ASEGURANDO EL SGSI DE LA EMPRESA QWERTY S.A.

JOHANN LEONARDO GUTIÉRREZ MEDINA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2020

ASEGURANDO EL SGSI DE LA EMPRESA QWERTY S.A.

JOHANN LEONARDO GUTIÉRREZ MEDINA

Proyecto aplicado como opción de grado para optar el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director: Edilberto Bermúdez Penagos
Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2020

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá D.C. octubre 29 de 2020

DEDICATORIA

Este trabajo lo dedico a mi madre y a mis abuelos por su gran amor, comprensión y apoyo incondicional……

AGRADECIMIENTOS

Agradezco a Dios por mi vida, por darme fuerza en cada paso que he dado a lo largo de mi crecimiento personal, espiritual, laboral y académico, a mi mamá ya que es un motor y soporte incondicional, a cada docente que me brindó su apoyo a lo largo de esta especialización.

CONTENIDO

pág.

LISTADO DE TABLAS

pág.

LISTADO DE CUADROS

pág.

LISTADO DE FIGURAS

pág.

LISTADO DE ANEXOS

pág.

RESUMEN

Para el desarrollo de este proyecto se selecciona un escenario dado con anterioridad por la especialización en seguridad informática de la Universidad Nacional Abierta y a Distancia UNAD, en el cual la empresa QWERTY S.A. es el centro del proyecto aplicado. Esta es una compañia del sector TI que tiene como finalidad incrementar el desarrollo tecnológico en comunidades colombianas por medio de la utilización de las tecnologías de la información. Cuenta con 120 trabajadores en diferentes niveles ocupacionales. Tiene una dependencia de sistemas la cual debe dar soporte a la infraestructura tecnológica 24/7 y se divide en 3 áreas: la primera es de infraestructura, la segunda de desarrollo y la tercera de soporte; las cuales brindan un apoyo al servicio de correo electrónico institucional, en la gestión y cuidado de los dispositivos, en la administración de usuarios y contraseñas y a la dependencia de nómina y facturación. Actualmente, cuenta con posibles vulnerabilidades por las cuales puede ser afectada, como falta de control y un sistema de seguridad de la información.

A partir de ello se gestionaron los riesgos presentes en la compañía Qwerty S.A. desde dos enfoques; en el primer enfoque, directivo – administrativo; se diseñó un sistema de gestión de seguridad de la información (SGSI), el cual se fundamentó en la norma ISO/IEC 27001:2013, en donde se realizó la identificación y valoración de activos, dimensiones de seguridad, gestión del riesgo, análisis de amenazas, riesgo intrínseco, salvaguardas, riesgo residual y aceptable para la empresa. Se detectaron diferentes vulnerabilidades que generarían impacto negativo en la seguridad de la compañía. En el segundo enfoque, técnico – estratégico; se administraron los riesgos de ciberseguridad presentes en la empresa apoyándose en la norma ISO/IEC 27005, en donde se fortaleció la seguridad de los sistemas operativos, redes, bases de datos y servidores, a través de los códigos de buenas prácticas de TI.

Palabras claves: Amenaza, confidencialidad, contraseña, datos, debilidad, disponibilidad, gestión, información, integridad, recursos, riesgo, seguridad, vulnerabilidad.

ABSTRACT

For the development of this project, a scenario given previously by the specialization in computer security of the National Open and Distance University UNAD is selected, in which the company QWERTY S.A. it is the center of the applied project. This is a company in the IT sector that aims to increase technological development in Colombian communities through the use of information technologies. It has 120 workers at different occupational levels. It has a systems dependency which must support the technological infrastructure 24/7 and is divided into 3 areas: the first is infrastructure, the second is development and the third is support; which provide support to the institutional email service, in the management and care of the devices, in the administration of users and passwords and the payroll and billing unit. Currently, it has possible vulnerabilities by which it may be affected, such as lack of control and an information security system.

Based on this, the risks present in the company Qwerty S.A. were managed. from two approaches; in the first approach, managerial - administrative; An information security management system (ISMS) was designed, which was based on the ISO / IEC 27001: 2013 standard, where the identification and valuation of assets, security dimensions, risk management, analysis of threats, intrinsic risk, safeguards, residual risk and acceptable to the company. Different vulnerabilities were detected that would generate a negative impact on the security of the company. In the second approach, technical - strategic; The cybersecurity risks present in the company were managed based on the ISO / IEC 27005 standard, where the security of operating systems, networks, databases and servers was strengthened, through the codes of good IT practices.

Palabras claves: Threat, confidentiality, password, data, weakness, availability, management, information, integrity, resources, risk, security, vulnerability.

INTRODUCCIÓN

La utilización de herramientas tecnológicas para la administración de la información cada día es más útil y está en permanente cambio dentro de los procesos de comunicación entre personas o empresas con diferentes fines, sean económicos, sociales, políticos, religiosos, entre otros; esto por supuesto involucra a la empresa Qwerty S.A., siendo esta una compañía que tiene como objetivo principal el de incentivar el desarrollo tecnológico de las comunidades colombianas a través de las tecnologías TI. De acuerdo con la identificación y análisis, actualmente la compañía no cuenta con un control de ingreso y egreso de personal a sus instalaciones, los servidores DHCP, HTTP y PBX se encuentran en un espacio donde no cumplen con las condiciones de climatización óptimas, la configuración de la red de comunicaciones está en un mismo segmento, el cortafuegos no tiene las reglas implementadas para la autorización, denegación o transmisión de datos. Por tal motivo, y siendo consecuente con los riesgos analizados y encontrados, la organización es consciente de la importancia de mantener la disponibilidad, integridad y confidencialidad de la información, razón por la cual ha decidido diseñar una estrategia que le permita identificar y solucionar estas posibles vulnerabilidades en su infraestructura informática, con el fin de prevenir eventuales ataques cibernéticos.

En el presente documento se plantea el diseño de un sistema de gestión de seguridad de la información para la compañía QWERTY S.A. con el cual se genera protección a sus activos informáticos y se establecen políticas de seguridad con el fin de disminuir el riesgo ante un eventual ataque cibernético. Para esto se realizan diferentes procesos focalizados en cuatro objetivos. El primero se basa en la identificación de la situación actual de la empresa QWERTY S.A a través del reconocimiento de activos, valoración de estos y dimensiones de seguridad con las que cuenta actualmente la compañía. En el segundo objetivo se ejecuta el análisis de riesgos, amenazas y vulnerabilidades, fundamentado en la metodología MAGERIT, lo cual permite realizar gestión del riesgo, análisis de amenazas, riesgo intrínseco, salvaguardas, riesgo residual y aceptable para la empresa. En el tercer objetivo se desarrolla un plan de monitoreo de los activos informáticos, mediante el cual, se establece el control y seguimiento de estos. En el cuarto objetivo se organiza un manual de seguridad informática, de acuerdo con los códigos de buenas prácticas orientadas a la ciberseguridad.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES

La empresa QWERTY S.A. es consciente de los riesgos que está adquiriendo con la falta de controles sobre la seguridad de sus activos ya que no cuenta con elementos indispensables para ofrecer seguridad en los servicios, como un sistema de control de ingreso y egreso del personal interno y externo, los servidores DHCP, HTTP Y PBX no se encuentran en condiciones ambientales favorables, la red de comunicaciones se encuentra en un mismo segmento y el firewall no tiene todas sus propiedades activas. Todos estos aspectos generan inseguridad tanto para las directivas como para sus usuarios. A través del trabajo realizado se evidencia que, al ser una compañía dedicada a fomentar el uso de las tecnologías de la información, presenta diferentes falencias que la hacen vulnerable a los ataques cibernéticos.

1.2 FORMULACIÓN

Con el constante aumento en el uso de herramitas TIC crecen los casos de ataques cibernéticos a compañías por diferentes motivos, los cuales pueden ser económicos o simplemente por dañar una reputación, como se evidencia en la empresa QWERTY S.A., la cual no cuenta con las suficientes herramientas que permitan mitigar un ataque de este tipo, por tal motivo surge la siguiente pregunta:
¿Cuáles serían los beneficios al diseñar un sistema de gestión de seguridad de la información para los activos informáticos de la empresa QWERTY S.A., y de planear una estrategia para la gestión de riesgos cibernéticos en esta organización?

1.3 DESCRIPCIÓN

La problemática presentada por la empresa QWERTY S.A. radica en la falta de una serie de mecanismos que permitan mitigar los riesgos presentes en la implementación de la tecnología, además, cuenta con una oficina de sistemas la cual ofrece cuatro grandes servicios, como son; correo institucional, gestión y

mantenimiento en los activos de información, gestión de usuarios y contraseñas, y apoyo a la dependencia de nómina y facturación. Para garantizar el funcionamiento de estos servicios, QWERTY S.A. muestra en su inventario servidores DELL en torre PowerEdge T440, impresora HP LaserJet Enterprise serie 600, impresora SMART MultiXpress M4370LX, servidores DELL en torre PowerEdge T130, computadores, cortafuegos ASA 5505, HUB, switches cisco catalyst 2960, teléfonos ip, puntos de acceso; los servidores DHCP, HTTP Y PBX presentan condiciones ambientales no favorables; la red de comunicaciones se encuentra en un mismo segmento y el firewall no tiene todas sus propiedades activas. Todo esto aumenta las vulnerabilidades que hacen propensa la compañía a un eventual ataque cibernético.

2. JUSTIFICACIÓN

Uno de los activos más importantes a proteger es la información que posee una empresa, en la actualidad, se está incrementando el uso de las herramientas basadas en la tecnología para gestionar y proteger los datos que tienen las compañías, facilitando así su trabajo, pero a la vez, se puede observar también la presencia de diversos ataques cibernéticos a las organizaciones, que impactan negativamente en su disponibilidad, integridad y privacidad.

La empresa QWERTY S.A. teniendo como finalidad incrementar el desarrollo tecnológico en comunidades colombianas por medio de la utilización de las tecnologías de la información y al ser promotora del uso de las mismas, no es ajena a los diversos ataques cibernéticos de la actualidad, razón por la cual surge la necesidad de realizar este proyecto con el fin de diseñar un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2013 que genere protección a los activos informáticos y disminuya los riesgos ante un eventual ataque cibernético.

El diseño de un sistema de seguridad de la información basado en la norma ISO/IEC 27001 en la empresa QWERTY S.A. permitirá identificar, analizar, evaluar y monitorear los riesgos informáticos presentes actualmente en la compañía, con el fin de determinar los controles y mecanismos necesarios para minimizar posibles ataques cibernéticos, este proceso se realizará teniendo en cuenta las necesidades manifiestas y encontradas, favoreciendo considerablemente todo el engranaje de la empresa, proporcionando así seguridad, estabilidad, buen nombre y confianza de los usuarios y colaboradores.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un sistema de gestión de seguridad de la información para la compañía QWERTY S.A., el cual genere protección a su infraestructura tecnológica y disminuya los riesgos ante un eventual ataque cibernético.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar la situación actual de la empresa QWERTY S.A., a través del reconocimiento de los activos que posee y sus características.

- Realizar análisis de riesgos, amenazas y vulnerabilidades a través de la metodología MAGERIT.

- Desarrollar un plan de monitoreo de los activos informáticos de la empresa, el cual permita el control y seguimiento de estos.

- Establecer un manual de seguridad informática, basándose en los códigos de buenas prácticas orientadas a la ciberseguridad.

4. MARCO REFERENCIAL

Para desarrollar el proyecto aplicado de QWERTY S.A. es fundamental identificar los diferentes conceptos y técnicas implementadas a la hora de diseñar un sistema de gestión de seguridad de la información y brindar protección cibernética a una empresa. Por tal motivo dentro del marco teórico se realizará una descripción detallada de cada uno de los elementos que serán utilizados en el desarrollo del objeto de estudio y dentro del marco conceptual se definirán los principales conceptos que involucran el mismo.

4.1 MARCO TEÓRICO

4.1.1 Norma ISO/IEC 27001:2013. En el contexto de seguridad de la información esta norma brinda los pasos que se deben tener en cuenta a la hora del diseño e implementación de un sistema de gestión de seguridad de la información. "ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa"[1], razón por la cual esta norma brinda las herramientas necesarias para establecer un SGSI en cualquier empresa. Para esto se deben tener en cuenta los 15 pasos que se describen a continuación:

1. Obtener apoyo de la dirección: esto es fundamental para el desarrollo de un sistema de gestión de seguridad de la información, como lo dice Segovia[2], en este primer momento el director del proyecto debe contar con el apoyo de la alta dirección para desarrollar y ejecutar un SGSI de manera práctica y enfocada al negocio, ya que sin este paso el proyecto fracasaría.

2. Utilizar un mecanismo de administración: dependiendo del enfoque que tenga el SGSI existen diferentes metodologías en la gestión de este tipo de proyectos, las

[1] SEGOVIA Antonio. ¿Qué es la ISO 27001?. [En línea]. (consultado 7 de mayo de 2019). España. Advisera., Disponible en: https://advisera.com/27001academy/es/que-es-iso-27001/.
[2] SEGOVIA Antonio. Beneficios de ISO 27001: Como obtener el apoyo de la dirección. [En línea]. (consultado 7 de mayo de 2019). España. Advisera., Disponible en: https://advisera.com/27001academy/wpcontent/uploads/sites/5/2015/06/ISO_27001_Benefits_How_To_Obtain_Management_Support4_ES_presentation_deck.pdf

más utilizadas según Ciospain[3] son:

- Cascada o Waterfall, se realiza de manera secuencial, implementada en diferentes industrias ya que se compone de etapas estáticas como lo son: análisis de requisitos, diseño, prueba, implementación y mantenimiento. Utilizada normalmente por empresas de desarrollo de software donde se emplea una planificación formal.

- Agile, se implementa en proyectos de gran velocidad y flexibilidad, se compone de ciclos cortos, es interactiva, es viable para realizar ajustes en el desarrollo del proyecto, reduce el riesgo y produce resultados rápidos.

3. Definir el alcance del SGSI: es un requisito indispensable "La definición del alcance es un requisito (de carácter obligatorio) descrito en la cláusula 4.3 de ISO/IEC 27001:2013, por lo que las características de este requisito tienen la intención de dejar en claro todo lo que es de interés para el sistema de gestión"[4], por lo tanto, en este paso como lo describe Mendoza se plasman los límites y la extensión que tendrá el proyecto, refiriéndose esto a ubicaciones físicas, activos, sucursales, procesos sensibles para la entidad. Es la primera decisión trascendental a tener en cuenta para la elaboración del SGSI.

4. Construir un manual de políticas: se plantea la elaboración de las guías que enrutan el comportamiento sobre la información manejada y administrada por la compañía y los diferentes cargos que en esta existen, acorde con la siguiente definición de política. "Declaración de alto nivel que describe la posición de la entidad sobre un tema específico"[5].

5. Implementar la metodología de evaluación de riesgos: se define la metodología de riesgos a implementar en la empresa, con el fin de detectar los presentes,

[3] CIOSPAIN. Las metodologías de gestión de proyectos más populares. [En línea]. (consultado 7 de mayo de 2019). España., Disponible en: https://www.ciospain.es/gobierno-ti/las-metodologias-de-gestion-de-proyectosmas-Populares

[4] MENDOZA Miguel. ¿Cómo definir el alcance del SGSI?. [En línea]. (consultado 7 de mayo de 2019). Mexico welivesecurity. 2018., Disponible en: https://www.welivesecurity.com/laes/2018/01/09/definir-alcance-sgsi/

[5] COLOMBIA. Ministerio de Tecnologías de la Información y las Comunicaciones. Elaboración de la politica general de seguridad y privacidad de la informacion. [En línea]. (consultado 7 de mayo de 2019). Bogotá MINTIC. 2016., 8 p. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

según Isotools[6], esta debe contener como mínimo un marco de evaluación, un identificador en donde se debe realizar un análisis y evaluación de riesgos y posteriormente seleccionar las opciones de gestión del riesgo y realizar un informe que contenga los resultados para decidir sobre las medidas que se deben aplicar.

6. Efectuar la detección y tratamiento de riesgos: es uno de los más importantes en la norma, ya que hace parte de la filosofía principal de ISO 27001 y consiste en analizar los problemas que se pueden producir y encontrar las soluciones pertinentes. Este paso se basa en 6 ítems para la evaluación y tratamiento del riesgo: "metodología para la evaluación de riesgos, implementación de la valoración del riesgo, implementación para el tratamiento de riesgos, informe de evaluación de riesgos, elaboración del documento - declaración de aplicabilidad, plan de cura de los peligros"[7].

7. Redactar la SoA: también llamada declaración de aplicabilidad trata de "un documento que enlista los controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001 (un conjunto de 114 controles agrupados en 35 objetivos de control, en la versión de 2013 de esta norma de seguridad)" [8], ya que después de que los riesgos han sido identificados y analizados se procede a mitigar en aras de reducir el impacto, transferir si es necesario la mitigación a un tercero o aceptar estos cuando el riesgo es minimo o cuando su costo supera el valor del activo.

8. Redactar el plan de tratamiento de peligros: identificar y registrar el proceso que se debe tener en cuenta ante un eventual ataque cibernético, en donde se identifican responsables, tiempos y presupuestos requeridos para la ejecución del mismo, como se afirma en Academy[9], se redacta un documento en el cual se determina de manera precisa el encargado de la implementación de controles por

---

[6] ISOTOOLS. ISO 27001 2013: Pasos a seguir en una evaluación de riesgos. [En línea]. (consultado 7 de mayo de 2019). ISOTools Excellence. 2016., Disponible en: https://www.pmgssi.com/2016/05/iso-27001-2013-pasos-seguir-evaluacion-riesgos/

[7] ISOTOOLS. ISO 27001: Evaluacion y tratamiento de riesgos en 6 pasos. [En línea]. (consultado 7 de mayo de 2019). ISOTools Excellence. 2016., Disponible en: https://www.isotools.org/2017/06/18/evaluacion-de-riesgos-segun-iso-27001/

[8] MENDOZA Miguel, ¿Qué es una declaración de aplicabilidad (SoA) y para que sirve?. [En línea]. (consultado 7 de mayo de 2019). Mexico welivesecurity. 2015., Disponible en: https://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/

[9] ACADEMY. Plan de tratamiento de riesgos. [En línea]. (consultado 7 de mayo de 2019). España. Advisera., Disponible en: https://advisera.com/27001academy/es/documentation/plan-de-tratamiento-deriesgos/

tiempo y presupuesto.

9. Ejecutar las medidas correctivas: implementar las mejoras descritas anteriormente en los numerales 7 y 8, de igual manera es fundamental el desarrollo de políticas que faciliten la implementación de los controles establecidos en el Anexo A de la norma ISO 27001, de acuerdo con lo expuesto por Cuervo[10], es necesario que se imponga una política y un manual de seguridad con el fin de minimizar los riesgos, vulnerabilidades y amenazas identificadas y evaluados en el análisis de riesgos.

10. Ejecutar jornadas de capacitación y educación: aunque se vea como un gasto innecesario, no lo es, ya que en la medida que la tecnología avanza es necesario que los colaboradores de una compañia cuenten con los conocimientos necesarios para poder afrontar con efectividad un eventual ataque cibernetico, esto lo expresa Rodriguez[11], donde menciona que con el conocimiento de mecanismos y prácticas de seguridad los trabajadores de una empresa pueden cumplir sus funciones y apoyar el correcto funcionamiento del SGSI.

11. Realizar todos los trabajos diarios: es fundamental para el correcto funcionamiento de lo establecido en los documentos del SGSI y asi alcanzar un nivel de seguridad que minimice posibles ataques cibernéticos.

12. Evaluar y valorar SGSI: se realiza el proceso de monitorización para saber si el sistema planteado está surtiendo los efectos deseados y no está causando riesgos residuales, por tal motivo se implementan diferentes indicadores referidos a continuación: “definición de controles de función de los riesgos detectados y las mejoras a los sistemas, controlar la capacitación según jerarquías”[12].

13. Realizar auditoria interna: se ejecuta una actividad independiente dentro de la

[10] CUERVO Sara. Implementación iso 27001. [En línea]. (consultado 7 de mayo de 2019). España., Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/64827/10/scuervoTFM0617presentaci%C3%B3n.pdf

[11] RODRIGUEZ María. 3 Razones para implementar un plan de capacitación en sus empresas. [En línea]. (consultado 7 de mayo de 2019). España., Disponible en: https://blog.acsendo.com/3-razones-para-implementar-un-plan-de-capacitacion-ensu-empresa/

[12] AGESIC. Indicadores para un SGSI guía metodológica. [En línea]. (consultado 7 de mayo de 2019). gub.uyy Uruguay. 2016., Disponible en: https://www.agesic.gub.uy/innovaportal/file/7004/1/anexo-iv_indicadores.pdf

empresa y tiene como finalidad según se menciona en Gerencie[13], diagnosticar sobre el estado actual del modelo de protección que se está implementando en la compañía.

14. Realizar revisión por parte de la dirección: se debe realizar una revisión por parte de la dirección de la empresa a los procesos que se evidencian dentro ella, los cuales son resultado de la implementación del SGSI, con el fin de verificar la "idoneidad, la adecuación, la eficiencia y la alineación continuas con la dirección estratégica de la empresa"[14], para así poder comprobar que las medidas tomadas no se encuentran en contra del objetivo de la compañía.

15. Implementar medidas correctivas: en esta fase según lo mencionado en Isotools[15], la directiva de la empresa debe implementar las acciones correctivas a las falencias encontradas en los archivos informáticos que se encuentran en estado activo con el fin de reparar las inconformidades presentadas, para que asi la compañía brinde de forma eficiente y segura los servicios que ofrece, generando buena reputación y confiabilidad en sus usuarios y trabajadores.

