DISEÑAR ESTRATEGIAS COMPLEMENTARIAS PARA MEJORAR LA SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN EN LA COMPAÑÍA QWERTY S.A. UTILIZANDO LA NORMA ISO 27001

JEFFERSON OSWALDO TRUJILLO ALVIRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
LA PLATA HUILA
2021

DISEÑAR ESTRATEGIAS COMPLEMENTARIAS PARA MEJORAR LA SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN EN LA COMPAÑÍA QWERY S.A. UTILIZANDO LA NORMA ISO 27001.

JEFFERSON OSWALDO TRUJILLO ALVIRA

PROYECTO APLICADO PRESENTADA(O) COMO REQUISITO PARCIAL PARA OPTAR AL TÍTULO DE:
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

DIRECTOR
CHRISTIAN REYNALDO ANGULO RIVERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
LA PLATA HUILA
2021

NOTA DE ACEPTACIÓN

JURADO 1

JURADO 2

La Plata Huila, 23 de diciembre de 2021

DEDICATORIA

A mi madre y hermana que me apoyan en cada decisión que tomo, me fortalecen para seguir adelante y obtener un logro más en mi proyecto de vida aportando cada día cosas que me fortalecen en el ámbito personal y profesional.

AGRADECIMIENTOS

A Dios por permitirme realizar una vez más lo que quiero gracias a las bendiciones y oportunidades que me ofrece, a mi familia por ser mi pilar y mayor motivación para superarme, a la Universidad que brindó una nueva ayuda para fortalecer mi profesión, además de todas las herramientas y conocimientos obtenidos en este proyecto aplicado, gracias a los tutores que siempre están dispuestos y atentos a colaborarme con dudas y aportes que afianzaron el desarrollo de mi trabajo.

RESUMEN

En el presente proyecto aplicado se realiza una auditoría a los sistemas de información de la entidad QWERTY S.A. se descubre que tienen un sistema de seguridad ya implementado, pero no cumple con los estándares de seguridad de la información. Para la implementación de los mecanismos de seguridad y configuración correcta de los distintos dispositivos de seguridad se utiliza la norma ISO 27001.

Como primer paso se crea un plan de ejecución donde se determina los tiempos de implementación de la auditoría y los documentos a generar. Se realiza el plan de seguridad donde se define los activos más importantes, la situación actual de la entidad, donde se da un breve reconocimiento a la organización, las personas responsables de la parte administrativa, oficina de sistemas y a que se dedica cada área. De igual manera, se crea el alcance del plan de ejecución que abarca toda la empresa.

Para la identificación de todos los activos y los riesgos, se emplea la metodología MAGERIT, la cual es compatible con la norma ISO 27001; de igual manera, da una guía para la valoración y calificación de las amenazas. Al momento de la valoración final se determina la importancia y alta ocurrencia de las amenazas, por ende, se implementa los controles que se encuentra en la metodología y son pertenecientes a la norma ISO 27002 y el objetivo es minimizar la ocurrencia de dichas vulnerabilidades en los sistemas de información.

Al determinar los controles se crea el plan de tratamiento de riesgos donde se determinan las acciones a realizar teniendo en cuenta los controles y los objetivos

de estos; así se minimiza la ocurrencia de las vulnerabilidades y asegurando los activos de la compañía.

Una vez implementado el plan de tratamiento y las políticas de seguridad se evalúan los distintos controles, esto con el objetivo de verificar si cumplen con los objetivos propuestos y aseguran correctamente los activos de información. Como primer paso se ejecuta de nuevo la metodología MAGERIT; para la verificación de los activos y los controles, esto para determinar si hay nuevas vulnerabilidades o se realizaron correctamente las configuraciones. Por último, se realiza una valoración de los controles para verificar si es óptimo, sino se debe realizar el cambio.

Palabras claves: Ataques, seguridad, equipos, reglas, firewall, sistemas, informática, información, riesgos, amenazas, vulnerabilidades, filtración de datos, ingeniería social, phishing.

ABSTRACT

In the present applied project, an audit of the information systems of the QWERTY S.A. entity is carried out. It is discovered that they have a security system already implemented, but it does not comply with the information security standards. For the implementation of the security mechanisms and correct configuration of the different security devices, the ISO 27001 standard is used.

As a first step, an execution plan is created where the audit implementation times and the documents to be generated are determined. The security plan defines the most important assets, the current situation of the entity, where a brief recognition of the organization is given, the people responsible for the administrative part and the systems office and what each area is dedicated to. In the same way, the scope of the execution plan that covers the whole company is created.

For the identification of all assets and risks, the MAGERIT methodology is used, which is compatible with the ISO 27001 standard; it also provides a guide for the valuation and qualification of threats. At the time of the final assessment, the importance and high occurrence of threats is determined, therefore, controls are implemented, which are found in the methodology and belong to the ISO 27002 standard and whose objective is to minimize the occurrence of such vulnerabilities in the information systems.

Once the controls are determined, the risk treatment plan is created, where the actions to be taken are determined, considering the controls and their objectives, thus minimizing the occurrence of vulnerabilities and securing the company's assets.

Once the treatment plan and the security policies have been implemented, the different controls are evaluated in order to verify if they comply with the proposed objectives and correctly secure the information assets. As a first step, the MAGERIT

methodology is run again to verify the assets and controls, to determine if there are new vulnerabilities or if the configurations were performed correctly. Finally, an assessment of the controls is performed to verify whether it is optimal or should be changed.

Keywords: Attacks, security, equipment, rules, firewall, systems, computing, information, risks, threats, vulnerabilities, data breach, social engineering, phishing.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

1. INTRODUCCIÓN

En el presente proyecto aplicado se va a realizar el diseño de estrategias complementarias para mejorar la seguridad informática y de la información en la compañía QWERY S.A. donde se utiliza la norma ISO 27000; se evita y bloquea los diferentes ataques que existen hoy en día. Se escoge este proyecto porque se pone en práctica los diferentes conocimientos que se han adquirido durante el desarrollo de la especialización.

Al revisar el esquema de seguridad se tienen resultados que afectan directamente los pilares de la información comprometiendo su disponibilidad, integridad y confidencialidad del activo más importante para una compañía. Como no se realiza la debida configuración de los mecanismos principales que protegen los sistemas de comunicación, son víctimas de diferentes ataques que buscan beneficios económicos.

Se toma como objetivo para el desarrollo de la actividad el diseño de estrategias para la empresa QWERTY S.A donde se presenta problemas de seguridad, robo y filtración de información; a través de la implementación de mecanismos que cumpla con los estándares según la norma ISO 27001. Se da solución a los diferentes inconvenientes encontrados en el escenario, mejorando los sistemas, además, implementado políticas donde se indique cuáles son los diferentes pasos que se deben seguir para contrarrestar los ataques a los sistemas. Se crea el plan de continuidad de negocio para que no haya interrupción en los servicios que presta la compañía. Para la identificación de los diferentes problemas y activos se realiza un tipo de investigación cuantitativa correlacional y se emplean mecanismos de recolección de información como lo son: encuestas y aplicación de checklist.

Algunos métodos que se deben tener en cuenta para la correcta interpretación del presente proyecto es conocer sobre qué es una política de seguridad, qué normas se deben aplicar para mantener seguros los diferentes activos de la compañía. También, tener conocimiento sobre el enfoque MAGERIT que se utiliza para la identificación de activos, responsables y amenazas, y realiza mediciones aritméticas para encontrar los riesgos. Estos procedimientos se pueden hallar en la norma ISO 27000 donde se detalla los diferentes parámetros que se deben tener en cuenta.

2. PLANTEAMIENTO DEL PROBLEMA

Al verificar los aspectos de la compañía y del departamento de sistemas en el escenario, se enfocan algunos inconvenientes y al momento de realizar los análisis correspondientes se verifica que son problemas de seguridad, y que pueden comprometer los activos informáticos, pero hay que proteger la integridad, disponibilidad y confidencialidad de la información, pues cuenta con firewall que no tiene configurado las diversas reglas que sirven para realizar un primer filtrado de peticiones de conexión e identificar las amenazas y bloquearlas.

Al no contar con sistemas de protección de acceso y privilegio en los usuarios con los que cuenta la compañía, se tienen inconvenientes de seguridad con los accesos no autorizados; esto puede tener repercusiones y ataques al pilar fundamentar de la seguridad.

Al verificar la conexión a la red inalámbrica de la compañía, se encuentra que tanto directivos como visitantes se conectan directamente a un solo SSID, esto es un inconveniente puesto que se presentan ataques desde la red interna, además, interceptación de datos al momento de realizar el envío de alguna información confidencial.

Se debe asegurar que los servidores cumplan con las normas y reglas de protección de información, además, de cumplir con la certificación TIA 942 que indica los aspectos que se deben tener en cuenta para identificar el lugar donde se debe configurar e implementar el Centro de Datos, puesto que debe ser confiable a nivel de control de acceso y resistir los contratiempos o desastres naturales.

Al no contar con un agente de antivirus se tiene el inconveniente de no saber si las actualizaciones son completas y confiables. Se presentan serios problemas de seguridad que pueden comprometer los activos informáticos de la compañía, se deben implementar medidas. ¿Cómo un sistema de gestión de seguridad de la información, a partir del estándar ISO 27001 puede mitigar los problemas que se pueden presentar en cuanto a seguridad, robo y filtración de información en la empresa QWERTY S.A.?

3. JUSTIFICACIÓN

La necesidad de implementar estrategias de seguridad en una compañía es para asegurar la información, el activo más importante. En el mercado existe diversos equipos que pueden complementar los sistemas de seguridad sin inconvenientes, su principal objetivo son la protección de los activos. Toda empresa se debe preocupar por implementar mecanismos que ayuden a mantener seguros tanto los equipos como los usuarios de la organización.

Se necesita realizar un alcance del proyecto y cuáles son las necesidades halladas, esto para implementar los sistemas correctos y se solucione los problemas encontrados. En el proyecto aplicado escenario 2, presenta una compañía que cuenta con un sistema de seguridad implementado, pero no cumple con los estándares de seguridad. No se han realizado las revisiones ni las auditorias pertinentes, esto para evitar distintos problemas a futuro y que se ponga en evidencia las dificultades para dar solución efectiva y minimizar las amenazas. De igual manera, disponen de un sistema de servidores que no cuentan con equipos de climatización optimas; sufriendo posibles tipos de calentamiento que entorpece el rendimiento, incumpliendo con los aspectos de disponibilidad de los servicios.

Se implementan mecanismos de seguridad que cumplan con los estándares de la norma ISO 27001 como se solicita en el escenario, esto para determinar lo que se debe mejorar y realizar las respectivas correcciones a los problemas identificados. Se realizan políticas de seguridad para complementar los mecanismos y evidenciar el correcto funcionamiento de los controles, minimizando la ocurrencia de los riesgos y asegurando los activos encontrados y catalogados como importantes. Capacitar al personal sobre las implementaciones y dar solución a los riesgos es blindar los activos de la ciberdelincuencia.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Diseñar estrategias para la empresa QWERTY S.A la cual presenta problemas de seguridad, robo y filtración de información, a través de la implementación de mecanismos que cumplan con los estándares según la norma ISO 27001

4.2 OBJETIVOS ESPECÍFICOS

- Planificar la implementación del sistema de gestión basado en la norma ISO 27001 para la correcta ejecución de la auditoría de sistemas.

- Identificar los activos y analizar las diferentes amenazas y riesgos de la empresa mediante la metodología MAGERIT.

- Realizar el plan de tratamiento de los riesgos detectados en la entidad, implementando las estrategias y mecanismos seleccionados para mitigar los riesgos y las amenazas.

- Analizar y evaluar los mecanismos para la verificación de su correcto funcionamiento y que cumpla con los objetivos propuestos.

5. MARCO TEÓRICO

Antecedentes:

Hoy en día, la información es considerada para muchas entidades como el activo más importante, protegerla se ha convertido en un reto, debido a que existen muchos métodos para sustraerla sin autorización por intrusos. Para asegurar los distintos activos de la información se debe tener en cuenta el termino seguridad informática. La Universidad Internacional de Valencia define así la seguridad informática: “como el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de los recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente. La seguridad informática es en realidad una rama de un término más genérico que es la seguridad de la información, aunque en la práctica se suelen utilizar de forma indistinta ambos términos”[1].

Al reconocer qué embarca la seguridad informática se considera importante determinar si aplica a empresas tanto del sector público como privado, además, es conveniente verificar lo importante que es la implementación. Rosa María Zambrano Burbano en su monografía identifica si es posible la implementación en un hospital: “frente a las vulnerabilidades existentes propusieron desarrollar metodologías que permitieran asegurar los activos de información del hospital San Antonio de Puente Nacional. Así mismo, plantearon diseñar políticas de seguridad de la información que estén de acuerdo con los lineamientos del gobierno en línea y así mantener la integridad, confiabilidad y disponibilidad de los activos de información del hospital.”[2],

[1] Equipos expertos, ¿Qué es la seguridad informática y como puede ayudarme?, Universidad Valencia

[2] Zambrano R. M, Estudio sobre el conocimiento y la aplicabilidad de la seguridad informática en las empresas médicas de Bogotá, 2016, P. 30

Se determina que se puede realizar en diferentes compañías, se identifica que tan importante es la implementación en las empresas, pymes, medias y grandes. Se deben crear manuales para realizar un paso a paso y cómo se debe efectuar, cómo se verifica con Julián Barreto en su monografía “Manual de seguridad informática para Pymes”, se identifica lo siguiente: “De acuerdo con el auge y la necesidad primordial del uso de equipos de comunicación de red de datos, para la comunicación de servicios como: videos, correos, imágenes, documentos y demás servicios de red que deba tener una empresa para el esquema de productividad diaria. Se hace necesario el diagnóstico e implementación de controles que permitan la conexión y buena administración de dichos equipos, con el fin de detectar y evitar inseguridades y posibles accesos por empleados de la misma empresa o usuarios externos con vínculos de visitantes, de acuerdo con el análisis propuesto, es necesario evaluar como primera medida los recursos más relevantes de la compañía y así evaluar el impacto que tendrán o el riesgo a que están expuestos”.[3]

Al momento de verificar los inconvenientes que se presentan en una empresa en cuanto a temas de seguridad se deben implementar los mecanismos bajo normas para que sean más confiables. Como lo informa Julio Cesar Alcántara en su tesis, “La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información”[4], se demuestra lo importante que es para la norma Internacional ISO 27001 para la gestión de las vulnerabilidades.

[3] BARRETO J. Diseño de manual de diagnóstico y prevención de vulnerabilidades en redes de datos para pymes, 2018, P 30

[4] ALCÁNTARA J. Guía de implementación de la seguridad basado en la Norma iso/iec 27001, para apoyar la seguridad en los Sistemas informáticos de la comisaria del norte P.N.P En la ciudad de Chiclayo, 2015. P 19.

La norma ISO 27001:2013 es un estándar internacional que brinda las herramientas y guías para minimizar la ocurrencia de los riesgos de seguridad; Julio Cesar Nacipucha define lo siguiente: “La norma ISO/IEC 27001:2013, es un estándar internacional que gestiona el tratamiento de la seguridad de la información de una empresa u organización, fueron desarrolladas por la International Organization for Standartization (ISO) e International Electrotechnical Commission (IEC). Determinan los requerimientos que deben cumplir las organizaciones privadas, públicas pequeñas o grandes, para mejorar continuamente la seguridad física y lógica de la información”[5]. Se debe gestionar correctamente los procesos de verificación para obtener resultados que puedan cumplir con los objetivos propuestos. Para Jesús Armando Coral en su tesis define “La familia ISO/IEC 27000 son estándares de seguridad de la información, provee estándares y guías sobre buenas prácticas en sistemas de gestión de seguridad de la información, generalmente aceptadas”[6]. Para la entidad QUERTY S.A. se van a ejecutar los estándares y las guías propuestas por la norma ISO para mitigar las vulnerabilidades y asegurar correctamente los activos de información.

Bases teóricas:

“La seguridad de la información es el conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger la integridad, confidencialidad y disponibilidad de la información.”[7] Dan una breve definición de lo que es seguridad informática, pero como se puede implementar a una empresa que busca mejorar sistemas de seguridad, para esto se debe considerar cuales son los activos más importantes.

[5] NACIPUCHA J. Análisis y diseño para un modelo de gestión de seguridad de la información basados en normas ISO/IEC 27001:2013 para la empresa artehogar en la ciudad de guayaquil, 2019. P 35

[6] CORAL J. Diseño de un sistema de gestión de seguridad para la red datos bajo la norma iso27001:2013 en el centro de Estudios Emssanar Cetem de la ciudad de Pasto, 2016. P 36

[7] ESCRIVA G. Seguridad Informática, 2013. P. 7

Para el sector público es muy importante asegurar la información de los delitos informáticos. En el siguiente artículo, el autor quiere informar acerca de la seguridad de la información para las entidades gubernamentales de Colombia “La información del sector público por estar ligada a la Nación y a la ciudadanía, se convierte en un bien público que debe ser protegido. A esta información se le debe conservar su confidencialidad, integridad y disponibilidad. La información pública atañe a la Nación y la ciudadanía, por lo tanto, se ve expuesta a cualquier amenaza que represente un manejo antijurídico que puede afectar sus propiedades.”[8] Es importante generar confianza en la ciudadanía que los datos de información van a estar protegidos y que los servicios de seguridad cumplen los estándares de seguridad. Para cualquier entidad tanto pública como privada, debe invertir los suficientes recursos para cumplir con las normas nacionales e internacionales de seguridad, además, de asegurar los activos que son considerados como importantes.

Al verificar el activo en la compañía se implementan medidas que aseguren, además, mantengan este activo en condiciones óptimas que cumpla con los requerimientos del pilar de la información. En la siguiente cita se pueden verificar lo que es y significa un activo como información “Uno de los activos más valiosos para cualquier empresa es la información que maneja. La información es el conjunto de datos que da sentido a una empresa, datos que la definen, datos con los que trabaja y datos que, en manos inadecuadas, pueden llevar a la misma a la ruina. Extendiendo este concepto de seguridad al mundo de las telecomunicaciones y la informática, puede entenderse desde dos puntos de vista: seguridad de la información y seguridad informática”[9].

[8] CAMPOS, J. Seguridad de la información en el sector público colombiano. P. 2
[9] ESCRIVA G. Seguridad Informática, 2013. P.20

Se comprende lo importante que es la implementación de la seguridad para mantener seguro el activo, pero se deben considerar los diferentes ataques que existen a la seguridad informática y que es perjudicial para cualquier compañía que no cuente con un sistema de seguridad, se debe saber cómo es un ataque y que fases comprende, para Álvaro Gómez Vieites, "los ataques contra redes de ordenadores y sistemas informáticos suelen constar de las etapas o fases que se presentan a continuación:

- Descubrimiento y exploración del sistema informático.
- Búsqueda de vulnerabilidades en el sistema.
- Explotación de las vulnerabilidades detectadas (para ello, se suelen utilizar herramientas específicamente construidas para tal fin, conocidas como exploits).

Corrupción o compromiso del sistema: modificación de programas y ficheros del sistema para dejar instaladas determinadas puertas traseras o troyanos; creación de nuevas cuentas con privilegios administrativos que faciliten el posterior acceso del atacante al sistema afectado; etcétera." [10].

Hay distintos métodos que se pueden utilizar y que son compatibles con la norma ISO 27001. Ayudan a identificar los activos que son vulnerables, y que tan probable es la ocurrencia de un ataque a la seguridad, utilizan distintos métodos, que aprovechan la fragilidad de los mecanismos de seguridad; para el proyecto y la identificación de dichas vulnerabilidades, inventario de los activos e implementación de controles de seguridad se maneja el método MAGERIT que el Gobierno de la comisión estratégica TIC de España crea y promueve como "respuesta a la percepción de que la Administración Pública (y en general toda la sociedad) depende de forma creciente de los sistemas de información para alcanzar los

[10] VIEITES A. Seguridad en equipos informáticos, 2014. P 41

objetivos. El uso de tecnologías de la información y comunicaciones (TIC) supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben gestionarse prudentemente con medidas de seguridad que sustenten la confianza de los usuarios de los servicios."[11]

Al identificar los diferentes tipos de ataques, se implementan los mecanismos para realizar un sistema de seguridad basado en las normas ISO 27000, "Un Sistema de Gestión de Seguridad de la Información (SGSI), según la Norma UNE-ISO/IEC 27001, es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. Esto significa que se va a dejar de operar de una manera intuitiva y se va a empezar a tomar el control sobre lo que sucede en los sistemas de información y sobre la propia información que se maneja en la organización. Permitirá conocer mejor la organización, cómo funciona y qué se puede hacer para que la situación mejore"[12]. Luis Gómez Fernández y Ana Andrés Álvarez muestran porqué es tan importante la implementación de este mecanismo.

Para toda entidad es importante la implementación de un plan de continuidad del negocio que garantice la continuidad de los servicios si ocurre una amenaza tanto interna como externa. Para la Escuela Superior de Administración Pública en su plan de continuidad del negocio expresa la siguiente necesidad: "El incremento de las amenazas externas e internas ha llevado a las entidades públicas y privadas a considerar la importancia de la implementación de planes, procedimientos, y estructuras que garanticen la continuidad de sus productos y servicios críticos del negocio ante eventualidades de diversas categorías y diferentes niveles de impacto.

[11] Dirección General de administración, 2012, versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, P. 6

[12] Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para Pymes, 2012 P. 13

Estos factores, han llevado a que en la actualidad la presencia de estos planes sean un factor común a lo largo de la cadena de suministro de los productos y servicios”[13]. Es indispensable que se implemente el plan de continuidad del negocio para la entidad QWERTY S.A. para que no se vea afectado los servicios que ofrecen.

[13] Escuela superior de administración pública, 2018, Plan de continuidad del negocio BCP, P. 4

6. MARCO CONCEPTUAL

En el presente proyecto aplicado se van a manejar términos que son de gran importancia para la interpretación del trabajo. Se definen a continuación.

