1,00	1	1	Mantenimiento local	1	BAJO	Aceptar	Preventivo	Compra de un generador para el edifico	1	1	1	BAJO
				Degradacion natural	1,00	2	3	Mantenimiento local	6	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	1	1	1	BAJO
				Mala estimacion de la carga	1,00	1	1	Mantenimiento local	1	BAJO	Aceptar	Preventivo	Compra de un generador para el edifico	1	1	1	BAJO

E40		APC SRT2200 XLA		Tiempo de vida de uso prolongado	1,00	2	3	Mantenimiento local	6	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	1	1	1	BAJO
				Sobrecargas, descargas electricas	1,00	1	1	Mantenimiento local	1	BAJO	Aceptar	Preventivo	Compra de un generador para el edifico	1	1	1	BAJO
				Degradacion natural	1,00	2	3	Mantenimiento local	6	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	1	1	1	BAJO
				Mala estimacion de la carga	1,00	1	1	Mantenimiento local	1	BAJO	Aceptar	Preventivo	Compra de un generador para el edifico	1	1	1	BAJO
E41		APC SRT2200 XLA		Tiempo de vida de uso prolongado	1,00	2	3	Mantenimiento local	6	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	1	1	1	BAJO
				Sobrecargas, descargas electricas	1,00	1	1	Mantenimiento local	1	BAJO	Aceptar	Preventivo	Compra de un generador para el edifico	1	1	1	BAJO
				Degradacion natural	1,00	2	3	Mantenimiento local	6	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	1	1	1	BAJO
				Mala estimacion de la carga	1,00	1	1	Mantenimiento local	1	BAJO	Aceptar	Preventivo	Compra de un generador para el edifico	1	1	1	BAJO
E42		Forza FDC-003K		Tiempo de vida de uso prolongado	1,00	2	3	Mantenimiento local	6	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	1	1	1	BAJO
				Sobrecargas, descargas electricas	1,00	1	1	Mantenimiento local	1	BAJO	Aceptar	Preventivo	Compra de un generador para el edifico	1	1	1	BAJO
				Degradacion natural	1,00	2	3	Mantenimiento local	6	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	1	1	1	BAJO
				Mala estimacion de la carga	1,00	1	1	Mantenimiento local	1	BAJO	Aceptar	Preventivo	Compra de un generador para el edifico	1	1	1	BAJO

E43	Dominio/IP Y Subdominios	emapal.gob.ec/207.174.XXX.XXX/egob, edoc, etc	Explotacion de vulnerabilidades relacionadas con Open SSH 7.4	Vulnerabilidades en el puerto 22 y 2222 relacionadas al uso de Open SSH 7.4	2,00	2	3	Sin control	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Actualizar la version de Open SSH	1	1	2	BAJO
			Panel de logeo a CPANEL publica, ingreso no autorizado a traves de fuerza bruta, diccionarios, pishing,ingenieria social.	Acceso publico al puerto 2082 y 2083	2,00	2	3	Sin control	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Asignar direcciones IP especificas para su acceso	1	1	2	BAJO
			Panel de logeo a WebHostManager publica, ingreso no autorizado a traves de fuerza bruta, diccionarios, pishing,ingenieria social.	Acceso publico al puerto 2086 y 2087	2,00	2	3	Sin control	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Asignar direcciones IP especificas para su acceso	1	1	2	BAJO
E44	Pagina Web	www.emapal.gob.ec	Informacion erronea	Web desactualizada	1,33	3	2	Mantenimiento local	7,98	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Actualizar constantemente la	1	1	1,33	BAJO

													informacion de la web				
			Falta de informacion	Web desactualizada	1,33	3	2	Mantenimiento local	7,98	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Actualizar constantemente la informacion de la web	1	1	1,33	BAJO
			Explotacion de vulnerabilidades propias de la plataforma/ servicio	Puerto y subdominio visible en el servicio de recursos humanos	1,33	1	3	Mantenimiento local	3,99	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Ocultar el puerto y el subdominio de la url	1	1	1,33	BAJO
			Ataques de fuerza bruta	Puerto y subdominio visible en el servicio de recursos humanos	1,33	1	3	Mantenimiento local	3,99	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Ocultar el puerto y el subdominio de la url	1	1	1,33	BAJO
			Informacion sensible de la estructura de la plataforma vuelta publica	Puerto y subdominio visible en el servicio de recursos humanos	1,33	1	3	Mantenimiento local	3,99	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Ocultar el puerto y el subdominio de la url	1	1	1,33	BAJO
E45	Servicio de Correo Masivo	Correo Masivo	Desconeccion con el servicio	Problemas tecnicos	2,00	1	1	Control tercerisado	2	BAJO	Aceptar	Preventivo	Control de terceros	1	1	2	BAJO
			Desconeccion con el servicio	Desconeccion de la intranet de la empresa con internet	2,00	1	1	Control tercerisado	2	BAJO	Aceptar	Preventivo	Control de terceros	1	1	2	BAJO

			Perdida del control de datos	No ser dueños del servicio	2,00	1	1	Control tercerisado	2	BAJO	Aceptar	Preventivo	Control de terceros	1	1	2	BAJO
			Ataques de fuerza bruta o de diccionarios	Contraseñas inadecuadas	2,00	2	1	Politica de contraseñas	4	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Politica de contraseñas	1	1	2	BAJO
E46	Servicio de Correo Corporatico	Correo Corporativo	Desconeccion con el servicio	Problemas tecnicos	2,00	1	1	Control tercerisado	2	BAJO	Aceptar	Preventivo	Control de terceros	1	1	2	BAJO
			Desconeccion con el servicio	Desconeccion de la intranet de la empresa con internet	2,00	1	1	Control tercerisado	2	BAJO	Aceptar	Preventivo	Control de terceros	1	1	2	BAJO
			Perdida del control de datos	No ser dueños del servicio	2,00	1	1	Control tercerisado	2	BAJO	Aceptar	Preventivo	Control de terceros	1	1	2	BAJO
			Filtracion de informacion	Uso de correo institucional para servicios externos	2,00	2	2	Politicas de uso de correos	8	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Politica de uso del correo institucional	1	1	2	BAJO
			Descargas de malware	Uso de correo institucional para servicios externos	2,00	2	2	Politicas de uso de correos	8	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Politica de uso del correo institucional	1	1	2	BAJO
			Filtracion de credenciales y/o informacion persona o de la empresa	Correos con Pishing	2,00	2	3	Sin control	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Politica de uso del correo institucional	1	1	2	BAJO
			Infeccion de la red/ terminal	Correos infectados de malware	2,00	2	1	Firewall / Antivirus	4	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Firewall/Antivirus	1	1	2	BAJO