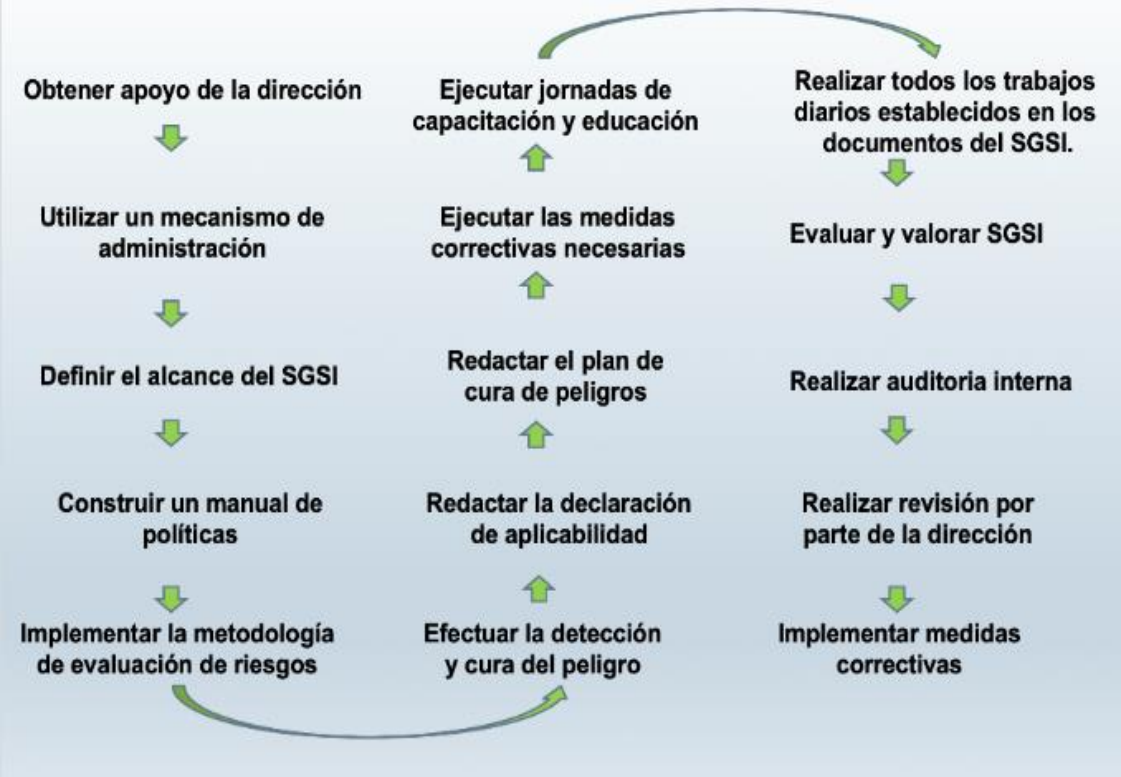
En la Figura 1 se evidencia de forma gráfica los 15 pasos que de acuerdo a la norma ISO/IEC 27001:2013 son fundamentales para el diseño de cualquier SGSI requerido por una empresa; estos se mencionaron y describieron anteriormente de forma explicita; a continuación, se estipulan de manera secuencial y sucinta estas fases a tener en cuenta en el proceso de diseño e implementación de un sistema de gestión de seguridad de la información.

[13] GERENCIE. Auditoria interna. [En línea]. (consultado 7 de mayo de 2019). Disponible en: https://www.gerencie.com/auditoria-interna.html

[14] NUEVA ISO 9001:2015. 9.3 Revisión por la dirección. [En línea]. (consultado 7 de mayo de 2019). Escuela Europea de Excelencia. Santiago de Chile. 2013., Disponible en: https://www.nueva-iso-9001-2015.com/9-3-revision-por-la-direccion/

[15] ISOTOOLS. Acciones preventinas o correctivas en el SG-SST. [En línea]. ISOTOOLS excellence 2016., (consultado 7 de mayo de 2019). Disponible en: https://www.isotools.org/2016/11/22/acciones-preventivas-correctivas-sg-sst/

Figura 1. Pasos norma ISO/IEC 27001:2013



Fuente: Autor basado en SEGOVIA, Antonio. Beneficios de ISO 27001. [En línea]. (Consultado 8 de mayo de 2019) Disponible en: https://advisera.com/27001academy/wpcontent/uploads/sites/5/2015/06/ISO_27001_Benefits_How_To_Obtain_Management_Support4_ES_presentation_deck.pdf

Es de gran importancia el manejo adecuado y seguro de la información, entendiendo por información una serie de datos ordenados y significativos para una entidad; siendo estos el alma de una organización, corporación o empresa, ya que permiten mantener la rentabilidad y competitividad. Con el fin de mantener esta información segura surge el modelo de seguridad de la información "como una herramienta de gestión que nos va a permitir conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la información en nuestra empresa."[16], es decir, es un mecanismo que tiene como propósito identificar y proteger las posibles inseguridades de los sistemas de información presentes en una entidad.

[16] INTECO. Implantación de un SGSI en la empresa. [En línea]. (consultado 8 de mayo de 2019). INTECO. 2014. p 3., Disponible en:https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

4.1.2 Norma ISO/IEC 27005. Es una estándar internacional que surge en reemplazo de las normas de Gestión de la Información, Comunicaciones y Tecnología de Seguridad, la norma ISO / IEC TR 13335-3:1998 y la norma ISO / IEC TR 13335-4:2000, y tiene como objetivo apoyar la ISO/IEC 27001:2013 en los requisitos exigidos en el diseño e implementación del sistema de gestión de seguridad de la información, está enfocada en la ciberseguridad; actualmente se puede evidenciar que tiene 17 secciones relacionadas a continuación: “prefacio, introducción, referencias normativas, términos y definiciones, estructura, fondo, descripción del proceso de ISRM, establecimiento contexto, información sobre la evaluación de riesgos de seguridad (ISRA), tratamiento de Riesgos Seguridad de la Información, admisión de riesgos seguridad de la información, comunicación de riesgos de seguridad de información, información de seguridad seguimiento de riesgos y revisión, anexo A: definición del alcance del proceso, anexo B: valoración de activos y evaluación de impacto, anexo C: ejemplos de amenazas típicas, anexo d: Las vulnerabilidades y métodos de evaluación de la vulnerabilidad y enfoques ISRA: anexo E”[17].

La norma ISO 27005 apoya con la gestión de riesgos a la ISO 27001, brindando de manera permanente actualizaciones que permiten a la empresa estar a la vanguardia de la tecnología, ofreciendo asi un mejor servicio a sus clientes y adquiriendo visibilidad competitiva en el mercado TI, por tal motivo es importante “La actualización del establecimiento, mantenimiento y mejora continua de un SGSI ofrecen una clara indicación de que una organización está utilizando un enfoque sistemático para la identificación, evaluación y gestión de riesgos de seguridad de la información.”[18], razón por la cual es favorable la implementación de códigos de buenas prácticas TI, como los relacionados en el Cuadro 1.

[17] SGSI. ISO/IEC 27005. Gestión de riesgos de la Seguridad la Información. [En línea]. (consultado 19 de marzo de 2020). ISOTools Excellence.2014., Disponible en: https://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/

[18] SGSI. ISO/IEC 27005. ISO 27005: ¿Cómo identificar los riesgos?. [En línea]. (consultado 19 de marzo de 2020) ISOTools Excellence.2014., Disponible en: https://www.pmg-ssi.com/2017/01/iso-27005-como-identificar-los-riesgos/

Cuadro 1. Códigos de buenas prácticas TI

CÓDIGOS DE BUENAS PRÁCTICAS TI	DESCRIPCIÓN
ITIL	Desarrollada a finales de 1980 por el gobierno británico, actualmente es el enfoque más aceptado en el mundo para la gestión de servicios TI, ya que ofrece un conjunto de buenas prácticas que proviene del sector público y privado a nivel internacional. Consiste en cinco etapas las cuales son: • Estrategia del servicio • diseño del servicio • Transición del servicio • Operación del servicio • Mejora continua del servicio También hay un conjunto de publicaciones complementarias de ITIL que brindan asesoramiento específico para distintos sectores económicos, tipos de organizaciones, modelos de operación y arquitectura de tecnología.
COBIT	Es una guía de buenas prácticas TI que está dirigida al control y supervisión de tecnología de la información, cuenta con unos recursos que pueden servir de modelo de referencia para la gestión de las tecnologías de la información, las cuales son: • Resumen ejecutivo • Framework • Objetivos de control • Mapas de auditoría • Herramientas para su implementación • Guía de técnicas de gestión.
CMMI-SVC	Es un conjunto de mejores prácticas en áreas de proceso, para los proveedores de servicios, normalmente de TI, cuenta con un modelo de evaluación de implantación de los procesos en la organización, denominado SCAMPI (Standard CMMI Appraisal Method for Process Improvement)
ISO 20000	Según lo mencionado por NormaISO[19] es una norma internacional sobre los servicios TI, que fue publicada por ISO, es aceptada por la mayoría de los países, describe un conjunto de procesos de gestión diseñados para ayudar a brindar servicios de TI más eficaces (tanto dentro de su empresa como para sus clientes). ISO 20000 le proporciona la metodología y el marco que le ayuda a gestionar ITSM y, al mismo tiempo, permite demostrar que una empresa sigue las mejores prácticas. Con los requerimientos de la norma se logrará mejores procesos que ayudarán a al fortalecimiento en la prestación de los servicios TI. Además, ISO 20000 se puede aplicar a cualquier tamaño de empresa de cualquier sector económico.

Fuente: Autor

[19] NORMAS ISO. ISO 20000 CALIDAD DE LOS SERVICIOS TI. [En línea]. (consultado 19 de marzo de 2020) Normas ISO. España, Disponible en: https://www.normas-iso.com/iso-20000/

De igual forma, junto con las buenas prácticas relacionadas en el Cuadro 1, para la ejecución de la norma ISO/IEC 27005 es necesario establecer mecanismos de seguridad informática que permitan minimizar posibles ataques cibernéticos en diferentes áreas de una empresa, entre las que se encuentran la seguridad en sistemas operativos, bases de datos, páginas web y uso de herramientas como lo es la criptografía.

- Seguridad en redes: con el aumento del uso del internet por parte de las personas y empresas y de acuerdo con lo expresado con Fruhlinger[20] es necesario establecer una metodología que fortalezca el intercambio y el tráfico de información para que se realice de manera segura, buscando como principal objetivo la prevención y la ejecución de técnicas y herramientas que permitan evitar la intrusión de personas no autorizadas a las redes.

- Seguridad en base de datos: gran parte de la información importante para las empresas, organizaciones o personas, se encuentra almacenada en sistemas de gestores de bases de datos, los más utilizados son las bases de datos relacionales como Oracle, Microsoft SQL Server, My SQL y por parte de las no relaciones son Apache Cassandra. Según Villalobos[21] con el aumento del uso de BD aumentan los ataques a las mismas, razón por la cual es necesario implementar las técnicas y herramientas pertinentes para proteger estas, por lo tanto, es fundamental seguir los siguientes pasos, como son la identificación de las BD, realización de la evaluación de vulnerabilidades, configuraciones, ejecución de auditorías y monitoreo.

- Seguridad en páginas web: ya que actualmente existen diferentes tipos de ataques web que realizan inyección de secuencias de códigos con malas intenciones a través de ventanas emergentes y engaños como el Cross-site Scripting XSS, como lo expresa Sineray[22] la seguridad web permite proteger sitios en donde las corporaciones, organizaciones, empresas y personas interactúan con diferentes fines comerciales, sociales entre otros.

[20] FRUHLINGER Josh. ¿Qué es la seguridad de la red?. [En línea]. (consultado 19 de marzo de 2020) Network world.2018., Disponible en: https://www.networkworld.es/seguridad/que-es-la-seguridad-de-la-red

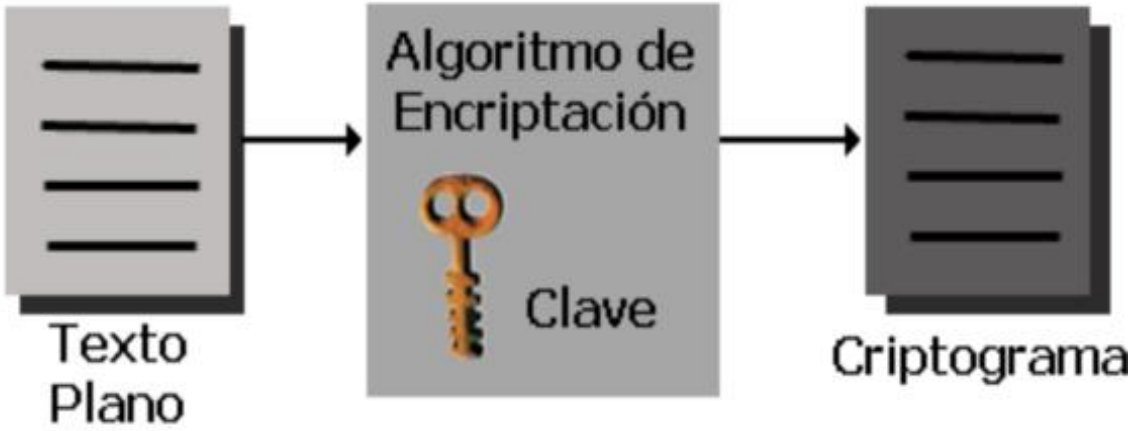
[21] VILLALOBOS Johnny. PRINCIPIOS BÁSICOS DE SEGURIDAD EN BASES DE DATOS. [En línea]. (consultado 19 de marzo de 2020) Disponible en:https://revista.seguridad.unam.mx/numero-12/principios-basicos-de-seguridad-en-bases-de-datos

[22] MOZ://A. Seguridad de Sitios Web. [En línea]. (consultado 19 de marzo de 2020) Disponible en: https://developer.mozilla.org/es/docs/Learn/Server-side/Primeros_pasos/seguridad_sitios_web

- Seguridad en sistemas operativos: Es la técnica y/o herramienta con la cual se pretende tener fuera de peligro, daño o riesgo el SO manteniendo la información confidencial, integra y disponible en todo momento, razón por la cual se debe proteger del acceso de personas no autorizadas con el fin de evitar la pérdida de datos. Como dice Sineray[23] al ser el sistema operativo el administrador de todos los recursos es pertinente ejercer medidas drásticas de seguridad para que no sea vulnerable a las catástrofes ambientales, errores de software, hardware y humano.

- Criptografía: es una técnica con la que se pretende ocultar información a personas no autorizadas, "la cual consiste en convertir datos de texto plano mediante un algoritmo de encriptación con claves a un criptograma"[24], como se puede observar en la Figura 2.

Figura 2. Encriptación



Fuente: BORGHELLO, Cristian. Criptología. [En línea]. (Consultado 19 de marzo de 2020) Disponible en: https://www.segu-info.com.ar/criptologia/criptologia.html

[23] SINERAY. Concepto de seguridad y sus estándares. [En línea]. (consultado 19 de marzo de 2020) Disponible en: http://sistoperasinequi.blogspot.com/2016/06/concepto-de-seguridad-y-sus-estandares.html

[24] BORGHELLO Cristian. Criptología. [En línea]. (consultado 19 de marzo de 2020) Disponible en: https://www.segu-info.com.ar/criptologia/criptologia.html

4.1.3 Ciclo PDCA. Es un requisito fundamental a la hora de implementar un SGSI basado en la norma ISO/IEC 27001, ya que describe los 4 pasos que se deben desarrollar de manera sistemática, para obtener disminución de fallos, aumentando eficiencia, eficacia y eliminación de vulnerabilidades. "El objetivo es la mejora continua y se adopta el modelo Plan-Do-Check-Act (PDCA o ciclo Demming) para todos los procesos de la organización."[25] Este permite que los procesos se encuentren en continua revisión verificando así la seguridad e identificando posibles mejoras que fortalezcan la seguridad cibernética de la compañía. Este ciclo cuenta con 4 fases que se evidencian en la Figura 3 y se relacionan a continuación:

- Plan - Planificar: en esta fase se identifican todos los aspectos que se van a involucrar a lo largo de la ejecución del proyecto. Pero se deben tener en cuenta unas premisas como las que mencionan Garcia, Quispe y Ráez[26] siendo estas, relacionar a las personas adecuadas, compilar la informacion disponible e identificar las necesidades de la compañía.

- Do – Hacer: en este paso es indispensable "implementar mejora, verificar las causas de los problemas y recopilar los datos apropiados"[27] con el fin de aplicar todas las acciones planeadas en la fase anterior.

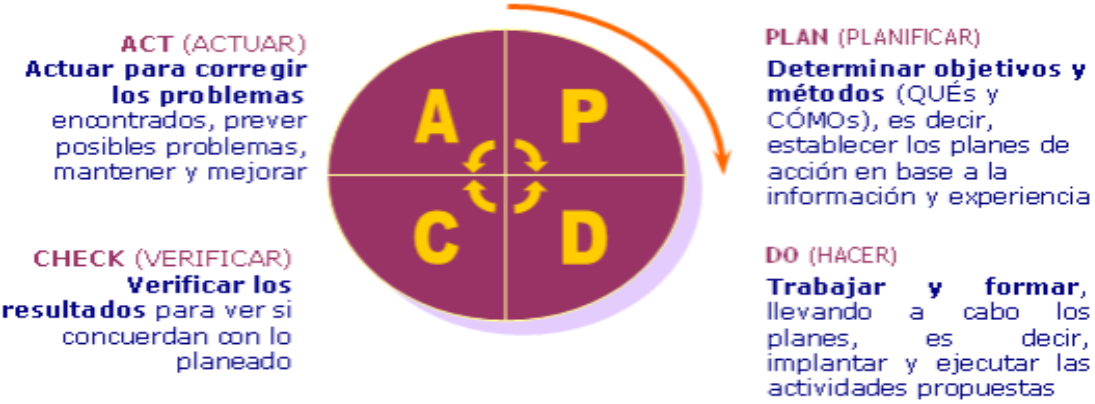
- Check – Verificar: en esta fase se deben resolver unas preguntas las cuales permitirán comprobar si las medidas implementadas están cumpliento con su función. Estos interrogantes podrían ser "¿Se han alcanzado los resultados deseados?, ¿Qué se aprendió? y ¿Qué queda aún por resolver?"[28].

- Act – Actuar: en este paso es fundamental efectuar las mejoras contempladas a las empresas con base en las siguientes premisas "la comprensión y el cumplimiento de los requisitos, la necesidad de considerar los procesos en términos que aporten valor, la obtención de resultados de desempeño y eficacia del proceso y la mejora continua de

[25] GOBIERNO DE ESPAÑA. ISO/IRC 27001: PDCA. [En línea]. (consultado 9 mayo de 2019) Ministerio de Educación, Cultura y Deporte. España, Disponible en: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/isoirc_27001_pdca.html
[26] GARCIA, Manuel; QUISPE, Carlos y RÁEZ, Luis. Mejora continua en la calidad de los procesos. [En línea]. (consultado 9 mayo de 2019 Industria data revista de investigación. Lima. 2003 P.5., Disponible en: https://www.redalyc.org/pdf/816/81606112.pdf
[27] Ibid., p. 5
[28] Ibid., p. 5

los procesos con base en medicones objetivas”[29].

Figura 3. Ciclo PDCA



Fuente: QUALITAS. Herramientas para la planificación y mejora de la calidad-unidad 4. [En línea]. (Consultado 18 de marzo de 2020) Disponible en: http://formacion.desarrollando.net/cursosfiles/femz/curso_240/ct0605-unidad04-rev0.pdf

4.1.4 Metodología MAGERIT. Es una herramienta que tiene como finalidad el análisis y gestión de riesgos por el uso de las tecnologías de la información, la cual fue desarrollada por el Consejo Superior de Administración Electrónica de España como respuesta al aumento y dependencia que tiene actualmente la humanidad en el uso de herramientas TI, “MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza”[30].

Actualmente, en el mercado existen diferentes metodologías que permiten realizar análisis y gestión de riesgos referentes al uso de las tecnologías de la información, entre estas se encuentran la NIST 800-30 y OCTAVE. Como se puede observar en

[29] Ibid., p. 6
[30] GOBIERNO DE ESPAÑA. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. (consultado 19 de marzo de 2020) Ministerio de Educación, Cultura y Deporte. Madrid, Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

el Cuadro 2 se plasman las ventajas y desventajas que tienen tres metodologías de análisis y gestión de riesgos, dando como resultado, que la Metodología MAGERIT, cuenta con fortalezas frente a las otras, como lo menciona el Gobierno de España[31], ya que tiene herramientas de software, análisis cuantitativos y amplios inventarios de recursos, que la hacen sobresalir, razón por la cual es la más utilizada al aplicar la norma ISO/IEC: 27001:2013.

Cuadro 2. Metodologías de gestión de riesgos

Metodologías	Ventajas	Desventajas
MAGERIT	• Ofrece un método sistematizado para analizar los riesgos • Ayuda a identificar y diseñar las medidas necesarias para reducir los riesgos • Cuenta con herramientas que ayudan a identificar riesgos. • Brinda un análisis de carácter cuantitativo y cualitativo • Brinda un extenso inventario de bienes.	• Al tener que traducir la valoración en valores económicos implica más gastos. • No incluye procesos ni recursos • No brinda varias políticas
NIST 800-30	• Bajo costo • Cuenta con una guía • Cuenta con un banco de elementos que son claves de las pruebas de seguridad técnicas y la evaluación con énfasis en técnicas	No tiene contemplado los elementos como los procesos, los activos ni las dependencias.
OCTAVE	• Implementa una metodología auto dirigida lo que implica que sus usuarios utilizan una evaluación de riesgos a través de su propio equipo multidisciplinar • Incluye procesos de gestión de riesgos • Involucra a toda la entidad • Se considera de las completas	• Implementa varios documentos • Requiere de personal altamente capacitado • No determina de manera clara la definición de los activos • No tiene presente el principio del no repudio.

Fuente: Autor

[31] Ibid., p. 1

4.2 MARCO CONCEPTUAL

4.2.1 Amenaza informática. Toda acción que puede afectar o atacar la seguridad de la información y surge de las vulnerabilidades de un sistema, normalmente ocasionadas por usuarios inexpertos o malware como por ejemplo “virus informático, los spywares, los troyanos, los gusanos y los hackers; existen amenazas internas y externas”[32].

4.2.2 Autenticación. Es un método con el cual se puede confirmar algo como verdadero ya que “se puede definir como un proceso en el que se busca confirmar algo como verdadero, no se busca verificar un usuario, ya que la autenticación no siempre está relacionada con estos, en muchos casos se quiere saber si un cambio o un dato es correcto”[33], actualmente se suele pensar en este proceso de validación únicamente con un usuario y contraseña, técnica que es bastante implementada en la informática debido a que brinda un portafolio amplio de seguridad, pero cualquier persona con usuario y clave de alguien más puede ingresar sin ningún inconveniente, debido a esto han surgido diferentes maneras de validar la autenticidad, algunas de estas se mencionan a continuación:

- Tokens o números aleatorios enviados al usuario.
- Tarjetas inteligentes.
- Características físicas como lo son la voz, huellas dactilares o la escritura de los usuarios.