Activo de información: Información, datos y sistemas de una entidad que pueden ser susceptibles a ataques por parte de los ciberdelincuentes.

Análisis de riesgos: Es el proceso por el cual se realiza la identificación de los riesgos y amenazas a los cuales están expuestos los activos de información de una entidad, para iniciar con el proceso de valoración e implementación de controles.

Asignación de privilegios: Es la asignación de permisos a los perfiles de usuario, teniendo en cuenta los roles y áreas en los que se desempeñan las personas o empleados de la entidad.

Auditoria de sistemas de seguridad: Es el proceso por el cual se realiza el análisis de los sistemas de seguridad de una organización con el objetivo de identificar vulnerabilidades; se realizan informes y procesos de gestión de las amenazas.

Centro de datos de información: Es un espacio donde se almacenan y procesan todos los datos de información de una entidad, además, del almacenamiento de los sistemas de seguridad y equipos de telecomunicaciones.

Control de acceso a la red: Son protocolos de seguridad que se encargan de implementar las políticas de seguridad de la entidad a equipos antes que se conecten a la red corporativa.

Gestión de la seguridad de la información: Son políticas que se implementan para gestionar efectivamente la confidencialidad, integridad y disponibilidad de los activos de información de una entidad.

Implementación de mecanismos complementarios: Se define como la instalación y aplicación de procesos para complementar o perfeccionar un sistema de seguridad.

Plan continuidad del negocio: Son contingencias establecidas para mantener los servicios activos de una entidad en caso de que suceda una emergencia tanto interna como externamente.

Protección de datos de información: Sistemas de seguridad que se encarga de asegurar la información y activos de una entidad.

Sistema de detención de intrusos o sus siglas en inglés (IDS): Son sistemas de seguridad que se encargan de vigilar y encontrar diferentes anomalías dentro de las infraestructuras de telecomunicaciones, con el objetivo de bloquear e informar de los intrusos.

Sistema de gestión de seguridad de la información: Son un conjunto de políticas y normas que se encargan de administrar y gestionar la confidencialidad, integridad y

disponibilidad de la información donde se asegura la confidencialidad, integridad y disponibilidad en una entidad, para implementar entandares de seguridad.

Suplantación de identidad: Es un delito informático, donde se suplanta la identidad de otra persona para obtener privilegios y accesos de información para fines delictivos.

Ya definidos los diferentes términos que se van a manejar en el proyecto aplicado, se escogen los diferentes aportes que se van a tener en cuenta para el desarrollo y cumplimiento de los objetivos mencionados; se van a tener en cuenta todos los aportes y referencias que se manejan en el marco teórico puesto que cumplen con las diferentes características que se necesitan para la realización del proyecto, además, que se toma como base para la realización y desarrollo de la actividad.

7. MARCO LEGAL

Ley 1273 de 5 enero del 2009: Ley Colombiana de delitos informáticos y la protección de la información y de los sistemas de las tecnologías y telecomunicaciones.

Ley 1581 de 2012: Ley Colombiana donde se especifica las disposiciones en general para la protección de los datos personales.

Ley 527 de 1999: Ley Colombiana donde se reglamenta el acceso y el uso referente a las firmas digitales y el comercio de mensajes de correo electrónico.

Decreto 1008 de 2018: En su artículo 2.2.9.1.1.3 define la seguridad informática como un principio de todas las políticas del gobierno digital.

CONPES 3701 de 2011 (lineamientos de política para ciberseguridad y ciberdefensa): Se generan políticas de ciberseguridad y ciberdefensa con el objetivo de contrarrestar las amenazas a la seguridad de la información que afectan al País.

CONPES 3854 de 2016 (política nacional de seguridad digital): Se especifican las políticas para la seguridad nacional digital de la información en las distintas organizaciones públicas.

CONPES 3995 de 2020 (Política Nacional De Confianza y Seguridad Digital): Se crean políticas donde se busca incrementar la confianza en la era digital tanto en sectores públicos como privados. Se desea cumplir con el objetivo incrementando la capacidad de la seguridad digital en personas, empresas públicas y privadas.

Norma ISO 27001:2013: Norma Internacional que da marcos para la implementación de un SGSI (sistema de gestión de la seguridad informática), buscando la confidencialidad, disponibilidad e integridad de los activos de información.

8. MARCO METODOLÓGICO

Al verificar el problema planteado en el escenario, se evidencia que la empresa tiene inconvenientes de seguridad, los equipos con los que cuenta no están configurados ni respaldados correctamente. Se debe implementar un sistema de auditoría según la norma ISO 27001 para la recolección de información, que permita tener un informe detallado sobre los diferentes inconvenientes presentados, con el objetivo de evitar pérdida de la información e indisponibilidad de los equipos tecnológicos.

Al implementar el esquema se debe dar enfoques y capacitaciones sobre el buen uso de los sistemas de información, esto para aprovechar al máximo los recursos informáticos. Antes de realizar la auditoría a los sistemas de la compañía se debe realizar una identificación de los activos para los respectivos análisis.

Se emplearán técnicas y herramientas para la solución del problema planteado, pero teniendo en cuenta los objetivos como eje principal. Como primer paso se identifican los activos, amenazas y vulnerabilidades, para esto, se debe realizar recolección de información preliminar al respecto. Al obtener está información y la identificación del problema real, se debe buscar alternativas de solución, se utilizarán lluvias de ideas para adoptar la que mejor se ajuste a lo requerido. Al momento de haber elegido la idea que más se adapte, se deben realizar diseños preliminares, se utilizan programas al respecto; además de uso del flujograma para describir cada proceso.

Antes de poner en funcionamiento la solución planteada, se debe realizar análisis y evaluaciones a los diferentes aspectos de los controles, esto para evitar inconvenientes futuros; para estos análisis y evaluaciones se utilizarán checklist

donde se identifiquen los procesos y estados críticos que se deben tener en cuenta; es indispensable contar con un sistema de valoración para saber si cumple o no con los requisitos de solución.

Para la recolección de información y análisis de los datos se utiliza la metodología cuantitativa correlacional, debido a que permite evaluar la relación de dos o más variables, con el objetivo de identificar el nivel de cumplimiento en cuanto a seguridad de la información. Se evalúa con la metodología los activos, amenazas, vulnerabilidades y los controles que se encuentren ya implementados.

Al obtener los resultados se debe diseñar un plan de mejora con la implementación de controles y políticas donde se evidencie la minimización de la ocurrencia de los riesgos y solución al problema de seguridad que se encuentra en la organización.

9. MARCO ESPACIAL

QWERTY S.A. es una empresa del sector tecnológico que busca el desarrollo tecnológico en comunidades colombianas a través del uso de Tecnologías de Información. Actualmente, cuenta con 120 colaboradores entre directivos, administrativos y operativos, quienes hacen uso de forma regular de los medios de información para consulta de datos.

10. DESARROLLO DE LA INVESTIGACIÓN

10.1. OBJETIVO 1 – PLANIFICACIÓN DE LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN

10.1.1. PLANIFICACIÓN

Para la implementación SGSI se tendrá en cuenta la norma ISO 27001, donde se dan a conocer los diferentes pasos que se deben seguir para la ejecución de un sistema de seguridad, enfocado al mejoramiento continuo de los procesos, además, de la implementación de mecanismos que buscan dar solución a los problemas ya expuestos y sobre todo que atentan contra los pilares de la información, que son la integridad, disponibilidad y confidencialidad.

10.1.1.1. Plan de implementación

El plan de implementación está proyectado para una duración de 12 meses y se ejecuta en el plazo estimado, se tendrá en cuenta los ítems y periodos de ejecución de cada uno, teniendo como referencia esto, se realiza el plan de implementación y los periodos de ejecución.

Tabla 1 Plan de implementación.

Ítem	Periodo de ejecución
Creación del plan de trabajo.	Mes 1.
Definición del alcance.	Mes 1.
Definición de las Políticas de seguridad.	Mes 2.
Identificación de los activos de información de la compañía.	Mes 2.
Definición del enfoque y análisis de los riesgos.	Mes 3.

Tabla 1 Continuación

Análisis de riesgos.	**Mes 3.**
Tratamiento de los riesgos.	Mes 4.
Selección de los controles a implementar.	Mes 4.
Gestión de los riesgos identificados.	Mes 5.
Aprobación y gestión de los recursos.	Mes 6.
Plan de tratamiento de los diferentes riesgos identificados.	Mes 6.
Definición y delimitación de los objetivos.	Mes 7.
Asignación de responsabilidades a personal Recursos informáticos.	Mes 8.
Capacitación personal de oficina de sistemas.	Mes 9.
Implementación y puesta en marcha del plan.	Mes 10.
Evaluación de los sistemas implementados	Mes 11.
Entrega informe final.	Mes 12.

Fuente: autor

Se crea el cronograma para la ejecución de la auditoría teniendo en cuenta el plan de implementación detallando las acciones a realizar por semanas; el cronograma se puede visualizar en el ***ANEXO A.***

Para la implementación de la auditoría se crea un documento para la gerencia donde se indica los distintos procedimientos a realizar y de igual forma, los documentos, formatos y matrices a ejecutar durante el desarrollo de la auditoría a la seguridad, dicho documento se puede encontrar en el ***ANEXO I.***

10.1.1.2. Documentos generados

Al realizar el plan de implementación de los mecanismos, se define los documentos que se generan durante el desarrollo de los ítems ya especificados y seleccionados.

Tabla 2 Títulos Generados

Ítem	Documentos
Creación del plan de trabajo.	Plan de trabajo.
Definición de las Políticas de seguridad.	Políticas de seguridad.
Análisis de riesgos.	Análisis de los riesgos.
Tratamiento de los riesgos.	Tratamiento de los riesgos.
Capacitación personal.	Registro de asistencias.
Entrega informe final	Informe de implementación.

Fuente: Autor

Además, se entregan también documentos que se deben implementar antes, durante y después de cada ataque, como lo son listas de chequeo, instrucciones, formularios, procedimientos y mecanismos de control. Estos documentos son de suma importancia en la gestión de incidentes de seguridad.

10.1.2. PLAN DE SEGURIDAD

10.1.2.1. Descripción de la empresa

La empresa sobre la cual se va a implementar los mecanismos y mejoramiento de los sistemas de seguridad será denominada QWERTY, es del sector tecnológico que busca el desarrollo en comunidades colombianas a través del uso de Tecnologías de Información, su principal objetivo es llegar a todas aquellas comunidades que no tienen acceso a las tecnologías.

Actualmente, cuenta con 120 colaboradores entre directivos, administrativos y operativos, quienes hacen uso de forma regular de los medios de información para consulta de datos.

10.1.2.2. Objetivos

Los principales motivos por los que se ha decidido realizar la implementación de estrategias de seguridad complementarias, utilizando la norma ISO 27001 se puede definir de la siguiente manera.

- Contar con sistemas de respaldo o backup tanto de la información como de los diferentes aplicativos con los que cuenta la compañía.

- Contar con un canal seguro de comunicación entre las diferentes áreas de la empresa y con personas externas.

- Implementar un sistema de detención de intrusos, además, de un firewall de base de datos y bloqueo de ataques.

- Contar con un plan de continuidad de negocio por si ocurre algún tipo de incidente.

- Implementación de agentes de antivirus que monitoreen y actualicen los equipos de cómputo.

- Implementar perfiles de acceso a la información, teniendo en cuenta, el cargo en la empresa y la información que debe manejar.

- Configurar correctamente los puntos de acceso inalámbrico para directivos, administrativos, estudiantes y puntos de acceso libre.

10.1.2.3. Situación empresa QWERTY S.A.

❖ Organización empresa QWERTY S.A.

La compañía QWERTY S.A. cuenta con 120 colaboradores entre directivos, administrativos y operativos, se describe a continuación.

- **Directivo:** El gerente de la compañía es quien hace parte de este departamento y el responsable de la actuación de las áreas.

- **Administrativos:** Son los encargados de la gestión administrativa y además, de la contabilidad y almacenamiento de información de las bases de datos.

- **Operativos:** Encargados de la gestión de los proyectos y desarrollo del mismos.

- **Sistemas:** Son los encargados de la administración y soporte de los recursos TIC, se dividen en tres dependencias las cuales son: infraestructura, se encarga del soporte en las áreas de telecomunicaciones; área de desarrollo se encarga del desarrollo y soporte de aplicaciones para que los administrativos y operativos ejecuten sus tareas, además, del mantenimiento de las bases de datos; el área de soporte que se encarga del mantenimiento de los equipos informáticos y respaldo de información en equipos y discos locales.

  Los directivos, administradores y operativos se encargan de gestionar toda la información de forma interna, hace referencia a que alimentan las bases de datos, implementan pagos de nómina y administración desde la empresa, cuando realizan las visitas a los sectores en donde se va a implementar las tecnologías, llenan formularios en los equipos asignados al personal para que después diligencien la información en los respectivos aplicativos que trabajan en la intranet de la compañía.

El departamento de sistemas es el responsable de los sistemas tecnológicos, se encargan de realizar las copias de seguridad de información, son responsables de prestar el soporte a los aplicativos y bases de datos de la compañía, además, del soporte a los equipos y los sistemas de comunicación y telecomunicaciones.

10.1.2.4. Equipos tecnológicos de la empresa.

Para la identificación de los equipos tecnológicos con los que cuenta la empresa, se divide en sectores para saber qué área es responsable por el manejo de cada activo.

- Directivos, administrativos y operativos, se comunican entre ellos por un solo segmento de red y son los responsables del manejo de información, de alimentar los aplicativos y bases de datos, además cada uno cuenta con un equipo de cómputo, se conectan a un servidor de almacenamiento FTP y de servicio de impresiones, además, de los servidores de almacenamiento de base de datos.

- Sistemas, es el área más importante puesto que desde allí se monitorea los servicios que se han implementado en la compañía, además, son los encargados de dar soporte a los servicios con los que cuenta la entidad y la administración de los sistemas de seguridad y equipos de comunicación, tanto, a internet como a intranet.

La infraestructura tecnológica de la compañía está compuesta por:

- Equipos de cómputo, tanto portátiles como de escritorio, que cuentan con sistemas operativos Windows.

- HUB, que se encarga de la conexión de los equipos de cómputo a la red corporativa.

- Un equipo firewall que se encarga de monitorear y bloquear las conexiones no autorizadas desde internet.

- Un servidor de impresiones, que administra dos impresoras, una con función de impresión y la otra con función de escaneo.

- Servidor de archivos FTP, que se encarga del almacenamiento de información y que es compartida a todos los trabajadores internos de la compañía.

- Servidor de aplicaciones internas, sistema de facturación y nómina, se encarga de almacenar las bases de datos de la compañía.

- Servidor DHCP, servidor que se encarga de administrar el direccionamiento IP dinámico en la compañía.

- Switch, encargado de la conexión de las redes de comunicación en la compañía.

- Teléfonos IP, telefonía IP encargada de comunicar al personal de la compañía.

10.1.2.5. Alcance del plan de seguridad

Una vez identificados los objetivos de la implementación de las estrategias y conocer la organización, la responsabilidad y la infraestructura de la compañía y el personal que está directamente relacionado con ello, se determina que el plan de seguridad será implementado a los procesos y áreas del departamento de sistemas, puesto que prestan el soporte a las áreas de la compañía y además, son

directamente responsables del funcionamiento de los equipos que conforman la infraestructura de QWERTY S.A.

También están incluidos dentro de la implementación todos los equipos y la infraestructura que conforma la red de comunicación, además, de la implementación de un dispositivo IPS y la correcta configuración del firewall con las reglas, puesto que filtra las conexiones tanto internas como externas, se incluyen los servidores que existen y el personal que maneja los departamentos para la correcta capacitación donde se informa sobre el buen uso de los recursos informáticos.

Para asegurar la información de las bases de datos, además, de las aplicaciones que maneja la entidad se implementará un firewall WAF, el cual se encarga de filtrar las diferentes conexiones y peticiones que se realizan a los aplicativos.

Es importante implementar los mecanismos de seguridad seleccionados para cada riesgo que se encuentra en la entidad, para disminuir su ocurrencia y evitar incidentes de seguridad que pueda poner en peligro la información y los activos que son catalogados de suma importancia.

10.1.3. DEFINICIÓN DE LAS POLÍTICAS DE SEGURIDAD

Se deben definir las políticas de seguridad donde se especifican los distintos criterios que se siguen para garantizar la disponibilidad, integridad y confidencialidad de la información. Son normas y procedimientos que se deben implementar para cumplir con los criterios de seguridad, toda persona que sea empleado en la empresa debe conocer, cumplir y aceptar las políticas.

Estás políticas se realizan teniendo como eje fundamental la norma ISO 27001, la cual se va a implementar en la empresa QWERTY S.A.

10.1.3.1. Objetivos

Los objetivos que QWERTY S.A. ha tenido en cuenta para la implementación de las estrategias son:

- Asegurar toda la información que se maneja en la compañía QWERTY S.A, puesto que es catalogada como de alta importancia.

- Crear cronogramas de capacitaciones a todo el personal de la entidad sobre seguridad informática y lo importante que es prevenir y conocer los ataques que se puedan presentar; además, de los procesos que se deben ejecutar al momento que se presente una incidencia.

- Definir los procesos de gestión de incidentes, en caso de que se presenten inconvenientes de seguridad.

- Definir las responsabilidades del personal que labora en la empresa, teniendo el marco de seguridad empresarial como respaldo.

- Establecer en las políticas de seguridad los mecanismos legales que tomará la empresa en caso de que se infrinjan las normas descritas en el plan de políticas de seguridad.

10.1.3.2. Alcance

La implementación de las políticas de seguridad afecta a todos los sectores de la empresa, puesto que son normas que se crean para proteger los recursos TIC, desde el personal que labora en la empresa como los sistemas y recursos tecnológicos, además, de los distintos aplicativos y páginas de la compañía.

10.1.3.3. Políticas de seguridad.

Hace referencia a las directrices que seguirá la entidad para cumplir con los sistemas de protección y seguridad, ya seleccionados para la organización.

10.1.3.4. Aprobaciones políticas de seguridad.

El documento de políticas tiene que ser presentado a las directrices de la compañía para su análisis y posterior aprobación, luego será socializado con los sectores y personas que hacen parte de la compañía para su estricto cumplimiento.

Se deben realizar estudios periódicos y de más adecuaciones si son pertinentes, estas mejoras deben ser aprobados por las directrices y posteriormente socializar los cambios realizados.

10.1.3.5. Organización

- Se deben definir cada una de las responsabilidades de la seguridad de la información una vez implementada.

- Definir e implementar el debido proceso que se debe realizar para la autorización cuando se realice la gestión de nuevos recursos o activos de información.

- Definir los contactos y enlaces en cuanto a continuidad de plan de negocio.

- Revisar uno a uno los controles de seguridad de la información.

10.1.3.6. Gestión de activos

- Toda la información que se maneja en la compañía debe ser clasificada teniendo en cuenta su valor, importancia y criticidad para la compañía.

- Crear procedimientos que puedan tratar la información ya clasificada y que es importante para la compañía.

- Implementar sistemas que garanticen siempre la disponibilidad, integridad y confidencialidad de dicha información.

10.1.3.7. Recursos humanos

- Se debe dictar la capacitación adecuada a las personas que hacen parte de la compañía para que tengan conocimiento sobre las políticas de seguridad.

- Se debe dar cumplimiento a los procesos disciplinarios para aquel empleado que haya incumplido con las normativas y que haya provocado problemas a la seguridad de los recursos informáticos.

10.1.3.8. Seguridad física.

- Implementar sistemas de seguridad perimetrales para proteger los sistemas de intrusos y accesos no autorizados.

- Se deben implementar sistemas de acceso biométrico a áreas críticas de la organización.

- Diseñar e implementar el plan de continuidad de negocio, para esto se utilizará la norma ISO 22301.

- Proteger los equipos de comunicación de amenazas y accesos no autorizados, además, de interrupción de servicios.

- Implementar sistemas para llevar un control sobre la copia de información sin previa autorización en dispositivos USB.

- Implementar medidas de seguridad para aquellos equipos que se utilizan por fuera de la entidad.

10.1.3.9. Control de acceso

- Implementación de sistemas de directorio activo para tener control de acceso a los equipos y manejos de información, además, para revocar permisos.

- Implementar políticas para limitar los tiempos de conexión a las aplicaciones y sistemas críticos que se hayan detectado.

- Los sistemas considerados críticos o centro de datos deben estar aislados y en un sitio donde se limite el acceso a personal no autorizado, además, se debe llevar un registro de aquellas personas que ingresan e implementación de un sistema de acceso biométrico al área.

10.1.3.10. Gestión de incidentes

- Los eventos que se presenten y que atenten contra la seguridad, deben ser reportados al área designada lo ~~más~~ antes posible.

- Todo el personal que labore con la compañía debe reportar las fallas de seguridad que se encuentren en la red.

- Se debe definir los mecanismos para la gestión y el levantamiento de registros de los incidentes.

- Definir las responsabilidades para la correcta gestión de todos aquellos incidentes que hayan sido detectados.

- Levantamiento de información y evidencia cuando ocurra un incidente de seguridad para realizar las respectivas denuncias y procesos legales según corresponda.

10.1.3.11. Plan de continuidad de negocio

- Crear un plan de continuidad de negocio que abarque todos los servicios y equipos de la entidad.

- Identificar los eventos que puedan provocar alguna amenaza a los sistemas de continuidad.

- Establecer planes para asegurar la continuidad de los procesos que son indispensables.

- Mantener y mejorar el plan de continuidad de negocio, para que esté siempre disponible por si ocurre alguna eventualidad.

10.2. OBJETIVO 2 – IDENTIFICACIÓN DE ACTIVOS, AMENAZAS Y RIESGOS EN LA ENTIDAD

10.2.1. DEFINICIÓN DEL ENFOQUE DE ANÁLISIS DE RIESGO.

Para escoger el enfoque con el cual se va a realizar el análisis de los riesgos, se debe tener en cuenta que hay muchos métodos que son compatibles con la norma ISO 27001, pero hay una metodología que es muy completa y que realiza el análisis y valoración de las diferentes amenazas y es recomendada por la norma, se utilizará MAGERIT.

"MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información" [14].

[14]Dirección General de administración, 2012, versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, P. 17

10.2.2. RECOLECCIÓN DE INFORMACIÓN

Para la recolección de la información e identificación de los distintos inconvenientes que se están presentando en la entidad, se realizan entrevistas y encuestas a todos los empleados entre áreas administrativas, funcionarios, directivos y en especial al departamento de sistemas; donde se enfoca los cuestionarios técnicos para obtener información más detallada de los equipos tecnológicos y las configuraciones que existen.

Es importante obtener una perspectiva general en cuanto a seguridad, debido a que enfoca el problema mucho más rápido y se puede determinar los controles más adecuados que se encarguen de minimizar las amenazas a la seguridad de la información. El departamento en el que más se va a enfatizar las pruebas y las entrevistas va a ser el de sistemas, puesto que están encargados de los equipos tecnológicos, manejan las configuraciones de los sistemas de seguridad y los diferentes servidores que son considerados importantes y de gran impacto para la entidad. Se debe indagar muy a fondo en cada activo para determinar los riesgos y dar solución efectiva a la problemática. Para la visualización de los resultados obtenidos de las entrevistas se puede observar el ***ANEXO B***.

De igual manera se realiza una revisión de los controles que se encuentran en la norma ISO 27002 y son formulados como preguntas; el nivel de calificación va a ser el siguiente:

CUMPLE: cuando se determina que se ha implementado correctamente el control en la entidad.

CUMPLE PARCIALMENTE: cuando el control es implementado, pero no funciona correctamente al 100%.

NO CUMPLE: no se ha implementado el control en la entidad.

De igual manera, es importante dar un ponderado para evidenciar si el dominio está implementado correctamente en la entidad y efectuar mejoras en el mismo, esto

ayuda en la identificación de los riesgos y los controles a ejecutar en la entidad. Para la visualización de los resultados obtenidos en la evaluación de los controles se puede observar en el ***ANEXO C***.

Estos resultados sirven para diligenciar la información que se solicita en la metodología MAGERIT, para iniciar con el proceso de análisis de los riesgos y las vulnerabilidades.

10.2.3. ANÁLISIS DE RIESGO

10.2.3.1. Valoración de Riesgos

Para la evaluación del riesgo se tienen en cuenta las siguientes categorías: Critico, Importante, Apreciable, Bajo, Despreciable, se puede observar las categorías en la siguiente tabla y la valoración de cada una.

Tabla 3 Valoración de Riesgos.

	Nomenclatura	Categoría	Valoración
Valoración del riesgo	MA	Crítico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Fuente: Plantilla matriz de análisis de riesgo

De igual manera, se realizará tratamiento de los distintos riesgos que sean calificados como inaceptables con la calificación 16 – 26; se aceptan los riesgos que sean aceptables 1 – 5 y moderados 6 – 15; teniendo en cuenta los diferentes tipos de calificaciones y los riesgos que se van a aceptar, se realiza la identificación de los riesgos y la calificación de estos en la matriz.

10.2.3.2. Inventario de Activos

Se procede a realizar el levantamiento de inventario de la entidad, además, de los responsables de estos activos, teniendo en cuenta el enfoque se procede a realizar la identificación mediante la siguiente tabla:

Tabla 4 Inventario de activos.

DATOS DEL ACTIVO DE INFORMACION		
Nombre del activo de información	**Proceso propietario del activo**	**Responsable**
Personal administrativo	Dirección general	Marcos Ramos
Equipos de cómputo administrativos	Departamento de sistemas	Marisol Gonzales
Servidor Bases de datos	Departamento de sistemas	Milton Vanegas
Servidor de archivos FTP	Departamento de sistemas	Julián Benítez
Servidor DHCP	Departamento de sistemas	Julián Benítez
Servidor de Impresión	Departamento de sistemas	Milton Vanegas
Servidor de Nomina y facturación	Departamento de sistemas	Milton Vanegas
Página WEB	Proveedor	Godaddy
Equipos de cómputo para desarrollo tecnológico	Departamento de sistemas	Marisol Gonzales
Cortafuegos Cisco ASA 5505	Departamento de sistemas	Julián Benítez
Sistemas operativos	Departamento de sistemas	Marisol Gonzales
Puntos de acceso HUB	Departamento de sistemas	Milton Vanegas
Switches cisco catalyst 2960	Departamento de sistemas	Milton Vanegas
Puntos de acceso AP´s	Departamento de sistemas	Ramiro Ramírez
Personal Mantenimiento de sistemas	Departamento de soporte	Julián Benítez
Teléfonos IP	Departamento de sistemas	Ramiro Ramírez
Centro de Datos	Departamento de sistemas	Julián Benítez

Edificio de la entidad	Departamento de infraestructura	Pablo Cáceres
Administradores de sistemas	Departamento de sistemas	Julián Benítez
Personal desarrollo de software	Departamento de desarrollo	Clara Ortigoza
Correo Electrónicos	Proveedor	Google
Credenciales	Departamento de sistemas	Milton Vanegas
Plataformas de facturación y nomina	Departamento de sistemas	Milton Vanegas
Servidor PBX	Departamento de sistemas	Milton Vanegas
equipos de climatización	Departamento de infraestructura	Pablo Cáceres
Bases de datos	Departamento de desarrollo	Clara Ortigoza

Fuente: Plantilla matriz de análisis de riesgo – diligenciado por el Autor

10.2.3.3. Valoración de los activos

Después de identificar los activos con los que cuenta la entidad, es importante realizar la valoración de estos teniendo en cuenta las siguientes dimensiones: **Dimensión autenticidad**, **Dimensión trazabilidad, Dimensión confidencialidad, Dimensión integridad** y **Dimensión disponibilidad.**

Como primer paso, se realiza una clasificación según el libro 2 de la metodología MAGERIT del tipo de activo, después se realiza un análisis cualitativo de la importancia de acuerdo con las dimensiones, según la nomenclatura y otros factores que pueden ser determinantes; se puede visualizar en la tabla 5.

Tabla 5 Valoración cualitativa de los activos.

No.	DATOS DEL ACTIVO DE INFORMACION			TIPO										DIMENSION					ATRIBUTOS									UBICACIÓN	
	Nombre del activo de información	Proceso propietario del activo	Responsable	[D] DATOS	[K] CLAVES CRIPTOGRAFICAS	[S] SERVICIOS	[SW] SOFTWARE	[HW] EQUIPAMENTO INFORMÁTICO	[COM] REDES DE COMUNICACIONES	[Media] SOPORTE DE INFORMACIÓN	[AUX] EQUIPAMENTO AUXILIAR	[L] INSTALACIONES	[P] PERSONAL	Dimensión Autenticidad (B / M /A / MA/ MB)	Dimensión Trazabilidad (B / M /A / MA/ MB)	Dimensión Confidencialidad (B / M /A / MA/ MB)	Dimensión Integridad (B / M /A / MA/ MB)	Dimensión Disponibilidad (B / M /A / MA/ MB)	¿Es activo de información de terceros o de clientes que debe protegerse?	¿Activo de información que debe ser restringido a un número limitado de empleados?	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes o corrupción	Activo de información que es muy crítico para las operaciones internas	Activo de información que es muy crítico para el servicio hacia terceros	Activo de información que, en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera:			Físico	Electrónico
																										Leve	Importante	Grave		
1	Personal administrativo	Dirección general	Marcos Ramos										X	A	A	MA	MA	A	NO	NO	NO	SI	SI	NO		X		X	
2	Equipos de cómputo administrativos	Departamento de sistemas	Marisol Gonzales					X						A	A	A	A	A	NO	SI	SI	SI	SI	SI		X		X	
3	Servidor Bases de datos	Departamento de sistemas	Milton Vanegas			X								MA	MA	MA	MA	MA	NO	SI	SI	SI	SI	SI			X	X	
4	Servidor de archivos FTP	Departamento de sistemas	Julián Benítez			X								A	A	MA	MA	MA	NO	SI	SI	SI	SI	SI			X	X	
5	Servidor DHCP	Departamento de sistemas	Julián Benítez			X								A	A	MA	MA	MA	NO	SI	SI	SI	SI	SI			X	X	
6	Servidor de Impresión	Departamento de sistemas	Milton Vanegas			X								M	M	A	A	A	NO	SI	SI	SI	SI	SI		X		X	

Tabla 5 Continuación.

7	Servidor de Nomina y facturación	Departamento de sistemas	Milton Vanegas			X								MA	MA	MA	MA	MA	NO	SI	SI	SI	SI	SI			X		X
8	Página WEB	Proveedor	Godaddy				X							B	B	B	B	B	NO	NO	NO	SI	NO	NO		X			X
9	Equipos de cómputo para desarrollo tecnológico	Departamento de sistemas	Marisol Gonzales					X						A	A	A	A	A	NO	SI	SI	SI	SI	SI		X		X	
10	Cortafuegos Cisco ASA 5505	Departamento de sistemas	Julián Benítez					X						A	A	MA	MA	MA	NO	SI	SI	SI	SI	SI			X	X	
11	Sistemas operativos	Departamento de sistemas	Marisol Gonzales				X							B	B	A	A	A	NO	SI	NO	SI	SI	SI		X			X
12	Puntos de acceso HUB	Departamento de sistemas	Milton Vanegas					X						M	B	A	A	A	NO	SI	SI	SI	SI	SI			X	X	
13	Switches cisco catalyst 2960	Departamento de sistemas	Milton Vanegas					X						M	B	A	A	A	NO	SI	SI	SI	SI	SI			X	X	
14	Puntos de acceso AP´s	Departamento de sistemas	Ramiro Ramírez					X						A	A	MA	MA	MA	NO	SI	SI	SI	SI	SI			X	X	
15	Personal Mantenimiento de sistemas	Departamento de soporte	Julián Benítez										X	A	A	MA	MA	A	NO	NO	NO	SI	SI	NO			X	X	
16	Teléfonos IP	Departamento de sistemas	Ramiro Ramírez						X					B	B	A	A	A	NO	SI	SI	NO	SI	NO			X	X	
17	Centro de Datos	Departamento de sistemas	Julián Benítez									X		MA	B	MA	MA	MA	NO	SI	SI	SI	SI	SI		X		X	
18	Edificio de la entidad	Departamento de infraestructura	Pablo Cáceres									X		A	B	MA	MA	MA	NO	SI	SI	SI	SI	SI			X	X	
19	Administradores de sistemas	Departamento de sistemas	Julián Benítez										X	B	B	MA	MA	A	NO	SI	SI	SI	SI	SI			X	X	
20	Personal desarrollo de software	Departamento de desarrollo	Clara Ortigoza										X	B	B	MA	MA	A	NO	SI	SI	SI	SI	SI		X		X	
21	Correo Electrónicos	Proveedor	Google				X							B	B	A	A	A	SI	NO	NO	SI	SI	SI			X		X

Tabla 5 Continuación.

22	Credenciales	Departamento de sistemas	Milton Vanegas	X										MA	MA	MA	MA	MA	NO	SI	SI	SI	SI	SI			X		X
23	Plataformas de facturación y nomina	Departamento de sistemas	Milton Vanegas				X							MA	A	MA	MA	MA	NO	SI	SI	SI	SI	SI			X		X
24	Servidor PBX	Departamento de sistemas	Milton Vanegas			X								A	A	MA	MA	MA	NO	SI	SI	SI	SI	SI			X	X	
25	equipos de climatización	Departamento de infraestructura	Pablo Cáceres								X			B	B	M	A	A	NO	SI	SI	NO	SI	NO			X	X	
26	Bases de datos	Departamento de desarrollo	Clara Ortigoza				X							A	MA	MA	MA	MA	NO	SI	SI	SI	SI	SI			X		X

Fuente: Plantilla matriz de análisis de riesgo – diligenciado por el Autor

Después de realizar el análisis se tiene en cuenta los valores asignados según la tabla 3 de acuerdo con la nomenclatura y se valora cada activo, da como resultado los activos catalogados como importantes para la entidad, además, de la clasificación de los riesgos; se puede visualizar en la tabla 6.

Tabla 6 Valoración de activos.

Nombre	Riesgo	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
Personal administrativo	CRITICO	20	20	25	25	20	22
Equipos de cómputo administrativos	IMPORTANTE	20	20	20	20	20	20
Servidor Bases de datos	CRITICO	25	25	25	25	25	25
Servidor de archivos FTP	CRITICO	20	20	25	25	25	23
Servidor DHCP	CRITICO	20	20	25	25	25	23
Servidor de Impresión	IMPORTANTE	20	20	25	25	25	18
Servidor de Nomina y facturación	CRITICO	25	25	25	25	25	25

Tabla 6 Continuación.

Página WEB	BAJO	9	9	9	9	9	9
Equipos de cómputo para desarrollo tecnológico	IMPORTANTE	20	20	20	20	20	20
Cortafuegos Cisco ASA 5505	CRITICO	20	20	25	25	25	23
Sistemas operativos	IMPORTANTE	9	9	20	20	20	16
Puntos de acceso HUB	IMPORTANTE	15	9	20	20	20	17
Switches cisco catalyst 2960	IMPORTANTE	15	9	20	20	20	17
Puntos de acceso AP´s	CRITICO	20	20	25	25	25	23
Personal Mantenimiento de sistemas	CRITICO	20	20	25	25	20	22
Teléfonos IP	IMPORTANTE	9	9	20	20	20	16
Centro de Datos	CRITICO	25	9	25	25	25	22
Edificio de la entidad	CRITICO	20	9	25	25	25	21
Administradores de sistemas	IMPORTANTE	9	9	25	25	20	18
Personal desarrollo de software	IMPORTANTE	9	9	25	25	20	18
Correo Electrónicos	IMPORTANTE	9	9	20	20	20	16
Credenciales	CRITICO	25	25	25	25	25	25
Plataformas de facturación y nomina	CRITICO	25	20	25	25	25	24
Servidor PBX	CRITICO	20	20	25	25	25	23
equipos de climatización	APRECIABLE	9	9	15	20	20	15
Bases de datos	CRITICO	20	25	25	25	25	24

Fuente: Plantilla matriz de análisis de riesgo – diligenciado por el Autor

10.2.3.4. Identificación de amenazas

Se realiza una identificación de las amenazas, teniendo en cuenta el libro número 2 del método de MAGERIT V3, donde se encuentran descritas las amenazas que puedan existir, teniendo en cuenta los distintos tipos de activos de la información, de igual manera, la organización de los activos en ciertas categorías. En la tabla 7 se puede visualizar las vulnerabilidades encontradas teniendo en cuenta los activos identificados en la entidad QWERTY S.A.

Tabla 7 Identificación de amenazas

Activos de Información	No.	Nombre del activo de información	Valoración	Amenazas Metodología Magerit	Vulnerabilidades
[P] PERSONAL	1	Personal administrativo	22	[E28] Indisponibilidad del personal	No se cuenta con sistema de Teletrabajo
[P] PERSONAL	2	Personal administrativo	22	[A30] Ingeniería social (picaresca)	No hay cronogramas de capacitaciones documentadas
[P] PERSONAL	3	Personal administrativo	22	[E19] Fugas de información	No se han creado criterios de confidencialidad
[HW] EQUIPAMENTO INFORMÁTICO	4	Equipos de cómputo administrativos	20	[A6] Abuso de privilegios de acceso	No hay jerarquización de usuarios según su perfil
[HW] EQUIPAMENTO INFORMÁTICO	5	Equipos de cómputo administrativos	20	[A7] Uso no previsto	Uso de equipos para fines no previstos
[HW] EQUIPAMENTO INFORMÁTICO	6	Equipos de cómputo administrativos	20	[A11] Acceso no autorizado	No existen políticas donde se especifique el cambio constante de contraseñas
[S] SERVICIOS	7	Servidor Bases de datos	25	[A15] Modificación deliberada de la información	No hay procesos documentados de sistemas de copias periódicas.
[S] SERVICIOS	8	Servidor Bases de datos	25	[A18] Destrucción de información	Borrado de información por acceso no autorizado.
[S] SERVICIOS	9	Servidor Bases de datos	25	[A11] Acceso no autorizado	Credenciales de acceso generales.
[S] SERVICIOS	10	Servidor de archivos FTP	23	[A15] Modificación deliberada de la información	No hay procesos documentados de sistemas de copias periódicas.
[S] SERVICIOS	11	Servidor de archivos FTP	23	[A18] Destrucción de información	Borrado de información por acceso no autorizado.
[S] SERVICIOS	12	Servidor de archivos FTP	23	[A11] Acceso no autorizado	Credenciales de acceso generales.
[S] SERVICIOS	13	Servidor DHCP	23	[A15] Modificación deliberada de la información	No hay procesos documentados de sistemas de copias periódicas.
[S] SERVICIOS	14	Servidor DHCP	23	[A18] Destrucción de información	Borrado de información por acceso no autorizado.
[S] SERVICIOS	15	Servidor DHCP	23	[A11] Acceso no autorizado	Credenciales de acceso generales.
[S] SERVICIOS	16	Servidor de Impresión	18	[A15] Modificación deliberada de la información	No hay procesos documentados de sistemas de copias periódicas.

Tabla 7 Continuación.

[S] SERVICIOS	17	Servidor de Impresión	18	[A18] Destrucción de información	Borrado de información por acceso no autorizado.
[S] SERVICIOS	18	Servidor de Impresión	18	[A11] Acceso no autorizado	Credenciales de acceso generales.
[S] SERVICIOS	19	Servidor de Nomina y facturación	25	[A15] Modificación deliberada de la información	No hay procesos documentados de sistemas de copias periódicas.
[S] SERVICIOS	20	Servidor de Nomina y facturación	25	[A18] Destrucción de información	Borrado de información por acceso no autorizado.
[S] SERVICIOS	21	Servidor de Nomina y facturación	25	[A11] Acceso no autorizado	Credenciales de acceso generales.
[SW] SOFTWARE	22	Página WEB	9	[A15] Modificación deliberada de la información	Cambio de información del sitio WEB
[HW] EQUIPAMENTO INFORMÁTICO	23	Equipos de cómputo para desarrollo tecnológico	20	[A6] Abuso de privilegios de acceso	No hay jerarquización de usuarios según su perfil
[HW] EQUIPAMENTO INFORMÁTICO	24	Equipos de cómputo para desarrollo tecnológico	20	[A7] Uso no previsto	Uso de equipos para fines no previstos
[HW] EQUIPAMENTO INFORMÁTICO	25	Equipos de cómputo para desarrollo tecnológico	20	[A11] Acceso no autorizado	No existen políticas donde se especifique el cambio constante de contraseñas
[HW] EQUIPAMENTO INFORMÁTICO	26	Cortafuegos Cisco ASA 5505	23	[E2] Errores del administrador	No se encuentran configuradas las reglas ni se lleva registro de actividades.
[SW] SOFTWARE	27	Sistemas operativos	16	[E2] Errores del administrador	No se encuentra configuración de actualizaciones
[SW] SOFTWARE	28	Sistemas operativos	16	[A8] Difusión de software dañino	No cuenta con actualización de los parches de seguridad del sistema
[HW] EQUIPAMENTO INFORMÁTICO	29	Puntos de acceso HUB	17	[E2] Errores del administrador	No hay segmentación de red LAN
[HW] EQUIPAMENTO INFORMÁTICO	30	Switches cisco catalyst 2960	17	[E2] Errores del administrador	Usuarios y contraseñas por defecto
[HW] EQUIPAMENTO INFORMÁTICO	31	Puntos de acceso AP´s	23	[E2] Errores del administrador	No hay segmentación de red WIFI
[P] PERSONAL	32	Personal Mantenimiento de sistemas	22	[E28] Indisponibilidad del personal	No se cuenta con sistema de Teletrabajo
[P] PERSONAL	33	Personal Mantenimiento de sistemas	22	[A30] Ingeniería social (picaresca)	No hay cronogramas de capacitaciones documentadas
[P] PERSONAL	34	Personal Mantenimiento de sistemas	22	[E19] Fugas de información	No se han creado criterios de confidencialidad
[COM] REDES DE COMUNICACIONES	35	Teléfonos IP	16	[A9] [Re-]encaminamiento de mensajes	interceptación de llamadas
[L] INSTALACIONES	36	Centro de Datos	22	[A11] Acceso no autorizado	No existe sistema de seguridad biométrico ni de monitoreo
[L] INSTALACIONES	37	Centro de Datos	22	[N*] Desastres naturales	No existe un plan de continuidad del negocio
[L] INSTALACIONES	38	Edificio de la entidad	21	[N*] Desastres naturales	No existe un plan de continuidad del negocio
[L] INSTALACIONES	39	Administradores de sistemas	18	[E28] Indisponibilidad del personal	No se cuenta con sistema de Teletrabajo

Tabla 7 Continuación.