			Ataques de fuerza bruta o de diccionarios	Contraseñas inadecuadas	2,00	1	3	Politica de contraseñas	6	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Politica de contraseñas	1	1	2	BAJO
E47	Software	Consolas	Ataques de fuerza bruta o de diccionarios	Contraseñas inadecuadas	3,00	2	1	Politica de contraseñas	6	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Politica de contraseñas	1	1	3	BAJO
			Codigo malicioso	Exploits de software	3,00	1	1	Software actualizado	3	BAJO	Aceptar	Preventivo	Software actualizado	1	1	3	BAJO
			Codigo malicioso	Inyeccion de codigo	3,00	1	1	Software actualizado	3	BAJO	Aceptar	Preventivo	Software actualizado	1	1	3	BAJO
E48	BACK UPS	Respaldo disco duro externo	Perdida	Objeto transportable y accesible	2,67	2	2	Almacenamiento bajo llave	10,68	ALTO	Mitigar/Evitar/Transferir	Preventivo	Compra de un servidor para respaldos a nivel operativo, y de almacenamiento	1	1	2,67	BAJO
			Destruccion	Sensible a agentes fisicos, caidas, golpes	2,67	2	2	Almacenamiento bajo llave	10,68	ALTO	Mitigar/Evitar/Transferir	Preventivo	Compra de un servidor para respaldos a nivel operativo, y de almacenamiento	1	1	2,67	BAJO
			Hurto	Objeto transportable y accesible	2,67	2	2	Almacenamiento bajo llave	10,68	ALTO	Mitigar/Evitar/Transferir	Preventivo	Compra de un servidor para respaldos a nivel operativo, y de almacenamiento	1	1	2,67	BAJO
			Perdida de datos	Daño mecanico, caidas golpes, agentes fisicos	2,67	1	2	Manejo adecuado	5,34	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un servidor para respaldos a nivel operativo, y de almacenamiento	1	1	2,67	BAJO
			Robo de datos	Falta de contraseña/encriptacion	2,67	1	1	Disco duro cifrado	2,67	BAJO	Aceptar	Preventivo	Compra de un servidor para respaldos a nivel operativo, y de almacenamiento	1	1	2,67	BAJO

E49		Respaldo Telconet	Robo/Alteracion de la informacion	Acceso no autorizado	2,67	1	1	Control tercerisado	2,67	BAJO	Aceptar	Preventivo	Respaldos en la nube a nivel operativo, y de almacenamiento	1	1	2,67	BAJO
			Corrupcion /Perdida de datos	Error humano	2,67	1	1	Control tercerisado	2,67	BAJO	Aceptar	Preventivo	Respaldos en la nube a nivel operativo, y de almacenamiento	1	1	2,67	BAJO
			Corrupcion /Perdida de datos	Fallos en el hardware donde se almacena	2,67	1	1	Control tercerisado	2,67	BAJO	Aceptar	Preventivo	Respaldos en la nube a nivel operativo, y de almacenamiento	1	1	2,67	BAJO
			Destruccion del hardware donde se almacena el respaldo	Desastres naturales	2,67	1	1	Control tercerisado	2,67	BAJO	Aceptar	Preventivo	Respaldos en la nube a nivel operativo, y de almacenamiento	1	1	2,67	BAJO
			Destruccion del hardware donde se almacena el respaldo	Amenazas ambientales	2,67	1	1	Control tercerisado	2,67	BAJO	Aceptar	Preventivo	Respaldos en la nube a nivel operativo, y de almacenamiento	1	1	2,67	BAJO
E50	ANTIVIRUS	Kaspersky	Malware	Antivirus desactualizado	1,00	1	1	Antivirus actualizado	1	BAJO	Aceptar	Preventivo	Antivirus Actualizado	1	1	1	BAJO
E51	ASISTENCIA	MB360 ZKTECO	Registro erroneo	Fecha y hora incorrectas	2,00	1	1	Mantenimiento local	2	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	2	BAJO
			Registro erroneo	Identificacion erronea	2,00	1	1	Mantenimiento local	2	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	2	BAJO
			Daño	Daño mecanico, caidas golpes, agentes fisicos	2,00	1	1	Mantenimiento local	2	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	2	BAJO

			Destruccion	Daño mecanico, caidas golpes, agentes fisicos	2,00	1	1	Mantenimiento local	2	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	2	BAJO
E52		Biotime 8.0	Explotacion de vulnerabilidades	Firmware desactualizado	2,00	1	1	Mantenimiento local	2	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	2	BAJO
			Ataques de fuerza bruta o de diccionarios	Contraseñas inadecuadas	2,00	2	2	Politica de contraseñas	8	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Politica de contraseñas	1	1	2	BAJO
			Robo de informacion biometrica	Firmware desactualizado	2,00	1	1	Firmware actualizado	2	BAJO	Aceptar	Preventivo	Firmware actualizado	1	1	2	BAJO
			Robo de informacion biometrica	Contraseñas inadecuadas	2,00	1	1	Politica de contraseñas	2	BAJO	Aceptar	Preventivo	Politica de contraseñas	1	1	2	BAJO
E53	SEGURIDAD	Camaras de seguridad	Vandalismo o robo	Activos en lugares accesibles	1,00	2	1	Camaras/Guardias de seguridad	2	BAJO	Aceptar	Preventivo	Camaras/Guardias de seguridad	1	1	1	BAJO
			Daño	Daño mecanico, caidas golpes, agentes fisicos	1,00	3	3	Sin control	9	ALTO	Mitigar/Evitar/Transferir	Preventivo	Mantenimineto	2	2	4	MEDIO
			Destruccion	Daño mecanico, caidas golpes, agentes fisicos	1,00	3	3	Sin control	9	ALTO	Mitigar/Evitar/Transferir	Preventivo	Mantenimiento	2	2	4	MEDIO

			Fallos en el funcionamiento, baja resolucion de las imágenes	Camaras antiguas	1,00	3	3	Sin control	9	ALTO	Mitigar/Evitar/Transferir	Preventivo	Adquisicion de nuevas camaras	1	1	1	BAJO
			Puntos ciegos ubicados en los lugares donde las camaras no funcionan	Camaras sin funcionamiento	1,00	3	3	Sin control	9	ALTO	Mitigar/Evitar/Transferir	Preventivo	Adquisicion de nuevas camaras	1	1	1	BAJO
			Acceso no autorizado , intrusiones	Asignacion de una ip publicas a traves del dominio para que esten disponibles para el director administrativo desde su dispositivo movil	1,00	2	3	Sin control	6	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Administracion de las camaras por parte del area de TI	1	1	1	BAJO
			Inyeccion de codigo malicioso y/o spyware	Asignacion de una ip publicas a traves del dominio para que esten disponibles para el director administrativo desde su dispositivo movil	1,00	2	3	Sin control	6	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Administracion de las camaras por parte del area de TI	1	1	1	BAJO