[32] INSIGNIA. Amenaza. [En línea]. (consultado 19 de marzo de 2020) 2017. Disponible en: https://blog.elinsignia.com/2017/11/28/tipos-de-amenazas-informaticas/
[33] Ibid., p. 16

4.2.3 Control de accesos. Es un sistema automatizado de seguridad altamente eficiente por medio del cual las empresas, compañías, entidades o personas administran los ingresos a sus instalaciones. Actualmente existen diferentes tipos de control de acceso dependiendo de las dimensiones del espacio en el que se van a colocar o por la fuente de información que utilice la lectora. A continuación, se relacionan algunas:

- Sistemas complejos que implican operaciones en red, destinados a grandes plantas industriales. Generalmente, requieren la apertura de más de 4 puertas.
- Sistemas para establecimientos comerciales de mediana envergadura donde se suele necesitar la apertura de 2 a 4 puertas.
- Sistemas pequeños destinados a locales de poco metraje o pocas puertas. Requieren la apertura de 1 o 2 puertas.
- Tarjeta.
- Huella digital.
- Reconocimiento facial[34].

4.2.4 E MAIL SPOOFING. Consiste en la fabricación de un encabezado de correo electrónico con el fin de engañar al usuario para que piense que este se originó en un lugar de confianza. Debido a que los protocolos principales de correos electrónicos no tienen un método incorporado de autenticación, es común ver que las bandejas de entrada se encuentren llenas de mensajes no deseados y de phishing, ya que esta utiliza la metodología de suplantación de identidad para engañar al destinatario y lograr que confíe en el origen del mensaje.

El objetivo final de la suplantación de identidad por correo electrónico, es hacer que los destinatarios abran y posiblemente respondan una solicitud, por ejemplo lo mencionado en Barracuda[35], un correo electrónico falsificado puede ser de una empresa reconocida, pidiéndole al destinatario que proporcione información personal como un usuario, una contraseña, un número de tarjeta de crédito o incluso podría pedirle al destinatario que haga clic en un enlace que ofrece un beneficio por tiempo limitado, lo que en realidad es solo un enlace para descargar e instalar

[34] SISCA. ¿Qué es un control de acceso?. [En línea]. (consultado 19 de marzo de 2020) Caracas. 2015., Disponible en: http://sisca.co/nosotros-sisca-sistemas-integrales-de-seguridad/
[35] BARRACUDA. Email Spoofing. [En línea]. (consultado 19 de marzo de 2020) 2011 Disponible en: https://www.barracuda.com/glossary/email-spoofing

malware en el dispositivo del destinatario.

4.2.5 Firewall. Son elementos de hardware o de software que permiten o niegan a los computadores de una red el acceso a determinados sitios, de acuerdo a las políticas con las cuales sean administrados, se basan en la RFC 2979, que define las características de comportamiento y requerimientos de interoperabilidad en una red. Normalmente un cortafuego es el punto de conexión de la red LAN de una empresa con el internet; “de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna”.[36]

4.2.6 IP SPOOFING. La suplantación de IP es la creación de paquetes de Protocolo de Internet, que tienen una dirección de origen modificada con el fin de ocultar o suplantar la identidad del remitente, según lo mencionado en Cloudflare[37], frecuentemente es una técnica utilizada por los ciberdelincuentes para invocar ataques DDoS contra un dispositivo objetivo o la infraestructura circundante, ya que al enviar y recibir paquetes IP el destinatario automáticamente responde con envío de paquetes que se pierden y ocasionando saturación en la red y posteriormente DDoS.

4.2.7 Ley de mínimos privilegios. Para diseñar cualquier sistema que permita la administración de los recursos y activos de una empresa es necesario definir que cada usuario o herramienta solo debe ingresar o utilizar lo imprescindible para cumplir con las funciones de su cargo, como lo expresa Romero “son permisos de actuación que un usuario, sea una persona o un sistema tiene para actuar sobre otros recursos”[38].

[36] PEREZ-ROCA. Jesus; PEREIRA. Jose. Firewall. [En línea]. (consultado 19 de marzo de 2020) p 4., Disponible en: http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/06%20-%20Firewalls%20%5Bupdated%5D.pdf
[37] CLOUDFLARE. What is IP Spoofing? [En línea]. (consultado 19 de marzo de 2020) 2011 Disponible en: https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/
[38] Ibid., p. 32

4.2.8 Principios en gestión de la información. Existen 3 principios fundamentales que se deben cumplir al momento de tratar con algún tipo de información, lo cual permite que los datos almacenados de una entidad, empresa o persona permanezcan seguros. Estos se describen a continuación:

- Confidencialidad: la información nunca este a disposición de personas o entidades no autorizadas.
- Integridad: la información debe ser exacta e inalterable en todo momento independiente al proceso que se está ejecutando.
- Disponibilidad: en todo momento las personas o entidades autorizadas deben contar con acceso a los sistemas en los cuales se trate la información[39].

4.2.9 Servidores web. Son piezas de software de comunicaciones, las cuales sirven de puente entre la base de datos que contiene la información y el usuario que la solicita; "permiten las conexiones de manera unidireccional o bidireccional, de manera asíncrona o síncrona, estas están a la espera que llegue por parte del navegador web la solicitud de datos, siendo el más común el HTTP"[40].

4.2.10 Sistema de identificación biométrica. Método que permite la identificación de las personas por medio de sus características fisiológicas, este intenta imitar la manera por medio de las cuales los individuos renocen a sus semejantes como, por ejemplo, la voz, fisionomía o firma. "El procedimiento que realiza este sistema se basa en recolectar la información de las personas y compararla con la almacenada en las bases de datos"[41].

[39] ISO27000. Sistema de Gestión de la Seguridad de la Información. [En línea]. (consultado 19 de marzo de 2020) ISO27000. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

[40] RAFFINO Maria. Servidor web. [En línea]. (consultado 19 de marzo de 2020) Argentina. concepto.de. 2019., Disponible en: https://concepto.de/servidor-web/

[41] INSTITUTO NACIONAL DE CIBERSEGURIDAD. Tecnologías biométricas aplicadas a la ciberseguridad. [En línea]. (consultado 19 de marzo de 2020) Madrid. Gobierno de España. p 4., Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf

4.2.11 Virus informáticos. Son programas completos o partes de ellos diseñados con el fin de dañar o alterar el funcionamiento del equipo en el que se alojen, suelen ser creados con la función de autoreplicación, lo cual quiere decir que se multiplica el mismo en varias ocasiones, permitiéndole expandirse de manera rápida. A continuación se relacionan algunos de ellos: "virus de sector de arranque (BOOT), virus de archivos ejecutables, virus de macros, virus de lenguajes de Script, malware, gusanos, troyanos, spyware, keyloggers, adwares, dialers, backdoors, rootkits, bacterias y bombas de tiempo"[42].

4.2.12 Vulnerabilidad informática. Las vulnerabilidades informáticas son "fallos en un sistema que puede ser explotada por un atacante generando un riesgo para la organización o para el mismo sistema"[43], es decir, una ventana existente en la seguridad de una entidad, la cual abre la entrada a una amenaza para posteriormente producir un riesgo ante posibles ataques realizados por ciberdelincuentes, existen dos tipos de vulnerabilidades unas físicas y otras lógicas.

- Vulnerabilidades físicas: son las producidas por desastres naturales y por la falta de controles físicos en la infraestructura de una empresa, como por ejemplo incendios, inundaciones, terremotos, huracanes, violación de puertas, secuestro de instalaciones, conexión de dispositivos extraíbles sin autorización que roben datos o infecten el sistema, entre otras afecciones; frecuentemente estas "vulnerabilidades producen negación en el servicio, perdida de disponibilidad y privacidad en la información"[44].

- Vulnerabilidades lógicas: son las producidas por falta de configuración, actualización y desarrollo, las cuales afectan de manera directa la infraestructura informática de la empresa. Las vulnerabilidades de

[42] ROMERO CASTRO, Martha Irene, *et al.* Introducción a la seguridad informática y el análisis de vulnerabilidades. [En línea]. (consultado 19 de marzo de 2020) Alicante. Universidad estatal del sur de Manabi. 2018. p 15., Disponible en: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

[43] ROMERO, Martha, *et al.* Introducción a la seguridad informática y el análisis de vulnerabilidades. [En línea]. (consultado 19 de marzo de 2020) Alicante. Universidad estatal del sur de Manabi. 2018. p 41., Disponible en: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

[44] Ibid., p. 41

configuración, se refieren a las que traen por defecto los sistemas operativos o al realizar de manera equivocada la instalación tanto del SO o de aplicaciones posteriores; las vulnerabilidades de actualización, “hacen referencia a la no realización de las renovaciones pertinentes a medida que avanza la tecnología; las vulnerabilidades de desarrollo, son aquellas que permiten la intrusión de atacantes por medio de códigos de inyección”[45].

[45] Ibid., p. 42

5. DISEÑO METODOLÓGICO

5.1 TIPO DE PROYECTO

En el desarrollo del presente proyecto aplicado dentro de la empresa QWERTY S.A., fue necesario el uso de técnicas de diagnóstico cuantitativo como la realización de una encuesta y el análisis de la guía propuesta en el escenario, con el fin de obtener información de la organización con respecto a sus características y así establecer aspectos importantes, como lo es el alcance y los objetivos del SGSI. Para iniciar con el proceso fue necesario la realización de consulta sobre las normas ISO 27001, ISO 27005, Códigos de buenas prácticas informáticas, ciclo PDCA y metodologías de análisis y gestión de riesgos, donde se opta por MAGERIT, la cual permite la medición de riesgos, vulnerabilidades y amenazas con el ánimo de establecer un plan de mejora.

5.2 LÍNEA DE INVESTIGACIÓN

Este proyecto se relaciona directamente con la línea de investigación de Gestion de Sistemas, planteada por la cadena de formación en sistemas de la escuela de ciencias básicas tecnología e ingeniería de la Universidad Nacional Abierta y a Distancia UNAD.

5.3 METODOLOGÍA DEL DESARROLLO

Para el desarrollo del presente trabajo se abarcan diferentes tareas, esto con el fin de dar cumplimiento a los dos objetivos específicos trazados para cada enfoque propuesto en el escenario de QWERTY S.A. En el capítulo 6 denominado resultados se encuentran los subcapítulos 6.1 y 6.2 que hacen referencia al enfoque directivo – administrativo mientras que el 6.3 y 6.4 al enfoque técnico – estratégico; en estos subcapítulos se evidencian las actividades realizadas para cumplir con el objetivo general del proyecto.

En los subcapítulos 6.1 y 6.2 hacen referencia al enfoque directivo – administrativo, se desarrollan los dos primeros objetivos específicos. El primer objetivo se basa en la identificación de la situación actual de la empresa QWERTY S.A a través del reconocimiento de activos, valoración de estos y dimensiones de seguridad con las que cuenta actualmente la compañía y en el segundo objetivo se ejecuta el análisis de riesgos, amenazas y vulnerabilidades, fundamentado en la metodología MAGERIT, lo cual permite realizar gestión del riesgo, análisis de amenazas, riesgo intrínseco, salvaguardas, riesgo residual y aceptable para la empresa.

Dentro de los subcapitulos 6.3 y 6.4 se desembuelve el enfoque técnico – estratégico, se desarrollan los dos últimos objetivos específicos de la siguiente manera: en el primer objetivo se diseña un plan de monitoreo de los activos informáticos, mediante el cual se establece el control y seguimiento de estos, y en el segundo, se organiza un manual de seguridad informática basado en lo códigos de buenas prácticas orientadas a la ciberseguridad.

6. RESULTADOS

En los siguientes numerales se desarrolla el enfoque directivo – administrativo en el cual se realiza la descripción de la empresa QWERTY S.A., identificación de los activos informáticos, red de datos, equipos, aplicaciones, análisis con respecto a ISO/IEC 27001:2013, metodología, inventario de activos, evaluación de bienes de la empresa, evaluación y análisis de resultado de la organización del sistema de control interno, metodología y técnicas para el tratamiento del riesgo.

6.1 IDENTIFICACION DE QWERTY S.A.

Se desarrolla el cronograma del SGSI, costos del diseño del SGSI, identificación de la situación actual de la empresa QWERTY S.A a través del reconocimiento de activos, valoración de estos y dimensiones de seguridad con las que cuenta actualmente la compañía.

6.1.1 Tiempo de diseño del SGSI. Para el desarrollo del proyecto se establece un plazo de 6 meses contados a partir del 01/06/2019 al 01/12/2019, en los cuales se realizarán diferentes actividades que iran conformando el sistema de gestion de seguridad de la información en la compañía QWERTY S.A., estas acciones se evidenciaran mediante la identificación de los activos informáticos, un análisis con respecto a ISO/IEC 27001:2013, inventario de activos, evaluación de bienes de la empresa, evaluación del sistema de control interno de organización, resultado del análisis de la evaluación del sistema de control interno de la organización, metodología para el tratamiento del riesgo, técnicas para tratamiento de riesgos, plan de mejora de riesgos, política de seguridad SGSI, controles recomendados, monitoreo y un manual de seguridad. En Cuadro 3 se encuentra el cronograma detallado de actividades.

Cuadro 3. Cronograma detallado del SGSI

Actividad	Duración (días)	Comienzo	Fin
Descripción de la empresa QWERTY S.A.	5	04/06/2019	8/06/2019
Identificación de los activos informáticos, red de datos, equipos, aplicaciones.	5	05/06/2019	10/06/2019
Análisis con respecto a ISO/IEC 27001:2013	20	10/06/2019	04/07/2019
Metodología	10	11/06/2019	22/06/2019
Inventario de activos	5	22/06/2019	28/06/2019
Evaluación de bienes de la empresa	15	28/06/2019	16/07/2019
Evaluación del sistema de control interno de organización	20	16/07/2019	10/08/2019
Resultado del análisis de la evaluación del sistema de control interno de la organización	15	10/08/2019	28/08/2019
Metodología para el tratamiento del riesgo	15	28/08/2019	13/09/2019
Técnicas para tratamiento de riesgos	10	13/09/2019	24/09/2019
Plan de mejora de riesgos	15	24/09/2019	10/10/2019
Política de seguridad SGSI	15	24/09/2019	10/10/2019
Controles recomendados	15	24/09/2019	10/10/2019
Monitoreo	77	28/08/2019	30/11/2019
Manual de seguridad	15	24/09/2019	10/10/2019

Fuente: Autor

6.1.2 Costos del diseño del SGSI. Para el desarrollo del proyecto se requieren recursos humanos, siendo estos, 1 director de proyecto con un valor representativo por su trabajo de 16.000 COP por hora y 2 ingenieros TI con salario de 15.000 COP cada uno; el costo del recurso tecnológico se percibe monetariamente solo una vez, ya que la compañía realiza su compra. En el Cuadro 4, se evidencian las actividades requeridas para el desarrollo del SGSI junto con el valor total de cada una. El costo final del SGSI para la empresa QWERTY S.A. es de 79.720.000 COP.

Cuadro 4. Costos SGSI

Actividad	Recurso humano	Valor recurso humano X hora (COP)	Recurso recurso humano X dia (COP)	Recurso tecnológico	Valor recurso tecnológico (COP)	Total días de desarrollo	Total (COP)
Descripción de la empresa QWERTY S.A.	Director proyecto	16.000	128.000	PC IMAC	5.200.000	5	11.680.000
	Ingeniero TI1	15.000	120.000	PC IMAC	5.200.000		
Identificación de los activos informáticos, red de datos, equipos, aplicaciones.	Director proyecto	16.000	128.000	-	-	5	7.040.000
	Ingeniero TI1	15.000	120.000	-	-		
	Ingeniero TI2	15.000	120.000	PC IMAC	5.200.000		
Análisis con respecto a ISO/IEC 27001:2013	Director proyecto	16.000	128.000	-	-	20	7.360.000
	Ingeniero TI1	15.000	120.000	-	-		
	Ingeniero TI2	15.000	120.000	-	-		
Metodología	Ingeniero TI1	15.000	120.000	-	-	10	2.400.000
	Ingeniero TI2	15.000	120.000	-	-		
Inventario de activos	Director proyecto	16.000	128.000	-	-	5	640.000
Evaluación de bienes de la empresa	Director proyecto	16.000	128.000	-	-	15	3.720.000
	Ingeniero TI2	15.000	120.000	-	-		
Evaluación del sistema de control interno de organización	Director proyecto	16.000	128.000	-	-	20	7.360.000
	Ingeniero TI1	15.000	120.000	-	-		
	Ingeniero TI2	15.000	120.000	-	-		
Resultado del análisis de la evaluación del sistema de control interno de la organización	Director proyecto	16.000	128.000	-	-	15	1.920.000
Metodología para el tratamiento del riesgo	Director proyecto	16.000	128.000	-	-	15	3.720.000
	Ingeniero TI1	15.000	120.000	-	-		

Cuadro 4. (Continuación)

Actividad	Recurso humano	Valor recurso humano X hora (COP)	Recurso recurso humano X dia (COP)	Recurso tecnológico	Valor recurso tecnológico (COP)	Total días de desarrollo	Total (COP)
Técnicas para tratamiento de riesgos	Ingeniero TI1	15.000	120.000	-	-	10	2.400.000
	Ingeniero TI2	15.000	120.000	-	-		
Plan de mejora de riesgos	Director proyecto	16.000	128.000	-	-	15	3.720.000
	Ingeniero TI2	15.000	120.000	-	-		
Política de seguridad SGSI	Director proyecto	16.000	128.000	-	-	15	3.720.000
	Ingeniero TI1	15.000	120.000	-	-		
Actividad	Recurso humano	Valor recurso humano X hora (COP)	Recurso recurso humano X dia (COP)	Recurso tecnológico	Valor recurso tecnológico (COP)	Total días de desarrollo	Total (COP)
Controles recomendados	Director proyecto	16.000	128.000	X	X	15	3.720.000
	Ingeniero TI2	15.000	120.000	X	X		
Monitoreo	Ingeniero TI1	15.000	120.000	X	X	77	18.480.000
	Ingeniero TI2	15.000	120.000	X	X		
Manual de seguridad	Director proyecto	16.000	128.000	X	X	15	1.920.000
Total							79.720.000

Fuente: Autor

6.1.3 Objetivos de seguridad de la información. La confidencialidad, integridad y disponibilidad son 3 principios fundamentales que se deben cumplir para gestionar la información de la empresa QWERTY S.A., lo cual permite que los datos almacenados permanezcan seguros y disponibles; razón por la cual se escogen como base para el diseño del SGSI, de las políticas y del manual de usuario. Teniendo en cuenta estas premisas, a continuación, se relacionan los objetivos de seguridad de la información:

- Definir la informacion de la empresa como uno de los activos más importantes a proteger, por ende, debe salvaguardase en todo momento utilizando medidas de seguridad físicas y digitales.

- Implantar perfiles y responsabilidades a todos los colaboradores de la empresa, verificando el control sobre el acceso a la información de la compañía.

- Implementar sistemas de protección de las buenas prácticas TI a todos los procesos tecnológicos de la empresa.

- Fijar sanciones legales y/o penales a violaciones de seguridad de la información por parte de cualquier persona no autorizada.

6.1.4 Riesgos inherentes del SGSI. Al diseñar el sistema de gestión de seguridad de la información de la empresa QWERTY S.A. o de cualquier organización, se deben tener presentes algunos preligros o imprevistos que pueden detener de manera parcial o completa el proyecto. Con base en esta deducción, a continuación, se relacionan los riesgos inherentes al sistema que pueden interferir con SGSI de la compañía:

- Perdida de interés por parte de la alta dirección de QWERTY S.A.

- Falta de recursos económicos de la empresa QWERTY S.A. para el diseño del SGSI.

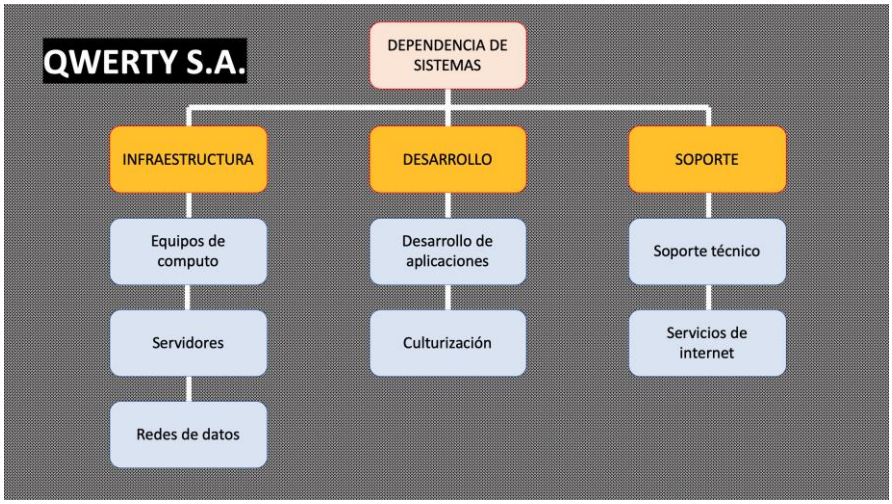
- Errores humanos.

- Retraso del diseño del SGSI.

- Aumento de costos en el diseño del SGSI.

6.1.5 Descripción de la empresa QWERTY S.A. La empresa QWERTY S.A., es una empresa del sector TI, donde su principal objetivo es contribuir al desarrollo tecnológico de las comunidades colombianas por medio de la utilización de herramientas de la tecnología de la información; cuenta con 120 trabajadores de diferentes niveles ocupacionales quienes son los que administran los activos informáticos para realizar las consultas, igualmente cuenta con una dependencia de sistemas que opera 24/7, distribuida en tres grandes grupos, como se observa en la Figura 4.

Figura 4. Distribución dependencia de sistemas



Fuente: Autor

Como se observa en la Figura 4 cada área cuenta con una serie de elementos que la definen y a la vez estos generan actividades las cuales se encuentran estipuladas en Cuadro 5, el cual define las responsabilidades que tienen asignadas cada una de las áreas y por medio de las cuales la dependencia de sistemas de QWERTY S.A. viene garantizando hasta el momento el funcionamiento de la compañía.