[L] INSTALACIONES	40	Administradores de sistemas	18	[A30] Ingeniería social (picaresca)	No hay cronogramas de capacitaciones documentadas
[P] PERSONAL	41	Administradores de sistemas	18	[E19] Fugas de información	No se han creado criterios de confidencialidad
[P] PERSONAL	42	Personal desarrollo de software	18	[E28] Indisponibilidad del personal	No se cuenta con sistema de Teletrabajo
[P] PERSONAL	43	Personal desarrollo de software	18	[A30] Ingeniería social (picaresca)	No hay cronogramas de capacitaciones documentadas
[P] PERSONAL	44	Personal desarrollo de software	18	[E19] Fugas de información	No se han creado criterios de confidencialidad
[SW] SOFTWARE	45	Correo Electrónicos	16	[E19] Fugas de información	No se han creado criterios de confidencialidad
[SW] SOFTWARE	46	Correo Electrónicos	16	[E1] Errores de los usuarios	No se cambia las contraseñas frecuentemente
[D] DATOS	47	Credenciales	25	[A11] Acceso no autorizado	No se cambia frecuentemente las claves de acceso
[D] DATOS	48	Credenciales	25	[A5] Suplantación de la identidad del usuario	No hay un proceso de inicio de sesión seguro.
[D] DATOS	49	Credenciales	25	[A6] Abuso de privilegios de acceso	No hay jerarquización de usuarios según su perfil
[SW] SOFTWARE	50	Plataformas de facturación y nomina	24	[A5] Suplantación de la identidad del usuario	No hay un proceso de inicio de sesión seguro.
[SW] SOFTWARE	51	Plataformas de facturación y nomina	24	[A6] Abuso de privilegios de acceso	Modificación de información
[SW] SOFTWARE	52	Plataformas de facturación y nomina	24	[A15] Modificación deliberada de la información	No hay procesos documentados de sistemas de copias periódicas.
[SW] SOFTWARE	53	Plataformas de facturación y nomina	24	[A11] Acceso no autorizado	No se cambia frecuentemente las claves de acceso
[SW] SOFTWARE	54	Servidor PBX	23	[A15] Modificación deliberada de la información	No hay procesos documentados de sistemas de copias periódicas.
[SW] SOFTWARE	55	Servidor PBX	23	[A18] Destrucción de información	Borrado de información por acceso no autorizado.
[S] SERVICIOS	56	Servidor PBX	23	[A11] Acceso no autorizado	Credenciales de acceso generales.
[L] INSTALACIONES	57	equipos de climatización	15	[I7] Condiciones inadecuadas de temperatura o humedad	Equipos no climatizan correctamente.
[SW] SOFTWARE	58	Bases de datos	24	[A5] Suplantación de la identidad del usuario	No hay un proceso de inicio de sesión seguro.
[SW] SOFTWARE	59	Bases de datos	24	[A6] Abuso de privilegios de acceso	Modificación de información
[SW] SOFTWARE	60	Bases de datos	24	[A15] Modificación deliberada de la información	No hay procesos documentados de sistemas de copias periódicas.
[SW] SOFTWARE	61	Bases de datos	24	[A11] Acceso no autorizado	No se cambia frecuentemente las claves de acceso

Fuente: Plantilla matriz de análisis de riesgo, hoja amenazas – plan de tratamiento, diligenciado por el Autor

10.2.3.5. Valoración de riesgos por activo

Al valorar los riesgos por lo activos se tienen en cuenta aspectos como la probabilidad de vulneración y se califica de 1 a 5, donde 1 es poco probable y 5 prácticamente seguro. Estos datos se pueden visualizar en la tabla 8.

Tabla 8 Probabilidad de ocurrencia del riesgo

	Nomenclatura	Categoría	Valoración
Probabilidad	MA	Probablemente seguro	5
	A	Probable	4
	M	Posible	3
	B	Poco probable	2
	MB	Muy raro	1

Fuente: Autor

Al tener los resultados de la calificación, se debe, de igual manera, verificar si existen ya controles para minimizar la ocurrencia de dichos riesgos, en esta parte se valora de 1 a 4, donde 1 significa que no existen controles; 2 existen, pero no son efectivos; 3 existen, pero no están documentados y 4 existen, están documentados y son efectivos, se pueden visualizar en la tabla 9; al realizar los cálculos arroja una valoración final donde se puede determinar si el riesgo es aceptable, moderado e inaceptable.

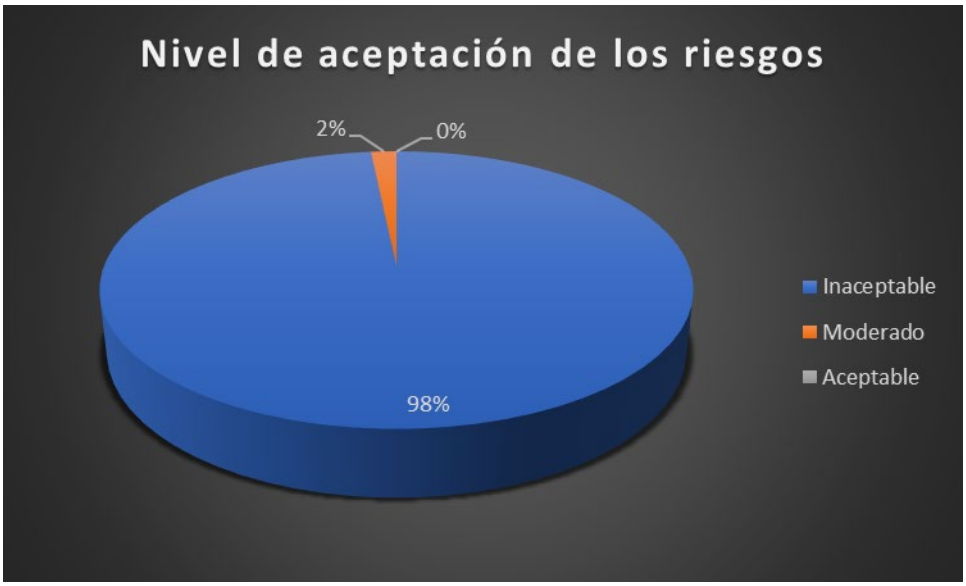
Tabla 9 Valoración de controles

Valoración	Categoría
1	**No existe controles**
2	**Existen, pero no son efectivos**
3	**Existen, pero no están documentados**
4	**Existen, están documentados y son efectivos.**

Fuente: Autor

Una vez identificado como se va a calificar cada activo con su vulnerabilidad se obtiene los siguientes resultados.

Figura 1 Nivel de aceptación de la amenaza.



Fuente: Autor

El 98% de las vulnerabilidades son inaceptables y solo el 2% son moderados, lo cual indica que los niveles de inseguridad son altos en la entidad y se deben implementar correctivos urgentemente. Para la visualización completa de la valoración y niveles de aceptación de las amenazas, observar en ***ANEXO D*** (hoja de cálculo amenazas – plan de tratamiento).

Al valorar los riesgos se debe iniciar con el tratamiento de los distintos riesgos que sean catalogados como inaceptables, se deben implementar controles que ayuden a minimizar la posible ocurrencia de estos. En este caso no se implementará un mecanismo al riesgo número 22 en la matriz, puesto que da como puntuación final: moderado y se encuentra entre los niveles aceptables.

10.3. OBJETIVO 3 – IMPLEMENTACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS EN LA ENTIDAD

10.3.1. PLAN DE TRATAMIENTO DE RIESGOS.

Para el plan de tratamiento de los riesgos, teniendo en cuenta las valoraciones, se implementan controles que se pueden encontrar en la norma ISO 27002, es importante identificar cada mecanismo y si disminuye la ocurrencia de cada una de las amenazas y suprime las vulnerabilidades encontradas, puesto que ese es el objetivo centrar del plan de tratamiento.

Es importante que la gerencia de la entidad destine los recursos necesarios para implementar los mecanismos escogidos, además, sean aprobados por el comité de seguridad y así cumplir con las metas ya expuestas en cuanto a seguridad de la información.

Una vez aprobados los controles, es importante la implementación de los mecanismos para mejorar la seguridad de la entidad, de igual manera, cada uno debe estar documentado con los procedimientos en las políticas de seguridad, así mismo de los responsables que todo funcione correctamente. Es trascendental un seguimiento constate a cada control y mecanismo por si se presenta un incidente de seguridad sea inmediatamente identificado y suprimido.

Al igual que el plan de tratamiento de riesgos, se van a crear las políticas de seguridad y los procedimientos para la ejecución de labores.

10.3.1.1. Controles y mecanismos de seguridad.

Los controles y mecanismos de seguridad se deben implementar a cada riesgo que tenga como valoración y nivel de calificación inaceptable, estos controles y mecanismos se encuentran en la norma ISO 27002.

Tenemos como resultado la siguiente distribución de controles con cantidad de riesgos:

Figura 2 Distribución controles plan tratamiento de riesgos.

Fuente: autor

Podemos determinar que el control que minimiza más cantidad de riesgos es el A12.3.1 con 8 y sigue el control A9.4.3 con 7; para la visualización completa del plan de tratamiento de riesgo con las mejoras a aplicar con el objetivo de los riesgos, se pueden visualizar en el ***ANEXO D*** (hoja de cálculo amenazas - plan de tratamiento).

10.3.2. DECLARACIÓN DE APLICABILIDAD SOA (STATEMENT OF APLICABILITY)

Es importante que para la declaración de aplicabilidad SOA por sus siglas en inglés (Statement of Aplicability), se tengan en cuenta los controles de la norma ISO 27002; se debe evaluar cada uno para determinar si aplica a los distintos riesgos o están ya implementados en la organización.

Tabla 10 Declaración de aplicabilidad SOA.

Declaración de aplicabilidad SOA			
Entidad	*QWERTY S.A.*	***Versión***	***1***
Dominio	***A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION***		
Subdominio	***A5.1 Orientación de la dirección para la gestión de la seguridad de la información***		
Objetivo	***Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes***		
Controles aplicados	***A5.1.1***	***A5.1.2***	
Dominio	***A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION***		
Subdominio	***A6.1 Organización interna***		
Objetivo	***Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.***		
Controles aplicados	***A6.1.1***		
Subdominio	***A6.2 Organización interna***		
Objetivo	***Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles***		
Controles aplicados	***A6.2.2***		
Dominio	***A.7 SEGURIDAD DE LOS RECURSOS HUMANOS***		
Subdominio	***A7.1 Antes de asumir el empleo***		
Objetivo	***Hay que asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.***		
Controles aplicados	***A7.1.2***		
Subdominio	***A7.2 Durante la ejecución del empleo***		
Objetivo	***Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.***		
Controles aplicados	***A7.2.2***		
Dominio	***A.9 CONTROL DE ACCESO***		
Subdominio	***A9.2 Gestión de acceso de usuarios***		

Tabla 10 Continuación.

Objetivo	***Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.***		
Controles aplicados	***A9.2.3***	***A9.2.5***	
Subdominio	***A9.3 Control de acceso a sistemas y aplicaciones***		
Objetivo	***Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.***		
Controles aplicados	***A9.4.1***	***A9.4.2***	***A9.4.3***
Dominio	***A.11 SEGURIDAD FISICA Y DEL ENTORNO***		
Subdominio	***A11.1 Área seguras***		
Objetivo	***Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.***		
Controles aplicados	***A11.1.2***	***A11.1.4***	
Subdominio	***A11.2 Equipos***		
Objetivo	***Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.***		
Controles aplicados	***A11.2.1***	***A11.2.3***	***A11.2.4***
Dominio	***A.12 SEGURIDAD DE LAS OPERACIONES***		
Subdominio	***A12.1 Procedimientos operacionales y responsabilidades***		
Objetivo	***Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.***		
Controles aplicados	***A12.1.1***	***A12.1.2***	
Subdominio	***A12.2 Protección contra códigos maliciosos***		
Objetivo	***Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.***		
Controles aplicados	***A12.2.1***		
Subdominio	***A12.3 Copias de respaldo***		
Objetivo	***Proteger contra la perdida de datos***		
Controles aplicados	***A12.3.1***		
Subdominio	***A12.4 Registro y seguimiento***		
Objetivo	***Registrar eventos y generar evidencia***		
Controles aplicados	***A12.4.1***	***A12.4.2***	***A12.4.3***
Subdominio	***A12.6 Gestión de la vulnerabilidad técnica***		
Objetivo	***Prevenir el aprovechamiento de las vulnerabilidades técnicas***		
Controles aplicados	***A12.6.1***		
Dominio	***A.13 SEGURIDAD DE LAS COMUNICACIONES***		
Subdominio	***A13.1 Gestión de la seguridad de las redes***		
Objetivo	***Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.***		
Controles aplicados	***A13.1.1***	***A13.1.2***	***A13.1.3***
Subdominio	***A13.2 Transferencia de información***		

Tabla 10 Continuación.

Objetivo	***Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.***			
Controles aplicados	***A13.2.3***		***A13.2.4***	
Dominio	***A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION***			
Subdominio	***A16.1 Gestión de incidentes y mejoras en la seguridad de la información.***			
Objetivo	***Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.***			
Controles aplicados	***A16.1.1***	***A16.1.4***	***A16.1.5***	***A16.1.6***
Dominio	***A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO***			
Subdominio	***A17.1 Continuidad de Seguridad de la información***			
Objetivo	***La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.***			
Controles aplicados	***A17.1.1***		***A17.1.2***	***A17.1.3***
Subdominio	***A17.2 Redundancias***			
Objetivo	***Asegurar la disponibilidad de instalaciones de procesamiento de información.***			
Controles aplicados	***A17.2.1***			

Fuente: Autor.

Al visualizar la **Tabla 10 Declaración de aplicabilidad SOA.** Se identifican los controles que son aplicados a la entidad y que ayudan a la minimización de ocurrencia de las amenazas detectadas, asegurando los activos de información; para la visualización completa de la declaración de aplicabilidad SOA, se puede encontrar en el **ANEXO E**.

10.3.3. RECOMENDACIONES PARA LA ENTIDAD QWERTY S.A.

Se deben implementar los distintos controles escogidos para la mitigación de los riesgos, además, de la actualización de las políticas de seguridad y sobre todo realizar cronogramas de capacitación a los empleados, donde se dé a conocer las políticas y lo importancia de la identificación a tiempo de los ataques a la seguridad.

Los temas para tratar son varios y priorizar los riesgos a los que se enfrenta la seguridad continuamente y como identificarlos, de igual manera, dar a conocer los métodos de comunicación para reportar los incidentes de seguridad y cuáles son los protocolos que se deben seguir para evitar inconvenientes y se incumpla con las políticas.

Así mismo, crear cronogramas de simulacros donde se evidencie el manejo de los incidentes de seguridad y qué tiempo de respuesta tienen los encargados para mitigar los riesgos, lo más importante es revisar los informes y crear los planes de mejoras o si se debe realizar el cambio de algún control o mecanismo ya implementado.

Se debe realizar auditorías de seguridad cada año para la verificación más a fondo de los mecanismos y todo lo concerniente a la seguridad de la información, verificar la ejecución de los protocolos y si los controles cumplen con el objetivo. Se obtienen los informes y los resultados se procede a realizar las mejoras pertinentes para evitar futuros ataques a la seguridad, se deben implementar las mejoras aconsejadas inmediatamente.

Por parte de la gerencia, se debe comprometer con la seguridad para que autoricen los procedimientos, ante todo, los presupuestos para la mejora e implementación de los mecanismos para obtener los resultados esperados y que se proteja los 4 pilares fundamentales de la seguridad, se debe involucrar a todos los departamentos para que la seguridad sea más fuerte y minimice los riesgos que se encuentran.

Es importante que se revisen los registros de eventos periódicamente, para evidenciar si los equipos encargados de la seguridad cumplen con sus objetivos, de igual manera, qué activos son objetivos de los atacantes, para así crear protocolos de aseguramiento o si los mecanismos han cumplido con el objetivo, además, estos informes sirven para determinar que errores se cometen y como se puede evitar.

Revisar constantemente el plan de continuidad de negocio para verificar que funcione correctamente cuando se necesite y así asegurar la continuidad de los servicios y que se cumplan con los objetivos y sobre todo con la misión de la organización, de igual manera, verificar la seguridad y las actualizaciones de los sistemas de seguridad, además, de las copias espejo de las bases de datos, información, aplicaciones y demás programas importantes para la organización.

En cuanto al departamento de sistemas, se implementen los protocolos para realizar correctamente las copias de seguridad de la información y que estás copias estén siempre disponibles solo para las personas autorizadas. Que se cumplan con la confidencialidad, integridad y disponibilidad de esta. Las copias de seguridad deben estar resguardadas en un ambiente Cloud, donde se gestione los permisos y perfiles según corresponda.

Los mantenimientos que se realicen a los sistemas deben ser periódicos y con un manual de procedimiento, los sistemas operativos deben estar siempre actualizados y se instalen los parches de seguridad desplegados por las organizaciones dueñas de los sistemas. De igual manera, siempre optar por instalar la última versión del sistema operativo disponible y estable.

Para la seguridad física de los equipos de comunicación, se instale un sistema de acceso biométrico para evitar que personas no autorizadas tengan acceso a los dispositivos y puedan afectar intencionalmente el funcionamiento de estos, además, de evitar la modificación no autorizada de la configuración de los componentes y dar acceso no autorizado a la información.

Se deben crear cronogramas de revisión y análisis de cumplimiento de los términos y condiciones firmados con los proveedores para evitar futuros inconvenientes en cuanto a seguridad y se especifiquen los responsables directamente cuando haya un incidente, realizar los seguimientos pertinentes y enfocar los esfuerzos para resolver estos problemas.

Se entrega a la gerencia el informe de auditoría con todos los hallazgos encontrados en la entidad, además, de las pruebas que se realizaron para obtener dicha información, las recomendaciones y soluciones a ejecutar en cada caso; se puede visualizar el informe en el ***ANEXO J***.

10.3.4. POLÍTICAS DE SEGURIDAD

Una vez realizado el plan de tratamiento de riesgos, es importante crear las políticas de seguridad con los controles implementados, con el objetivo de que los empleados cumplan a cabalidad con las normas y así minimizar la ocurrencia de las vulnerabilidades encontradas.

10.3.4.1. Objetivos

- Objetivo general

Definir las políticas que rigen la seguridad de la información en la compañía QWERTY S.A y cumplen con los estándares de seguridad, minimizando los riesgos y vulnerabilidades.

- Objetivos específicos

  - Asegurar toda la información que se maneja en la compañía QWERTY S.A puesto que es catalogada como importancia alta.
  - Definir los procesos de gestión de incidentes en caso de que se presentes inconvenientes de seguridad.
  - Definir las responsabilidades del personal que labora en la empresa, teniendo el marco de seguridad empresarial como respaldo.

10.3.4.2. Alcance

La implementación de las políticas de seguridad afecta a todas las áreas de la empresa, puesto que son normas que se crean para proteger los recursos TIC, desde el personal que labora en la empresa como los sistemas y recursos tecnológicos, además, de los distintos aplicativos y páginas de la compañía.

10.3.4.3. Comité seguridad de la información

Es importante que el comité de seguridad sea el encargo de la verificación de la correcta aplicación de las políticas de seguridad escogidas e implementadas para la entidad QWERTY; se deben realizar reuniones periódicas para el estudio de informes detallados en cuanto a seguridad; es de igual importancia la revisión de las distintas políticas si cumplen con los objetivos de seguridad, además, con lo estipulado en el documento.

El comité está conformado por una persona de las siguientes áreas:

- Gerente de la entidad.
- Representante de los directivos
- Representante de los administrativos
- Representante Área de sistemas
- Profesional en Seguridad informática.

Al momento de realizar las distintas reuniones es importante llevar control de las actividades y temas que se tratan mediante actas administrativas, los cambios que se realicen a las políticas y procedimientos de seguridad deben estar documentados y aprobados por todas las personas del comité y plasmados en las actas.

10.3.4.4. Políticas de seguridad de la información.

❖ **Políticas de seguridad**

- Directrices de la dirección en seguridad de la información.

Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.

- Conjunto de políticas para la seguridad de la información.

Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.

- Revisión de las políticas para la seguridad de la información

Control: Las políticas para la seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.

Políticas:

- ✓ Se debe crear las políticas de seguridad para la entidad, que contenga los distintos controles implementados. Para la actualización de los controles es importante que se programen auditorías a los sistemas de información y seguridad, para la mejora continua de los controles y normas; el comité de seguridad y la directiva, deben aprobar dichas mejoras y realizar las respectivas actualizaciones a las políticas de seguridad. Al finalizar se deben dar a conocer dichas mejoras a todo el personal de la organización.

❖ **Organización de la seguridad de la información**

- ➢ Organización interna

Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.

- Roles y responsabilidades para la seguridad de información

Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.

Políticas:

- ✓ Es importante que se definan los roles y las responsabilidades en cuanto a seguridad de la información, de igual manera, en el departamento de sistemas, se tengan claro los roles que se van a manejar y como es el proceder si se presenta un incidente de seguridad y se cumplan con los criterios de atención y registro.
- ✓ Es importante que los distintos activos de la entidad estén asignados a las personas correspondientes para que se hagan cargo de la información y la seguridad de estos, además, de la gestión de los permisos de acceso y constante verificación del cumplimiento de las normas.
- ✓ Se debe reportar de inmediato a las personas pertinentes según los procesos de informe de incidentes de seguridad, para asegurar la información y los activos que son un pilar fundamental para el cumplimiento de los objetivos y la misión de la entidad.

- ➢ Dispositivos móviles y teletrabajo

Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

- ▪ Teletrabajo

Control: Se debería implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo

Políticas:

- ✓ Se debe cumplir con los protocolos de teletrabajo para que se cumpla con las responsabilidades de las personas, se debe cumplir con los horarios establecidos de trabajo y con los distintos protocolos de seguridad informática y conexiones seguras y encriptadas a la red corporativa de la

entidad, además, de los manejos de los aplicativos, esto mediante conexión VPN.

- ✓ Se debe cumplir con los protocolos de seguridad para la información, en los lugares donde se haya implementado teletrabajo, se debe cumplir con los procesos de aseguramiento, almacenamiento y modificación de esta.

❖ **Seguridad de los recursos humanos**

- Antes de asumir el empleo

Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.

- Términos y condiciones del empleo

Control: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.

Políticas:

- ✓ Se debe indicar a los distintos empleados de la entidad de lo importante que es dar buen uso a los distintos equipos tecnológicos y con énfasis en cumplir la misión y objetivos de la organización, además, del estricto cumplimiento de las políticas de seguridad.

- Durante la ejecución del empleo

Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.

- Toma de conciencia, educación y formación en la seguridad de la información

Control: Todos los empleados de la organización y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.

Políticas:

- ✓ Se deben crear los cronogramas de capacitación de seguridad informática para los empleados, es importante, de igual manera, que se brinde información sobre seguridad informática y los diferentes delitos que existen y las políticas de seguridad con las que cuenta la entidad, se deben dar a conocer las actualizaciones que se realicen a las políticas.