E54		DVR modelo desconocido	Intrusiones por credenciales debiles/nulas	Sistema de camaras a cargo de la direccion administrativa	1,67	2	3	Sin control	10,02	ALTO	Mitigar/Evitar/Transferir	Correctivo	Administracion del DVR por parte del area de TI	1	1	1,67	BAJO
			Intruciones a puertos abiertos	Sistema de camaras a cargo de la direccion administrativa	1,67	2	3	Sin control	10,02	ALTO	Mitigar/Evitar/Transferir	Correctivo	Administracion del DVR por parte del area de TI	1	1	1,67	BAJO
			Explotacion de vulnerabilidades por software desactualizado	Sistema de camaras a cargo de la direccion administrativa	1,67	2	3	Sin control	10,02	ALTO	Mitigar/Evitar/Transferir	Correctivo	Administracion del DVR por parte del area de TI	1	1	1,67	BAJO
			Infecciones de malware	Sistema de camaras a cargo de la direccion administrativa	1,67	2	3	Sin control	10,02	ALTO	Mitigar/Evitar/Transferir	Correctivo	Administracion del DVR por parte del area de TI	1	1	1,67	BAJO
			Fallos debido a configuracion inadecuada	Sistema de camaras a cargo de la direccion administrativa	1,67	2	3	Sin control	10,02	ALTO	Mitigar/Evitar/Transferir	Correctivo	Administracion del DVR por parte del area de TI	1	1	1,67	BAJO
			Hurto	Seguridad inadecuada	1,67	2	2	Sin control	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Traslado al centro de datos	1	1	1,67	BAJO
			Destruccion del equipo	Manipulacion del dispositivo	1,67	1	2	Sin control	3,34	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Traslado al centro de datos	1	1	1,67	BAJO
			Recalentamiento del equipo	Ubicación inadecuada	1,67	2	3	Sin control	10,02	ALTO	Mitigar/Evitar/Transferir	Preventivo	Traslado al centro de datos	1	1	1,67	BAJO

			Daño por agentes ambientales (Agua, polvo, fuego,sismo)	Ubicación inadecuada	1,67	2	2	Sin control	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Traslado al centro de datos	1	1	1,67	BAJO
			Subidas o bajadas de tension	Fallo en la red electrica	1,67	1	3	Sin control	5,01	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	1	1	1,67	BAJO
E55	RACKS	Rack 1 Centro de Datos 1	Daño por fallas mecánicas	Derrame de líquidos	1,00	1	1	Mantenimiento Local	1	BAJO	Aceptar	Preventivo	Mantenimiento Local	1	1	1	BAJO
			Daño por fallas mecánicas	Humedad y corrosión	1,00	1	1	Mantenimiento Local	1	BAJO	Aceptar	Preventivo	Mantenimiento Local	1	1	1	BAJO
			Daño por fallas mecánicas	Vibración excesiva	1,00	1	1	Mantenimiento Local	1	BAJO	Aceptar	Preventivo	Mantenimiento Local	1	1	1	BAJO
			Daño por fallas mecánicas	Sobrecarga de peso	1,00	1	1	Mantenimiento Local	1	BAJO	Aceptar	Preventivo	Mantenimiento Local	1	1	1	BAJO
			Daño por fallas mecánicas	Fallas en los soportes	1,00	1	1	Mantenimiento Local	1	BAJO	Aceptar	Preventivo	Mantenimiento Local	1	1	1	BAJO
E56		Rack 2 Centro de datos 2	Daño por fallas mecánicas	Derrame de líquidos	1,00	1	1	Mantenimiento Local	1	BAJO	Aceptar	Preventivo	Mantenimiento Local	1	1	1	BAJO
			Daño por fallas mecánicas	Humedad y corrosión	1,00	1	1	Mantenimiento Local	1	BAJO	Aceptar	Preventivo	Mantenimiento Local	1	1	1	BAJO
			Daño por fallas mecánicas	Vibración excesiva	1,00	1	1	Mantenimiento Local	1	BAJO	Aceptar	Preventivo	Mantenimiento Local	1	1	1	BAJO
			Daño por fallas mecánicas	Sobrecarga de peso	1,00	1	1	Mantenimiento Local	1	BAJO	Aceptar	Preventivo	Mantenimiento Local	1	1	1	BAJO

			Daño por fallas mecánicas	Fallas en los soportes	1,00	1	1	Mantenimiento Local	1	BAJO	Aceptar	Preventivo	Mantenimiento Local	1	1	1	BAJO
E57		Rack Centro de Datos 2	Daño por fallas mecánicas	Derrame de líquidos	1,00	1	1	Mantenimiento Local	1	BAJO	Aceptar	Preventivo	Mantenimiento Local	1	1	1	BAJO
			Daño por fallas mecánicas	Sol, Humedad Corrosión	1,00	1	1	Mantenimiento Local	1	BAJO	Aceptar	Preventivo	Mantenimiento Local	1	1	1	BAJO
			Daño por fallas mecánicas	Vibración excesiva	1,00	1	1	Mantenimiento Local	1	BAJO	Aceptar	Preventivo	Mantenimiento Local	1	1	1	BAJO
			Daño por fallas mecánicas	Sobrecarga de peso	1,00	1	1	Mantenimiento Local	1	BAJO	Aceptar	Preventivo	Mantenimiento Local	1	1	1	BAJO
			Daño por fallas mecánicas	Fallas en los soportes	1,00	1	1	Mantenimiento Local	1	BAJO	Aceptar	Preventivo	Mantenimiento Local	1	1	1	BAJO
E58		Rack Piso 1	Daño por fallas mecánicas	Sol Humedad , Corrosión	1,00	2	2	Mantenimiento Local	4	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Cerrar el rack y ubicarlo en un lugar no tan expuesto a la luz solar	1	1	1	BAJO
			Daño por fallas mecánicas	Vibración excesiva	1,00	1	1	Mantenimiento Local	1	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1	BAJO
			Daño por fallas mecánicas	Sobrecarga de peso	1,00	1	1	Mantenimiento Local	1	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1	BAJO
			Daño por fallas mecánicas	Fallas en los soportes	1,00	1	1	Mantenimiento Local	1	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	1	BAJO
			Incendios/ Desastres ambientales	Rack abierto	1,00	2	3	Sin control	6	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Cerrar el rack	1	1	1	BAJO