Cuadro 5. Funciones de la dependencia de sistemas

Área	Función
Área de infraestructura	Verificación de diseños de cableado estructurado.
	Soporte de acceso a la red interna y a internet.
Área de desarrollo	Apoyo técnico a las demás dependencias de la organización del centro en desarrollo de medios eficientes para lograr actividades basadas en usos de tecnologías de la informática y las telecomunicaciones.
Área de soporte	Mantenimiento únicamente de los equipos de la empresa.
	Generar conceptos para dar de baja equipos de la empresa.
	Realizar backups de todas las herramientas que almacenan datos y servidores virtuales que se encuentran en las dependencias de la compañía QWERTY S.A.

Fuente: Autor basado en Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. (Consultado 19 de marzo de 2020) Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

La dependencia de sistemas presta sus servicios a directivos, administrativos y operarios para cumplir con el objetivo de la compañía como es el de contribuir al desarrollo tecnológico de los colombianos y con el animo de lograr esta meta, estableció 3 áreas los cuales cuentan con personal capacitado en diferentes cargos y funciones. En cuadro 6 se plasman los perfiles y funciones de los colaboradores.

Cuadro 6. Cargos y funciones dependencia de sistemas

Cargo	Funciones
Gerente departamento de sistemas	Administrar el presupuesto del área informática.
	Dirigir y supervisar equipos de trabajo.
	Realizar la comunicación con la rectoría general.
	Coordinar la implementación de proyectos tecnológicos.
Coordinador de infraestructura	Supervisar el correcto funcionamiento de los recursos físicos y lógicos del Centro a nivel nacional.
	Asignar funciones y responsabilidades.
	Realizar la comunicación con el gerente del departamento de sistemas y otros coordinadores.
Ingeniero de redes	Administrar los recursos de red como router, swtiches y firewall.
	Administrador el direccionamiento de cada una de las sedes del centro.
	Comunicar al coordinador incidentes o eventos relacionados con la red de la organización.
	Brindar soporte de nivel II a los fallos de la red o el internet reportados en el centro.

Cuadro 6. (Continuación)

Cargo	Funciones
Ingeniero de sistemas	Realizar la administración de los servidores de bases de datos, web, DHCP, DNS, Dominio, correo, PBX y archivos.
	Administrar el licenciamiento de cada uno de los softwares utilizados por el centro.
	Coordinar la adquisición de nuevos equipos de cómputo o dispositivos tecnológicos.
	Comunicar al coordinador incidentes o eventos relacionados con los servidores, equipos de cómputo, licenciamiento y demás recursos tecnológicos del centro.
Coordinador de desarrollo	Coordinar el desarrollo e implementación de nuevos proyectos de software en el centro.
	Asignar funciones y responsabilidades.
	Realizar la comunicación con el gerente del departamento de sistemas y otros coordinadores.
Ingeniero de software	Realizar la toma de requerimientos para el desarrollo de aplicaciones tecnológicas.
	Diseñar los respectivos diagramas según los requerimientos.
	Validar el cumplimiento de los requerimientos en los aplicativos.
	Comunicar al coordinador incidentes o eventos relacionados con el proceso de diseño del aplicativo tecnológico.

Cuadro 6. (Continuación)

Cargo	Funciones
Programador	Realizar el desarrollo del aplicativo tecnológico según los requerimientos del centro.
	Brindar soporte de nivel III a los fallos reportados en los softwares desarrollados por la organización.
	Comunicar al coordinador incidentes o eventos relacionados con el proceso de desarrollo del aplicativo tecnológico.
Coordinador de soporte	Coordinar la prestación del servicio de soporte en el centro. Supervisar la calidad en la prestación del servicio de soporte.
	Asignar funciones y responsabilidades.
	Realizar la comunicación con el gerente del departamento de sistemas y otros coordinadores.
Técnico de soporte	Brindar soporte nivel I a equipos de cómputo y demás recursos tecnológicos de la compañía.
	Realizar mantenimientos preventivos y correctivos a los activos tecnológicos.
	Apoyar la gestión en el uso de usuarios y contraseñas.
	Comunicar al coordinador incidentes o eventos relacionados con la prestación del soporte técnico.

Fuente: Autor

6.1.6 Identificación de activos informáticos: en el Cuadro 7, se especifica la información general que va a ser utilizada para la gestión de activos de la compañía QWERTY S.A., donde se desglosa el objetivo, el alcance, el contexto legal y el enfoque metodológico que va a tener, el cual está basado en la metodología MAGERIT; estos servirán de premisas a la hora de realizar el análisis de riesgos de cada componente perteneciente a la infraestructura tecnológica de la empresa.

Cuadro 7. Premisas gestión de activos

Objetivo	Realizar el análisis de riesgos sobre los activos TI y de información en la compañía QWERTY S.A.
Alcance	El análisis de riegos se realizará en los activos tecnológicos y de información de la empresa QWERTY S.A.
Nombre de la empresa	QWERTY S.A.
Contexto legal	NTC ISO/IEC 27001
Enfoque metodológico	El enfoque de gestión de riesgos a aplicar está basado en la metodología MAGERIT

Fuente: Autor basado en Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. (Consultado 19 de marzo de 2020) Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

6.1.6.1 Red de datos. Actualmente las actividades de las empresas requieren para su funcionamiento cotidiano realizar carga y descarga de archivos pesados, soporte de aplicaciones multimedia, servidores de correo, web y de información. La empresa QWERTY S.A. no es ajena a estas necesidades ya que su objetivo principal es incrementar el desarrollo tecnológico en comunidades colombianas mediante la utilización de las tecnologías de la información, razón por la cual cuenta con un canal de internet de 25 Megas en ancho de banda dedicado, por medio del cual realiza todas sus actividades.

6.1.6.2 Equipos informáticos QWERTY S.A. Según lo reportado por la dependencia de sistemas actualmente la compañía cuenta con 47 dispositivos electrónicos que prestan el servicio pertinente para el funcionamiento y cumplimiento del objetivo de la empresa, estos equipos se encuentran distribuidos en las diferentes oficinas, departamentos y dependencias que forman parte de QWERTY S.A., como se evidencia en el Cuadro 8.

Cuadro 8. Equipos informáticos de QWERTY S.A.

Equipo	Ubicación	Cantidad
Servidor DELL en torre PowerEdge T440	N/A	4
Impresora HP LaserJet Enterprise serie 600	Oficina de nómina y facturación	1
Impresora SMART MultiXpress M4370LX	Dependencia directiva y administrativa	1
Servidor DELL en torre PowerEdge T130	Oficina antigua de sistemas	1
Computadores	Dependencias del centro	21
Cortafuegos ASA 5505	N/A	1
HUB	Red de datos del centro	4
Switches cisco catalyst 2960	Red de datos del centro	6
Teléfonos ip	Dependencias del centro	6
Puntos de acceso	Departamento de sistemas	2

Fuente: Autor

6.1.6.3 Aplicaciones QWERTY S.A. De acuerdo con lo reportado por la dependencia de sistemas, actualmente la compañía cuenta con diferentes programas que prestan el servicio pertinente para el funcionamiento y cumplimiento del objetivo de la empresa según lo estipulado en los protocolos de la misma; estas herramientas informáticas intangibles cuentan con características las cuales cumplen una función específica, en el Cuadro 9 se muestran.

Cuadro 9. Software

Aplicación	Características
Página web	Servicio contratado con GoDaddy, en el cual el gestor de contenidos es Joomla y cuenta con un servidor apache, PHP y MySQL
Servidor de nómina y facturación	Montado sobre Apache 2.4.25 PHP 5.6.30 – 7.11 MySQL 5.7.17 phpMyAdimin 4.6.6
Sistema operativo Windows 10 pro	

Fuente: Autor

6.1.7 Análisis con respecto a ISO/IEC 27001:2013. Al realizar el estudio de la situación actual de QWERTY S.A. se implementa un análisis basado en la ISO/IEC 27001:2013, con el fin de evaluar el contexto de la organización en cuanto a liderazgo, operación, planificación, valoración del desempeño y aplicación de las mejoras pertinentes, con el fin de lograr elaborar este diagnóstico inicial, es necesario tener presente los controles del anexo A de la norma, nombrados a continuación:

- A.5 Política de seguridad.
- A.6 Organización de la seguridad de la información.
- A.7 Administración de recursos.
- A.8 Seguridad de los recursos humanos.
- A.9 Seguridad física y del entorno.

- A.10 Administración de las comunicaciones y operaciones.
- A.11 Control de acceso.
- A.12 Adquisición de sistemas de información, desarrollo y mantenimiento.
- A.13 Administración de los incidentes de seguridad
- A.14 Administración de la continuidad del negocio
- A.15 Cumplimiento (legales, de estándares, técnicas y auditorias)[46]

De acuerdo con la información obtenida de la empresa QWERTY S.A., se implementa una encuesta en la cual se indagan los controles que exige la norma ISO 27001 en su Anexo A y que es diligenciada por parte del director de proyecto, con la información suministrada por la dependencia de sistemas. Esta encuesta se encuentra anexada al documento en el anexo A. Para la tabulación y análisis de la información obtenida de la encuesta, se tomarán 3 criterios de valoración los cuales tendrán diferentes siglas y estados como se evidencian en el Cuadro 10.

Cuadro 10. Criterios de estado

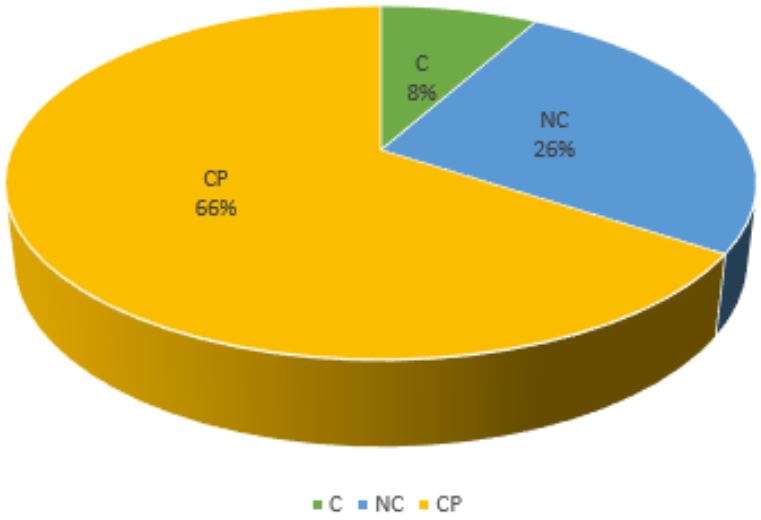
Sigla	Estado
NC	No cumple con control
CP	Cumple parcialmente con control
C	Cumple con control

Fuente: Autor

La encuesta inicial realizada por el director del proyecto de acuerdo con la información brindada por el jefe de la oficina de sistemas, presenta como resultado el estado actual de la compañía QWERTY S.A., siendo este, que de los 111 controles evaluados únicamente 9 se encuentran en estado (C) cumple con el control, 73 cumplen parcialmente (CP) y 29 no cumplen, como se especifica a continuación en la Figura 5.

[46] ISOTOOLS. Anexo A en ISO 27001, objetivos de control y controles de referencia. [En línea]. ISOTOOLS excellence 2020., (consultado 6 de marzo de 2020). Disponible en: https://www.pmg-ssi.com/2020/03/anexo-a-en-iso-27001-objetivos-de-control-y-controles-de-referencia/

Figura 5. Gráfica de resultado encuesta inicial



Fuente: Autor

De acuerdo con este resultado se puede deducir, que en este momento, la empresa QWERTY S.A. no cuenta con los mínimos requisitos que solicita la norma ISO 27001, ya que según los controles evaluados, el 26% de ellos, que equivalen a 29 controles, no se están implementando; el 66%, es decir, 73 controles cumplen parcialmente y el 8 % ósea en 9 controles se evidencia el cumplimento, lo que significa una amplia ventana de vulnerabilidades, sobre todo a través de los 3 controles donde se marca un incumplimiento del 100%, como se evidencia en el Cuadro 11, el cual contiene los resultados de manera cuantitativa.

Cuadro 11. Resultados encuesta

CONTROL	C	NC	CP	TOTAL DE ÍTEMS	% C	% NC	% CP
A.5 Política de seguridad.		1	1	2	0%	50%	50%
A.6 Disposición de los mecanismos de control de los datos		6	1	7	0%	86%	14%
A.7 Administración de recursos.		6		6	0%	100%	0%
A.8 Seguridad de los recursos humanos.	1	3	6	10	10%	30%	60%

Cuadro 11. (Continuación)

CONTROL	C	NC	CP	TOTAL DE ÍTEMS	% C	% NC	% CP
A.9 Seguridad física y del entorno.	1	2	11	14	7%	14%	79%
A.10 Administración de las comunicaciones y operaciones.		2		2	0%	100%	0%
A.11 Control de acceso.	5		10	15	33%	0%	67%
A.12 Adquisición de sistemas de información, desarrollo y mantenimiento.		1	12	13	0%	8%	92%
A.13 Administración de los incidentes de seguridad			7	7	0%	0%	100%
A.14 Administración de la continuidad del negocio	2		11	13	15%	0%	85%
A.15 Cumplimiento (legales, de estándares, técnicas y auditorias)		5		5	0%	100%	0%

Fuente: Autor basado en Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. (Consultado 19 de marzo de 2020) Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

6.2 ANÁLISIS DE RIESGOS.

Fundamentado en la metodología MAGERIT, lo cual permite realizar gestión del riesgo, análisis de amenazas, riesgo intrínseco, salvaguardas, riesgo residual y aceptable para la empresa QWERTY S.A.

6.2.1 Metodología análisis de riesgos. Para la elaboración del plan de mejora se opta por implementar la metodología MAGERIT, la cual permite realizar análisis y gestión del riesgo de los sistemas de información, contiene 3 capítulos en los cuales se desglosa el paso a paso a realizar e implementar esta herramienta, para ISO 27001 este método es el centro de todo análisis de riesgos porque es uno de los más completos.

6.2.2 Inventario de activos. Según lo expuesto, en esta metodología el primer paso es realizar un inventario de activos con el fin de determinar los componentes o las funcionalidades que posee la empresa. A continuación, se describen las siglas utilizadas en la metodología MAGERIT, para posteriormente implementarlas en el Cuadro 12.

Columna 1:
Según el tipo de activo

- D: activo de datos.

Columna 2:
Según el tipo de datos

- ADM: Datos para implementar al interior de una organización.
- COM: Tiene valor para los servicios de la Organización.
- TEST: Se usan para pruebas antes de salir a producción.

Columna 3:
Según el nivel de confidencialidad

- CON: Confidencial.
- INT: Interno.
- PUB: Publico.

Adicional se utiliza un consecutivo para cada activo para este caso sería (D01, D02, DO3 y así sucesivamente)

Cuadro 12. Inventario de activos

Código	MAGERIT			Activo de información	Responsable	Disponibilidad
D01	D	ADM	CON	Correo electrónico	Dependencia de sistemas	24/7
D02	D	COM	CON	Mantenimiento de activos informáticos	Dependencia de sistemas	24/7

D03	D	COM	CON	Gestión de usuarios y contraseñas	Dependencia de sistemas	24/7
D04	D	ADM	CON	Nómina de trabajadores	Dependencia de nómina y facturación	24/7
D05	D	ADM	CON	Recibos de pago	Dependencia de nómina y facturación	24/7
D06	D	ADM	CON	Hojas de vida	Dependencia de nómina, facturación y sistemas	24/7
D07	D	COM	CON	Seguimiento al talento humano	Dependencia de nómina y facturación	24/7
D08	D	COM	CON	Certificados laborales	Dependencia de nómina y facturación	24/7
D09	D	COM	CON	Servidor DELL en torre PowerEdge T440	Dependencia de sistemas	24/7
D10	D	COM	CON	Impresora HP LaserJet Enterprise serie 600	Dependencia de sistemas	24/7
D11	D	COM	CON	Impresora SMART MultiXpress M4370LX	Dependencia de sistemas	24/7
D12	D	COM	CON	Servidor DELL en torre PowerEdge T130	Dependencia de sistemas	24/7
D13	D	COM	CON	Computadores	Dependencia de sistemas	24/7
D14	D	COM	CON	Cortafuegos ASA 5505	Dependencia de sistemas	24/7
D15	D	COM	CON	HUB	Dependencia de sistemas	24/7
D16	D	COM	CON	Switches cisco catalyst 2960	Dependencia de sistemas	24/7
D17	D	COM	CON	Teléfonos ip	Dependencia de sistemas	24/7

Cuadro 12. (Continuación)

Código	MAGERIT			Activo de información	Responsable	Disponibilidad
D18	D	COM	CON	Puntos de acceso	Dependencia de sistemas	24/7

Fuente: Autor basado en Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. (Consultado 19 de marzo de 2020) Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

6.2.3 Evaluación de bienes de la empresa. Con base en los activos identificados dentro de la empresa QWERTY S.A. es necesario asignarle a cada activo su correspondiente valoración, en la Tabla 1 se estipulan los criterios a seguir, los cuales tiene una valoración que va desde 0 a 10, los cuales permitirán ejercer una calificación cuantitativa que brindará apoyo al desarrollo del SGSI.

Tabla 1. Criterios de valoración

Valor	Pauta
10	N 10
9	N 9
8	N 8 (+)
7	A
6	A (-)
5	M (+)
4	M
3	M (-)
2	B (+)
1	B
0	D

Fuente: Autor basado en Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. (Consultado 19 de marzo de 2020) Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

En la Cuadro 13 se evidencia el valor propio de los activos, el cual es el resultado de establecer a cada uno de ellos un criterio de valoración junto con un criterio de evaluación, los cuales son:

- [D] Disponible
- [I] Integridad de la información
- [C] Privacidad de los datos
- [A] Autenticación de ingresos
- [T] Seguimiento de los servicios

Cuadro 13. Valor propio de los activos

Activos		**Dimensiones**				
Código	**Activo de información**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
D01	Correo electrónico	9	9	9	9	9
D02	Mantenimiento de activos informáticos	8	8	5	5	5
D03	Gestión de usuarios y contraseñas	9	9	9	9	9
D04	Nómina de trabajadores	9	8	7	7	7
D05	Recibos de pago	6	6	6	6	6
D06	Hojas de vida	7	7	7	7	7
D07	Seguimiento al talento humano	8	8	5	5	2
D08	Certificados laborales	6	6	6	6	6
D09	Servidor DELL en torre PowerEdge T440	9	9	9	9	8
D10	Impresora HP LaserJet Enterprise serie 600	6	0	0	5	8

Cuadro 13. (Continuación)

Activos		Dimensiones				
Activo de información	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	
D11	Impresora SMART MultiXpress M4370LX	6	0	0	5	8
D12	Servidor DELL en torre PowerEdge T130	9	9	9	9	9
D13	Computadores	9	8	9	8	8
D14	Cortafuegos ASA 5505	10	7	7	10	7
D15	HUB	8	8	8	8	8
D16	Switches cisco catalyst 2960	8	8	8	8	8
D17	Teléfonos ip	5	5	5	5	0
D18	Puntos de acceso	7	7	7	7	7

Fuente: Autor basado en Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. (Consultado 19 de marzo de 2020) Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Una vez se tiene el valor del activo para la empresa QWERTY S.A., se procede a establecer los peligros que podrían dañar cada dispositivo, existen 4 grandes grupos de amenazas mencionadas en esta metodología y a su vez cada una cuentan con sus subgrupos, los cuales son:

- [N] Desastres naturales
- [N.1] Fuego

- [N.2] Daños por agua
- [N.*] Desastres naturales
- [I] De origen industrial
- [I.1] Fuego
- [I.2] Daños por agua
- [I.*] Desastres industriales
- [I.3] Contaminación mecánica
- [I.4] Contaminación electromagnética
- [I.5] Avería de origen físico o lógico
- [I.6] Corte del suministro eléctrico
- [I.7] Condiciones inadecuadas de temperatura o humedad
- [I.8] Fallo de servicios de comunicaciones
- [I.9] Interrupción de otros servicios y suministros esenciales
- [I.10] Degradación de los soportes de almacenamiento de la información
- [I.11] Emanaciones electromagnéticas
- [E] Errores y fallos no intencionados
- [E.1] Errores de los usuarios
- [E.2] Errores del administrador
- [E.3] Errores de monitorización (log)
- [E.4] Errores de configuración
- [E.7] Deficiencias en la organización
- [E.8] Difusión de software dañino
- [E.9] Errores de [re-]encaminamiento
- [E.10] Errores de secuencia
- [E.14] Escapes de información
- [E.15] Alteración accidental de la información
- [E.18] Destrucción de información
- [E.19] Fugas de información
- [E.20] Vulnerabilidades de los programas (software)
- [E.21] Errores de mantenimiento / actualización de programas (software)
- [E.23] Errores de mantenimiento / actualización de equipos (hardware)
- [E.24] Caída del sistema por agotamiento de recursos
- [E.25] Pérdida de equipos
- [E.28] Indisponibilidad del personal
- [A] Ataques intencionados
- [A.3] Manipulación de los registros de actividad (log)
- [A.4] Manipulación de la configuración
- [A.5] Suplantación de la identidad del usuario
- [A.6] Abuso de privilegios de acceso
- [A.7] Uso no previsto
- [A.8] Difusión de software dañino
- [A.9] [Re-] encaminamiento de mensajes
- [A.10] Alteración de secuencia
- [A.11] Acceso no autorizado

- [A.12] Análisis de tráfico
- [A.13] Repudio
- [A.14] Interceptación de información (escucha)
- [A.15] Modificación deliberada de la información
- [A.18] Destrucción de información
- [A.19] Divulgación de información
- [A.22] Manipulación de programas
- [A.23] Manipulación de los equipos
- [A.24] Denegación de servicio
- [A.25] Robo
- [A.26] Ataque destructivo
- [A.27] Ocupación enemiga
- [A.28] Indisponibilidad del personal
- [A.29] Extorsión
- [A.30] Ingeniería social (picaresca)[47]

Ahora bien, con base en estos grupos se procede a realizar la tabla de identificación de amenazas, vulnerabilidades, riesgo, nivel de riesgo, probabilidad de ocurrencia, nivel de impacto y salvaguardas, con el fin de determinar el estado actual de la seguridad de la información de la empresa QWERTY S.A., como se evidencia el Cuadro 14.