❖ **Control de acceso**

- ➢ Gestión de acceso de usuarios

Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios. Gestión de derechos de acceso privilegiado.

- ▪ Gestión de derechos de acceso privilegiado

Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.

- ▪ Revisión de los derechos de acceso de usuarios

Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.

Políticas:

- ✓ Para crear los usuarios que se van a manejar en los distintos aplicativos y equipos en la entidad, se debe tener en cuenta el cargo de cada uno y las funciones que desempeñan esto para evitar que realice acciones no

autorizadas; estos usuarios deben estar ligados directamente con el directorio activo para la correcta gestión de los permisos.

- ✓ Se deben desactivar los usuarios que existen por defecto en los equipos y aplicativos de la entidad, es de suma importancia realizar estos cambios en las primeras configuraciones y crear nuevas credenciales con los perfiles indicados teniendo en cuenta los cargos a desempeñar.

- Control de acceso a sistemas y aplicaciones

Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.

- Restricción de acceso información

Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones, se debería restringir de acuerdo con la política de control de acceso.

- Procedimiento de ingreso seguro

Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.

- Sistema de gestión de contraseñas

Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.

Políticas:

- ✓ Se debe restringir el acceso a la información que es catalogada como importante y confidencial, solo el personal autorizado puede acceder y realizar las respectivas acciones como modificación y eliminación; se debe llevar un registro de eventos de cada uno de los usuarios y eliminación de estos si se termina el contrato.

- ✓ Para el manejo de aplicativos de nómina, pagos, manejo de inventario, acceso a configuraciones importantes u otros programas o equipos catalogados como importantes, se debe gestionar el ingreso seguro mediante sistemas de autenticación avanzados como token o llaves de inicio de sesión.
- ✓ Se debe realizar el cambio periódico de todas las claves de inicio de sesión de los diferentes programas, equipos tecnológicos, usuarios de ingreso a FTPs, y demás, estás claves deben ser complejas y de longitud no menor a 8 caracteres, estos cambios se aconsejan realizarlos cada 72 días como máximo.

❖ **Seguridad física y del entorno**

- ➢ Áreas seguras

Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.

- Controles físicos de entrada

Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.

- Protección contra amenazas externas y ambientales

Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.

Políticas:

- ✓ Es importante que se restringa el ingreso a personal no autorizado a áreas de suma confidencialidad como centros de datos y servidores, estos equipos

deben estar protegidos mediante accesos biométricos y monitoreo constante, esto para evitar modificaciones a las configuraciones sin previa autorización.

- ✓ Se debe poner en marcha el plan de continuidad del negocio por si ocurre algún desastre natural, ataques maliciosos o accidentes. Todos los sistemas deben estar operativos, actualizados y disponibles por si se requieren en cualquier momento, los aplicativos y bases de datos, deben estar actualizadas y toda la información requerida siempre disponible.

- Equipos

Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.

- Ubicación y protección de los equipos

Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas, peligros del entorno y las oportunidades para acceso no autorizado.

- Seguridad del cableado

Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.

- Mantenimiento de equipos

Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.

Políticas:

- ✓ Se deben resguardar los equipos que sean considerados importantes para el alcance de los objetivos de la entidad, se debe restringir el acceso a estos de

personas no autorizadas y protegidos por sistemas de ingreso seguro o autenticación biométrico.

- ✓ Se debe cifrar las distintas conexiones de la entidad como llamadas por telefonía IP, conexiones a intranet e internet, esto para evitar interceptación de datos y fuga de información; todas estas conexiones se deben realizar mediante conexiones Ipsec o MPLS. En caso de que se esté realizando teletrabajo se debe realizar conexiones mediante VPN autorizados por la entidad.
- ✓ Se deben realizar mantenimientos preventivos periódicos a los equipos de la entidad, esto para alargar la vida útil y prevenir daños ocasionados por suciedad en el hardware o indisponibilidad por falta de mantenimiento y optimización del software; estos mantenimientos deben estar autorizados por la directiva y realizado por el personal del departamento de sistemas, con los procedimientos debidamente documentados.

❖ **Seguridad de las operaciones**

- ➢ Protección contra códigos maliciosos

Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

- ▪ Controles contra códigos maliciosos

Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos

Políticas:

- ✓ Se debe siempre contar con un agente de antivirus, que se encargue de proteger los diferentes equipos de malware, de igual manera, es importante capacitar a los empleados sobre los distintos códigos maliciosos que existen

y que inconvenientes pueden ocasionar en los sistemas de la organización; los agentes deben estar siempre actualizados y realizar la debida instalación de los parches de seguridad de los sistemas operativos.

- Copias de respaldo

Objetivo: Proteger contra la perdida de datos.

- Respaldo de información

Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

Políticas:

- ✓ Se deben realizar copias de seguridad diarias a bases de datos y semanales a información almacenada en los equipos de cómputo, copias espejo de los servidores, siempre y cuando haya modificación de la información, es importante contar con los protocolos documentados y los procedimientos donde se encuentre un paso a paso de la correcta ejecución de estos.
- ✓ Todas las copias de seguridad deben estar respaldadas en un servidor en la nube para que se tenga acceso desde cualquier parte y solo por personal autorizado; el ingreso debe ser mediante correo electrónico al igual que la contraseña, deben ser personales y no pueden ser compartidas.

- Registro y seguimiento

Objetivo: Registrar eventos y generar evidencia.

- Registro de eventos

Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

Políticas:

- ✓ Se debe llevar un registro de todos los eventos de los movimientos realizados en bases de datos, copias de seguridad, cambio de configuraciones, es importante que una vez detectadas dichas modificaciones se especifiquen porque se realizaron y quién autoriza los cambios.

- Gestión de la vulnerabilidad técnica

Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.

- Gestión de las vulnerabilidades técnicas

Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización y tomar las medidas apropiadas para tratar el riesgo asociado.

Políticas:

- ✓ Se debe realizar una revisión constante a las configuraciones que tienen los equipos TIC, es importante que se supriman las configuraciones por defecto en los equipos de telecomunicación y demás, para evitar ataques de abusos de privilegios, además, de la correcta configuración de los equipos de seguridad.

❖ **Seguridad de las comunicaciones**

- ➢ Gestión de la seguridad de las redes

Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.

- Controles de redes

Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones

- Separación en las redes

Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.

Políticas:

- ✓ Se debe implementar un sistema IPS para el monitoreo continuo de las redes y el tráfico que se maneja, es importante realizar las correctas configuraciones para que la seguridad sea optima, de igual manera, la ejecución de un firewall WAF para la protección de las aplicaciones y bases de datos.
- ✓ Se debe segmentar las redes en VLAN distintas teniendo en cuenta los perfiles del personal y los equipos tecnológicos que se van a manejar, es importante restringir el acceso a los equipos de telecomunicaciones, servidores, firewall entre otros. Desde otras VLANs y computadores no autorizados.

- ➢ Transferencia de información

Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

- Acuerdos de confidencialidad o de no divulgación.

Control: Se deberían identificar, documentar y revisar regularmente los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.

Políticas:

- ✓ Se deben establecer acuerdos de confidencialidad entre los empleados y el empleador, para que no exista inconvenientes de fuga de información, los acuerdos deben ser firmados, de igual manera, entendidos por todos los empleados; se deben explicar los correctivos que aplican si se incumple con los términos.

❖ **Gestión de incidentes de seguridad de la información.**

- ➢ Gestión de incidentes y mejoras en la seguridad de la información.

Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

- Responsabilidad y procedimientos.

Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

- Evaluación de eventos de seguridad de la información y decisiones sobre ellos.

Control: Los eventos de seguridad de la información se deberían evaluar y decidir si se van a clasificar como incidentes de seguridad de la información.

- Respuesta a incidentes de seguridad de la información

Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.

- Aprendizaje obtenido de los incidentes de seguridad de la información

Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.

Políticas:

- ✓ Se debe determinar las responsabilidades en las respuestas cuando se presente un incidente de seguridad, se deben aplicar los distintos procedimientos para la atención eficaz y oportuna, además, de asegurar los activos y disminuir la ocurrencia de los incidentes.
- ✓ Se deben guardar un registro detallado sobre los incidentes de seguridad, es importante evaluar cada evento, implementar las listas de chequeo para identificar las causas de ocurrencias y corregir los fallos de seguridad en el menor tiempo posible, llevar un registro histórico de las actividades.
- ✓ Se deben poner en marcha los protocolos establecidos para la atención de incidentes reportados y dar solución oportuna a las incidencias para evitar comprometer los activos y no interrumpir los servicios de la entidad.
- ✓ Se debe llevar un histórico de los distintos incidentes de seguridad reportados y detectados, de igual manera, las soluciones o mejoras realizadas que se implementaron para controlar los riesgos, es importante salvaguardar estos registros para futuros incidentes.

❖ **Aspectos de seguridad de la información de la gestión de continuidad de negocio.**

- ➢ Continuidad de seguridad de la información.

Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.

- Planificación de la continuidad de la seguridad de la información.

Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.

- Implementación de la continuidad de la seguridad de la información

Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

- Verificación, revisión y evaluación de la continuidad de la seguridad de la información

Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

Políticas:

- ✓ La seguridad de la información debe tener alcance en el plan de continuidad del negocio para que se proteja de igual forma los equipos de respaldo y la información que allí se maneja, es importante que toda actualización en las políticas y mecanismos de seguridad, se implementen en el plan.
- ✓ Se debe verificar constantemente los distintos procedimientos de seguridad en el plan de continuidad, que se cumplan con los mecanismos y controles para evitar futuras amenazas a la información, se deben implementar las actualizaciones y mejoras continuas también en el plan de continuidad.

10.3.5. PROCESOS DOCUMENTADOS

Se crean procedimientos para la ejecución de actividades catalogadas como importantes para la entidad. Es fundamental que se ejecuten todas las secuencias, para que las operaciones sean exitosas.

Para la entidad es importante determinar los procedimientos que deben estar documentados, se aplican las listas de chequeo pertinentes para evitar inconvenientes y impedir pérdidas de información o activos catalogados como importantes.

Se van a documentar los siguientes procedimientos:

- Copias de seguridad de información.
- Mantenimiento preventivo equipos tecnológicos.
- Adquisición y gestión de los activos de software.
- Gestión de incidentes de seguridad.

10.3.5.1. Copias de seguridad de la información

Se efectúa el siguiente procedimiento para realizar copias de seguridad en la entidad QWERTY S.A.

❖ Objetivo:

Establecer los procedimientos para realizar copias de seguridad en la entidad QWERTY S.A.

❖ Alcance:

Se establece que el alcance de este procedimiento es en toda la entidad y para cualquier copia de seguridad que se requiera realizar.

❖ Base legal:

Políticas de seguridad de la entidad.

❖ Condiciones generales

Para la realización de las copias de seguridad se deben tener en cuenta las políticas de seguridad y los requerimientos especificados por la entidad, se deben destinar los almacenamientos apropiados para dicha copia de seguridad, en el caso de la entidad QWERTY S.A. se realizará almacenamiento en la nube como OneDrive, está directamente ligado a los correos de los funcionarios de la entidad.

Para las copias de seguridad de la información en bases de datos, se realizan backup en frío puesto que es importante la confiabilidad de la información, se deben realizar diariamente y cuando se termine la jornada laboral, para evitar perdida de información o copias incompletas.

Para la restauración de información es importante que se envíe una petición a la persona responsable para que se encargue de identificar la información y realice el respectivo procedimiento de restablecimiento con todos los protocolos de seguridad y el plan de procedimiento.

❖ **Descripción de actividades.**

- Copias de seguridad bases de datos y configuración equipos informaticos.

Ejecución de las copias de seguridad.

Tabla Solicitud copias de seguridad.

ACTIVIDAD	RESPONSABLE	PUNTO DE CONTROL	REGISTRO
Identificar los sistemas de información con los que cuenta la entidad**.**	Oficina de sistemas	Políticas de seguridad	Plan copias de seguridad.
Elaborar el plan de backup, teniendo en cuenta la cantidad y el peso de la información, determinar el tiempo y los responsables.	Líder Departamento de copias de seguridad de la oficina de sistemas.		Plan copias de seguridad.
Seleccionar al personal encargado de realizar las copias de seguridad.	Líder departamento de copias de seguridad de la oficina de sistemas.	Plan copias de seguridad	Plan copia de seguridad.
Programar las copias de seguridad con los respectivos tiempos de ejecución y cronogramas.	Responsable copias de seguridad y líder del departamento.	Cronograma	Plan copias de seguridad.
Realizar las copias de seguridad según cronograma de ejecución.	Responsable copias de seguridad.	Cronograma	Plan copias de seguridad.
Verificar si se realizó correctamente el backup	Responsable copias de seguridad	Plan copias de seguridad	Plan copias de seguridad
Si se encuentran fallas, realizar las respectivas correcciones y realizar de nuevo la copia de seguridad.	Responsable copias de seguridad.	Plan copias de seguridad	Plan copias de seguridad
Entrega de copia de seguridad a la persona encargada de guardar el backup en un sitio adecuado.	Responsable almacenamiento.	Plan copias de seguridad.	Plan copias de seguridad.
Verificación de las copias de seguridad.	Responsable almacenamiento.	Plan copias de seguridad	Plan copias de seguridad
Si se encuentran errores se deben informar al responsable de realizar las copias de seguridad, y realizar	Responsable almacenamiento.	Plan copias de seguridad	Plan copias de seguridad

de nuevo el proceso de backup.			
Almacenamiento de las copias de seguridad.	Responsable almacenamiento.	Plan copias de seguridad.	Plan copias de seguridad.
Verificación del correcto almacenamiento de la información	Responsable almacenamiento	Plan copias de seguridad	Plan copias de seguridad
Si presenta errores corregirlos y realizar de nuevo el proceso de almacenamiento	Responsable almacenamiento	Plan copias de seguridad	Plan copias de seguridad
Diligenciar formato de recepción de información	Responsable de almacenamiento	Políticas de seguridad	Plan copias de seguridad

Fuente: Autor.

- Copias de seguridad información de equipos de cómputo.

Tabla 11 Procedimiento copia de seguridad.

ACTIVIDAD	RESPONSABLE	PUNTO DE CONTROL	REGISTRO
Solicitud de backup de información por parte de los usuarios.		Plan copia de información.	Plan copia de información
Verificación de la solicitud de copia de información si es correcta.	Líder departamento de copias de seguridad de la oficina de sistemas	Plan copia de información	Plan copia de información
Programar copia de seguridad, teniendo en cuenta el tamaño de la información.	Líder departamento de copias de seguridad de la oficina de sistemas	Cronograma	Plan copia de información
Seleccionar al personal encargado de realizar las copias de seguridad.	Líder departamento de copias de seguridad de la oficina de sistemas.	Plan copias de seguridad	Plan copia de seguridad.
Realizar las copias de seguridad según cronograma de ejecución.	Responsable copias de seguridad.	Cronograma	Plan copias de seguridad.
Verificar si se realizó correctamente el backup	Responsable copias de seguridad	Plan copias de seguridad	Plan copias de seguridad
Si se encuentran fallas, realizar las respectivas correcciones y realizar	Responsable copias de seguridad.	Plan copias de seguridad	Plan copias de seguridad

de nuevo la copia de seguridad.			
Entrega de copia de seguridad a la persona encargada de guardar el backup en un sitio adecuado.	Responsable almacenamiento.	Plan copias de seguridad.	Plan copias de seguridad.
Verificación de las copias de seguridad.	Responsable almacenamiento.	Plan copias de seguridad	Plan copias de seguridad
Si se encuentran errores se deben informar al responsable de realizar las copias de seguridad, y realizar de nuevo el proceso de backup.	Responsable almacenamiento.	Plan copias de seguridad	Plan copias de seguridad
Almacenamiento de las copias de seguridad.	Responsable almacenamiento.	Plan copias de seguridad.	Plan copias de seguridad.
Verificación del correcto almacenamiento de la información	Responsable almacenamiento	Plan copias de seguridad	Plan copias de seguridad
Si presenta errores corregirlos y realizar de nuevo el proceso de almacenamiento	Responsable almacenamiento	Plan copias de seguridad	Plan copias de seguridad
Diligenciar formato de recepción de información	Responsable de almacenamiento	Políticas de seguridad	Plan copias de seguridad

Fuente: Autor.

- Restauración copias de seguridad

Tabla 12 Restauración copias de seguridad.

ACTIVIDAD	RESPONSABLE	PUNTO DE CONTROL	REGISTRO
Solicitud restauración de copias de seguridad por escrito mediante correo.		Políticas de seguridad.	Plan copias de seguridad.
Verificación de la solicitud de copia de seguridad.	Líder departamento de copias de seguridad de la oficina de sistemas	Políticas de seguridad.	Plan copias de seguridad.

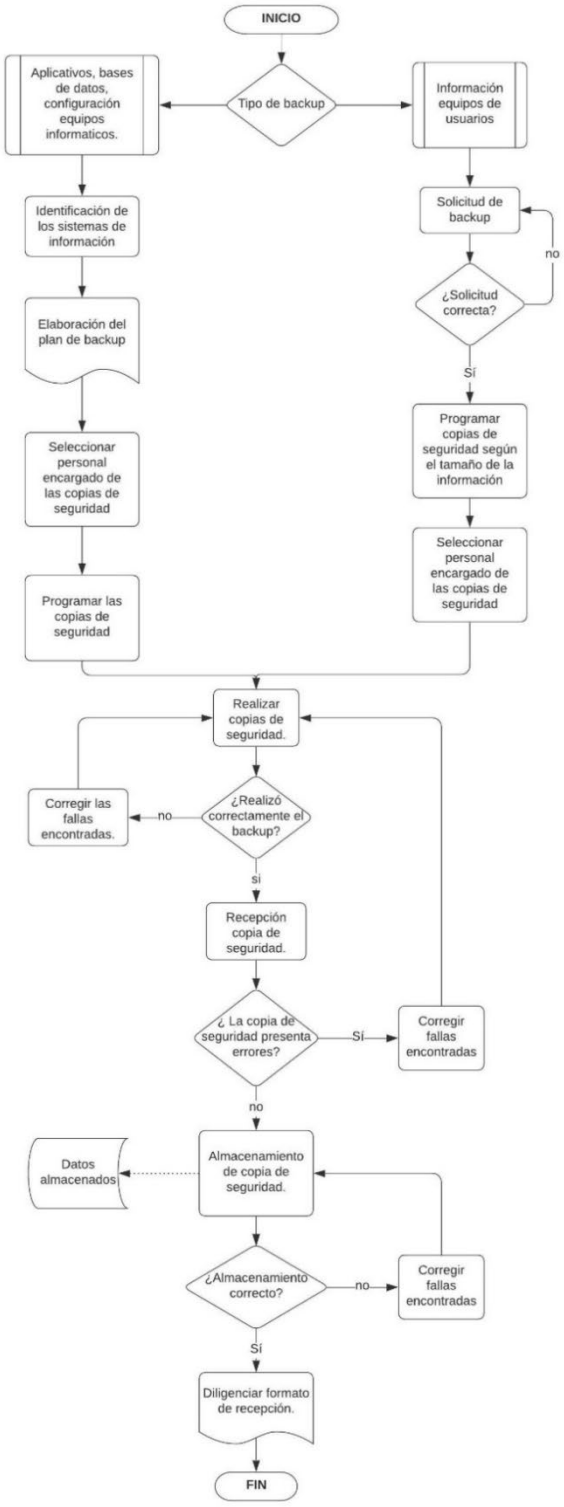
Si la solicitud es correcta se autoriza la restauración	Líder departamento de copias de seguridad de la oficina de sistemas	Políticas de seguridad.	Plan copias de seguridad.
Identificación de la copia de seguridad teniendo en cuenta la solicitud.	Responsable almacenamiento.	Plan copias de seguridad.	Plan copias de seguridad.
Restaurar la copia de seguridad en frío en las bases de datos o equipos informáticos.	Responsable copias de seguridad.	Políticas de seguridad.	Plan copias de seguridad.
Verificación de la correcta restauración de la copia de seguridad.	Responsable copias de seguridad.	Plan copias de seguridad.	Plan copias de seguridad.
Si se presenta errores en la restauración, corregir fallas y realizar de nuevo la restauración	Responsable copias de seguridad.	Plan copias de seguridad.	Plan copias de seguridad
Diligenciar formato de restauración de información.	Responsable copias de seguridad.	Políticas de seguridad.	Plan copias de seguridad.

Fuente: Autor

- Flujograma de proceso

Se realiza el flujograma de proceso correspondiente a las copias de seguridad de las bases de datos, aplicativos y configuración de equipo informáticos.

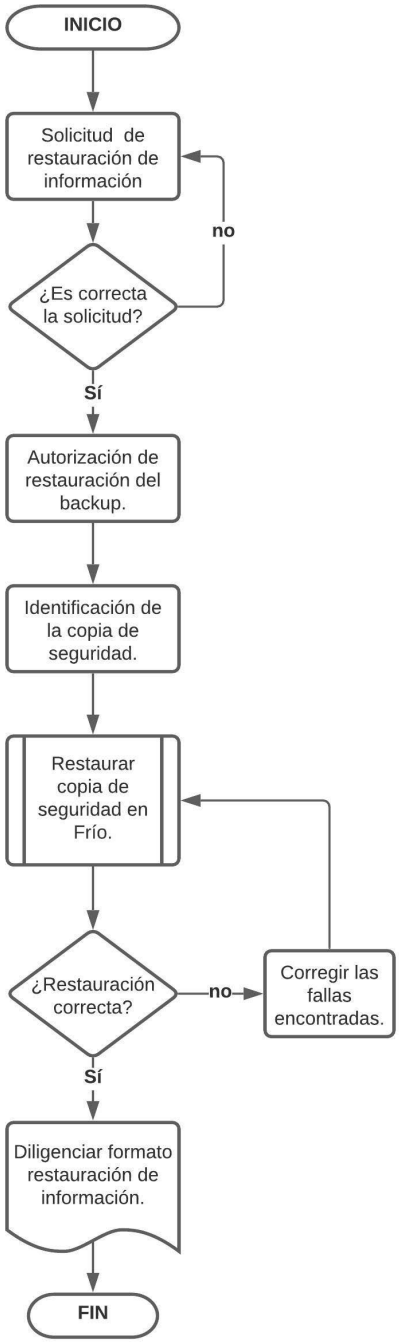
Figura 3 Flujograma copias de seguridad.