			Daño en los equipos al momento de mitigar un incendio	Falta de extintores de CO2	1,00	1	3	Extintores tradicionales	3	BAJO	Aceptar	Preventivo	Adquisicion de extintores de CO2	1	1	1	BAJO
E59		Rack Piso 2	Daño por fallas mecánicas	Humedad y corrosión	1,00	2	2	Mantenimiento Local	4	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Mantenimiento Local	1	1	1	BAJO
			Daño por fallas mecánicas	Vibración excesiva	1,00	1	1	Mantenimiento Local	1	BAJO	Aceptar	Preventivo	Mantenimiento Local	1	1	1	BAJO
			Daño por fallas mecánicas	Sobrecarga de peso	1,00	1	1	Mantenimiento Local	1	BAJO	Aceptar	Preventivo	Mantenimiento Local	1	1	1	BAJO
			Daño por fallas mecánicas	Fallas en los soportes	1,00	1	1	Mantenimiento Local	1	BAJO	Aceptar	Preventivo	Mantenimiento Local	1	1	1	BAJO
			Incendios/ Desastres ambientales/Hurto	Rack abierto	1,00	2	3	Sin control	6	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Cerrar el rack	1	1	1	BAJO
			Incendio/Acumulacion de polvo	Almacenamiento de documentacion fisica cercana	1,00	1	3	Sin control	3	BAJO	Aceptar	Preventivo	Cerrar el rack y ubicarlo en un lugar mas adecuado	1	1	1	BAJO
			Daño en los equipos al momento de mitigar un incendio	Falta de extintores de CO2	1,00	1	3	Extintores tradicionales	3	BAJO	Aceptar	Preventivo	Adquisicion de extintores de CO2	1	1	1	BAJO
E60	UBICACIÓN FISICA	Edificio Matriz	Robo, Vandalismo	Seguridad Fisica Inadecuada	2,33	1	2	Camaras / Seguridad privada	4,66	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Camaras de seguridad/ Guardias / Detectores de movimiento / Proteccion en las entradas y ventanas/	1	1	2,33	BAJO

													Cerramiento mas adecuado				
			Inundacion	Desborde del rio	2,33	1	1	Sin control	2,33	BAJO	Aceptar	Preventivo	Sin control	1	1	2,33	BAJO
			Destruccion del edificio	Incendios	2,33	1	3	Extintores	6,99	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Detectores de humo, extintores, alarma de incendios en las diferentes locaciones	1	1	2,33	BAJO
			Daños	Daño por agentes medioambientales, climatologicos	2,33	1	1	Mantenimiento	2,33	BAJO	Aceptar	Preventivo	Mantenimiento local	1	1	2,33	BAJO
E61		Centro de Datos 1	Sobrecalentamiento/Acumulacion de polvo	Ventilacion y climatizacion inadecuada	2,33	2	3	Ventilacion natural a traves de dos ventanas enrejadas	13,98	ALTO	Mitigar/Evitar/Transferir	Preventivo	Aire acondicionado	2	2	9,32	ALTO
			Intrusiones/Hurto/Destruccion de equipos	Poca seguridad para el ingreso al centro de datos	2,33	2	2	Entrada bajo llave	9,32	ALTO	Mitigar/Evitar/Transferir	Preventivo	Uso de credenciales para el ingreso	1	1	2,33	BAJO
			Intrusiones/Hurto/Destruccion de equipos	Ventana que da al exterior	2,33	1	3	Camaras/Guardias	6,99	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Sellar la ventana	1	1	2,33	BAJO
			Inundacion	Colinda con un baño	2,33	1	3	Sin control	6,99	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Clausurar el baño colindante	1	1	2,33	BAJO
			Inundacion	Ubicado en la primera planta	2,33	1	3	Sin control	6,99	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Trasladar el centro de datos a un piso superior	1	1	2,33	BAJO
			Incendios/Desastres ambientales/Polvo	Piso flotante	2,33	2	3	Sin control	13,98	ALTO	Mitigar/Evitar/Transferir	Preventivo	Reemplazar el piso existente por uno adecuado	1	1	2,33	BAJO

			Incendios/ Desastres ambientales	Racks abiertos	2,33	2	3	Sin control	13,98	ALTO	Mitigar/Evitar/Transferir	Preventivo	Cerrar los racks	2	1	4,66	MEDIO
			Acumulacion de polvo	Almacenamiento de equipos en desuso	2,33	2	3	Equipos en desuso acomodados en una esquina	13,98	ALTO	Mitigar/Evitar/Transferir	Preventivo	Traslado de equipos en desuso	2	1	4,66	MEDIO
			Daño en los equipos al momento de mitigar un incendio	Falta de extintores de CO2	2,33	3	3	Sin control	20,97	ALTO	Mitigar/Evitar/Transferir	Preventivo	Compra de extintores de CO2	1	1	2,33	BAJO
			Intrusiones/ Hurto/Destruccion de equipos	Falta de monitoreo de seguridad	2,33	1	3	Sin control	6,99	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Camaras y sensor de movimiento	1	1	2,33	BAJO
			Cambios ambientales	Falta de monitoreo ambiental	2,33	2	3	Sin control	13,98	ALTO	Mitigar/Evitar/Transferir	Preventivo	Medicion de temperatura, humedad, detectores de humo, detectores de fluidos	1	1	2,33	BAJO
			Subidas , bajadas de tension o cortes electricos	Falta de monitoreo electrico	2,33	1	2	Sin control	4,66	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Medicion de voltaje y detectores de sobrecarga	1	1	2,33	BAJO
			Ingresos no autorizados	Registro de ingreso	2,33	1	2	Sin control	4,66	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Uso de credenciales para el ingreso	1	1	2,33	BAJO
E62		Centro de Datos 2	Sobrecalentamiento/Acumulacion de polvo	Ventilacion y climatizacion inadecuada	2,33	2	3	Ventana abierta hacia el centro de datos 1	13,98	ALTO	Mitigar/Evitar/Transferir	Preventivo	Aire acondicionado	1	2	4,66	MEDIO
			Intrusiones/ Hurto/Destruccion de equipos	Poca seguridad para el ingreso al	2,33	1	2	Entrada bajo llave	4,66	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Uso de credenciales para el ingreso	1	1	2,33	BAJO