Cuadro 14. Identificación de amenazas

Código	Activo	Tipo	Amenaza	Vulnerabilidad	Riesgo	Nivel de riesgo	Probabilidad de ocurrencia	Nivel de impacto	Salvaguardas
D01	Correo electrónico	[S] Servicios	[E.4] Errores de configuración [E.19] Fugas de información [E.20] Vulnerabilidades de los programas	Inexistencia de procedimientos para la implementación de configuraciones de seguridad en el correo electrónico	Accesos no autorizados al correo electrónico	Importante	Media	Moderado	Ninguna

[47] GOBIERNO DE ESPAÑA. MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos [En línea]. Madrid 2012., (consultado 7 de mayo de 2019). Disponible en: http://administracionelectronica.gob.es/

Cuadro 14. (Continuación)

Código	Activo	Tipo	Amenaza	Vulnerabilidad	Riesgo	Nivel de riesgo	Probabilidad de ocurrencia	Nivel de impacto	Salvaguardas
D02	Mantenimiento de activos informáticos	[S] Servicios	[E.1] Fallos de usuarios [E.20] Vulnerabilidades de los programas [E.10] Errores de secuencia [E.18] Eliminación de activos	Inexistencia de procedimiento para la realización del mantenimiento de los activos de información	Deterioro, fallo o afectación de los activos de información	Bajo	Bajo	Leve	Hoja de datos con los registros de los mantenimientos realizados
D03	Gestión de usuarios y contraseñas	[D] Datos	[A.5] Suplantación de la identidad del usuario [I.5] Deterioro de origen físico o lógico [E.1] Errores de los usuarios [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas [E.24] Caída del sistema por el agotamiento de recursos [E.4] Errores de monitorización	Inexistencia de política para la creación de contraseñas seguras de acceso	Accesos o usos no autorizados de la información y recursos tecnológicos	Critico	Alto	Catastrófico	Ninguno
D04	Nómina de trabajadores	[D] Datos	[A.5] Suplantación de la identidad del usuario [E.1] Errores de los usuarios [E.2] Errores del administrador	Carencia de controles para el acceso a la información de los trabajadores	Modificación o eliminación de la información de los trabajadores	Critico	Medio	Catastrófico	Ninguna

Cuadro 14. (Continuación)

Código	Activo	Tipo	Amenaza	Vulnerabilidad	Riesgo	Nivel de riesgo	Probabilidad de ocurrencia	Nivel de impacto	Salvaguardas
D05	Recibos de pago	[D] Datos	[I.5] Deterioro de origen físico o lógico [A.6] Abuso de privilegios de acceso [A.18] Destrucción de la información [E.3] fallos de vigilancia [E.18] Eliminación de activos [E.19] Fugas de información	Inexistencia de procedimiento de backup	Indisponibilidad de la información por afectaciones físicas o lógicas de los recursos tecnológicos	Importante	Medio	Moderado	Ninguna
D06	Hojas de vida	[D] Datos	[I.5] Deterioro de origen físico o lógico [A.6] Abuso de privilegios de acceso [A.18] Destrucción de la información [E.3] fallos de vigilancia [E.18] Eliminación de activos [E.19] Fugas de información	Carencia de controles para el acceso a la información de las hojas de vida	Modificación o eliminación de la información de las hojas de vida	Importante	Medio	Moderado	Ninguna
D07	Seguimiento al talento humano	[D] Datos	[I.5] Deterioro de origen físico o lógico [A.6] Abuso de privilegios de acceso [A.18] Destrucción de la información [E.3] fallos de vigilancia [E.18] Eliminación de activos	Falta de medidas de seguimiento para el acceso a la información por parte del personal de talento humano	Alteración o eliminación de la información de la compañía	Apreciable	Bajo	Moderado	Ninguna
D08	Certificados laborales	[D] Datos	[N.1] Fuego [N.2] Daños por agua [I.1] Fuego [I.2] Daños por agua [I.5] Avería de origen físico o lógico [E.23] Errores de mantenimiento/actualización de equipos [E.25] Perdida de equipos	Inexistencia de procedimiento de backup	Indisponibilidad de la información por afectaciones físicas o lógicas de los recursos tecnológicos	Apreciable	Medio	Leve	Ninguna

Cuadro 14. (Continuación)

Código	Activo	Tipo	Amenaza	Vulnerabilidad	Riesgo	Nivel de riesgo	Probabilidad de ocurrencia	Nivel de impacto	Salvaguardas
D09	Servidor DELL en torre PowerEdge T440 (DHCP, HTTP)	[HW] Equipamiento informático	[I.5] Deterioro de origen físico o lógico [A.6] Abuso de privilegios de acceso [A.18] Destrucción de la información [E.3] Errores de monitorización [E.18] Destrucción de la información [E.19] Fugas de información	Condiciones de climatización no optimas	Indisponibilidad de la información por afectaciones físicas o lógicas de los recursos tecnológicos	Importante	Alto	Catastrófico	Ninguna
D10	Impresora HP LaserJet Enterprise serie 600	[HW] Equipamiento informático	[I.5] Deterioro de origen físico o lógico [A.6] Abuso de privilegios de acceso [A.18] Destrucción de la información [E.3] Errores de monitorización [E.18] Destrucción de la información [E.19] Fugas de información	Falta de procedimientos para la realización de mantenimientos físicos y/o lógicos	Indisponibilidad de la información por afectaciones físicas o lógicas de los recursos tecnológicos	Apreciable	Alto	Leve	Hoja de datos con los registros de los mantenimientos realizados
D11	Impresora SMART MultiXpress M4370LX	[HW] Equipamiento informático	[E.1] Fallos del personal [E.2] Fallos de administración [E.3] Fallos de vigilancia [E.20] Vulnerabilidades de los programas [E.20] Fallos de autoría [A.8] Difusión de software dañino [A.12] Análisis de trafico [A.27] Ocupación enemiga	Falta de procedimientos para la realización de mantenimientos físicos y/o lógicos	Indisponibilidad de la información por afectaciones físicas o lógicas de los recursos tecnológicos	Apreciable	Alto	Leve	Hoja de datos con los registros de los mantenimientos realizados
D12	Servidor DELL en torre PowerEdge T130 (PBX)	[HW] Equipamiento informático	[N.1] Fuego [N.2] Daños por agua [I.1] Fuego [I.2] Daños por agua [I.5] Deterioro de origen físico o lógico [A.6] Abuso de privilegios de acceso [E.1] Fallos del personal [E.2] Fallos de administración [E.3] Fallos de equipo	No existe controles de acceso para el acceso físico a los servidores	Robo, daño, alteración o eliminación de la información o los elementos físicos del activo	Importante	Medio	Catastrófico	Ninguna

Cuadro 14. (Continuación)

Código	Activo	Tipo	Amenaza	Vulnerabilidad	Riesgo	Nivel de riesgo	Probabilidad de ocurrencia	Nivel de impacto	Salvaguardas
D13	Computadores	[HW] Equipamiento informático	[E.1] Errores de los usuarios [E.2] Errores del administrador [E.3] Errores de monitorización	Inexistencia de procedimientos para el acceso a la información contenida en los equipos	Robo, alteración o eliminación de la información contenida en los equipos	Importante	Alto	Catastrófico	Ninguna
D14	Cortafuegos ASA 5505	[COM] Redes de comunicaciones	[E.1] Fallos del personal [E.2] Fallos de administración [E.3] Fallos de vigilancia [A.8] Difusión de software dañino [E.20] Errores de mantenimiento/actualización de programas	Inexistencia de reglas de seguridad	Afectación de los recursos tecnológico y de información de la compañía por ataques informáticos	Importante			Ninguna
D15	HUB	[COM] Redes de comunicaciones	[I.5] Deterioro de origen físico o lógico [A.6] Abuso de privilegios de acceso [E.1] Fallos del personal [E.2] Fallos de administración [E.3] Fallos de vigilancia [E.20] Vulnerabilidades de los programas [E.20] Errores de mantenimiento/actualización de programas	No existe segmentación de la red	Acceso a la información por usuarios no autorizados	Importante	Medio	Catastrófico	Ninguna
D16	Switches cisco catalyst 2960	[COM] Redes de comunicaciones	[A.6] Abuso de privilegios [A.18] Destrucción de la información [A.15] Modificación deliberada de la información [A.22] Manipulación de programas [A.23] Manipulación de equipos	No existe segmentación de la red	Acceso a la información por usuarios no autorizados	Importante	Medio	Catastrófico	Ninguna

Cuadro 14. (Continuación)

Código	Activo	Tipo	Amenaza	Vulnerabilidad	Riesgo	Nivel de riesgo	Probabilidad de ocurrencia	Nivel de impacto	Salvaguardas
D17	Teléfonos ip	[AUX] Equipamiento auxiliar	[A.6] Abuso de privilegios [A.18] Eliminación de activos [A.15] Modificación deliberada de los activos [A.22] Utilización de software [A.23] Utilización de equipos [A.30] Ingeniería social (picaresca)	Instalaciones con riesgos de colapso	Indisponibilidad del recurso tecnológico	Bajo	Bajo	Leve	Ninguno
D18	Puntos de acceso	[COM] Redes de comunicaciones	[N.1] Fuego [N.2] Daños por agua [I.1] Fuego [I.2] Daños por agua [I.5] Deterioro de origen físico o lógico [A.6] Abuso de privilegios de acceso [[E.1] Fallos del personal [E.2] Fallos de administración [E.3] Fallos de vigilancia [E.20] Vulnerabilidades de los programas [E.20] Errores de mantenimiento/actualización de programas [A.8] Difusión de software dañino [A.12] Análisis de tráfico [A.27] Ocupación enemiga	No existe procedimientos para la protección de las redes inalámbricas	Afectación de los recursos tecnológico y de información de la compañía por ataques informáticos	Apreciable	Medio	Moderado	Ninguna
D19	Página web	[S] Servicios	[A24] Denegación de servicio	Carencia de reglas de seguridad en el firewall	Afectación de la disponibilidad de la página web por ataque informático	Critico	Alto	Catastrófico	Hospedaje del sitio web en dominio de respaldo
D20	Software antivirus	[SW] Software	[E21] Errores de mantenimiento / actualización de programas (software)	Falta de seguimiento al estado del software	Ejecución de software malicioso en los equipos de la organización	Importante	Medio	Moderado	Herramientas de reinstalación del software

Cuadro 14. (Continuación)

Código	Activo	Tipo	Amenaza	Vulnerabilidad	Riesgo	Nivel de riesgo	Probabilidad de ocurrencia	Nivel de impacto	Salvaguardas
D12	Base de datos MySQL	[D] Datos	[A15] Modificación deliberada de la información	No existe trazabilidad en la asignación de permisos de usuario	Alteración o eliminación de información de manera no autorizada	Critico	Alto	Catastrófico	Copia de seguridad de las bases de datos

Fuente: Autor basado en Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. (Consultado 20 de marzo de 2020) Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Ahora se deben valorar las amenazas, vulnerabilidades, riesgo, nivel de riesgo, probabilidad de ocurrencia, nivel de impacto y salvaguardas identificadas, para esto se tiene en cuenta la degradación de valor las cuales se establecen en diferentes rangos desde muy alta hasta baja tal cual se evidencia en la Tabla 2.

Tabla 2. Degradación del valor

MA	MUY ALTA
A	ALTA
M	MEDIA
B	BAJA
MB	MUY BAJA

Fuente: Autor basado en Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. (Consultado 19 de marzo de 2020) Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

En la Tabla 3 se establecen las probabilidades de ocurrencia dentro de las que se encuentran muy rara, siglos, poco probable, posible, muy alto y casi seguro; las cuales serán aplicadas a las amenazas, vulnerabilidades, riesgos, nivel de riesgo, probabilidad de ocurrencia, nivel de impacto y salvaguardas identificadas

Tabla 3. Probabilidad de ocurrencia

CS	CASI SEGURO
MA	MUY ALTO
P	POSIBLE
PP	POCO PROBABLE
MB	SIGLOS
MR	MUY RARA

Fuente: Autor basado en Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. (Consultado 20 de marzo de 2020) Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Con base en lo pautado anteriormente se procede a realizar la valoración de amenazas encontradas en los activos informáticos de la empresa QWERTY S.A. como se evidencia en el Cuadro 15.

Cuadro 15. Valoración de amenazas

Activos		Amenazas	P	D	I	C	A	T
Código	Activo de información							
D01	Correo electrónico	[E.4] Errores de configuración	MA	A	A	A	A	M
		[E.19] Fugas de información	P	A	MA	A	A	M
		[E.20] Vulnerabilidades de los programas	p	A	A	A	A	M
D02	Mantenimiento de activos informáticos	[E.1] Fallos de personal	P	A	A	A	MA	M

Cuadro 15. (Continuación)

Activos		Amenazas	P	D	I	C	A	T
Código	Activo de información							
		[E.20] Vulnerabilidades de los programas	P	M	M	A	-	M
		[E.10] Errores de secuencia						
		[E.18] Eliminación de información	P	A	M	M	-	M
D03	Gestión de usuarios y contraseñas	[I.5] Deterioro de origen físico o lógico	P	A	M	A	MA	A
		[E.1] Errores de los usuarios	MA	A	A	A	MA	A
		[E.8] Difusión de software dañino	P	A	M	A	-	A
		[E.20] Vulnerabilidades de los programas	P	A	A	A	-	A
		[E.24] Caída del sistema por el agotamiento de recursos	-	-	-	-	-	-
		[E.4] Errores de monitorización	PP	A	A	A	-	A
D04	Nómina de trabajadores	[A.5] Suplantación de la identidad del usuario	P	A	MA	A	A	A
		[E.1] Errores de los usuarios	-	-	-	-	-	-
		[E.2] Errores del administrador	P	A	MA	A	A	A
		[E.3] Errores de monitorización	P	A	A	A	A	A
		[E.7] Deficiencias en la organización	P	A	A	A	A	A

Cuadro 15. (Continuación)

Activos		Amenazas	P	D	I	C	A	T
Código	Activo de información							
D05	Recibos de pago	[I.5] Deterioro de origen físico o lógico	P	A	A	A	MA	A
		[A.6] Abuso de privilegios de acceso	P	A	A	A	MA	A
		[A.18] Destrucción de la información	P	A	A	A	MA	A
		[E.3] Fallos de vigilancia	P	A	A	A	MA	A
		[E.18] Eliminación de activos	P	A	A	A	MA	A
		[E.19] Fugas de información	P	A	A	A	MA	A
D06	Hojas de vida	[I.5] Deterioro de origen físico o lógico	P	A	A	A	M	A
		[A.6] Abuso de privilegios de acceso	P	A	A	A	M	M
		[A.18] Destrucción de la información	P	A	A	A	M	A
		[E.3] Errores de monitorización	P	A	M	A	M	M
		[E.18] Destrucción de la información	P	A	A	M	M	A
		[E.19] Fugas de información	P	A	A	A	M	M
D07	Seguimiento al talento humano	[I.5] Deterioro de origen físico o lógico	MA	A	M	A	A	M
		[A.6] Abuso de privilegios de acceso	P	A	M	M	M	M
		[A.18] Destrucción de la información	P	A	M	A	A	M
		E.3] Fallos de vigilancia	P	A	M	M	M	M
		[E.18] Eliminación de activos	P	A	M	M	A	M
		[E.19] Fugas de información	P	A	M	M	M	M
D08	Certificados laborales	[N.1] Fuego	PP	A	A	A	M	M
		[N.2] Daños por agua	PP	A	A	A	M	M
		[I.1] Fuego	P	A	A	A	M	M
		[I.2] Daños por agua	P	A	A	A	M	M
		[I.5] Deterioro de origen físico o lógico	P	A	A	A	M	M
		[E.23] Errores de mantenimiento/actualización de equipos	P	A	A	A	M	M
		[E.25] Perdida de equipos	-	-	-	-	-	-
		[A.23] Manipulación de equipos	-	-	-	-	-	-

Cuadro 15. (Continuación)

Activos		Amenazas	P	D	I	C	A	T
Código	Activo de información							
D09	Servidor DELL en torre PowerEdge T440	[I.5] Deterioro de origen físico o lógico	P	M	M	M	A	M
		[A.6] Abuso de privilegios de acceso	P	M	M	M	A	M
		[A.18] Destrucción de la información	P	M	M	M	A	M
		E.3] Fallos de vigilancia	P	M	M	M	A	M
		[E.18] Eliminación de activos de la información	P	M	M	M	A	M
		[E.19] Fugas de información	P	M	A	M	A	M
D10	Impresora HP LaserJet Enterprise serie 600	[I.5] Deterioro de origen físico o lógico	P	B	A	A	M	A
		[A.6] Abuso de privilegios de acceso	P	B	A	A	M	A
		[A.18] Destrucción de la información	P	P	A	A	M	A
		E.3] Fallos de vigilancia	P	P	A	A	M	A
		[E.18] Eliminación de activos	P	P	A	A	M	A
		[E.19] Fugas de información	P	P	A	A	M	A
D11	Impresora SMART MultiXpress M4370LX	[E.1] Fallos de usuarios	P	A	B	M	A	A
		[E.2] Fallos de administrador	P	A	B	M	A	A
		[E.3] fallos de vigilancia	P	A	B	M	A	A
		[E.20] Vulnerabilidades de los programas	P	A	B	A	A	A
		[E.20] Errores de mantenimiento/actualización de programas	-	-	-	-	-	-
		[A.8] Difusión de software dañino	P	A	B	A	B	A
D12	Servidor DELL en torre PowerEdge T130	[N.1] Fuego	PP	M	M	M	M	B
		[N.2] Daños por agua	PP	M	M	M	M	B
		[I.1] Fuego	PP	M	M	M	M	B
		[I.2] Daños por agua	PP	M	M	M	M	B
		[I.5] Deterioro de origen físico o lógico	P	A	A	A	A	B
		[A.6] Abuso de privilegios de acceso	P	A	A	A	A	B
		[E.1] Fallos de usuarios	P	A	A	A	A	B
		[E.2] Fallos de administrador	P	A	M	A	A	M
		[E.3] fallos de vigilancia	P	A	M	A	A	M
		[E.20] Vulnerabilidades de los programas	P	A	M	A	A	M

Cuadro 15. (Continuación)

Activos		Amenazas	P	D	I	C	A	T
Código	Activo de información							
D13	Computadores	[E.1] Errores de los usuarios	PP	A	A	A	A	A
		[E.2] Errores del administrador	PP	A	A	A	A	A
		[E.3] Errores de monitorización	PP	A	A	A	A	A
D14	Cortafuegos ASA 5505	[E.1] Fallos de usuarios	P	A	M	M	A	M
		[E.2] Fallos de administrador	P	A	A	M	A	A
		[E.3] fallos de vigilancia	P	A	M	M	A	M
		[A.8] Difusión de software dañino	P	A	A	A	A	A
		[E.20] Errores de mantenimiento/actualización de programas	P	A	M	A	A	A
D15	HUB	[I.5] Deterioro de origen físico o lógico	P	A	M	A	A	A
		[A.6] Abuso de privilegios de acceso	P	A	A	B	A	A
		[[E.1] Fallos de usuarios	P	A	M	B	A	A
		[E.2] Fallos de administrador	P	A	M	B	A	A
		[E.3] fallos de vigilancia	P	A	M	B	A	M
		[E.20] Vulnerabilidades de los programas	P	A	-	-	-	-
		[E.20] Errores de mantenimiento/actualización de programas	-	-	-	-	-	-
D16	Switches cisco catalyst 2960	[A.6] Abuso de privilegios	PP	A	A	M	A	A
		[A.18] Eliminación de los datos	P	A	A	M	A	-
		[A.15] Modificación deliberada de la información	P	A	A	M	A	-
		[A.22] Manipulación de programas	-	-	-	-	-	-
		[A.23] Manipulación de equipos	P	A	A	M	M	M
D17	Teléfonos ip	[A.6] Abuso de privilegios	P	A	A	M	A	A
		[A.18] Destrucción de la información	P	A	A	A	A	A
		[A.15] Modificación deliberada de la información	P	A	A	A	A	A
		[A.22] Manipulación de programas	-	-	-	-	-	-
		[A.23] Manipulación de equipos	P	A	A	A	A	A
		[A.30] Ingeniería social (picaresca)	P	A	A	A	A	M

Cuadro 15. (Continuación)

Activos		Amenazas	P	D	I	C	A	T
Código	Activo de información							
D18	Puntos de acceso	[N.1] Fuego	PP	M	M	M	M	M
		[N.2] Daños por agua	PP	M	M	M	M	M
		[I.1] Fuego	P	-	A	-	A	-
		[I.2] Daños por agua	P	-	A	-	A	-
		[I.5] Deterioro de origen físico o lógico	P	-	A	-	A	-
		[A.6] Abuso de privilegios de acceso	P	-	A	-	A	-
		[E.1] Fallos de usuarios	P	-	A	-	A	-
		[E.2] Fallos de administrador	P	-	A	-	A	-
		[E.3] fallos de vigilancia	P	-	A	-	A	-
		[E.20] Vulnerabilidades de los programas	P	-	A	-	A	-
		[E.20] Errores de mantenimiento/actualización de programas	P	-	A	-	A	-
		[A.8] Difusión de software dañino	P	-	A	-	A	-
		[A.12] Análisis de tráfico	P	-	-	-	M	-
		[A.27] Ocupación enemiga	P	-	A	-	A	-

Fuente: Autor basado en Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. (Consultado 20 de marzo de 2020) Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

6.2.4 Evaluación del sistema de control interno de organización. En el cuadro 16 se evidencia la evaluación del sistema de control interno de la organización a partir de los controles propuestos en el Anexo A de la norma ISO/IEC 27001, realizado mediante la utilización del instrumento: *ISO27k ISMS and controls status with SoA and gaps Spanish.xlsx*

Cuadro 16. Controles de seguridad de la información en QWERTY S.A.