Fuente: Autor

Se puede de igual manera encontrar el flujograma de proceso de restauración de información.

Figura 4 Flujograma restauración copias de seguridad.



Fuente: Autor

10.3.5.2. Mantenimiento preventivo equipos técnologicos.

Es importante el mantenimiento preventivo para corregir posibles fallas antes de que ocurran problemas mayores, la limpieza de los equipos de cómputo para aumentar la vida útil de los mismos y cumplan con su ciclo de vida, igualmente, el software para que funcione correctamente, se deben seguir los diferentes lineamientos para que se cumplan los objetivos identificados.

- Objetivos:

Identificar los procedimientos que se deben seguir para realizar los mantenimientos preventivos en la entidad, además, de los cuidados y factores claves para aumentar la expectativa de vida de los equipos informáticos.

- Alcance

Se debe realizar el mantenimiento a los equipos informáticos de la entidad, desde la identificación de los equipos y tipo de mantenimiento, hasta la entrega final de los equipos.

- Base legal

Políticas de seguridad.

- Condiciones generales

Es importante mantener el inventario actualizado de los activos informáticos de la entidad y sobre todo los equipos en los cuales se realiza el mantenimiento preventivo, para que las programaciones sean optimas y se cumpla con los tiempos estipulados para dicha labor.

Se deben implementar las listas de chequeo antes de iniciar las labores para identificar el tipo de mantenimiento que necesita el equipo o si la falla es más compleja donde necesite cambio de partes o el equipo.

❖ Descripción de actividades

Tabla 13 Procedimiento mantenimiento equipos.

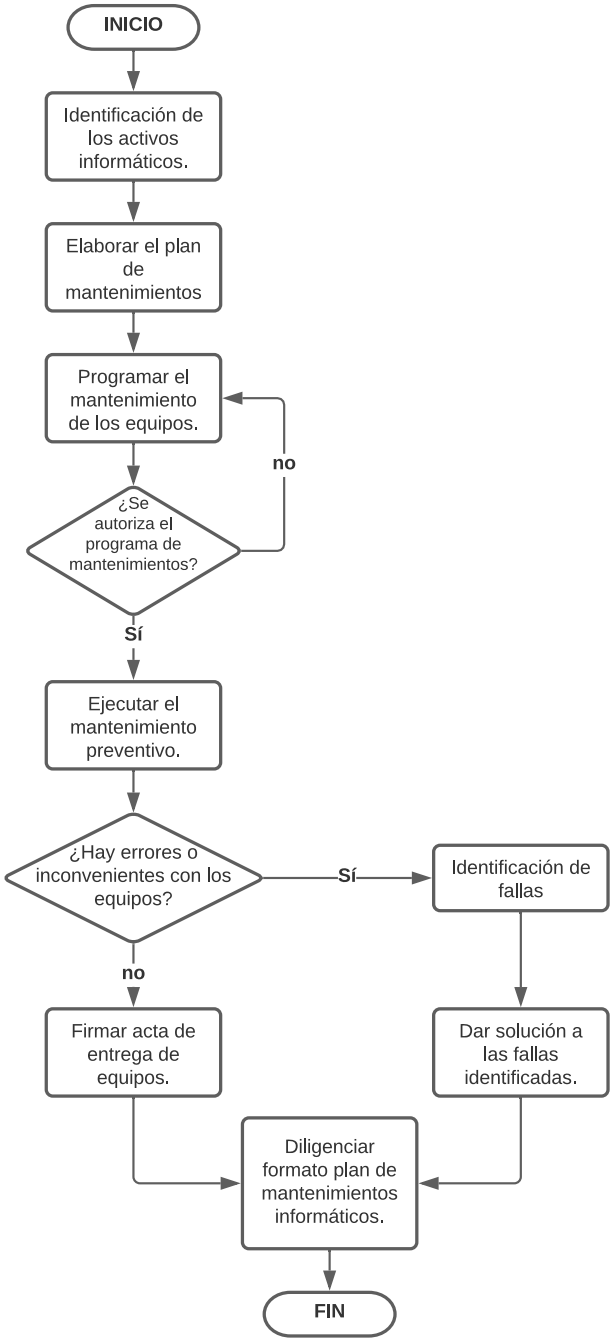
ACTIVIDAD	RESPONSABLE	PUNTO DE CONTROL	REGISTRO
Identificar los activos informáticos a los cuales se realizará el mantenimiento preventivo.	Líder departamento de sistemas.	Políticas de seguridad.	Políticas de seguridad.
Elaborar el plan de mantenimiento de equipos informáticos.	Líder departamento de mantenimientos.	Políticas de seguridad.	Políticas de seguridad.
Programar el mantenimiento de los equipos informáticos.	Líder departamento de mantenimientos.	Políticas de seguridad.	Plan de mantenimiento.
Autorizar el programa de mantenimientos en la entidad.	Líder departamento de sistemas.	Políticas de seguridad.	Plan mantenimiento.
Verificar la autorización del programa de mantenimientos.	Líder departamento de mantenimientos.	Políticas de seguridad.	Plan de mantenimiento.
Ejecutar el mantenimiento preventivo en la entidad teniendo en cuenta el programa de mantenimientos.	Personal responsable del mantenimiento preventivo.	Plan mantenimiento.	Plan mantenimiento.
Verificar si se presentaron errores, problemas o incidentes con los equipos informáticos.	Personal responsable del mantenimiento preventivo	Plan mantenimiento.	Plan mantenimiento.
Si hay inconvenientes, identificar la falla que se presenta.	Personal responsable del mantenimiento preventivo	Plan mantenimiento.	Plan mantenimiento.
Dar solución efectiva a la falla que se presenta.	Personal responsable del mantenimiento preventivo	Plan mantenimiento.	Plan mantenimiento.
Si no se presenta inconvenientes, se firma el acta de entrega de los equipos.	Personal responsable del mantenimiento preventivo	Políticas de seguridad.	Plan mantenimiento.
Se diligencia el formato del plan de mantenimiento informáticos.	Líder departamento de mantenimientos.	Políticas de seguridad.	Plan de mantenimiento.

Fuente: Autor.

❖ Flujograma de procesos

Se realiza el flujograma de procesos correspondiente al mantenimiento preventivo equipos tecnológicos.

Tabla 14 Flujograma mantenimiento de equipo.



Fuente: Autor

10.3.5.3. Adquisición y gestión de los activos de software.

❖ Objetivos:

Establecer los procedimientos para la gestión en todo el ciclo de vida y adquisición de software cumpliendo con los distintos estándares de calidad y seguridad.

❖ Alcance

La gestión y adquisición de software inicia con la fase de planeación en donde se identifica la necesidad por cada una de las áreas, cubre de igual manera la fase adquisición, implementación, administración y como último, la fase de retiro o desinstalación de los activos cuando cumplan con el ciclo de vida.

❖ Base legal

Políticas de seguridad.

❖ Condiciones generales

La gestión de los activos de software está ligada directamente con las políticas de seguridad, cumpliendo con los aspectos legales de funcionamiento y las etapas propuestas como la adquisición, implementación, administración y por último, la eliminación y desinstalación correcta de este.

La custodia y responsabilidad de los medios de instalación corresponde a la oficina de sistemas, son directamente responsables por uso indebido de los medios o perdida; se debe contar con una copia de seguridad de los medios de instalación.

❖ Descripción de actividades

Tabla 15 Adquisición de activos.

ACTIVIDADES	RESPONSABLES	PUNTO DE CONTROL	REGISTRO
Identificación de las necesidades de software en las diferentes áreas de la entidad; el software puede ser de uso propietario o libre.	Usuarios de la entidad, oficina de sistemas y líder departamento de software.	Políticas de seguridad.	Comunicaciones internas de necesidad de software.
Evaluar las funcionalidades, costo y beneficio del software; tanto para uso propietario o libre.	Líder departamento de software.	Políticas de seguridad.	Comunicaciones internas.
En el caso de que la información de la necesidad no sea suficiente, se identificará información adicional o nuevas alternativas.	Usuarios de la entidad, oficina de sistemas y líder departamento de software.	Políticas de seguridad.	Información de soluciones.
Seleccionar el software que cumpla con las condiciones.	Líder departamento de software.	Políticas de seguridad.	Políticas de seguridad.
Verificar si la solución del software es pertinente.	Líder departamento de software.	Políticas de seguridad.	Políticas de seguridad.
Una vez seleccionado el software a utilizar, se debe determinar si hay disponibilidad, de igual manera diligenciar la ficha técnica de producto de software.	Líder departamento de software.	Políticas de seguridad	Ficha técnica de producto de software.
Verificar la disponibilidad del software.	Líder departamento de software.	Políticas de seguridad	Ficha técnica de producto de software.
Es importante determinar qué tipo de software se va a implementar, si es software propietario o software libre.	Líder departamento de software.	Políticas de seguridad	Ficha técnica de producto de software.
Se debe evaluar el software libre como el tipo de licenciamiento que concede el propietario, la cantidad de licencias libres y las	Líder departamento de software.	Políticas de seguridad	Ficha técnica de producto de software.

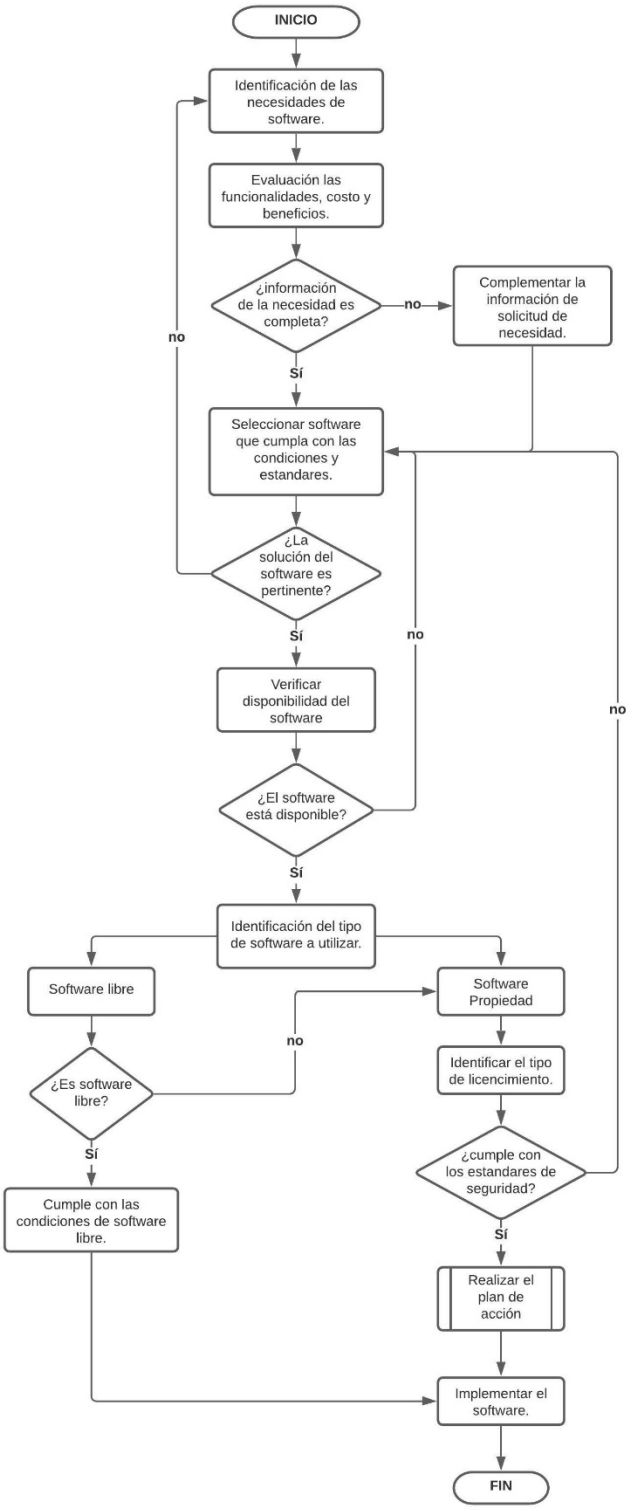
implicaciones al instalarlo.			
Verificar si cumple con las características de software libre.	Líder departamento de software.	Políticas de seguridad	Ficha técnica de producto de software.
Identificación del tipo de licenciamiento que se utilizará para el uso del software de propiedad.	Líder departamento de software.	Políticas de seguridad	Ficha técnica de producto de software.
Verificar si el tipo de licenciamiento cumple con los estándares de calidad y seguridad.	Líder departamento de software.	Políticas de seguridad	Ficha técnica de producto de software.
Realizar el plan de acción para gestión de los recursos para la implementación del software.	Líder departamento de software.	Políticas de seguridad	Ficha técnica de producto de software, concepto técnico
Implementación del software en las áreas donde se presente la necesidad.	Líder departamento de software.	Políticas de seguridad.	Políticas de seguridad.

Fuente: Autor

❖ Flujograma de proceso

Se realiza el flujograma de proceso correspondiente a la adquisición de e implementación del software.

Figura 5 Flujograma adquisición de activos.



Fuente: Autor

10.3.5.4. Gestión de incidentes de seguridad

La atención de incidentes de seguridad se encarga de brindar acompañamiento para el tratamiento de los riesgos que se puedan presentar con las tecnologías informáticas y que atente con los principios de la seguridad de la información.

Asegura todo el flujo desde la identificación hasta el cierre, además, teniendo en cuenta la valoración y las acciones para mitigar los riesgos presentados.

- Objetivos:

Identificar, registrar y mitigar los riesgos, aplicando los procedimientos de gestión de incidentes de seguridad.

- Alcance

Abarca las fases de procesamiento de riesgos, desde la identificación hasta el cierre de las incidencias para mitigar los riesgos y dar solución a los incidentes de seguridad.

- Base legal

Políticas de seguridad de la información.

- Condiciones generales

Para la identificación de los riesgos, además, de la correcta gestión de los incidentes se debe tener en cuenta las fases como se observa en la siguiente figura 1.

Figura 6 Gestión de incidentes de seguridad.

Fuente: Autor

- Fase 1 identificación

En esta fase se identifica los riesgos y se toma los incidentes de seguridad reportados, teniendo en cuenta las consecuencias, causas e impactos negativos en la organización que, además, puedan afectar negativamente los pilares de la seguridad informática.

Se deben tener en cuenta los siguientes datos para la identificación de los riesgos según las incidencias reportadas.

Tabla 16 Datos identificación de incidentes de seguridad.

CAMPO	DESCRIPCIÓN
ID	Consecutivo de incidentes reportados.
Fecha de registros	Fecha de registro de los incidentes de seguridad.
Tipo de Riesgo	Identificación del tipo riesgo en el que está catalogado el incidente identificado.
Descripción del riesgo.	Descripción detallada del riesgo identificado, además, de las afectaciones en la entidad.

Causas de ocurrencias.	Se debe identificar las causas de la ocurrencia de los riesgos identificados.
Consecuencias potenciales.	Qué consecuencias trae en la organización y que afectaciones a traído.
¿Los controles ya implementados son efectivos.?	Se debe identificar si los controles ya implementados son efectivos en tratar la incidencia, si no es así se debe continuar con la FASE 2. Es importante documentar el control efectivo o el control que no es efectivo.

Fuente: Autor

- Fase 2 medidas de control.

Se debe realizar un estudio detallado de los riesgos identificados en las incidencias reportadas, además, del análisis de las causas que llevaron a que se presentará esta incidencia de seguridad, es importante que el personal de seguridad primero analice el control ya implementado, si no funciona es correcto realizar un cambio para mitigar la incidencia lo más antes posible, implementar las correctivas y evitar así consecuencias mayores en la entidad.

De igual manera, se debe realizar las configuraciones pertinentes y los cambios necesarios para evitar la pérdida de información en la organización y realizar un análisis en los sectores por si las consecuencias del incidente son mayores y así, poner en funcionamiento el plan de continuidad del negocio para minimizar el impacto en los objetivos misionales de la entidad.

- Fase 3 seguimiento

Para la fase 3, se debe realizar un seguimiento al incidente, para determinar si afecta negativamente a los sistemas de seguridad o el mecanismo ya implementado pudo contrarrestar el ataque, sino es posible el control del riesgo por parte del mecanismo se debe realizar la verificación de funcionamiento y efectividad. Las correcciones se deben implementar en el menor tiempo posible o ejecutar el plan de continuidad si hay perdida de gestión de los servicios.

❖ Descripción de actividades

Tabla 17 Atención de incidentes de seguridad.

ACTIVIDAD	RESPONSABLES	PUNTO DE CONTROL	REGISTRO
Recibir los reportes de incidentes de seguridad.	Líder departamento de seguridad.	Políticas de seguridad	Matriz gestión de riesgos.
Identificar el riesgo al que está asociado el incidente de seguridad.	Líder departamento de seguridad.	Políticas de seguridad	Matriz gestión de riesgos.
Verificar la identificación del riesgo	Líder departamento de seguridad.	Políticas de seguridad	Matriz gestión de riesgos.
Asignar un ID al riesgo identificado.	Líder departamento de seguridad.	Políticas de seguridad	Matriz gestión de riesgos.
Identificar las causas de ocurrencia del incidente de seguridad.	Equipo de seguridad	Políticas de seguridad	Políticas de seguridad
Verificar la causa de ocurrencia del incidente.	Equipo de seguridad	Políticas de seguridad	Matriz gestión de riesgos.
Identificar los controles ya implementados para mitigación del riesgo.	Equipo de seguridad	Políticas de seguridad	Políticas de seguridad
Validar si los controles aplicados son efectivos ante la incidencia de seguridad.	Equipo de seguridad	Políticas de seguridad	Políticas de seguridad
Definir los planes de mitigación del riesgo.	Equipo de seguridad	Políticas de seguridad	Políticas de seguridad
Validar si los planes de mitigación son efectivos.	Equipo de seguridad	Políticas de seguridad	Políticas de seguridad
Autorizar el plan de mitigación de riesgos.	Líder departamento de seguridad.	Políticas de seguridad	Políticas de seguridad
Implementar el plan de mitigación de riesgos.	Equipo de seguridad	Políticas de seguridad	Políticas de seguridad
Realizar seguimiento a la efectividad del plan de mitigación de riesgos.	Equipo de seguridad	Políticas de seguridad	Formato de valoración efectividad de controles.
Verificar el plan de mitigación de riesgos.	Equipo de seguridad	Políticas de seguridad	Formato de valoración efectividad de controles.
Registrar el plan de mitigación de riesgos	Equipo de seguridad	Políticas de seguridad	Políticas de seguridad.

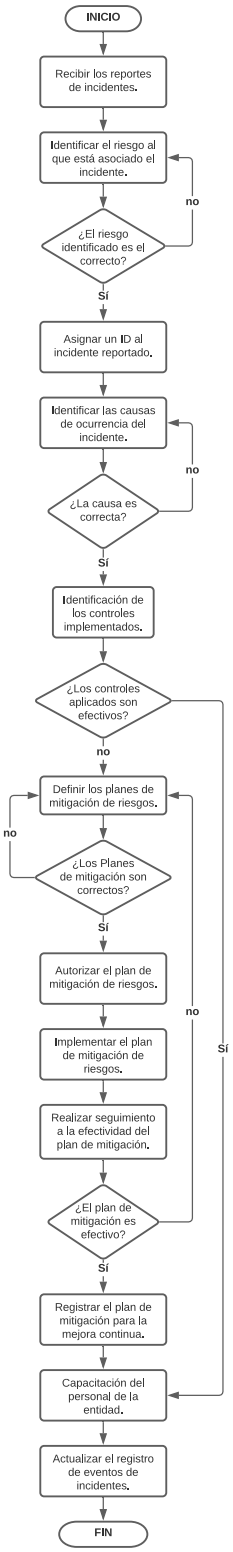
para la actualización de los controles y mejora continua de los procesos.			
Capacitación al personal de la entidad.	Equipo de seguridad	Políticas de seguridad	Políticas de seguridad.
Actualizar el registro de eventos con el ID del incidente y el plan de mitigación de riesgos.	Equipo de seguridad	Políticas de seguridad	Registro de eventos de seguridad.

Fuente: Autor.

Flujograma de proceso

Se realiza el flujograma de proceso correspondiente a la gestión de incidentes de seguridad.

Tabla 18 Flujograma atención de incidentes de seguridad.



Fuente: Autor

10.3.6. PLAN DE CONTINUIDAD DEL NEGOCIO

10.3.6.1. Introducción

Existe una alta probabilidad de la ocurrencia de amenazas externas que pueden inferir en la prestación de los servicios por parte de la entidad y atenten contra los objetivos y la misión, es importante que se creen alternativas que permitan mantener dichos servicios siempre disponibles.

Es indispensable que se implemente un plan de continuidad del negocio que se encargue de cubrir aquellos servicios que son indispensables para la entidad, esto realiza un análisis a los riesgos y determina que activos son dispensables y su disponibilidad afecta negativamente la entidad.

10.3.6.2. Objetivo

Establecer los lineamientos del plan de continuidad del negocio que se deben seguir al momento de que ocurra un evento donde se interrumpa los servicios de la entidad, con el fin de continuar con los servicios activos.

10.3.6.3. Alcance

Se inicia con la detección de los distintos activos que presentan riesgos y que son indispensables para la continuidad de los servicios en la entidad, es importante determinar el impacto y la valoración; finaliza implementado los mecanismos para el plan de continuidad del negocio.