				centro de datos													
			Inundacion	Colinda con un baño	2,33	1	1	Sin control	2,33	BAJO	Aceptar	Preventivo	Clausurar el baño colindante	1	1	2,33	BAJO
			Inundacion	Ubicado en la primera planta	2,33	1	1	Sin control	2,33	BAJO	Aceptar	Preventivo	Trasladar el centro de datos a un piso superior	1	1	2,33	BAJO
			Acumulacion de polvo, incendios	Almacenamiento de equipos en desuso y cajas	2,33	2	2	Limpieza ocacional	9,32	ALTO	Mitigar/Evitar/Transferir	Preventivo	Trasado de equipos en desuso y cajas	1	1	2,33	BAJO
			Daño en los equipos al momento de mitigar un incendio	Falta de extintores de CO2	2,33	3	3	Sin control	20,97	ALTO	Mitigar/Evitar/Transferir	Preventivo	Compra de extintores de CO2	1	1	2,33	BAJO
			Intrusiones/Hurto/Destruccion de equipos	Falta de monitoreo de seguridad	2,33	1	3	Sin control	6,99	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Camaras y sensor de movimiento	1	1	2,33	BAJO
			Cambios ambientales	Falta de monitoreo ambiental	2,33	2	3	Sin control	13,98	ALTO	Mitigar/Evitar/Transferir	Preventivo	Medicion de temperatura, humedad, detectores de humo, detectores de fluidos	1	1	2,33	BAJO
			Subidas , bajadas de tension o cortes electricos	Falta de monitoreo electrico	2,33	1	3	Sin control	6,99	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Medicion de voltaje y detectores de sobrecarga	1	1	2,33	BAJO
			Ingresos no autorizados	Falta de registro de ingreso	2,33	1	2	Sin control	4,66	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Uso de credenciales para el ingreso	1	1	2,33	BAJO

E63		Oficina de Sistemas	Sobrecalentamiento/Acumulacion de polvo	Ventilacion y climatizacion inadecuada	1,67	1	1	Abrir ventanas/ Limpieza	1,67	BAJO	Aceptar	Preventivo	Abrir ventanas/ Limpieza	1	1	1,67	BAJO
			Intrusiones/ Hurto/Destruccion de equipos	Poca seguridad para el ingreso a la oficina	1,67	1	2	Entrada bajo llave	3,34	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Uso de credenciales para el ingreso	1	1	1,67	BAJO
			Inundacion	Ubicado en la primera planta	1,67	1	1	Sin control	1,67	BAJO	Aceptar	Preventivo	Traslado a un piso superior, preferiblemente cerca del centro de datos	1	1	1,67	BAJO
			Acumulacion de polvo	Falta de limpieza	1,67	1	1	Limpieza	1,67	BAJO	Aceptar	Preventivo	Limpieza	1	1	1,67	BAJO
			Daño en los equipos al momento de mitigar un incendio	Falta de extintores de CO2	1,67	3	3	Sin control	15,03	ALTO	Mitigar/Evitar/Transferir	Preventivo	Compra de extintores de CO2	1	1	1,67	BAJO
			Intrusiones/ Hurto/Destruccion de equipos	Ventanas con acceso al exterior	1,67	2	2	Camaras	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Camaras / Sensores de movimiento /Seguridad en las ventanas	1	1	1,67	BAJO
			Destruccion o daño de los equipos	Subidas , bajadas de tension o cortes electricos	1,67	1	2	Sin control	3,34	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Comprar un generador para el edifcio	1	1	1,67	BAJO
			Ingresos no autorizados	Ausencia de registro de ingreso	1,67	1	3	Sin control	5,01	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Uso de credenciales para el ingreso	1	1	1,67	BAJO
			Destruccion o daño	Incendios/Desastres ambientales/Polvo	1,67	1	2	Sin control	3,34	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Plan de contingencia frente a desastres ambientales	1	1	1,67	BAJO

E64		Terraza y soporte de la antena	Intrusiones/ Hurto/Destruccion de equipos	Acceso no autorizado	1,67	1	2	Acceso limitado	3,34	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Vigilancia y Acceso limitado	1	1	1,67	BAJO
			Degradacion por agentes ambientales	Falta de mantenimiento y limpieza	1,67	2	2	Mantenimiento ocacional	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Mantenimiento local	1	1	1,67	BAJO
E65	TERMINALES DE LOS EMPLEADOS	Computadoras de escritorio	Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Terminales con OS WINDOWS 7(sin soporte)	2,00	3	3	Equipos actualizados a la ultima version	18	ALTO	Mitigar/Evitar/Transferir	Correctivo	Actualizacion de los equipos a WIN 10	1	1	2	BAJO
			Vulnerabilidades detectadas	Terminales desactualizadas	2,00	2	2	Mantenimiento Local	8	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Mantenimiento local	1	1	2	BAJO
			Fallos en los componentes	Terminales con una antigüedad estimada en 17 años	2,00	3	3	Mantenimiento Local	18	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Problemas de rendimiento		2,00	3	3	Mantenimiento Local	18	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Problemas de capacidad de almacenamiento		2,00	3	3	Mantenimiento Local	18	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Compatibilidad con Software Obsoleto		2,00	3	3	Mantenimiento Local	18	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO

			Problemas de escalabilidad		2,00	3	3	Mantenimiento Local	18	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Fallos en los componentes	Terminales con una antigüedad estimada en 11 años	2,00	2	3	Mantenimiento Local	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Problemas de rendimiento		2,00	2	3	Mantenimiento Local	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Problemas de capacidad de almacenamiento		2,00	2	3	Mantenimiento Local	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Compatibilidad con Software Obsoleto		2,00	2	3	Mantenimiento Local	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Problemas de escalabilidad		2,00	2	3	Mantenimiento Local	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Fallos en los componentes	Terminales con una antigüedad estimada en 7 años	2,00	1	2	Mantenimiento Local	4	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Problemas de rendimiento		2,00	1	2	Mantenimiento Local	4	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Problemas de capacidad de almacenamiento		2,00	1	2	Mantenimiento Local	4	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO

			Compatibilidad con Software Obsoleto		2,00	1	2	Mantenimiento Local	4	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Problemas de escalabilidad		2,00	1	2	Mantenimiento Local	4	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Rendimiento probre	Terminales con procesadores viejos y de poca capacidad	2,00	3	3	Mantenimiento Local	18	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Sobrecalentamiento		2,00	3	3	Mantenimiento Local	18	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Pantallasos azules		2,00	3	3	Mantenimiento Local	18	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Reinicios Inesperados		2,00	3	3	Mantenimiento Local	18	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Corrupcion /Perdida de datos		2,00	3	3	Mantenimiento Local	18	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Aplicaciones que no responden	Terminales con 2 - 3 GB de RAM	2,00	2	3	Mantenimiento Local	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Aumentar la capacidad de ram hasta al menos GB de ram / Comprar terminales actualizados	1	1	2	BAJO
			Bajo rendimiento		2,00	2	3	Mantenimiento Local	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Aumentar la capacidad de ram hasta al menos GB de ram / Comprar terminales actualizados	1	1	2	BAJO
			Reinicios Inesperados		2,00	2	3	Mantenimiento Local	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Aumentar la capacidad de ram hasta al menos GB de ram / Comprar	1	1	2	BAJO

												terminales actualizados					
			Corrupcion /Perdida de datos		2,00	2	3	Mantenimiento Local	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Aumentar la capacidad de ram hasta al menos GB de ram / Comprar terminales actualizados	1	1	2	BAJO
			Aplicaciones que no responden	Terminales con 4 GB de RAM	2,00	2	2	Mantenimiento Local	8	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Aumentar la capacidad de ram hasta al menos GB de ram / Comprar terminales actualizados	1	1	2	BAJO
			Bajo rendimiento		2,00	2	2	Mantenimiento Local	8	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Aumentar la capacidad de ram hasta al menos GB de ram / Comprar terminales actualizados	1	1	2	BAJO
			Conflicto de tareas	Terminales compartidas entre empleados	2,00	2	2	Cuentas de usuario	8	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Filtracion de datos		2,00	1	2	Cuentas de usuario	4	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Desorganizacion de archivos e informacion		2,00	2	2	Cuentas de usuario	8	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Uso ineficiente del terminal		2,00	1	2	Cuentas de usuario	4	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Infeccion de malware	Conexión de dispositivos personales a	2,00	2	2	Registro de actividades del terminal	8	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Politicas de uso de los terminales	1	1	2	BAJO

			Robo de datos	terminales de la empreza	2,00	2	2	Registro de actividades del terminal	8	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Politicas de uso de los terminales	1	1	2	BAJO
			Conflictos en la politica de seguridad		2,00	3	2	Registro de actividades del terminal	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Politicas de uso de los terminales	1	1	2	BAJO
			Accesos no autorizados	Contraseñas debiles para acceso al terminal	2,00	1	3	Politica de contraseñas	6	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Politicas de establecimiento uso y manejo de credenciales	1	1	2	BAJO
			Accesos no autorizados	Terminales sin contraseña	2,00	1	3	Sin control	6	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Politicas de establecimiento uso y manejo de credenciales	1	1	2	BAJO
			Accesos no autorizados	Terminales sin usuario	2,00	1	3	Sin control	6	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Politicas de establecimiento uso y manejo de credenciales	1	1	2	BAJO
			Llevarse los terminales de forma no autorizada fuera de la empresa	Poco control fisico de los terminales	2,00	1	3	Sin control	6	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Politicas de uso de los terminales	1	1	2	BAJO
			Subidas o bajadas de tension	Fallo en la red electrica	2,00	1	3	Sin control	6	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	1	1	2	BAJO
			Destruccion por inundacion	Aumento del caudal del rio/ lluvia	2,00	1	1	Sin control	2	BAJO	Aceptar	Preventivo	Sin control	1	1	2	BAJO
			Daños fisicos	Golpes o caidas	2,00	1	3	Sin control	6	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Politicas de manejo de los terminales	1	1	2	BAJO

E66		Computadoras portatiles	Fallos, interrupciones de funcionamiento y explotacion de vulnerabilidades	Terminales con OS WINDOWS 7(sin soporte)	2,00	3	3	Equipos actualizados a la ultima version	18	ALTO	Mitigar/Evitar/Transferir	Correctivo	Actualizacion de los equipos a WIN 10	1	1	2	BAJO
			Vulnerabilidades detectadas	Terminales desactualizadas	2,00	3	3	Mantenimiento Local	18	ALTO	Mitigar/Evitar/Transferir	Preventivo	Mantenimiento local	1	1	2	BAJO
			Fallos en los componentes	Terminales con una antigüedad estimada en 15 años	2,00	3	3	Mantenimiento Local	18	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Problemas de rendimiento		2,00	3	3	Mantenimiento Local	18	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Problemas de capacidad de almacenamiento		2,00	3	3	Mantenimiento Local	18	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Compatibilidad con Software Obsoleto		2,00	3	3	Mantenimiento Local	18	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Problemas de escalabilidad		2,00	3	3	Mantenimiento Local	18	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Fallos en los componentes	Terminales con una antigüedad estimada	2,00	2	3	Mantenimiento Local	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO

			Problemas de rendimiento	entre 9 - 11 años	2,00	2	3	Mantenimiento Local	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Problemas de capacidad de almacenamiento		2,00	2	3	Mantenimiento Local	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Compatibilidad con Software Obsoleto		2,00	2	3	Mantenimiento Local	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Problemas de escalabilidad		2,00	2	3	Mantenimiento Local	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Fallos en los componentes	Terminales con una antigüedad estimada en 7 años	2,00	2	2	Mantenimiento Local	8	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Problemas de rendimiento		2,00	2	2	Mantenimiento Local	8	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Problemas de capacidad de almacenamiento		2,00	2	2	Mantenimiento Local	8	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Compatibilidad con Software Obsoleto		2,00	2	2	Mantenimiento Local	8	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Problemas de escalabilidad		2,00	2	2	Mantenimiento Local	8	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO

			Rendimiento probre	Terminales con procesadores viejos y de poca capacidad	2,00	3	3	Mantenimiento Local	18	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Sobrecalentamiento		2,00	3	3	Mantenimiento Local	18	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Pantallasos azules		2,00	3	3	Mantenimiento Local	18	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Reinicios Inesperados		2,00	3	3	Mantenimiento Local	18	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Corrupcion /Perdida de datos		2,00	3	3	Mantenimiento Local	18	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Aplicaciones que no responden	Terminales con 2 - 3 GB de RAM	2,00	2	3	Mantenimiento Local	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Bajo rendimiento		2,00	2	3	Mantenimiento Local	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Reinicios Inesperados		2,00	2	3	Mantenimiento Local	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Corrupcion /Perdida de datos		2,00	2	3	Mantenimiento Local	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Aplicaciones que no responden	Terminales con 4 GB de RAM	2,00	2	2	Mantenimiento Local	8	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Bajo rendimiento		2,00	2	2	Mantenimiento Local	8	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Conflicto de tareas	Terminales compartidas entre empleados	2,00	2	2	Cuentas de usuario	8	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Filtracion de datos		2,00	1	2	Cuentas de usuario	4	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO

			Desorganizacion de archivos e informacion		2,00	2	2	Cuentas de usuario	8	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Uso ineficiente del terminal		2,00	1	2	Cuentas de usuario	4	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Compra de teminales actualizados	1	1	2	BAJO
			Infeccion de malware	Conexión de dispositivos personales a terminales de la empreza	2,00	2	2	Registro de actividades del terminal	8	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Politicas de uso de los terminales	1	1	2	BAJO
			Robo de datos		2,00	2	2	Registro de actividades del terminal	8	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Politicas de uso de los terminales	1	1	2	BAJO
			Conflictos en la politica de seguridad		2,00	3	2	Registro de actividades del terminal	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Politicas de uso de los terminales	1	1	2	BAJO
			Accesos no autorizados	Contraseñas debiles para acceso al terminal	2,00	1	3	Politica de contraseñas	6	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Politicas de establecimiento uso y manejo de credenciales	1	1	2	BAJO
			Accesos no autorizados	Terminales sin contraseña	2,00	1	3	Sin control	6	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Politicas de establecimiento uso y manejo de credenciales	1	1	2	BAJO
			Accesos no autorizados	Terminales sin usuario	2,00	1	3	Sin control	6	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Politicas de establecimiento uso y manejo de credenciales	1	1	2	BAJO
			Hurto	Poco control fisico de los terminales y portailidad de los mismos	2,00	2	3	Sin control	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Politicas de manejo de los terminales	2	1	4	MEDIO

			Llevarse los terminales de forma no autorizada fuera de la empresa	Poco control fisico de los terminales y portailidad de los mismos	2,00	3	3	Sin control	18	ALTO	Mitigar/Evitar/Transferir	Preventivo	Compra de un generador para el edifico	2	1	4	MEDIO
			Perdida	Poco control fisico de los terminales y portailidad de los mismos	2,00	2	3	Sin control	12	ALTO	Mitigar/Evitar/Transferir	Preventivo	Politicas de manejo de los terminales	1	1	2	BAJO
			Daños fisicos	Golpes o caidas	2,00	2	3	Sin control	12	ALTO	Mitigar/Evitar/Transferir	Preventivo	Politicas de manejo de los terminales	2	1	4	MEDIO
E67	TALENTO HUMANO	Personal del Area de Sistemas	Falta de supervisión y mantenimiento de los sistemas y equipos, lo que puede llevar a fallos técnicos y aumentar la probabilidad de i ataques.	Falta de personal	2,00	2	3	Division de tareas entre los empleados	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Contratacion estimada de 6 empleados	1	1	2	BAJO

			Dificultad para responder a emergencias y resolver problemas técnicos de manera eficiente.		2,00	2	3	Division de tareas entre los empleados	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Contratacion estimada de 6 empleados	1	1	2	BAJO
			Problemas para llevar a cabo las tareas diarias y garantizar la disponibilidad y continuidad del servicio.		2,00	2	3	Division de tareas entre los empleados	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Contratacion estimada de 6 empleados	1	1	2	BAJO
			Gasto de tiempo en la capacitacion de nuevo personal por contrato que tiende a rotar cada ciclo a la alcaldia de Azogues		2,00	2	3	Division de tareas entre los empleados	12	ALTO	Mitigar/Evitar/Transferir	Correctivo	Contratacion estimada de 6 empleados	1	1	2	BAJO
			Carga de trabajo exesiva		2,00	3	3	Division de tareas entre los empleados	18	ALTO	Mitigar/Evitar/Transferir	Correctivo	Contratacion estimada de 6 empleados	1	1	2	BAJO
			Falta de documentacion	Personal unico e indispensable	2,33	2	3	Sin control	13,98	ALTO	Mitigar/Evitar/Transferir	Correctivo	Correcta documentacion de	1	1	2,33	BAJO

												los sistemas y su funcionamiento					
			Conocimiento tecnico especifico de la infraestructura de TI para el personal nuevo		2,33	2	3	Sin control	13,98	ALTO	Mitigar/Evitar/Transferir	Correctivo	Correcta documentacion de los sistemas y su funcionamiento	1	1	2,33	BAJO
			Falta de conocimiento frente a sistemas personalizados para el personal nuevo		2,33	3	3	Sin control	20,97	ALTO	Mitigar/Evitar/Transferir	Correctivo	Correcta documentacion de los sistemas y su funcionamiento	1	1	2,33	BAJO
			Ausencia de un plan de continuidad frente a la ausencia permanente del personal		2,33	3	3	Sin control	20,97	ALTO	Mitigar/Evitar/Transferir	Correctivo	Creacion de un Plan de continuidad para personal de ti	1	1	2,33	BAJO
E68		Funcionarios de la empresa no pertenecientes al area de Sistemas	Acceso no autorizado a traves de diversos metodos	Contraseñas debiles	1,67	3	2	Politica de formato de contraseñas	10,02	ALTO	Mitigar/Evitar/Transferir	Correctivo	Politica de credenciales	1	1	1,67	BAJO
			Olvidos/Contraseñas expuestas y accesos no autorizados	Mal manejo de las contraseñas de ingreso al terminal	1,67	2	2	Sin control	6,68	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Politica de credenciales	1	1	1,67	BAJO

				Desconocimiento de credenciales de ingreso a la terminal	1,67	1	2	Sin control	3,34	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Politica de credenciales	1	1	1,67	BAJO
				Mal manejo de las contraseñas de ingreso a la plataforma de trabajo	1,67	2	2	Sin control	6,68	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Politica de credenciales	1	1	1,67	BAJO
				Desconocimiento de credenciales de ingreso a la terminal	1,67	1	2	Sin control	3,34	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Politica de credenciales	1	1	1,67	BAJO
			Contraseñas expuestas/ Accesos no autorizados /Alteracion de la informacion	Conocimiento de terceros de la contraseña de ingreso al terminal	1,67	2	2	Sin control	6,68	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Politica de credenciales	1	1	1,67	BAJO
			Credenciales expuestas/ Accesos no autorizados /Alteracion de la informacion	Conocimiento de terceros de las credenciales personales para el ingreso a la plataforma de trabajo	1,67	2	2	Sin control	6,68	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Politica de credenciales	1	1	1,67	BAJO