Sección	Controles de Seguridad de la Información	Estado
A5	**Políticas de seguridad de la información**	
A5.1	**Directrices de gestión de la seguridad de la información**	
A5.1.1	Políticas para la seguridad de la información	Inexistente
A5.1.2	Revisión de las políticas para la seguridad de la información	No aplicable
A6	**Organización de la seguridad de la información**	
A6.1	**Organización interna**	
A6.1.1	Roles y responsabilidades en seguridad de la información	Inexistente
A6.1.2	Segregación de tareas	? Desconocido
A6.1.3	Contacto con las autoridades	Inexistente
A6.1.4	Contacto con grupos de interés especial	No aplicable

Cuadro 16. (Continuación)

Sección	Controles de Seguridad de la Información	Estado
A6.1.5	Seguridad de la información en la gestión de proyectos	Inexistente
A6.2	**Los dispositivos móviles y el teletrabajo**	
A6.2.1	Política de dispositivos móviles	Inexistente
A6.2.2	Teletrabajo	No aplicable
A7	**Seguridad relativa a los recursos humanos**	
A7.1	**Antes del empleo**	
A7.1.1	Investigación de antecedentes	Definido
Sección	**Controles de Seguridad de la Información**	**Estado**
A7.1.2	Términos y condiciones del empleo	Definido
A7.2	**Durante el empleo**	
A7.2.1	Responsabilidades de gestión	Inicial
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Inexistente
A7.2.3	Proceso disciplinario	Inexistente
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**	

Cuadro 16. (Continuación)

Sección	Controles de Seguridad de la Información	Estado
A7.3.1	Responsabilidades ante la finalización o cambio	Inexistente
A8	**Gestión de activos**	
A8.1	**Responsabilidad sobre los activos**	
A8.1.1	Inventario de activos	Definido
A8.1.2	Propiedad de los activos	Definido
A8.1.3	Uso aceptable de los activos	Inexistente
A8.1.4	Devolución de activos	Inexistente
A8.2	**Clasificación de la información**	
A8.2.1	Clasificación de la información	Inexistente
A8.2.2	Etiquetado de la información	No aplicable
A8.2.3	Manipulado de la información	Inexistente
A8.3	**Manipulación de los soportes**	
A8.3.1	Gestión de soportes extraíbles	Inexistente
A8.3.2	Eliminación de soportes	No aplicable
A8.3.3	Soportes físicos en tránsito	No aplicable
A9	**Control de acceso**	
A9.1	**Requisitos de negocio para el control de acceso**	
Sección	**Controles de Seguridad de la Información**	**Estado**
A9.1.1	Política de control de acceso	Inexistente

Cuadro 16. (Continuación)

Sección	Controles de Seguridad de la Información	Estado
A9.1.2	Acceso a las redes y a los servicios de red	Inexistente
A9.2	**Gestión de acceso de usuario**	
A9.2.1	Registro y baja de usuario	? Desconocido
A9.2.2	Provisión de acceso de usuario	Inexistente
A9.2.3	Gestión de privilegios de acceso	? Desconocido
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Inicial
A9.2.5	Revisión de los derechos de acceso de usuario	? Desconocido
A9.2.6	Retirada o reasignación de los derechos de acceso	Inexistente
A9.3	**Responsabilidades del usuario**	
A9.3.1	Uso de la información secreta de autenticación	Inexistente
A9.4	**Control de acceso a sistemas y aplicaciones**	
A9.4.1	Restricción del acceso a la información	Inexistente
A9.4.2	Procedimientos seguros de inicio de sesión	Inicial
A9.4.3	Sistema de gestión de contraseñas	Inexistente

Cuadro 16. (Continuación)

Sección	Controles de Seguridad de la Información	Estado
A9.4.4	Uso de utilidades con privilegios del sistema	No aplicable
A9.4.5	Control de acceso al código fuente de los programas	Inicial
A10	**Criptografía**	
A10.1	**Controles criptográficos**	
A10.1.1	Política de uso de los controles criptográficos	No aplicable
A10.1.2	Gestión de claves	No aplicable
A11	**Seguridad física y del entorno**	
A11.1	**Áreas seguras**	
A11.1.1	Perímetro de seguridad física	Inexistente
A11.1.2	Controles físicos de entrada	Inexistente
A11.1.3	Seguridad de oficinas, despachos y recursos	? Desconocido
A11.1.4	Protección contra las amenazas externas y ambientales	Inexistente
A11.1.5	El trabajo en áreas seguras	Inexistente
A11.1.6	Áreas de carga y descarga	No aplicable
A11.2	**Seguridad de los equipos**	
A11.2.1	Emplazamiento y protección de equipos	Inicial
A11.2.2	Instalaciones de suministro	Inexistente

Cuadro 16. (Continuación)

Sección	Controles de Seguridad de la Información	Estado
A11.2.3	Seguridad del cableado	Definido
A11.2.4	Mantenimiento de los equipos	Definido
A11.2.5	Retirada de materiales propiedad de la empresa	No aplicable
A11.2.6	Seguridad de los equipos fuera de las instalaciones	No aplicable
A11.2.7	Reutilización o eliminación segura de equipos	Inexistente
A11.2.8	Equipo de usuario desatendido	No aplicable
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	No aplicable
A12	**Seguridad de las operaciones**	
A12.1	**Procedimientos y responsabilidades operacionales**	
A12.1.1	Documentación de procedimientos operacionales	Definido
A12.1.2	Gestión de cambios	No aplicable
A12.1.3	Gestión de capacidades	No aplicable
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	Inexistente
A12.2	**Protección contra el software malicioso (malware)**	

Cuadro 16. (Continuación)

Sección	Controles de Seguridad de la Información	Estado
A12.2.1	Controles contra el código malicioso	Inicial
A12.3	**Copias de seguridad**	
A12.3.1	Copias de seguridad de la información	Inicial
A12.4	**Registros y supervisión**	
A12.4.1	Registro de eventos	
A12.4.2	Protección de la información del registro	
A12.4.3	Registros de administración y operación	
A12.4.4	Sincronización del reloj	No aplicable
A12.5	**Control del software en explotación**	
A12.5.1	Instalación del software en explotación	Inicial
A12.6	**Gestión de la vulnerabilidad técnica**	
A12.6.1	Gestión de las vulnerabilidades técnicas	No aplicable
A12.6.2	Restricción en la instalación de software	

Cuadro 16. (Continuación)

Sección	Controles de Seguridad de la Información	Estado
A12.7	**Consideraciones sobre la auditoria de sistemas de información**	
A12.7.1	Controles de auditoría de sistemas de información	Inexistente
A13	**Seguridad de las comunicaciones**	
A13.1	**Gestión de la seguridad de las redes**	
A13.1.1	Controles de red	Inexistente
A13.1.2	Seguridad de los servicios de red	Inexistente
A13.1.3	Segregación en redes	Inexistente
A13.2	**Intercambio de información**	
A13.2.1	Políticas y procedimientos de intercambio de información	Inexistente
A13.2.2	Acuerdos de intercambio de información	No aplicable
A13.2.3	Mensajería electrónica	Inexistente
A13.2.4	Acuerdos de confidencialidad o no revelación	Inicial
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**	

Cuadro 16. (Continuación)

Sección	Controles de Seguridad de la Información	Estado
A14.1	**Requisitos de seguridad en los sistemas de información**	
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	No aplicable
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Inicial
A14.1.3	Protección de las transacciones de servicios de aplicaciones	Inexistente
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**	
A14.2.1	Política de desarrollo seguro	Inexistente
A14.2.2	Procedimiento de control de cambios en sistemas	No aplicable
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	No aplicable
A14.2.4	Restricciones a los cambios en los paquetes de software	No aplicable
A14.2.5	Principios de ingeniería de sistemas seguros	Inexistente
A14.2.6	Entorno de desarrollo seguro	Inexistente
A14.2.7	Externalización del desarrollo de software	Inexistente

Cuadro 16. (Continuación)

Sección	Controles de Seguridad de la Información	Estado
A14.2.8	Pruebas funcionales de seguridad de sistemas	Inicial
A14.2.9	Pruebas de aceptación de sistemas	No aplicable
A14.3	**Datos de prueba**	
A14.3.1	Protección de los datos de prueba	No aplicable
A15	**Relación con proveedores**	
A15.1	**Seguridad en las relaciones con proveedores**	
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	Inexistente
A15.1.2	Requisitos de seguridad en contratos con terceros	Inexistente
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	No aplicable
A15.2	**Gestión de la provisión de servicios del proveedor**	
A15.2.1	Control y revisión de la provisión de servicios del proveedor	No aplicable
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	No aplicable

Cuadro 16. (Continuación)

Sección	Controles de Seguridad de la Información	Estado
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**	
A16.1.1	Responsabilidades y procedimientos	Inexistente
A16.1.2	Notificación de los eventos de seguridad de la información	Inexistente
A16.1.3	Notificación de puntos débiles de la seguridad	Inexistente
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	No aplicable
A16.1.5	Respuesta a incidentes de seguridad de la información	Inexistente
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	No aplicable
A16.1.7	Recopilación de evidencias	No aplicable
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**	
A17.1	**Continuidad de la seguridad de la información**	
A17.1.1	Planificación de la continuidad de la seguridad de la información	Inexistente

Cuadro 16. (Continuación)

Sección	Controles de Seguridad de la Información	Estado
A17.1.2	Implementar la continuidad de la seguridad de la información	Inexistente
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	
A17.2	**Redundancias**	
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	Inexistente
A18	**Cumplimiento**	
A18.1	**Cumplimiento de los requisitos legales y contractuales**	
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	No aplicable
A18.1.2	Derechos de Propiedad Intelectual (DPI)	Inexistente
A18.1.3	Protección de los registros de la organización	No aplicable
A18.1.4	Protección y privacidad de la información de carácter personal	Inexistente
A18.1.5	Regulación de los controles criptográficos	No aplicable
A18.2	**Revisiones de la seguridad de la información**	

Cuadro 16. (Continuación)

Sección	Controles de Seguridad de la Información	Estado
A18.2.1	Revisión independiente de la seguridad de la información	No aplicable
A18.2.2	Cumplimiento de las políticas y normas de seguridad	Inexistente
A18.2.3	Comprobación del cumplimiento técnico	Inexistente

Fuente: Autor basado en Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. (Consultado 20 de marzo de 2020) Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

6.2.5 Resultado de la evaluación. El resultado del análisis de la evaluación realizada a la dependencia de sistemas de la compañía QWERTY S.A. permite definir el mecanismo a implementar en el sistema de seguridad de la información como se representan en la Cuadro 17.

Cuadro 17. Resultados

Estado	**Significado**	**Proporción de Controles de Seguridad de la Información**
? Desconocido	No ha sido verificado	**9%**
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	**45%**
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.	**10%**

Cuadro 17. (Continuación)

Estado	Significado	Proporción de Controles de Seguridad de la Información
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	**0%**
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.	**6%**
Administrado	El control se lleva a cabo de acuerdo con un procedimiento documentado, aprobado y formalizado.	**0%**
Optimizado	El control se aplica de acuerdo con un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	**0%**
No aplicable	A fin de certificar un SGSI, todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.	**31%**

Fuente: Autor basado en Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. (Consultado 20 de marzo de 2020) Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

6.2.6 Tratamiento del riesgo. Una vez se tienen determinados y analizados los riesgos y controles del Anexo A de la norma, se deben establecer las medidas a tomar con el fin de proteger, prevenir, minimizar y controlar los mismos, de igual manera se brindará una política de seguridad para así poder mantener en todo momento la confidencialidad, integridad y disponibilidad de la información. Teniendo en cuenta la matriz RASCI.

6.2.6.1 Metodología para el tratamiento del riesgo. Lo primero que se debe tener en cuenta para el tratamiento de los riesgos encontrados es analizar la situación presente en la empresa para determinar en cuál de los siguientes casos se ubica.

- Caso 1. Existe una vulnerabilidad y es necesario ejecutar mecanismos que garanticen que la limitación de esta.

- Caso 2. Existe una vulnerabilidad y se puede explotar es necesario la implementación de protección de capas, diseños arquitectónicos y los diferentes controles administrativos que garanticen la disminución del riesgo.

- Caso 3. Incrementar los costos para el atacante, con el fin de que sea mayor el costo del ataque que la ganancia potencial por el ataque.

- Caso 4. Determinar si la pérdida es muy grande para implementar principios de diseño, métodos y procedimientos con el fin de limitar el alcance del ataque.

Partiendo de lo anterior y la valoración de riesgos realizada, se plasma en la Figura 6. Estrategia para tratamiento de riesgos, la siguiente estrategia:

Figura 6. Estrategias para el tratamiento de riesgos

ESTRATEGIAS PARA EL TRATAMIENTO DEL RIESGO				
PROBABILIDAD	ALTA	3. ZONA DE RIESGO TOLERANTE PROCEDIMIENTO: MINIMIZAR LA POSIBILIDAD DE QUE OCURRA	6. ZONA DE RIESGO EXTREMO PROCEDIMIENTO: REDUCIR EL RIESGO EVITAR EL RIESGO COMPARTIR O TRANSFERIR	6. ZONA DE RIESGO EXTREMO PROCEDIMIENTO: REDUCIR EL RIESGO EVITAR EL RIESGO COMPARTIR O TRANSFERIR
	MEDIA	2. ZONA DE RIESGO BAJO PROCEDIMIENTO: MINIMIZAR LA POSIBILIDAD DE QUE OCURRA	3. ZONA DE RIESGO TOLERANTE PROCEDIMIENTO: MINIMIZAR LA POSIBILIDAD DE QUE OCURRA	6. ZONA DE RIESGO EXTREMO PROCEDIMIENTO: REDUCIR EL RIESGO EVITAR EL RIESGO COMPARTIR O TRANSFERIR
	BAJA	1. ZONA DE RIESGO BAJO TRATAMIENTO: ASUMIR EL RIESGO	1. ZONA DE RIESGO BAJO TRATAMIENTO: REDUCIR EL RIESGO	3. ZONA DE RIESGO TOLERANTE PROCEDIMIENTO: MINIMIZAR LA POSIBILIDAD DE QUE OCURRA
		BAJA	MEDIA	ALTA

Fuente: MOYANO. Luz y SUAREZ. Yasmin. Plan de implementación del sgsi basado en la norma iso 27001:2013 para la empresa interfaces y soluciones. [En línea]. (Consultado 20 de marzo de 2020) Disponible en: http://repository.udistrital.edu.co/bitstream/11349/6737/1/MoyanoOrjuelaLuzAdriana2017.pdf

6.2.6.2 Técnicas para tratamiento de riesgos. Para definir las técnicas a implementar es necesario conocer las prioridades de la empresa con el fin de que al riesgo detectado se apliquen diferentes técnicas según corresponda, en Cuadro 18 se realiza la evaluación final con la cual se pretende establecer un plan de mejora de riesgos tomando como directriz los siguientes casos:

- Aceptar (A): Indica la aceptación del riesgo ya que ha sido analizado y tiene muy baja ocurrencia de que suceda, esta técnica reconoce el riesgo y lo acepta de manera pasiva.

- Evitar (E): Por medio de esta técnica se pretende evitar el riesgo, ya que presenta una probabilidad medio-alta de que suceda, por lo cual puede ocasionar daños significativos dentro de la empresa. Razón por la cual busca suprimir completamente la amenaza.

- Controlar (C): Por medio de esta técnica se pretende tomar todas las acciones necesarias para impedir que un hecho suceda y cause daños en los sistemas de la empresa.

- Investigar (I): Por medio de esta técnica se pretende diferir las acciones que se realizan, ya que si no se tiene una respuesta clara incita a realizar una investigación más a fondo.

- Mitigar (M): Esta técnica se emplea en el momento que se presenta y se materializa una amenaza.

- Transferir (T): Por medio de esta técnica se pasa parcial o completamente el riesgo a otra empresa, a través de una póliza o de un contrato.

Cuadro 18. Evaluación y tratamiento de riesgos

ID	VULNERABILIDAD	A	C	E	I	M	T	TOTAL
VA_001	[E.4] Errores de configuración			1				1
VA_002	[E.19] Fugas de información		1					1
VA_003	[E.20] Vulnerabilidades de los programas				1			1

Cuadro 18. (Continuación)

ID	VULNERABILIDAD	A	C	E	I	M	T	TOTAL
VA_004	[E.1] Errores de los usuarios			1				1
VA_005	[E.20] Vulnerabilidades de los programas				1			1
VA_006	[E.10] Errores de secuencia				1			1
VA_007	[E.18] Destrucción de la información			1				1
VA_008	[I.5] Deterioro de origen físico o lógico			1				1
VA_009	[E.1] Errores de los usuarios			1				1
VA_010	[E.8] Difusión de software dañino		1					1
VA_011	[E.20] Vulnerabilidades de los programas				1			1
VA_012	[E.24] Caída del sistema por el agotamiento de recursos		1					1
VA_013	[E.4] Errores de monitorización		1					1
VA_014	[A.5] Suplantación de la identidad del usuario			1				1
VA_015	[E.1] Errores de los usuarios			1				1
VA_016	[E.2] Errores del administrador			1				1
VA_017	[E.3] Errores de monitorización		1					1
VA_018	[E.7] Deficiencias en la organización	1						1
VA_019	[I.5] Deterioro de origen físico o lógico			1				1
VA_020	[A.6] Abuso de privilegios de acceso			1				1
VA_021	[A.18] Destrucción de la información			1				1
VA_022	[E.3] Errores de monitorización		1					1
VA_023	[E.18] Eliminación de los datos			1				1
VA_024	[E.19] Escapes de datos		1					1
VA_025	[I.5] Deterioro de origen físico o lógico			1				1
VA_026	[A.6] Abuso de privilegios de acceso			1				1
VA_027	[A.18] Destrucción de la información			1				1
VA_028	[E.3] Errores de monitorización			1				1
VA_029	[E.18] Eliminación de la información			1				1

Cuadro 18. (Continuación)

ID	VULNERABILIDAD	A	C	E	I	M	T	TOTAL
VA_030	[E.19] Escape de datos			1				1
VA_031	[I.5] Deterioro de origen físico o lógico			1				1
VA_032	[A.6] Abuso de privilegios de acceso		1					1
VA_033	[A.18] Destrucción de la información		1					1
VA_034	[E.3] Errores de monitorización		1					1
VA_035	[E.18] Eliminación de los datos		1					1
VA_036	[E.19] Filtraciones de datos		1					1
VA_037	[N.1] Fuego		1					1
VA_038	[N.2] Daños por agua		1					1
VA_039	[I.1] Fuego		1					1
VA_040	[I.2] Daños por agua		1					1
VA_041	[I.5] Deterioro de origen físico o lógico			1				1
VA_042	[E.23] Errores de mantenimiento/actualización de equipos				1			1
VA_043	[E.25] Perdida de equipos		1					1
VA_044	[A.23] Manipulación de equipos		1					1
VA_045	[I.5] Deterioro de origen físico o lógico		1					1
VA_046	[A.6] Abuso de privilegios de acceso		1					1
VA_047	[A.18] Destrucción de la información		1					1
VA_048	[E.3] Errores de monitorización		1					1
VA_049	[E.18] eliminación de datos		1					1
VA_050	[E.19] Filtración de datos		1					1
VA_051	[I.5] Deterioro de origen físico o lógico				1			1
VA_052	[A.6] Abuso de privilegios de acceso				1			1
VA_053	[A.18] Destrucción de la información			1				1
VA_054	[E.3] Errores de monitorización			1				1
VA_055	[E.18] Destrucción de la información			1				1
VA_056	[E.19] Fugas de información			1				1
VA_057	[E.1] Errores de los usuarios			1				1

Cuadro 18. (Continuación)

ID	VULNERABILIDAD	A	C	E	I	M	T	TOTAL
VA_058	[E.2] Errores del administrador			1				1
VA_059	[E.3] Errores de monitorización				1			1
VA_060	[E.20] Vulnerabilidades de los programas				1			1
VA_061	[E.20] Errores de mantenimiento/actualización de programas			1				1
VA_062	[A.8] Difusión de software dañino			1				1
VA_063	[A.12] Análisis de trafico		1					1
VA_064	[A.27] Ocupación enemiga		1					1
VA_065	[N.1] Fuego		1					1
VA_066	[N.2] Daños por agua			1				1
VA_067	[I.1] Fuego			1				1
VA_068	[I.2] Daños por agua			1				1
VA_069	[I.5] Deterioro de origen físico o lógico			1				1
VA_070	[A.6] Abuso de privilegios de acceso			1				1
VA_071	[E.1] Errores de los usuarios		1					1
VA_072	[E.2] Errores del administrador		1					1
VA_073	[E.3] Errores de monitorización		1					1
VA_074	[E.20] Vulnerabilidades de los programas		1					1
VA_075	[E.20] Errores de mantenimiento/actualización de programas		1					1
VA_076	[A.8] Difusión de software dañino		1					1
VA_077	[A.12] Análisis de trafico		1					1
VA_078	[A.27] Ocupación enemiga		1					1
VA_079	[E.1] Errores de los usuarios		1					1
VA_080	[E.2] Errores del administrador		1					1
VA_081	[E.3] Errores de monitorización		1					1
VA_082	[E.1] Errores de los usuarios			1				1
VA_083	[E.2] Errores del administrador			1				1
VA_084	[E.3] Errores de monitorización			1				1

Cuadro 18. (Continuación)

ID	VULNERABILIDAD	A	C	E	I	M	T	TOTAL
VA_085	[A.8] Difusión de software dañino			1				1
VA_086	[E.20] Errores de mantenimiento/actualización de programas			1				1
VA_087	[I.5] Deterioro de origen físico o lógico			1				1
VA_088	[A.6] Abuso de privilegios de acceso			1				1
VA_089	[E.1] Errores de los usuarios			1				1
VA_090	[E.2] Errores del administrador			1				1
VA_091	[E.3] Errores de monitorización			1				1
VA_092	[E.20] Vulnerabilidades de los programas		1					1
VA_093	[E.20] Errores de mantenimiento/actualización de programas		1					1
VA_094	[A.6] Abuso de privilegios		1					1
VA_095	[A.18] Destrucción de la información	1						1
VA_096	[A.15] Edición grande de datos	1						1
VA_097	[A.22] Manipulación de programas	1						1
VA_098	[A.23] Manipulación de equipos	1						1
VA_099	[A.6] Abuso de privilegios		1					1
VA_100	[A.18] Destrucción de la información		1					1
VA_101	[A.15] Edición de información		1					1
VA_102	[A.22] Manipulación de programas		1					1
VA_103	[A.23] Manipulación de equipos		1					1
VA_104	[A.30] Ingeniería social (picaresca)		1					1
VA_105	[N.1] Fuego		1					1
VA_106	[N.2] Daños por agua		1					1
VA_107	[I.1] Fuego		1					1
VA_108	[I.2] Daños por agua		1					1
VA_109	[I.5] Deterioro de origen físico o lógico		1					1
VA_110	[A.6] Abuso de privilegios de acceso		1					1

Cuadro 18. (Continuación)