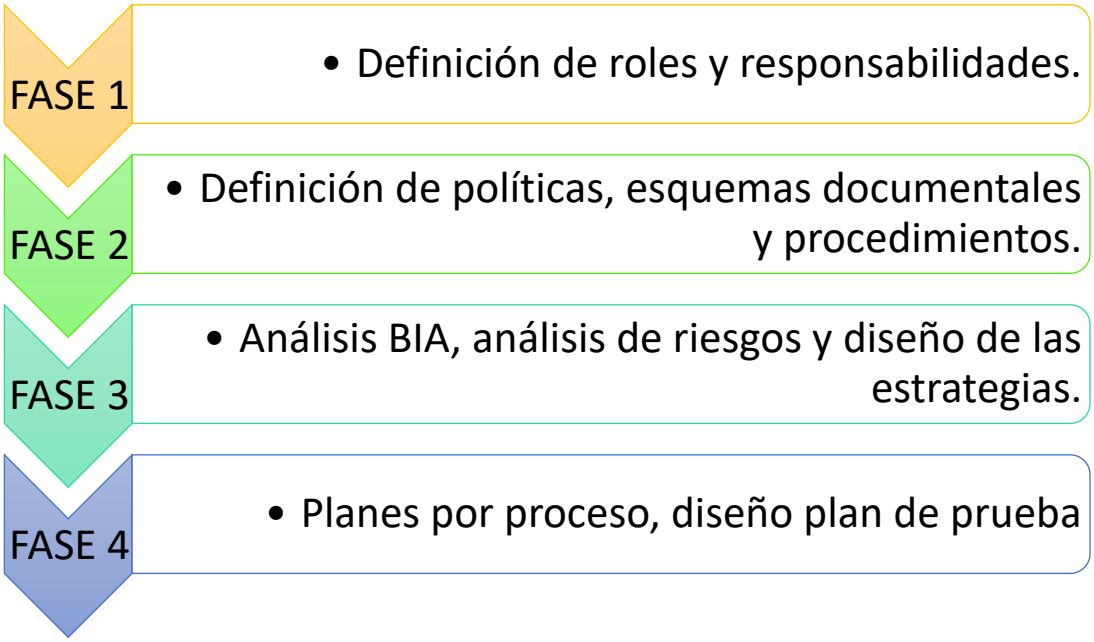
10.3.6.4. Marco legal

NTC/ISO 22301:2012: Norma internacional para el manejo y elaboración del plan de continuidad del negocio.

10.3.6.5. Plan de continuidad del negocio

En el plan de continuidad del negocio se busca establecer los lineamientos y procesos para la continuar con los servicios durante la ocurrencia de eventos que atenten contra la integridad de los activos de comunicación e interrumpa los servicios que presta la entidad, se busca respaldar dichos servicios para que no exista una interrupción prologada, se deben establecer los tiempos máximos de aceptación, además, los procesos para la activación del plan; para el desarrollo de el plan se tiene en cuenta la norma ISO 22302:2012 , para el desarrollo del plan de continuidad del negocio se tendrán en cuenta 4 FASES como se puede observar en la figura.

Tabla 19 Fases plan de continuidad.



Fuente: Autor

10.3.6.6. Roles y responsabilidades

Tabla 20 Roles y responsabilidades plan de continuidad del negocio.

ROL	RESPONSABLES	MECANISMOS
Asesor, coordinador plan de continuidad del negocio	• Jefe oficia de sistemas • Comité de riesgo e implementación plan de continuidad	Para la documentación del plan de continuidad se realiza mesas de trabajo, donde se realiza: • Análisis de la información en las reuniones. • Metodologías de los sistemas de riesgos. • Inclusión en el plan de acción anual
Aprobación del plan de continuidad del negocio y socialización	Comité de riesgo e implementación plan de continuidad	• Sesiones del comité. • Cronogramas de socialización. • Simulacros de ejecución del plan.
Activación del plan de emergencia	Comité de riesgo e implementación plan de continuidad	• Procedimiento de implementación. • Sistema de comunicación de emergencias.
Restablecer prestación de los servicios de la entidad	• Comité de riesgo. • Directivos. • Jefe departamento de sistemas.	• Reunión comité de análisis de riesgos. • Análisis y pruebas. • Verificación de resultados. • Autorización implementación de mecanismos de continuidad.

Fuente: Autor

10.3.6.7. Política de continuidad del negocio

Para la entidad QWERTY S.A. es indispensable que se estipule el tiempo óptimo para que todo el personal interesado tenga acceso a los servicios después de que ocurra algún evento adverso y que afecte las operaciones; es importante cumplir con los diferentes lineamientos estipulado en las siguientes políticas.

- Es indispensable para la entidad el restablecimiento oportuno de los servicios catalogados como críticos y que son importantes para la prestación de los servicios misionales.

- Es importante que todo el personal tenga conocimiento sobre el plan de continuidad del negocio, además, de los procedimientos definidos, los roles y responsabilidades ya establecidas para el plan, para esto se implementan capacitaciones de los temas.
- Se deben establecer los distintos métodos de comunicación tantos internos como externos, deben ser efectivos y comprobado su funcionamiento en simulacros.
- Todas las dependencias de la entidad deben ejecutar las etapas del plan de continuidad, siendo coordinadas por el departamento encargado de la oficina de sistemas.
- Los líderes de las diferentes áreas de la entidad deben designar un representante que será parte del comité, la principal función es apoyar las actividades del plan de continuidad en las dependencias de las que hace parte.
- Es importante que cada año se realicen simulacros para la ejecución del plan de continuidad del negocio para evaluar su funcionamiento y determinar las mejoras o los cambios a realizar.
- Se deben cumplir con los márgenes de tiempo en la recuperación de los servicios catalogados como críticos para la entidad.
- Para los servicios que sean contratados con terceros, estos deben tener implementado un plan de continuidad del negocio, por este motivo, es importante que el interventor del proyecto realice la verificación de los servicios.
- Los planes de contingencia deben estar siempre actualizados, desde el ámbito de seguridad hasta el ámbito de configuración y respaldo de información; es indispensable que se asegure la continuidad de la seguridad y los cambios se realicen a los dos sistemas.

10.3.6.8. Entendimiento de la organización

En la fase de recopilación de información se revisa los procedimientos de los procesos documentados, análisis de los activos dispensables para el cumplimiento de los objetivos de la entidad, al realizar la selección de los activos se implementan entrevistas con los responsables de dichos activos, para obtener información del manejo e importancia, para proceder a realizar el impacto de negocio BIA y análisis de riesgos.

La entidad QWERTY S.A. define los siguientes procesos teniendo en cuenta su mapa organizacional.

Figura 7 Mapa de procesos.

Fuente: Autor

10.3.6.9. Análisis de impacto de negocio

❖ Identificación de funciones y procesos

Se determina los productos y procesos que garantizan la continuidad del negocio y que son indispensables para la entidad, aparte de esto se debe implementar los

tiempos de recuperación óptimos de los procesos después de que ocurra una amenaza.

En el BIA (Business Impact Analysis) se determina los recursos para el respaldo de la continuidad, su criticidad, su impacto, RTO (Recovery Time Objective), RPO (Recovery Point Objective).

Los procesos determinados para respaldo y que aseguren los procesos estratégicos son

Procesos misionales:

- Infraestructura
- Desarrollo
- Soporte

Procesos de apoyo

- Administrativos
- Directivos
- Operativos.

❖ Evaluación de impactos operacionales.

Se realiza una evaluación de los impactos de operación de los activos considerados importantes y que se necesitan para el cumplimiento de los objetivos de la entidad.

Se tienen los siguientes criterios para evaluación.

- Nivel A: Operación que es considerada critica para el negocio.
- Nivel B: Operación integral del negocio, no puede operar normalmente pero no es crítica.
- Nivel C: no es una parte integral de la entidad.

Tabla 21 Evaluación de impacto de operación.

Categoría	Proceso	Nivel	Tolerancia (horas)	Descripción
Aplicaciones	Nómina y facturación	A	2 hr	Aplicación de nómina y facturación de la entidad
WEB	Página web	C	4 hr	Presentación de la entidad
Recurso humano	Personal de la entidad	A	2 hr	Personal que labora para la entidad en distintos cargos.
Bases de datos	SQL de nómina	A	2 hr	Almacenamiento SQL.
Equipos informáticos	Servidores, Equipos de cómputo	A	3 hr	Equipos de cómputo y servidores de la entidad.
Instalaciones	Edificio de la entidad	A	1 hr	Edificio principal de la entidad.
Proveedores	Correo electrónico	B	2 hr	Sistema de comunicación de mensajería interna.
Sistemas de almacenamiento	Servidores de FTP	A	3 hr	Sistemas de almacenamiento de información FTP.
Puntos de acceso	LAN / WLAN	A	1 hr	Puntos de acceso a la red corporativa de la entidad.
Sistemas de seguridad	firewall	A	1 hr	Sistemas de seguridad firewall de la entidad.
Centro de datos.	Centro de datos.	A	1 hr	Centro de datos de telecomunicaciones de la entidad.

Fuente: Autor

- Identificación de procesos críticos.

Se identifican los procesos críticos para la entidad teniendo en cuenta la clasificación del impacto operacional.

Tabla 22 Procesos críticos y de alto impacto.

Categoría	Proceso	Nivel	Tolerancia (horas)	Descripción
Aplicaciones	Nómina y facturación	A	2 hr	Aplicación de nómina y facturación de la entidad
Recurso humano	Personal de la entidad	A	2 hr	Personal que labora para la entidad en distintos cargos.
Bases de datos	SQL de nómina	A	2 hr	Almacenamiento SQL.
Equipos informáticos	Servidores, Equipos de cómputo	A	3 hr	Equipos de cómputo y servidores de la entidad.
Instalaciones	Edificio de la entidad	A	1 hr	Edificio principal de la entidad.
Sistemas de almacenamiento	Servidores de FTP	A	3 hr	Sistemas de almacenamiento de información FTP.
Puntos de acceso	LAN / WLAN	A	1 hr	Puntos de acceso a la red corporativa de la entidad.

Sistemas de seguridad	firewall	A	1 hr	Sistemas de seguridad firewall de la entidad.
Centro de datos.	Centro de datos.	A	1 hr	Centro de datos de telecomunicaciones de la entidad.

Fuente: Autor.

❖ Tiempos de recuperación

Se determina según procesos críticos, los tiempos máximos de tolerancia.

Tabla 23 Tiempos máximos de tolerancia.

Categoría	Procesos críticos.	MTD	Prioridad de recuperación
Aplicaciones	Nómina y facturación	1 días	2
WEB	Página web	3 días	4
Recurso humano	Personal de la entidad	0.5 días	1
Bases de datos	SQL de nómina	1 días	2
Equipos informáticos	Servidores, Equipos de cómputo	2 días	3
Instalaciones	Edificio de la entidad	0.5 días	1
Proveedores	Correo electrónico	3 días	4
Sistemas de almacenamiento	Servidores de FTP	1 día	2
Puntos de acceso	LAN / WLAN	1 día	2
Sistemas de seguridad	firewall	0.5 días	1
Centro de datos.	Centro de datos.	0.5 días	1

Fuente: Autor

❖ Identificación de recursos:

Se realiza la identificación de los recursos según su categorización y procesos críticos.

Tabla 24 Identificación de recursos.

Categoría	Procesos críticos	Identificación de recursos.
Aplicaciones	Nómina y facturación	Sistema encargado de administrar la nómina de la entidad, los procesos de facturación y pagos.
WEB	Página web	Página web donde se da a conocer la imagen de la entidad.

Recurso humano	Personal de la entidad	Personal administrativo, directivo y técnico de la entidad.
Bases de datos	SQL de nómina	Bases de datos de nómina de la entidad.
Equipos informáticos	Servidores, Equipos de cómputo	Servidores de impresión, DHCP, de aplicaciones y bases de datos.
Instalaciones	Edificio de la entidad	Instalaciones principales de la entidad.
Proveedores	Correo electrónico	Correo corporativo de la entidad.
Sistemas de almacenamiento	Servidores de FTP	Servidor de almacenamiento de FTP de información y backup.
Puntos de acceso	LAN / WLAN	Puntos de conexión a la red corporativa de la entidad.
Sistemas de seguridad	firewall	Reglas de configuración de entrada y salida de conexiones.
Centro de datos.	Centro de datos.	Sistema de telecomunicaciones, control de servidores, sistemas de bases de datos etc.

Fuente: Autor

❖ Disposición de los tiempos rto/rpo

Se realiza la evaluación de tolerancia de los procesos según RTO y RPO, además, se aplica el WTR que es el tiempo requerido para completar el trabajo.

Tabla 25 Evaluación de tolerancia según RTO y RPO.

Categoría	Procesos críticos	Identificación de recursos.	Tiempo de Recuperación Objetivo RTO	Punto de Recuperación Objetivo RPO	Tiempo de Recuperación de Trabajo WTR
Aplicaciones	Nómina y facturación	Sistema encargado de administrar la nómina de la entidad, los procesos de facturación y pagos.	7 hr	5 hr	19 hr
WEB	Página web	Página web donde se da a conocer la imagen de la entidad.	7 hr	1 día	2 días
Recurso humano	Personal de la entidad	Personal administrativo, directivo y técnico de la entidad.	12 hr	6 hr	6 hr

Bases de datos	SQL de nómina	Bases de datos de nómina de la entidad.	7 hr	5 hr	19 hr
Equipos informáticos	Servidores, Equipos de cómputo	Servidores de impresión, DHCP, de aplicaciones y bases de datos.	7 hr	1 día	1 día
Instalaciones	Edificio de la entidad	Instalaciones principales de la entidad.	12 hr	6 hr	6 hr
Proveedores	Correo electrónico	Correo corporativo de la entidad.	7 hr	1 día	2 días
Sistemas de almacenamiento	Servidores de FTP	Servidor de almacenamiento de FTP de información y backup.	7 hr	5 hr	19 hr
Puntos de acceso	LAN / WLAN	Puntos de conexión a la red corporativa de la entidad.	7 hr	5 hr	19 hr
Sistemas de seguridad	firewall	Reglas de configuración de entrada y salida de conexiones.	12 hr	6 hr	6 hr
Centro de datos.	Centro de datos.	Sistema de telecomunicaciones, control de servidores, sistemas de bases de datos etc.	12 hr	6 hr	6 hr

Fuente: Autor

❖ Identificación de procesos alternos

Se identifican los procesos alternos para implementar en los procesos identificados como críticos.

Tabla 26 Procesos alternos de ejecución.

Categoría	Procesos críticos	Escenarios de interrupción	Amenazas	Procesos Alternativos operativos
Aplicaciones	Nómina y facturación	No hay disponibilidad de los servicios tecnológicos.	• Fallas en el suministro eléctrico. • Desastres naturales. • Fallas en los dispositivos tecnológicos.	Activación de servidores alternos dependiendo de la falla pueden ser internos o externos a la sede.
WEB	Página web	No hay disponibilidad de proveedores o terceros.	• Fallas en el suministro eléctrico.	• Definir los proveedores alternos.

			• Desastres naturales. • Fallas en los dispositivos tecnológicos. • Pandemia. • No hay disponibilidad de los proveedores.	• Definir acuerdos de niveles de servicios.
Recurso humano	Personal de la entidad	No hay disponibilidad de colaboradores de la entidad.	• Huelgas del personal. • Pandemia. • Intoxicación de los colaboradores. • Indisposición por parte de los colaboradores.	• Teletrabajo. • Capacitación del personal. • Rotación del personal. • Documentación de los procedimientos con los que cuenta la entidad.
Bases de datos	SQL de nómina	No hay disponibilidad de los servicios tecnológicos.	• Fallas en el suministro eléctrico. • Desastres naturales. • Fallas en los dispositivos tecnológicos.	Activación de servidores alternos dependiendo de la falla pueden ser internos o externos a la sede.
Equipos informáticos	Servidores, Equipos de cómputo	No hay disponibilidad de los servicios tecnológicos.	• Fallas en el suministro eléctrico. • Desastres naturales. • Fallas en los dispositivos tecnológicos.	• Activación de servidores alternos dependiendo de la falla pueden ser internos o externos a la sede. • Procedimiento de implementación de contingencias.
Instalaciones	Edificio de la entidad	• Desastres naturales. • Actos de violencia. • Huelga.		• Teletrabajo. • Centro de trabajo alterno áreas administrativas.
Proveedores	Correo electrónico	No hay disponibilidad de proveedores o terceros.	• Fallas en el suministro eléctrico. • Desastres naturales.	• Definir los proveedores alternos.

			• Fallas en los dispositivos tecnológicos. • Pandemia • No hay disponibilidad de los proveedores.	• Definir acuerdos de niveles de servicios.
Sistemas de almacenamiento	Servidores de FTP	No hay disponibilidad de los servicios tecnológicos.	• Fallas en el suministro eléctrico. • Desastres naturales. • Fallas en los dispositivos tecnológicos.	Activación de servidores alternos dependiendo de la falla pueden ser internos o externos a la sede.
Puntos de acceso	LAN / WLAN	No hay disponibilidad de los servicios tecnológicos.	• Fallas en el suministro eléctrico. • Desastres naturales. • Fallas en los dispositivos tecnológicos.	Procedimiento de implementación de contingencias.
Sistemas de seguridad	firewall	No hay disponibilidad de los servicios tecnológicos.	• Fallas en el suministro eléctrico. • Desastres naturales. • Fallas en los dispositivos tecnológicos.	Procedimiento de implementación de contingencias.
Centro de datos.	Centro de datos.	No hay disponibilidad de los servicios tecnológicos.	• Fallas en el suministro eléctrico. • Desastres naturales. • Fallas en los dispositivos tecnológicos	• Centro de datos alterno. • Procedimientos de activación de contingencias.

Fuente: Autor.

❖ Gestión de riesgos

Para la identificación de activos y riesgos es necesario crear el plan de tratamiento de riesgos. Se utiliza la metodología MAGERIT.

En el presente archivo se encuentra el análisis y los resultados obtenidos, ya implementados en la matriz de análisis, la cual se puede visualizar en el ***ANEXO D***.

❖ Pruebas y verificación periódicas del plan.

Es indispensable que el comité de riesgos e implementación del plan de continuidad del negocio realice reuniones en las cuales se creen los planes de verificación de funcionamiento de los planes de seguridad.

El plan de pruebas se realiza creando simulacros aprobados por el comité y ejecutado por los responsables de la ejecución del plan de continuidad; se debe realizar las pruebas teniendo en cuenta los procesos críticos ya identificados y la activación de los procesos alternativos de continuidad de los servicios.

Se debe presentar un informe de los resultados obtenidos por el comité de riesgos e implementación de seguridad, es indispensable que se identifiques las fallas y en reunión con el Líder de departamento de sistemas y las directivas se encuentre los controles pertinentes para la ejecución de mejoras a las fallas encontradas.

Es indispensable que se realicen los cambios pertinentes aprobados en la reunión para mantener los dispositivos alternos disponibles, es importante que se mantengan siempre actualizados en información y manejo, además que se continúe con el plan de seguridad de la información.

❖ Pasos para la implementación del plan de continuidad.

Para la ejecución exitosa del plan de continuidad del negocio es indispensable que se siga una serie de pasos por los responsables de los procesos, los pasos son:

Figura 8 Pasos implementación plan de continuidad.

Fuente: Autor.

- ❖ Formatos para la implementación del plan de continuidad del negocio

Tabla 27 Formatos.

Descripción	Formato
Diligenciar el siguiente formato al momento que se presente la interrupción de los servicios	Visualizar ***ANEXO K.***
Diligenciar el siguiente formato al momento de la activación del plan de continuidad del negocio.	Visualizar ***ANEXO L.***
Diligenciar el siguiente formato en caso de interrupción de los servicios por parte de los proveedores.	Visualizar ***ANEXO M***.

Fuente: Autor.

10.4. OBJETIVO 4 – ANALISIS Y VERIFICACIÓN DEL FUNCIONAMIENTO DE LOS MECANISMOS.

10.4.1. EVALUACIÓN Y ANALISIS DE LOS CONTROLES

Al terminar de implementar los controles es importante que se realice una evaluación de estos para determinar su correcto funcionamiento y si cumplen con los objetivos de la seguridad el cual es disminuir los riesgos detectados.

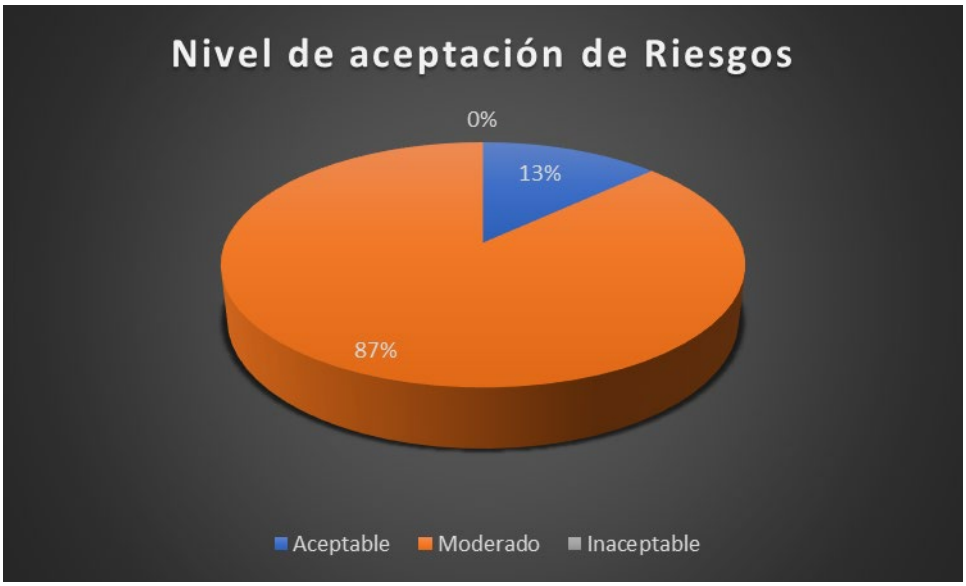
Si se determina que algún control no cumple con las expectativas y los objetivos, se realiza el estudio pertinente y el cambio de este, para así cumplir con la seguridad informática y asegurar la información y los activos considerados como importantes. Se debe analizar el mapa de calor para determinar si los diferentes riesgos son catalogados como aceptables o moderados.