			Accesos no autorizados /Alteracion de la informacion	Acceso a la terminal de trabajo por terceros en la empresa	1,67	2	2	Sin control	6,68	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Politica de credenciales y uso de teminales	1	1	1,67	BAJO
			Proteccion limitada del equipo frente a malware	Uso de terminales personales para laborar en el trabajo	1,67	3	3	Politica de no uso de dispositivos personales para laborar en la empresa	15,03	ALTO	Mitigar/Evitar/Transferir	Correctivo	Politica de uso de dispositivos personales en la empresa	1	1	1,67	BAJO
			Perdida de confidencialidad de la informacion		1,67	3	3	Politica de no uso de dispositivos personales para laborar en la empresa	15,03	ALTO	Mitigar/Evitar/Transferir	Correctivo	Politica de uso de dispositivos personales en la empresa	1	1	1,67	BAJO
			Problemas de compatiibilidad		1,67	2	3	Politica de no uso de dispositivos personales para laborar en la empresa	10,02	ALTO	Mitigar/Evitar/Transferir	Correctivo	Politica de uso de dispositivos personales en la empresa	1	1	1,67	BAJO
			Incumplimiento de normativas		1,67	3	3	Politica de no uso de dispositivos personales para laborar en la empresa	15,03	ALTO	Mitigar/Evitar/Transferir	Correctivo	Politica de uso de dispositivos personales en la empresa	1	1	1,67	BAJO
			Hurto	Horas extras en la empresa	1,67	1	3	Camaras / Registro de actividad de los terminales	5,01	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Controles a implementar de RRHH	1	1	1,67	BAJO
			Perdida de la confidencialidad de la informacion	Horas extras desde fuera de la empresa	1,67	2	2	Sin control	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Controles a implementar de RRHH	1	1	1,67	BAJO

			Proteccion limitada del equipo frente a malware	Horas extras desde fuera de la empresa	1,67	2	2	Sin control	6,68	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Controles a implementar de RRHH	1	1	1,67	BAJO
			Perdida de la integridad de la informacion debido a falta de imparcialidad y/o conflicto de intereses	Relaciones familiares en la empresa	1,67	1	2	Gestion de RRHH	3,34	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Controles a implementar de RRHH	1	1	1,67	BAJO
			Perdida de la integridad de la informacion debido a falta de imparcialidad y/o conflicto de intereses	Relaciones sentimentales/ afectivas en la empresa	1,67	1	2	Gestion de RRHH	3,34	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Controles a implementar de RRHH	1	1	1,67	BAJO
			Sabotajes/ Alteracion de la informacion	Ambiente laboral malo en la empresa	1,67	1	2	Gestion de RRHH	3,34	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Controles a implementar de RRHH	1	1	1,67	BAJO
			Sabotajes/ Alteracion de la informacion	Altercados entre empleados de la empresa	1,67	1	2	Gestion de RRHH	3,34	MEDIO	Mitigar/Evitar/Transferir	Correctivo	Controles a implementar de RRHH	1	1	1,67	BAJO

			Contaminacion de la red con malware	Uso de la red wifi de la empresa en dispositivos personales	1,67	1	1	Segmentacion de la red y firewall	1,67	BAJO	Aceptar	Preventivo	Segmentacion de la red	1	1	1,67	BAJO
			Accesos no autorizados /Alteracion de la informacion	Terminales activas por parte de los empleados al ausentarse por momentos(almuerzo,reunion,etc)	1,67	2	3	Politicas de uso de terminales	10,02	ALTO	Mitigar/Evitar/Transferir	Correctivo	Politicas de uso de terminales	1	1	1,67	BAJO
			Accesos no autorizados /Alteracion de la informacion	Terminales activas por parte de los empleados al finalizar con la jornada laboral	1,67	1	3	Politicas de uso de terminales	5,01	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Politicas de uso de terminales	1	1	1,67	BAJO
			Hurto/perdida de confidencialidad	Llevarse terminales de la empresa al hogar para realizar labores	1,67	2	3	Politicas de uso de terminales	10,02	ALTO	Mitigar/Evitar/Transferir	Correctivo	Politicas de uso de terminales	1	1	1,67	BAJO
			Pishing	Uso inadecuado del correo insitucional	1,67	1	3	Politicas de uso del correo	5,01	MEDIO	Mitigar/Evitar/Transferir	Preventivo	Politicas de uso del correo	1	1	1,67	BAJO
E69	Estructura Organi	Departamento de TI	Accionar a nivel de apoyo unicamente	Nivel incorrecto dentro del organigrama	1,00	3	3	Sin control	9	ALTO	Mitigar/Evitar/Transferir	Correctivo	Nivel de Asesoria	1	1	1	BAJO

	zacional		Reformas a planes operativos	Depende de la direccion administrativa	1,00	3	3	Sin control	9	ALTO	Mitigar/Evitar/Transferir	Correctivo	Creacion de la Direccion de TI	1	1	1	BAJO
			Cambios en la planeacion prevista	Depende de la direccion administrativa	1,00	3	3	Sin control	9	ALTO	Mitigar/Evitar/Transferir	Correctivo	Creacion de la Direccion de TI	1	1	1	BAJO
			Falta de autonomia, y operatividad	No cuenta con una estructura propia con sus propio departamentos y procesos	1,00	3	3	Division de tareas entre los empleados	9	ALTO	Mitigar/Evitar/Transferir	Correctivo	Creacion de una estructura interna con sus subdepartamentos y procesos	1	1	1	BAJO
			Falta de actualizacion y/o adquisicion de software y hardware	Excesiva burocratizacion para la adquisicion o renovacion de activos de TI	1,00	3	3	Solicitudes respectivas	9	ALTO	Mitigar/Evitar/Transferir	Correctivo	Simplificacion de la tramitacion necesaria para la adquisicion de activos de TI	1	1	1	BAJO

Francisco Javier Moncayo Ormaza portador de la cédula de ciudadanía Nº **0302894167**. En calidad de autor y titular de los derechos patrimoniales del trabajo de titulación **"Análisis De Vulnerabilidades Del Sistema De Información De La Empresa Pública EMAPAL"** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de éste trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Azogues, **27 de marzo de 2023**

Francisco Javier Moncayo Ormaza

C.I. 0302894167

José Miguel Izurieta López portador de la cédula de ciudadanía Nº **0301732723**. En calidad de autor y titular de los derechos patrimoniales del trabajo de titulación **"Análisis De Vulnerabilidades Del Sistema De Información De La Empresa Pública EMAPAL"** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de éste trabajo de titulación en elRepositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Azogues, **27 de marzo de 2023**

José Miguel Izurieta López

C.I. **0301732723**