ID	VULNERABILIDAD	A	C	E	I	M	T	TOTAL
VA_111	[E.1] Errores de los usuarios		1					1
VA_112	[E.2] Errores del administrador		1					1
VA_113	[E.3] Errores de monitorización		1					1
VA_114	[E.20] Vulnerabilidades de los programas				1			1
VA_115	[E.20] Errores de mantenimiento/actualización de programas					1		1
VA_116	[A.8] Difusión de software dañino					1		1
VA_117	[A.12] Análisis de trafico				1			1
VA_118	[A.27] Ocupación enemiga				1			1
	TOTAL	5	56	43	12	2	0	118

Fuente: Autor basado en Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. (Consultado 21 de marzo de 2020) Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

6.2.7 Informe de resultados. De acuerdo con los resultados de la identificación de la situación actual de la empresa QWERTY S.A, del reconocimiento de activos, de la valoración de estos, las dimensiones de seguridad con las que cuenta actualmente la compañía, del análisis de riesgos, amenazas y vulnerabilidades fundamentado en la metodología MAGERIT, se permite realizar la gestión del riesgo, análisis de amenazas, riesgo intrínseco, salvaguardas, riesgo residual y aceptable para la empresa, se encontraron 118 vulnerabilidades de las cuales 5 van a hacer aceptadas, 56 controladas, 43 evitadas, 12 investigadas y 2 mitigadas, como se relacionan a continuación:

Controladas (56)

- Fugas de información
- Difusión de software dañino
- Caída del sistema por el agotamiento de recursos
- Errores de monitorización
- Errores de monitorización

- Errores de monitorización
- Escapes de datos
- Abuso de privilegios de acceso
- Destrucción de la información
- Errores de monitorización
- Eliminación de los datos
- Filtraciones de datos
- Fuego
- Daños por agua
- Fuego
- Daños por agua
- Perdida de equipos
- Manipulación de equipos
- Deterioro de origen físico o lógico
- Abuso de privilegios de acceso
- Destrucción de la información
- Errores de monitorización
- Eliminación de datos
- Filtración de datos
- Análisis de trafico
- Ocupación enemiga
- Fuego
- Errores de los usuarios
- Errores del administrador
- Errores de monitorización
- Vulnerabilidades de los programas
- Errores de mantenimiento/actualización de programas
- Difusión de software dañino
- Análisis de trafico
- Ocupación enemiga
- Errores de los usuarios
- Errores del administrador
- Errores de monitorización
- Vulnerabilidades de los programas
- Errores de mantenimiento/actualización de programas
- Abuso de privilegios

- Abuso de privilegios
- Destrucción de la información
- Edición de información
- Manipulación de programas
- Manipulación de equipos
- Ingeniería social (picaresca)
- Fuego
- Daños por agua
- Fuego
- Daños por agua
- Deterioro de origen físico o lógico
- Abuso de privilegios de acceso
- Errores de los usuarios
- Errores del administrador
- Errores de monitorización

Evitadas (43)

- Errores de configuración
- Errores de los usuarios
- Destrucción de la información
- Deterioro de origen físico o lógico
- Errores de los usuarios
- Suplantación de la identidad del usuario
- Errores de los usuarios
- Errores del administrador
- Deterioro de origen físico o lógico
- Abuso de privilegios de acceso
- Destrucción de la información
- Eliminación de los datos
- Deterioro de origen físico o lógico
- Abuso de privilegios de acceso
- Destrucción de la información
- Errores de monitorización
- Eliminación de la información
- Escape de datos
- Deterioro de origen físico o lógico

- Deterioro de origen físico o lógico
- Destrucción de la información
- Errores de monitorización
- Destrucción de la información
- Fugas de información
- Errores de los usuarios
- Errores del administrador
- Errores de mantenimiento/actualización de programas
- Difusión de software dañino
- Daños por agua
- Fuego
- Daños por agua
- Deterioro de origen físico o lógico
- Abuso de privilegios de acceso
- Errores de los usuarios
- Errores del administrador
- Errores de monitorización
- Difusión de software dañino
- Errores de mantenimiento/actualización de programas
- Deterioro de origen físico o lógico
- Abuso de privilegios de acceso
- Errores de los usuarios
- Errores del administrador
- Errores de monitorización

Investigadas (12)

- Vulnerabilidades de los programas
- Vulnerabilidades de los programas
- Errores de secuencia
- Vulnerabilidades de los programas
- Errores de mantenimiento/actualización de equipos
- Deterioro de origen físico o lógico
- Abuso de privilegios de acceso
- Errores de monitorización
- Vulnerabilidades de los programas
- Vulnerabilidades de los programas

- Análisis de trafico
- Ocupación enemiga

Mitigadas (2)

- Errores de mantenimiento/actualización de programas
- Difusión de software dañino

Aceptadas (5)

- Deficiencias en la organización
- Destrucción de la información
- Edición grande de datos
- Manipulación de programas
- Manipulación de equipos

En los siguientes numerales se desarrolla el enfoque técnico – estratégico en el cual se propone la solución a las vulnerabilidades de ciberseguridad encontradas en la empresa, para lo cual se realiza un plan de mejora de riesgos, políticas de seguridad, controles recomendados, monitoreo, manual de seguridad y un software que permita apoyar estas medidas en la compañía para así proteger la información en que se encuentra en estado digital.

6.3 PLAN DE MONITOREO

Se desarrolla una política de seguridad la cual brinda protección respecto a vulnerabilidades encontradas, debe ser aprobada por la alta dirección de QWERTY S.A. y se díseña plan de monitoreo que permite realizar seguimiento a los activos informáticos.

6.3.1 Política de seguridad. Para la ejecución del plan del SGSI en la empresa QWERTY S.A., se exige el desarrollo de una política de seguridad en la que se establezcan las pautas que garanticen el cumplimiento de los tres principios fundamentales de la seguridad de la información, como lo son; confidencialidad, disponibilidad e integridad. Razón por la cual se debe definir y comunicar a los 120 colaboradores y visitantes de la empresa.

6.3.1.1 Objetivo general. QWERTY S.A. es una organización comprometida con la seguridad, razón por la cual se esmera en garantizar y salvaguardar la confidencialidad, integridad y disponibilidad de la información perteneciente a la empresa, teniendo en cuenta los objetivos de negocio y las normas legales vigentes. Por tal motivo publica esta política de seguridad para la compañía.

6.3.1.2 Objetivos específicos

- Establecer que uno de los activos importantes a proteger en la compañía es la información, por ende, debe salvaguardase en todo momento utilizando medidas de seguridad físicas y digitales.

- Implantar perfiles y responsabilidades a todos los colaboradores de la empresa, verificando el control sobre el acceso a la información de la compañía.

- Implementar sistemas de protección de las buenas prácticas TI a todos los procesos tecnológicos de la empresa.

- Fijar sanciones legales y/o penales a violaciones de seguridad de la información por parte de cualquier persona no autorizada.

6.3.1.3 Alcance. La presente política aplica para funcionarios, contratistas, practicantes y visitantes, con el ánimo de salvaguardar la información, como uno de los activos más importantes de la compañía.

6.3.1.4 Responsables. Toda persona que preste sus servicios a la empresa QWERTY S.A.

6.3.1.5 Normatividad. QWERTY S.A., como empresa que ofrece servicios a través de las tecnologías de la información, se acoje a la normatividad vigente con respecto a los sistemas de seguridad de la información, a continuación, se relaciona la norma y algunos decretos:

- ISOIIEC 27001- 27002:2013
- Decreto 2693 de 2012 MinTic
- Decreto 1008 de 2018 MinTic.
- Decreto 1078 de 2015 MinTic
- Decreto 415 de 2016 MinTic

6.3.1.6 Politica general.

- Gestionar los riesgos encontrados en el análisis realizado en el SGSI y tomar las medidas pertinentes.
- Implementar los controles necesarios en la compañía según lo encontrado en el SGSI y basado en la norma ISO/IEC:27001:2013 para disminuir probabilidades de riesgo y conservar la confidencialidad, integridad y disponibilidad de la información
- Crear espacios de enseñanza - aprendizaje para funcionarios, contratistas y aprendices sobre ataques cibernéticos comunes, por ejemplo, ingeniería social.
- Diseñar y publicar las responsabilidades de los funcionarios, contratistas y aprendices las cuales deben ser aceptadas y practicadas.
- Salvaguardar la información que se genere, se procese o se almacene producto de los procesos realizados al interior de la empresa.
- Se debe mitigar las eventualidades de seguridad y privacidad de la información resguardada en la compañía
- Implementar seguridad digital de forma efectiva, eficaz y eficiente.
- Proteger la información de las amenazas originadas por parte de los para funcionarios, contratistas y aprendices
- Generar conciencia a los funcionarios, contratistas y aprendices sobre el cambio que requiere la implementación de un SGSI
- Proteger las instalaciones de la empresa por medio de la adaptación de sistemas de control de ingreso y egreso del personal y visitantes
- Implementar control de acceso a los sitios que cuentan con información física de la empresa
- Ubicar de los servidores con los que cuenta la compañia en un lugar adecuado, el cual debe cumplir con las condiciones ambientales recomendadas por el fabricador.

6.3.1.7 Compromisos particulares de los consumidores de la información.

- La información de QWERTY S.A. debe ser usada únicamente para los propósitos que fue creada o almacenada.
- La confidencialidad de la información de QWERTY S.A. debe ser respetada y no divulgada.
- Los perfiles y sus contraseñas deben ser de uso personal y está prohibida su divulgación.
- Los funcionarios, contratistas, aprendices y visitantes deben ajustarse a las directrices de la clasificación de la información de la compañía.
- Bloquear la sesión de usuario al momento de ausentarse del puesto de trabajo
- Las impresiones realizadas deben ser recogidas al momento de realizarlas
- Una vez la relación laboral con la compañía cese, es obligación por parte de la persona devolver y no conservar ningún tipo de copia de la información de QWERTY S.A.
- Está prohibido el uso de activos tecnológicos para actividades distintas a las requeridas por la empresa
- Está prohibido el uso de software no licenciado en los recursos tecnológicos de la empresa.
- No se permite utilizar software licenciado de QWERTY S.A. en recursos tecnológicos ajenos a la compañía.
- Esta estrictamente prohibido el uso de unidades de almacenamiento como USB, cintas magnéticas o teléfonos celulares durante la jornada laboral.
- El uso del internet debe ser exclusivamente para realizar las actividades asociadas al cargo que se desempeñe.
- El usuario debe asegurar que toda la información provenga de fuentes conocidas.

6.3.1.8 Deberes de la dependencia de sistemas.

- Conceder permisos a los perfiles para acceder a la información de acuerdo con las obligaciones del cargo. Un usuario no debe tener autorización para crear, registrar, modificar, eliminar o compartir información sin control o revisión por parte de su jefe directo.
- Limitar el acceso de colaboradores o visitantes de la compañía a sitios restringidos, por ejemplo, el espacio donde se encuentran los servidores.

- Verificar por escrito con recursos humanos sobre los privilegios de acceso a la información que un usuario solicite.
- Mantener actualizado el registro de los usuarios y sus privilegios.
- Al reportar recursos humanos la ausencia prolongada de un usuario se deben suspender los privilegios de acceso a la información de este hasta su reincorporación.
- Si la vinculación laboral del usuario con la empresa ha finalizado el perfil de este debe ser suspendido de manera inmediata.
- Realizar mantenimientos preventivos a los activos tecnológicos de la compañía.

6.3.1.9 Manejo apropiado del software.

- Los puestos de trabajo de QWERTY S.A. únicamente pueden implementar software adquirido legalmente y licenciado a nombre de la empresa.
- El software perteneciente a QWERTY S.A. debe ser utilizado únicamente para los fines para los cuales fue adquirido.
- Los usuarios deben cumplir las normas de derechos de autor.

6.3.1.10 Control de virus.

- Realizar el documento que permita el seguimiento al estado actual del antivirus en los recursos tecnológicos de la empresa QWERTY S.A.
- Los recursos tecnológicos de la empresa QWERTY S.A. deben tener activos y actualizados los antivirus.
- Los recursos tecnológicos deben ser analizados periódicamente por el antivirus.
- Cualquier información que se transmita por medio magnético, correo electrónico o de información de internet, debe ser analizada por el antivirus antes de su descarga y ejecución.
- Realizar periódicamente copias de seguridad libres de virus.

6.3.1.11 Control de contraseñas.

- Los perfiles de usuario deben tener asignada una contraseña de manera individual.
- Cada usuario es responsable de su contraseña.
- No es permitido que un usuario divulgue su contraseña.
- El sistema de procesamiento no debe permitir la visualización clara de las contraseñas.
- Los usuarios cada 90 días deben cambiar la contraseña.
- No esta permitido repetir contraseñas que se utilizaron con anterioridad.
- No utilizar contraseñas que sean fácilmente identificadas, por ejemplo, nombres de hij@s, espos@s, placa de carro, número de teléfono entre otros.
- Las contraseñas deben tener como mínimo una longitud de 6 caracteres entre mayúsculas, minúsculas y números.

6.3.1.12 Backup.

- Implementar un sistema de realización automática de copias de respaldo.
- Las copias de respaldo se deben proteger en todo momento.
- Las copias de seguridad almacenadas de manera física se deben salvaguardar en un espacio que seguro.
- Las copias de seguridad físicas deben tener rótulos visibles, legibles y externos.
- Las copias de seguridad de la información se deben almacenar en lugares externos a la empresa, para así responder de manera rápida y oportuna ante un eventual ataque.
- Las copias de seguridad deben estar encriptadas.
- Es responsabilidad de los administradores realizar copias de seguridad a los sistemas operativos y servicios que se ofrecen.

6.3.1.13 Políticas de acceso áreas restringidas.

- Se determina como áreas restringidas todo espacio que contenga información física o digital de la empresa y solo se puede acceder a esta mediante autorización por escrito.

- Los servidores y bases de datos deben alojar en sitios que cuenten con puertas y en condiciones ambientales favorables.
- Las puertas de las zonas restringidas deben asegurarse en todo momento.
- Queda estrictamente prohibido ingresar a las áreas restringidas con móviles, Tablet, celulares, cámaras, computadores o cualquier otro dispositivo electrónico.

6.3.1.14 Responsable de la información.

- Es el encargado de salvaguardar la información creada, almacenada y disponible de la empresa QWERTY S.A.
- Verificar que únicamente los usuarios autorizados tengan acceso a la información.
- Informar de manera inmediata sobre cualquier tipo de anomalía detectada en la información.
- Implementar las medidas de seguridad necesarias para evitar que se modifique, copie o elimine la información.

6.3.1.15 Acuerdos de confidencialidad.

- Los funcionarios, contratistas, aprendices y terceros, que desarrollen actividades que involucren información de la empresa QWERTY S.A., deben conocer, aceptar y firmar un acuerdo de confidencialidad.
- Revisar periódicamente el acuerdo de confidencialidad verificando que cumple con las necesidades de la compañía.

6.3.1.16 Implementacion de plan de monitoreo del SGSI. Realizar un seguimiento a las vulnerabilidades encontradas en el sistema de gestion de seguridad de la información, permitiendo asi verificar que la implementación de este no esta interfiriendo con el objetivo de la compañía.

6.3.1.17 Sanciones. Cualquier colaborador de la empresa QWERTY S.A. que sea descubierto violando la política será sujeto a acciones disciplinarias según este estipulado en su contrato y dependiendo de la falta podrá acarrear efectos penales.

6.3.1.18 Controles recomendados. Una vez se determinaron los riesgos y basándose en lo que propone el Anexo A de la norma ISO, se definen los controles recomendados para implementar en la compañía QWERTY S.A. con el fin de brindar herramientas a la oficina de sistemas para poder establecer un ambiente seguro de trabajo.

6.3.2 Controles a implementar. Con base en la identificación y evaluación de los riesgos que se realizó a la empresa QWERTY S.A., se desarrolla la definición de los controles a efectuar para el tratamiento de las vulnerabilidades según lo estipulado en los dominios del Anexo A de la norma ISO 27001:2013.

Documentar las políticas que se encuentran en el numeral 6.3.1 del presente documento, ya que la mayoría de las vulnerabilidades encontradas hacen referencia a la falta de estas y de la documentación formal con respecto a la seguridad de la información de la empresa; por tal motivo se sugiere la implementación de la matriz con las políticas de seguridad, como se observa en el Cuadro 19.

Cuadro 19. Políticas desarrolladas QWERTY S.A.

				Nivel de riesgo		
ID	Dominio	Politica	Vulneravilidad	Alto	Medio	Bajo
P_0001	A5 - A18	Politica de seguridad de la información	Fugas de información	X		
			Abuso de privilegios de acceso		X	
			Destrucción de la información	X		
			Eliminación de los datos	X		
			Errores de los usuarios		X	
			Errores del administrador		X	
P_0002	A5, A6 y A9	Política de dispositivos móviles y teletrabajo	Caída del sistema por el agotamiento de recursos	X		
			Errores de monitorización	X		
			Escapes de datos	X		

Cuadro 19. (Continuación)

				Nivel de riesgo		
ID	Dominio	Politica	Vulneravilidad	Alto	Medio	Bajo
P_0003	A5 y A7	Política de seguridad de los recursos humanos	Errores de los usuarios		X	
			Errores del administrador	X		
			Errores de monitorización	X		
			Abuso de información privilegiada y actos no autorizados	X		
P_0004	A5 y A9	Política de control de accesos	Abuso de privilegios de acceso		X	
			Perdida de equipos			X
			Manipulación de equipos		X	
			Ocupación enemiga		X	
			Difusión de software dañino	X		
P_0005	A5 y A10	Política de controles criptográficos	Abuso de privilegios de acceso	X		
			Perdida de equipos		X	
			Ataque interno o externo	X		
			Abuso de información privilegiada y actos no autorizados	X		
			Filtraciones de datos	X		
			Escapes de datos	X		
			Ingenieria social	X		
P_0006	A5 y A11	Política de seguridad física y del entorno	Daños por agua	X		
			Fuego	X		
			Deterioro de origen físico o lógico		X	
			Ocupación enemiga		X	
P_0007	A5, A11 y A12	Política de almacenamiento y respaldo	Abuso de privilegios de acceso	X		
			Perdida de equipos		X	
			Filtraciones de datos	X		
			Abuso de información privilegiada y actos no autorizados	X		
P_0008	A5 y A13	Política de transferencia de información	Analisis de trafico	X		
			Filtraciones de datos	X		
P_0009	A15 y A14	Política de desarrollo seguro	Perdida de equipos		X	
			Ataque interno o externo	X		
			Abuso de información privilegiada y actos no autorizados	X		
P_0010	A5 y A16	Política de gestión de incidentes	Abuso de privilegios de acceso	X		
			Perdida de equipos		X	
			Ataque interno o externo	X		

Cuadro 19. (Continuación)

				Nivel de riesgo		
ID	Dominio	Politica	Vulneravilidad	Alto	Medio	Bajo
			Abuso de información privilegiada y actos no autorizados	X		
			Filtraciones de datos	X		
			Escapes de datos	X		
			Ingenieria social	X		
			Difusión de software dañino			
			Deficiencias en la organización	X		
			Destrucción de la información	X		
			Edición grande de datos	X		
			Manipulación de programas	X		
			Manipulación de equipos	X		
P_0011	A5 y A16	Política de gestión de la continuidad del negocio	Fugas de información	X		
			Abuso de privilegios de acceso		X	
			Destrucción de la información	X		
			Eliminación de los datos	X		
			Errores de los usuarios		X	
			Errores del administrador		X	

Fuente: Autor basado en Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. (Consultado 29 de octubre de 2020) Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

6.3.3 Plan tratamiento de riesgos. Con el fin de aplicar controles a los riesgos encontrados en el análisis realizado por medio de la metodología Magerit y garantizar la confidencialidad, integridad y disponibilidad de la informacion de la empresa QWERTY S.A., a continuación en el Cuadro 20 se presenta el plan de tratamiento de riesgos.