Para realizar la auditoría, se utiliza la metodología MAGERIT para la identificación de los activos se tiene en cuenta la **Tabla 4 Inventario de activos.** Donde se realiza el inventario de estos, como segundo paso se toma en cuenta la **Tabla 5 Valoración cualitativa de los activos**. Para la valoración de los activos cualitativamente, teniendo en cuenta las dimensiones, la **Tabla 6 Valoración de activos.** Para determinar el valor de impacto de los activos.

En la identificación de las amenazas se tiene en cuenta la **Tabla 7 Identificación de amenazas**, debido a que se van a evaluar las mismas vulnerabilidades y los controles aplicados, teniendo en cuenta estos datos se realiza la evaluación a los controles y la probabilidad de ocurrencia de los riesgos.

Al realizar las respectivas valoraciones y teniendo en cuenta los distintos controles aplicados, se obtiene los siguientes resultados:

Figura 9 Nivel de aceptación de riesgos post implementación de controles.



Fuente: Autor

Como se puede evidenciar en los resultados obtenidos, el 87% de las vulnerabilidades están en la escala de riesgo moderado y el 13% están en el nivel de rango aceptable. Se concluye que los controles aplicados cumplen con el objetivo de minimizar la ocurrencia de las amenazas. Para visualizar correctamente los resultados obtenidos, observar el ***ANEXO F***.

10.4.2. EVALUACIÓN DE EFECTIVIDAD DE LOS CONTROLES.

El formato utilizado para la evaluación de la efectividad de los controles, se pueden observar en el ***ANEXO G***. Donde se evalúa cada riesgo y el control implementado para mitigar la ocurrencia de la amenaza en la entidad.

Se tienen en cuenta los siguientes factores de evaluación para determinar la efectividad de los controles implementados teniendo en cuenta los riesgos.

Tabla 28 Aspectos para valoración de los controles.

Factores de evaluación	% factor de evaluación.	Puntos de factor.
Diseño del control	**25%**	**1,25**
1. ¿El control tiene un objetivo definido?		
2. ¿El Control reduce el Nivel de Riesgo?		
3. ¿Está Documentado el Control?		
4. ¿Se ha formalizado el Control en la Mesa de Trabajo?		
Esquema del control	**10%**	**0,5**
1. Manual		
2. Automático		
3. Mixto		
4.Otro		
Operación del control	**10%**	**0,5**
1. Preventivo		
2. Detectivo		
3. Correctivo		
4.Otro		
Frecuencia del control	**10%**	**0,5**
1. Optima		
2. Moderada		
3. Deficiente		
4. No tiene Frecuencia el control		
Madurez del control	**25%**	**1,5**
1. Optimo		
2. Monitoreado		
3. Estandarizado		
4. Informal		
5. Poco Confiable		
Resultados de la Auditoría y/o Verificación del control	**25%**	**1,5**
1. Se evidencia cumplimiento del objetivo del control		
2. Se evidencia disminución de la exposición al riesgo		
3. Considera usted, que el responsable de ejecutar el control conoce los riesgos que implica su omisión.		
4. Se ha realizado seguimiento al control.		

Fuente: Autor

Se tiene los siguientes criterios para saber si es efectivo el control.

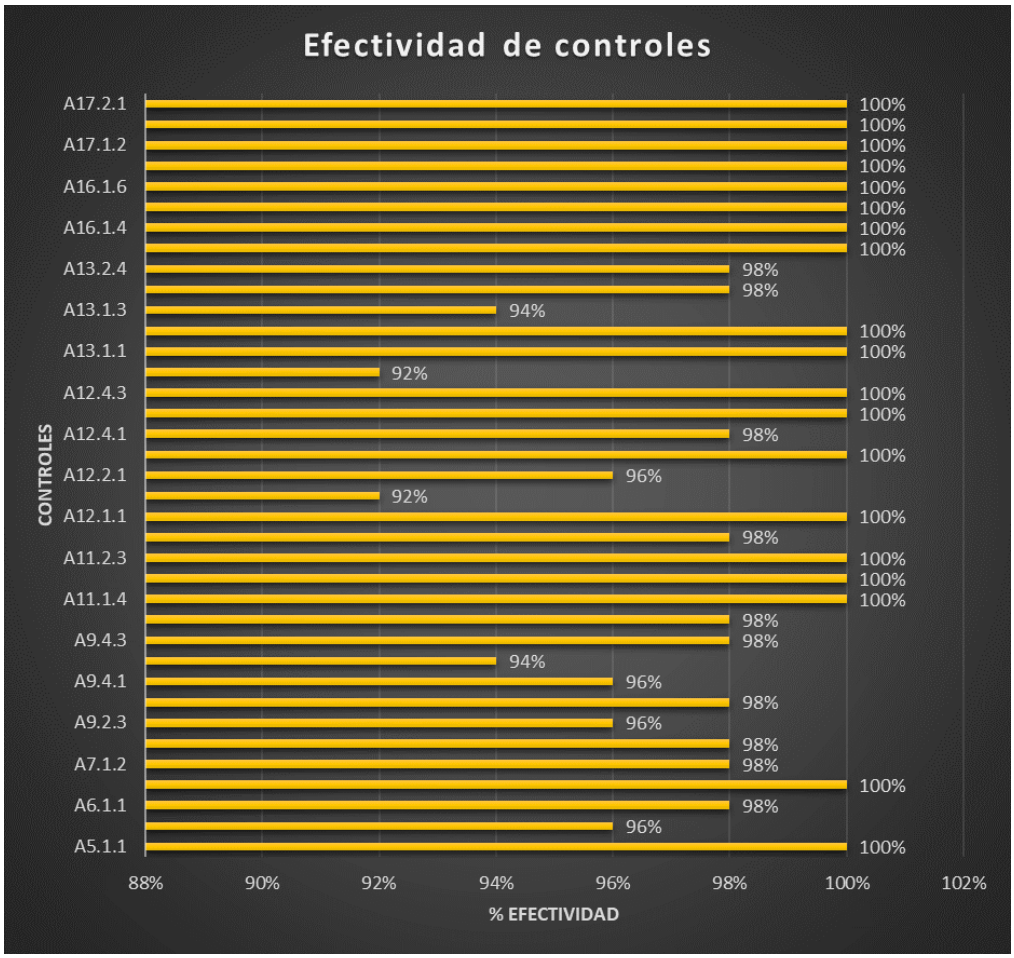
Tabla 29 Niveles de efectividad.

NIVEL DE EFECTIVIDAD DEL CONTROL			
DESCRIPCIÓN	RECOMENDACIÓN	PORCENTAJE DE EFECTIVIDAD	PUNTOS EFECTIVIDAD
ÓPTIMO	Se recomienda: No hay recomendaciones.	86% – 100%	Entre 4,5 y 5
ADECUADO	Se recomienda: Seguir haciendo seguimiento al control implementado.	66% - 85%	Entre 3,35 y 4,4
DEBIL	Se recomienda Reevaluar las distintas actividades del control implementado	45% - 65%	Entre 2,5 y 3,34
MUY DEBIL	Se Recomienda Reevaluar el control establecido.	0% - 44%	Entre 0 y 2,4

Fuente: Autor.

Al conocer el formato a utilizar y los factores de calificación se realiza la evaluación de efectividad de cada control y se obtiene los siguientes resultados.

Figura 10 Efectividad de los controles.



Fuente: Autor.

Al revisar los resultados obtenidos y verificando la **Tabla 31 Niveles de efectividad**, se concluye, que los controles son óptimos y cumplen con el objetivo de la seguridad informática. Se puede revisar la evaluación completa en el ***ANEXO H***.

4. CONCLUSIONES

Se realizó un plan de ejecución para implementar correctamente la auditoria al sistema de seguridad de la información de la entidad, al conocer adecuadamente la organización, el estado actual de la seguridad, la infraestructura tecnológica y como complemento, la elaboración del cronograma de actividades para cumplir con los tiempos estipulados.

Para la identificación de los activos se utilizó la metodología MAGERIT, puesto que da pautas para realizar adecuadamente la identificación y valoración de cada activo, se determinan los riesgos y las vulnerabilidades que están presentes, por último, se categorizan y se valoran según los riesgos encontrados y el impacto en la organización; se realiza el plan de tratamiento de riesgos y se implementan controles de acuerdo con la norma ISO 27001.

La implementación de la norma ISO27001 en la entidad QWERTY, ayudó con la correcta gestión de los riesgos, se obtiene como resultado la disminución de las amenazas a la seguridad y los activos, se determina que la norma es flexible y se puede implementar en cualquier organización, se busca siempre la mejora continua de los procesos.

Es importante siempre actualizar las políticas de seguridad según los controles que se apliquen al sistema, esto para que se cumplan estrictamente las normas y evitar que haya incidentes de seguridad y se ponga en riesgo los activos; siempre que sea necesario realizar las actualizaciones se debe capacitar e informar a los empleados sobre los cambios efectuados y porque motivo se hizo.

Se concluye que uno de los temas en los que se debe enfatizar es la creación de cronogramas para la capacitación continua del personal de la entidad, puesto que es considerado el objetivo principal de ataque, para obtener información sensible de la organización mediante diversas técnicas que son utilizadas para tal propósito, la idea es que conozcan como detectarlas a tiempo e informar según los protocolos al área encargada para que realice el debido proceso de mitigación.

5. RECOMENDACIONES

Al realizar una planificación de las auditorías de sistemas se consideran distintos puntos; para brindar una mejor información se debe dar a conocer el cronograma de actividades, donde se demuestre la ejecución completa y qué tiempo predeterminado que se va a emplear, desde la creación del plan de interventoría hasta la entrega del informe final. Es importante conocer la situación actual de la entidad para saber cómo se debe proceder a la hora de la identificación de los activos y qué problemas tiene de seguridad para la valoración correcta de las amenazas.

Al conocer los objetivos de la entidad, da una dirección correcta al proceso de gestión de seguridad para brindar mejores resultados, que la misión se cumpla y se aseguren correctamente los activos y la información, esto debido, a que están directamente entrelazados, de igual importancia es el análisis de la situación de la entidad para la verificación de la cantidad de empleados, la identificación de áreas; revisión del organigrama para conocer los líderes de procesos y por último y más importante conocer la infraestructura tecnológica, identificar las áreas, y como está compuesta dicha infraestructura y su seguridad; teniendo todos estos datos se puede determinar el alcance de la auditoría e implementación del sistema de gestión de riesgos.

Se recomienda que antes de realizar la identificación de los activos se escoja la metodología MAGERIT para tal propósito, debido a que da las pautas para la correcta identificación y ~~dar~~ una valoración de estos, de igual manera, las amenazas y las vulnerabilidades que se tienen en la entidad; esto ayuda a conocer el estado real en temas de seguridad de la información y brindar mecanismos según la norma ISO 27001 para la gestión de los riesgos.

Se debe considerar realizar entrevistas a todos los empleados para tener un panorama más amplio, adecuar dichas entrevistas según el personal y la interpretación de palabras técnicas por parte de las personas, por consiguiente, se deben crear encuestas de tipo general y tipo técnicas con preguntas concernientes al ámbito de utilización y configuración de los activos tecnológicos.

La correcta identificación de los riesgos y valoración, ayuda a determinar el estado de la empresa y es concerniente implementar un plan de tratamiento de riesgo, donde se apliquen controles según la norma ISO 27001, teniendo en cuenta los dominios para minimizar la ocurrencia de dichos eventos, por otra parte, se deben actualizar las políticas de seguridad con los nuevos controles, luego capacitar al personal de la entidad sobre seguridad y los cambios realizados a las políticas y porqué su actualización.

La norma ISO 27001 permite la mejora continua de los procesos, por eso es recomendable que se realice una evaluación a los controles implementados para determinar de esta manera la efectividad y si disminuyen los riesgos identificados. Se puede realizar un análisis mediante la metodología MAGERIT, teniendo en cuenta los aspectos antes mencionados; si los resultados son contrarios a lo esperado, se puede realizar el cambio del control y hacer la debida actualización de las políticas de seguridad.

Como recomendación final a las entidades; deben dar importancia a la implementación de un sistema de gestión de seguridad para evitar la pérdida de confiabilidad de la información que es considerado el activo más valioso, esto conlleva a retrasos sustanciales en el logro de los objetivos, la norma ISO 27001 es

una herramienta valiosa en la detección de vulnerabilidades en los sistemas y sobre todo ayuda a las organizaciones a blindarse de los ataques a la seguridad, permite una mejora continua de los procesos esto la hace más flexible a los cambios.

6. BIBLIOGRAFÍA

ZAMBRANO BURBANO, Rosa María. Estudio sobre el conocimiento y la aplicabilidad de la seguridad informática en las empresas. [En línea] 12 de 02 de 2012. https://repository.unad.edu.co/handle/10596/20152.

MATACHANA, Yansenis. Los virus informáticos: una amenaza para la sociedad. [En línea] 1 de 1 de 2009. http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=4&docID=10357400&tm=1466006227313.

VALENCIA, F. CARDONA, A. & ARTURO, D. Diseño del sistema de gestión de seguridad de la información basado en la familia de normas de la serie ISO/IEC 27000 para una entidad pública colombiana. [En línea] 2018. http://repositorio.autonoma.edu.co/jspui/handle/11182/721.

URECHE OSPINO, Manuel Esteban. Diseño de Políticas de Seguridad Informática basadas en la norma NTC-ISO-IEC 27001:2013 para la universidad de Cartagena centro tutorial Mompox Bolívar. [En línea] 06 de 04 de 2017. https://repository.unad.edu.co/handle/10596/12027.

UNIVERSIDAD LIBRE. El decálogo de la seguridad informática. [En línea] http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/247-el-decalogo-de-la-seguridad-informatica.

SENADO DE LA REPUBLICA. Ley 1273 de 2009. [En línea] 2009. https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf.

SANABRIA FLÓREZ, Yefferson. Seguridad informática en Claro Colombia en el área de cuidado al cliente-prevención. [En línea] 2014. https://repository.ucatolica.edu.co/handle/10983/1327.

REYES, J. MUÑOZ, C. & GUARDA, T. Seguridad Informática para Pequeñas y Medianas Empresas de la Provincia de Santa Elena. [En línea] 2017.

https://search.proquest.com/openview/ba8fb554f72bbe6b94735e926be36754/1?pq-origsite=gscholar&cbl=1006393.

RAYA, J. & RAYA, L. Implantación de sistemas operativos. [En línea] 2014. https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3228461.

PRADA HERNANDEZ, Nathalia. Diseño de un sistema de gestión de seguridad de la información, alineado con la Norma ISO. [En línea] 2010. https://repository.javeriana.edu.co/handle/10554/7515.

PLAZAS GARCIA, Edna Rocio. Ingeniería social en las empresas colombianas. [En línea] 2018. https://repository.unad.edu.co/handle/10596/18704.

PATIÑO ALPALA, Luis Olmedo. Propuesta de actualización, apropiación y aplicación de políticas de seguridad informática en una empresa corporativa, Propolsinecor. [En línea] 2014. https://repository.unad.edu.co/handle/10596/2742.

OJEDA PÉREZ, Jorge Eliecer. Delitos informáticos y entorno jurídico vigente en Colombia. [En línea] 2010. https://repository.javeriana.edu.co/handle/10554/23982.

MIN TIC. ¿Y de seguridad TI qué hacen las entidades? [En línea] https://www.mintic.gov.co/gestionti/615/w3-article-7083.html.

MIN TIC. Modelo de Seguridad. [En línea] https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html.

MENDOZA PENAGOS, Lina Patricia. Diseño de un sistema de gestión de seguridad informática para la Empresa GED (Gestión Estrategia y Desarrollo) de la ciudad de Bogotá. [En línea] 2018. https://repository.unad.edu.co/handle/10596/20723.

LEÓN CEPEDA, Laura Carolina. Estructuración del sistema de seguridad de la información en el área de protección de datos para un operador logístico bajo la norma NTC/ISO 27001:2013. [En línea] 2018. https://repository.ucatolica.edu.co/handle/10983/16149.

SANTOS, Jesús Costas. Seguridad informática. [En línea] 2014. https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3228430&ppg=1.

CANO, Jeimy. Ciber ataques—La inestabilidad de lo que hemos aprendido en seguridad y control . [En línea] 2016. https://www.isaca.org/Journal/archives/2016/volume-5/Pages/cyberattacks-the-instability-of-security-and-control-knowledge-spanish.aspx?utm_referrer=.

HOYO MALES, Camilo Ernesto. Seguridad en el transporte y gestión de correos electrónicos, implementación de seguridad en correo outlook 2010. [En línea] 2015. https://repository.unad.edu.co/handle/10596/3657.

GÓMEZ FERNÁNDEZ, L. & ÁLVAREZ, A. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. [En línea] 2012. https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3205110&ppg=1.

GIL VERA, V. GIL VERA, J. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. [En línea] 2012. https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3205110&ppg=1.

FERREYRO, A. & LONGHI, A. METODOLOGÍA DE LA INVESTIGACIÓN. [En línea] 2014. http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=847674&lang=es&site=eds-live.

FERNANDEZ SÁNCHEZ, C. & PIATTINI VELTHUIS, M. Modelo para el gobierno de las TIC basado en las normas ISO. [En línea] 2012. https://ebookcentral-proquest-

com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3205141&ppg=1.

ESPINOZA ZALLAS, E. & RODRIGUEZ PÉREZ, R. Seguridad informática una problemática de las organizaciones en el Sur de Sonora. [En línea] 2017. http://revistainvestigacionacademicasinfrontera.com/sistema/index.php/RDIASF/article/view/140.

DELVASTO RAMÍREZ, Ramiro Andrés. Modelo de Gestión de incidentes de seguridad de la información para PYMES. [En línea] 2016. https://repository.unad.edu.co/handle/10596/6170.

VILLAGÓMEZ, Carlos. Sistema de detección de intrusiones (IDS). [En línea] 6 de 12 de 2017. https://es.ccm.net/contents/162-sistema-de-deteccion-de-intrusiones-ids.

BARRETO CUITIVA, Julián Hernán. Manual de seguridad informática para Pymes. [En línea] 2018. https://repository.unad.edu.co/handle/10596/15026.

AYALA ROJAS, Nevardo Alonso. Monografía de estudio sobre la aplicación de seguridad biométrica para la identificación de usuarios en entornos WEB. [En línea] 2015. https://repository.unad.edu.co/handle/10596/3743.

ÁVILA PARDO, W. & RAMÍREZ RESTREPO, J. Escaneo de vulnerabilidades al servidor principal de la empresa. Caso de estudio. [En línea] 2018. https://repository.unad.edu.co/handle/10596/18321.

ARIZA BARRERA, Daniel Ricardo. Monografia protocolos copias de seguridad Oracle 2017. [En línea] 2017. https://repository.unilibre.edu.co/handle/10901/11163.

VIEITES, Álvaro. Seguridad en equipos informáticos. [En línea] 2014. https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3229330.

ALCANTÁRA FLORES, Julio César. Guía de implementación de la seguridad basado en la norma ISO/IEC27001, para apoyar la seguridad en los sistemas informáticos de la Comisaria del Norte P.N.P. en la ciudad de Chiclayo. [En línea] 2015. http://tesis.usat.edu.pe/handle/usat/539.

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA. MAGERIT – versión 3.0. [En línea] 2012. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA. MAGERIT – versión 3.0. *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* [En línea] 2013. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

MIN TIC. Controles de seguridad y privacidad de la información. [En línea] 15 de 12 de 2015. https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf.

MINISTERIO DE DEFENSA NACIONAL. Plan de tratamiento de riesgos de seguridad de la información. [En línea] 16 de 01 de 2020. https://www.justiciamilitar.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estrategia_planeacion/desa_organizacional/2020/Plan%20Tratamiento%20de%20Riesgos%20de%20Seguridad%20y%20Privacidad%20de%20la%20Informacion.pdf.

SUAREZ, H. TAPIERO, H. Políticas de seguridad. [En línea] 2017. http://repository.udistrital.edu.co/bitstream/11349/8322/4/Anexo%20C%20-%20Politicas%20de%20seguridad.pdf.

MIN TIC. Guía de gestión de riesgos. [En línea] 1 de 04 de 2016. https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.

RAMIREZ, Jefferson Faruk. Seguridad de la información en el sector público colombiano. [En línea] http://polux.unipiloto.edu.co:8080/00002657.pdf.

ANEXOS

- **ANEXO A CRONOGRAMA AUDITORÍA DE SISTEMAS.xlsx**
- **ANEXO B ENTREVISTAS Y ENCUESTAS.DOCX**
- **ANEXO C EVALUACIÓN DE CONTROLES NORMA ISO 27002.xlsx**
- **ANEXO D MATRIZ DE ANÁLISIS DE RIESGOS QWERTY S.A.xlsx**
- **ANEXO E DECLARACIÓN DE APLICABILIDAD SOA.xlsx**
- **ANEXO F MATRIZ DE ANÁLISIS DE RIESGOS QWERTY S.A POST IMPLEMENTACIÓN DE CONTROLES.xlsx**
- **ANEXO G EFECTIVIDAD DE CONTROLES.xlsx**
- **ANEXO H EVALUACIÓN EFECTIVIDAD DE LOS CONTROLES.xlsx**
- **ANEXO I PLAN DE AUDITORÍA DE SISTEMAS.docx**
- **ANEXO J INFORME AUDITORÍA.docx**
- **ANEXO K REPORTE INTERRUPCIÓN DE SERVICIOS.xlsx**
- **ANEXO L REPORTE ACTIVACIÓN PLAN CONTINUIDAD.xlsx**
- **ANEXO M REPORTE PROVEEDORES.xlsx**