Cuadro 20. Plan de tratamiento de riesgos

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_001	[E.4] Errores de configuración	Ausencia de seguimiento y revisión técnica de las aplicaciones	Probable	Medio	Moderado	Evitar	Establecer políticas de adquisición, desarrollo y mantenimiento de sistemas	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_002	[E.19] Fugas de información	Ausencia de políticas de seguridad de la información	Probable	Alto	Moderado	Evitar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_003	[E.20] Vulnerabilidades de los programas	Ausencia de gestión de las vulnerabilidades técnicas	Probable	Bajo	Moderado	Mitigar	Se debe documentar sobres las vulnerabilidades de los programas utilizados en la compañía	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_004	[E.1] Errores de los usuarios	Ausencia de políticas de seguridad de la información	Probable	Medio	Moderado	Evitar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_005	[E.20] Vulnerabilidades de los programas	Ausencia de gestión de las vulnerabilidades técnicas	Probable	Bajo	Moderado	Transferir	Se debe documentar sobres las vulnerabilidades de los programas utilizados en la compañía	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses

Cuadro 20. (Continuación)

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_006	[E.10] Errores de secuencia	Ausencia de seguimiento y revisión técnica de las aplicaciones	Probable	Medio	Moderado	Transferir	Establecer políticas de adquisición, desarrollo y mantenimiento de sistemas	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_007	[E.18] Destrucción de la información	Ausencia de políticas de seguridad de la información	Probable	Alto	Moderado	Evitar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_008	[I.5] Deterioro de origen físico o lógico	Ausencia de un lugar que brinde protección física a los activos TI de la empresa	Probable	Medio	Moderado	Mitigar	Establecer protección contra amenazas externas y ambientales	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_009	[E.1] Errores de los usuarios	Ausencia de políticas de seguridad de la información	Probable	Medio	Moderado	Aceptar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_010	[E.8] Difusión de software dañino	Ausencia de capacitaciones a los colaboradores de la empresa sobre ataques informáticos	Probable	Alto	Moderado	Mitigar	Realizar capacitaciones periódicas sobre las buenas practicas de las TI	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses

Cuadro 20. (Continuación)

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_011	[E.20] Vulnerabilidades de los programas	Ausencia de gestión de las vulnerabilidades técnicas	Probable	Bajo	Moderado	Mitigar	Se debe documentar sobres las vulnerabilidades de los programas utilizados en la compañía	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_012	[E.24] Caída del sistema por el agotamiento de recursos	Ausencia de política de dispositivos móviles y teletrabajo	Probable	Alto	Moderado	Mitigar	Establecer procedimientos para la gestión del uso de dispositivos móviles y teletrabajo	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_013	[E.4] Errores de monitorización	Ausencia de controles criptográficos para la información de la empresa	Probable	Medio	Moderado	Evitar	Establecer política sobre el uso de controles criptográficos	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_014	[A.5] Suplantación de la identidad del usuario	ausencia de controles criptográficos para la información de la empresa	Probable	Medio	Moderado	Evitar	Establecer política sobre el uso de controles criptográficos	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_015	[E.1] Errores de los usuarios	Ausencia de políticas de seguridad de la información	Probable	Medio	Moderado	Evitar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses

Cuadro 20. (Continuación)

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_016	[E.2] Errores del administrador	Ausencia de políticas de seguridad de la información	Probable	Alto	Moderado	Evitar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_017	[E.3] Errores de monitorización	Ausencia de política de dispositivos móviles y teletrabajo	Probable	Medio	Moderado	Evitar	Establecer procedimientos para la gestión del uso de dispositivos móviles y teletrabajo	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_018	[E.7] Deficiencias en la organización	ausencia de controles criptográficos para la información de la empresa	Probable	Medio	Moderado	Evitar	Establecer política sobre el uso de controles criptográficos	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_019	[I.5] Deterioro de origen físico o lógico	Ausencia de un lugar que brinde protección física a los activos TI de la empresa	Probable	Medio	Moderado	Mitigar	Establecer protección contra amenazas externas y ambientales	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_020	[A.6] Abuso de privilegios de acceso	Ausencia de políticas de seguridad de la información	Probable	Alto	Moderado	Mitigar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses

Cuadro 20. (Continuación)

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_021	[A.18] Destrucción de la información	Ausencia de seguridad de la información	Probable	Alto	Moderado	Evitar	Establecer política con asignación de roles, responsabilidades y separación de deberes	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_022	[E.3] Errores de monitorización	Ausencia de política de dispositivos móviles y teletrabajo	Probable	Medio	Moderado	Evitar	Establecer procedimientos para la gestión del uso de dispositivos móviles y teletrabajo	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_023	[E.18] Destrucción de la información	Ausencia de políticas de seguridad de la información	Probable	Alto	Moderado	Transferir	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_024	[E.19] Fugas de información	Ausencia de políticas de seguridad de la información	Probable	Medio	Moderado	Evitar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_025	[I.5] Deterioro de origen físico o lógico	Ausencia de un lugar que brinde protección física a los activos TI de la empresa	Probable	Medio	Moderado	Transferir	Establecer protección contra amenazas externas y ambientales	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses

Cuadro 20. (Continuación)

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_026	[A.6] Abuso de privilegios de acceso	Ausencia de políticas de seguridad de la información	Probable	Medio	Moderado	Mitigar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_027	[A.18] Destrucción de la información	Ausencia de seguridad de la información	Probable	Alto	Moderado	Evitar	Establecer política con asignación de roles, responsabilidades y separación de deberes	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_028	[E.3] Errores de monitorización	Ausencia de política de dispositivos móviles y teletrabajo	Probable	Medio	Moderado	Mitigar	Establecer procedimientos para la gestión del uso de dispositivos móviles y teletrabajo	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_029	[E.18] Destrucción de la información	Ausencia de políticas de seguridad de la información	Probable	Alto	Moderado	Evitar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_030	[E.19] Fugas de información	Ausencia de políticas de seguridad de la información	Probable	Alto	Moderado	Evitar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses

Cuadro 20. (Continuación)

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_031	[I.5] Deterioro de origen físico o lógico	Ausencia de un lugar que brinde protección física a los activos TI de la empresa	Probable	Medio	Moderado	Mitigar	Establecer protección contra amenazas externas y ambientales	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_032	[A.6] Abuso de privilegios de acceso	Ausencia de políticas de seguridad de la información	Probable	Alto	Moderado	Mitigar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_033	[A.18] Destrucción de la información	Ausencia de seguridad de la información	Probable	Alto	Moderado	Evitar	Establecer política con asignación de roles, responsabilidades y separación de deberes	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_034	[E.3] Errores de monitorización	Ausencia de política de dispositivos móviles y teletrabajo	Probable	Medio	Moderado	Evitar	Establecer procedimientos para la gestión del uso de dispositivos móviles y teletrabajo	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_035	[E.18] Destrucción de la información	Ausencia de políticas de seguridad de la información	Probable	Alto	Moderado	Evitar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses

Cuadro 20. (Continuación)

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_036	[E.19] Fugas de información	Ausencia de políticas de seguridad de la información	Probable	Medio	Moderado	Evitar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_037	[N.1] Fuego	Ausencia de un lugar que brinde protección física a los activos TI de la empresa	Probable	Alto	Moderado	Evitar	Establecer protección contra amenazas externas y ambientales	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_038	[N.2] Daños por agua	Ausencia de un lugar que brinde protección física a los activos TI de la empresa	Probable	Alto	Moderado	Evitar	Establecer protección contra amenazas externas y ambientales	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_039	[I.1] Fuego	Ausencia de un lugar que brinde protección física a los activos TI de la empresa	Probable	Alto	Moderado	Aceptar	Establecer protección contra amenazas externas y ambientales	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_040	[I.2] Daños por agua	Ausencia de un lugar que brinde protección física a los activos TI de la empresa	Probable	Alto	Moderado	Mitigar	Establecer protección contra amenazas externas y ambientales	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses

Cuadro 20. (Continuación)

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_041	[I.5] Deterioro de origen físico o lógico	Ausencia de un lugar que brinde protección física a los activos TI de la empresa	Probable	Medio	Moderado	Mitigar	Establecer protección contra amenazas externas y ambientales	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_042	[E.23] Errores de mantenimiento/actualización de equipos	Ausencia de seguimiento y revisión técnica de las aplicaciones	Probable	Medio	Moderado	Mitigar	Establecer políticas de adquisición, desarrollo y mantenimiento de sistemas	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_043	[E.25] Perdida de equipos	ausencia de controles criptográficos para la información de la empresa	Probable	Alto	Moderado	Evitar	Establecer política sobre el uso de controles criptográficos	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_044	[A.23] Manipulación de equipos	Ausencia de seguimiento y revisión técnica de las aplicaciones	Probable	Alto	Moderado	Evitar	Establecer políticas de adquisición, desarrollo y mantenimiento de sistemas	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_045	[I.5] Deterioro de origen físico o lógico	Ausencia de un lugar que brinde protección física a los activos TI de la empresa	Probable	Medio	Moderado	Transferir	Establecer protección contra amenazas externas y ambientales	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses

Cuadro 20. (Continuación)

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_046	[A.6] Abuso de privilegios de acceso	Ausencia de políticas de seguridad de la información	Probable	Alto	Moderado	Transferir	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_047	[A.18] Destrucción de la información	Ausencia de seguridad de la información	Probable	Medio	Moderado	Mitigar	Establecer política con asignación de roles, responsabilidades y separación de deberes	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_048	[E.3] Errores de monitorización	Ausencia de política de dispositivos móviles y teletrabajo	Probable	Medio	Moderado	Evitar	Establecer procedimientos para la gestión del uso de dispositivos móviles y teletrabajo	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_049	[E.18] Destrucción de la información	Ausencia de políticas de seguridad de la información	Probable	Alto	Moderado	Mitigar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_050	[E.19] Fugas de información	Ausencia de políticas de seguridad de la información	Probable	Alto	Moderado	Evitar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses

Cuadro 20. (Continuación)

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_051	[I.5] Deterioro de origen físico o lógico	Ausencia de un lugar que brinde protección física a los activos TI de la empresa	Probable	Medio	Moderado	Mitigar	Establecer protección contra amenazas externas y ambientales	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_052	[A.6] Abuso de privilegios de acceso	Ausencia de políticas de seguridad de la información	Probable	Medio	Moderado	Evitar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_053	[A.18] Destrucción de la información	Ausencia de seguridad de la información	Probable	Alto	Moderado	Mitigar	Establecer política con asignación de roles, responsabilidades y separación de deberes	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_054	[E.3] Errores de monitorización	Ausencia de política de dispositivos móviles y teletrabajo	Probable	Alto	Moderado	Evitar	Establecer procedimientos para la gestión del uso de dispositivos móviles y teletrabajo	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_055	[E.18] Destrucción de la información	Ausencia de políticas de seguridad de la información	Probable	Alto	Moderado	Transferir	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses

Cuadro 20. (Continuación)

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_056	[E.19] Fugas de información	Ausencia de políticas de seguridad de la información	Probable	Alto	Moderado	Evitar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_057	[E.1] Errores de los usuarios	Ausencia de políticas de seguridad de la información	Probable	Medio	Moderado	Evitar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_058	[E.2] Errores del administrador	Ausencia de políticas de seguridad de la información	Probable	Medio	Moderado	Evitar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_059	[E.3] Errores de monitorización	Ausencia de política de dispositivos móviles y teletrabajo	Probable	Medio	Moderado	Mitigar	Establecer procedimientos para la gestión del uso de dispositivos móviles y teletrabajo	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_060	[E.20] Vulnerabilidades de los programas	Ausencia de gestión de las vulnerabilidades técnicas	Probable	Medio	Moderado	Evitar	Se debe documentar sobres las vulnerabilidades de los programas utilizados en la compañía	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses

Cuadro 20. (Continuación)

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_061	[E.20] Errores de mantenimiento/actualización de programas	Ausencia de seguimiento y revisión técnica de las aplicaciones	Probable	Medio	Moderado	Evitar	Establecer políticas de adquisición, desarrollo y mantenimiento de sistemas	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_062	[A.8] Difusión de software dañino	Ausencia de capacitaciones a los colaboradores de la empresa sobre ataques informáticos	Probable	Alto	Moderado	Evitar	Realizar capacitaciones periódicas sobre las buenas practicas de las TI	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_063	[A.12] Análisis de trafico	ausencia de controles criptográficos para la información de la empresa	Probable	Alto	Moderado	Evitar	Establecer política sobre el uso de controles criptográficos	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_064	[A.27] Ocupación enemiga	ausencia de controles criptográficos para la información de la empresa	Probable	Alto	Moderado	Mitigar	Establecer política sobre el uso de controles criptográficos	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_065	[N.1] Fuego	Ausencia de un lugar que brinde protección física a los activos TI de la empresa	Probable	Alto	Moderado	Mitigar	Establecer protección contra amenazas externas y ambientales	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses

Cuadro 20. (Continuación)

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_066	[N.2] Daños por agua	Ausencia de un lugar que brinde protección física a los activos TI de la empresa	Probable	Alto	Moderado	Evitar	Establecer protección contra amenazas externas y ambientales	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_067	[I.1] Fuego	Ausencia de un lugar que brinde protección física a los activos TI de la empresa	Probable	Alto	Moderado	Mitigar	Establecer protección contra amenazas externas y ambientales	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_068	[I.2] Daños por agua	Ausencia de un lugar que brinde protección física a los activos TI de la empresa	Probable	Alto	Moderado	Mitigar	Establecer protección contra amenazas externas y ambientales	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_069	[I.5] Deterioro de origen físico o lógico	Ausencia de un lugar que brinde protección física a los activos TI de la empresa	Probable	Medio	Moderado	Mitigar	Establecer protección contra amenazas externas y ambientales	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_070	[A.6] Abuso de privilegios de acceso	Ausencia de políticas de seguridad de la información	Probable	Medio	Moderado	Evitar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses

Cuadro 20. (Continuación)

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_071	[E.1] Errores de los usuarios	Ausencia de políticas de seguridad de la información	Probable	Medio	Moderado	Evitar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_072	[E.2] Errores del administrador	Ausencia de políticas de seguridad de la información	Probable	Medio	Moderado	Evitar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_073	[E.3] Errores de monitorización	Ausencia de política de dispositivos móviles y teletrabajo	Probable	Medio	Moderado	Mitigar	Establecer procedimientos para la gestión del uso de dispositivos móviles y teletrabajo	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_074	[E.20] Vulnerabilidades de los programas	Ausencia de gestión de las vulnerabilidades técnicas	Probable	Medio	Moderado	Transferir	Se debe documentar sobres las vulnerabilidades de los programas utilizados en la compañía	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_075	[E.20] Errores de mantenimiento/actualización de programas	Ausencia de seguimiento y revisión técnica de las aplicaciones	Probable	Medio	Moderado	Evitar	Establecer políticas de adquisición, desarrollo y mantenimiento de sistemas	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses

Cuadro 20. (Continuación)

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_076	[A.8] Difusión de software dañino	Ausencia de capacitaciones a los colaboradores de la empresa sobre ataques informáticos	Probable	Alto	Moderado	Mitigar	Realizar capacitaciones periódicas sobre las buenas practicas de las TI	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_077	[A.12] Análisis de trafico	ausencia de controles criptográficos para la información de la empresa	Probable	Alto	Moderado	Mitigar	Establecer política sobre el uso de controles criptográficos	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_078	[A.27] Ocupación enemiga	ausencia de controles criptográficos para la información de la empresa	Probable	Alto	Moderado	Mitigar	Establecer política sobre el uso de controles criptográficos	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_079	[E.1] Errores de los usuarios	Ausencia de políticas de seguridad de la información	Probable	Alto	Moderado	Mitigar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_080	[E.2] Errores del administrador	Ausencia de políticas de seguridad de la información	Probable	Alto	Moderado	Mitigar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses

Cuadro 20. (Continuación)

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_081	[E.3] Errores de monitorización	Ausencia de política de dispositivos móviles y teletrabajo	Probable	Medio	Moderado	Mitigar	Establecer procedimientos para la gestión del uso de dispositivos móviles y teletrabajo	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_082	[E.1] Errores de los usuarios	Ausencia de políticas de seguridad de la información	Probable	Medio	Moderado	Mitigar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_083	[E.2] Errores del administrador	Ausencia de políticas de seguridad de la información	Probable	Medio	Moderado	Mitigar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_084	[E.3] Errores de monitorización	Ausencia de política de dispositivos móviles y teletrabajo	Probable	Alto	Moderado	Transferir	Establecer procedimientos para la gestión del uso de dispositivos móviles y teletrabajo	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_085	[A.8] Difusión de software dañino	Ausencia de capacitaciones a los colaboradores de la empresa sobre ataques informáticos	Probable	Alto	Moderado	Transferir	Realizar capacitaciones periódicas sobre las buenas practicas de las TI	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses

Cuadro 20. (Continuación)

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_086	[E.20] Errores de mantenimiento/actualización de programas	Ausencia de seguimiento y revisión técnica de las aplicaciones	Probable	Medio	Moderado	Transferir	Establecer políticas de adquisición, desarrollo y mantenimiento de sistemas	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_087	[I.5] Deterioro de origen físico o lógico	Ausencia de un lugar que brinde protección física a los activos TI de la empresa	Probable	Medio	Moderado	Transferir	Establecer protección contra amenazas externas y ambientales	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_088	[A.6] Abuso de privilegios de acceso	Ausencia de políticas de seguridad de la información	Probable	Alto	Moderado	Transferir	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_089	[E.1] Errores de los usuarios	Ausencia de políticas de seguridad de la información	Probable	Medio	Moderado	Transferir	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_090	[E.2] Errores del administrador	Ausencia de políticas de seguridad de la información	Probable	Medio	Moderado	Transferir	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses

Cuadro 20. (Continuación)

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_091	[E.3] Errores de monitorización	Ausencia de política de dispositivos móviles y teletrabajo	Probable	Medio	Moderado	Mitigar	Establecer procedimientos para la gestión del uso de dispositivos móviles y teletrabajo	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_092	[E.20] Vulnerabilidades de los programas	Ausencia de gestión de las vulnerabilidades técnicas	Probable	Medio	Moderado	Evitar	Se debe documentar sobres las vulnerabilidades de los programas utilizados en la compañía	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_093	[E.20] Errores de mantenimiento/actualización de programas	Ausencia de seguimiento y revisión técnica de las aplicaciones	Probable	Medio	Moderado	Evitar	Establecer políticas de adquisición, desarrollo y mantenimiento de sistemas	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_094	[A.6] Abuso de privilegios	Ausencia de políticas de seguridad de la información	Probable	Medio	Moderado	Evitar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_095	[A.18] Destrucción de la información	Ausencia de seguridad de la información	Probable	Medio	Moderado	Evitar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses

Cuadro 20. (Continuación)

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_096	[A.15] Modificación deliberada de la información	ausencia de controles criptográficos para la información de la empresa	Probable	Medio	Moderado	Evitar	Establecer política sobre el uso de controles criptográficos	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_097	[A.22] Manipulación de programas	Ausencia de seguimiento y revisión técnica de las aplicaciones	Probable	Medio	Moderado	Mitigar	Establecer políticas de adquisición, desarrollo y mantenimiento de sistemas	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_098	[A.23] Manipulación de equipos	Ausencia de seguimiento y revisión técnica de las aplicaciones	Probable	Medio	Moderado	Mitigar	Establecer políticas de adquisición, desarrollo y mantenimiento de sistemas	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_099	[A.6] Abuso de privilegios	Ausencia de políticas de seguridad de la información	Probable	Medio	Moderado	Mitigar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_100	[A.18] Destrucción de la información	Ausencia de seguridad de la información	Probable	Medio	Moderado	Evitar	Establecer política con asignación de roles, responsabilidades y separación de deberes	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses

Cuadro 20. (Continuación)

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_101	[A.15] Modificación deliberada de la información	ausencia de controles criptográficos para la información de la empresa	Probable	Medio	Moderado	Evitar	Establecer política sobre el uso de controles criptográficos	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_102	[A.22] Manipulación de programas	Ausencia de seguimiento y revisión técnica de las aplicaciones	Probable	Medio	Moderado	Evitar	Establecer políticas de adquisición, desarrollo y mantenimiento de sistemas	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_103	[A.23] Manipulación de equipos	Ausencia de seguimiento y revisión técnica de las aplicaciones	Probable	Medio	Moderado	Evitar	Establecer políticas de adquisición, desarrollo y mantenimiento de sistemas	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_104	[A.30] Ingeniería social (picaresca)	Ausencia de capacitaciones a los colaboradores de la empresa sobre ataques informáticos	Probable	Medio	Moderado	Evitar	Realizar capacitaciones periódicas sobre las buenas practicas de las TI	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_105	[N.1] Fuego	Ausencia de un lugar que brinde protección física a los activos TI de la empresa	Probable	Alto	Moderado	Mitigar	Establecer protección contra amenazas externas y ambientales	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses

Cuadro 20. (Continuación)

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_106	[N.2] Daños por agua	Ausencia de un lugar que brinde protección física a los activos TI de la empresa	Probable	Medio	Moderado	Transferir	Establecer protección contra amenazas externas y ambientales	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_107	[I.1] Fuego	Ausencia de un lugar que brinde protección física a los activos TI de la empresa	Probable	Medio	Moderado	Transferir	Establecer protección contra amenazas externas y ambientales	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_108	[I.2] Daños por agua	Ausencia de un lugar que brinde protección física a los activos TI de la empresa	Probable	Medio	Moderado	Transferir	Establecer protección contra amenazas externas y ambientales	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_109	[I.5] Deterioro de origen físico o lógico	Ausencia de un lugar que brinde protección física a los activos TI de la empresa	Probable	Medio	Moderado	Transferir	Establecer protección contra amenazas externas y ambientales	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_110	[A.6] Abuso de privilegios de acceso	Ausencia de políticas de seguridad de la información	Probable	Medio	Moderado	Transferir	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses

Cuadro 20. (Continuación)

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_111	[E.1] Errores de los usuarios	Ausencia de políticas de seguridad de la información	Probable	Medio	Moderado	Transferir	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_112	[E.2] Errores del administrador	Ausencia de políticas de seguridad de la información	Probable	Medio	Moderado	Mitigar	Establecer políticas para la seguridad de la información	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas y jurídica	6 meses
VA_113	[E.3] Errores de monitorización	Ausencia de política de dispositivos móviles y teletrabajo	Probable	Medio	Moderado	Mitigar	Establecer procedimientos para la gestión del uso de dispositivos móviles y teletrabajo	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_114	[E.20] Vulnerabilidades de los programas	Ausencia de gestión de las vulnerabilidades técnicas	Probable	Medio	Moderado	Mitigar	Se debe documentar sobres las vulnerabilidades de los programas utilizados en la compañía	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_115	[E.20] Errores de mantenimiento/actualización de programas	Ausencia de seguimiento y revisión técnica de las aplicaciones	Probable	Medio	Moderado	Mitigar	Establecer políticas de adquisición, desarrollo y mantenimiento de sistemas	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses

Cuadro 20. (Continuación)

ID	Riesgo	Tipo	Probabilidad	Impacto	Riesgo residual	Opción de tratamiento	Actividad de control	Soporte	Responsable	Tiempo
VA_116	[A.8] Difusión de software dañino	Ausencia de capacitaciones a los colaboradores de la empresa sobre ataques informáticos	Probable	Medio	Moderado	Mitigar	Realizar capacitaciones periódicas sobre las buenas practicas de las TI	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_117	[A.12] Análisis de trafico	ausencia de controles criptográficos para la información de la empresa	Probable	Alto	Moderado	Evitar	Establecer política sobre el uso de controles criptográficos	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses
VA_118	[A.27] Ocupación enemiga	ausencia de controles criptográficos para la información de la empresa	Probable	Medio	Moderado	Evitar	Establecer política sobre el uso de controles criptográficos	Política creada y comunicada a todos los colaboradores de QWERTY S.A.	Dependencia de sistemas	6 meses

Fuente: Autor basado en Guía para la administración del riesgo y el diseño de controles en entidades públicas. [En línea]. (Consultado 29 de octubre de 2020) Disponible en: https://www.mincit.gov.co/temas-interes/documentos/guia-para-la-administracion-del-riesgo-y-el-diseno.aspx

6.3.4 Monitoreo. Con el fin de verificar si el plan de tratamiento esta funcionado y corrigiendo las vulnerabilidades en el mayor porcentaje posible es necesario, realizar un plan de monitoreo en donde por cada vulnerabilidad encontrada en el análisis de riesgos se realiza un control preciso, además se afirman los responsables de cada actividad, como se evidencia en Cuadro 21.

En donde:

- Aceptar (A): Indica la aceptación del riesgo ya que ha sido analizado y tiene muy baja ocurrencia de que suceda, esta técnica reconoce el riesgo y lo acepta de manera pasiva.

- Evitar (E): Por medio de esta técnica se pretende evitar el riesgo, ya que presenta una probabilidad medio-alta de que suceda, por lo cual puede ocasionar daños significativos dentro de la empresa. Razón por la cual busca suprimir completamente la amenaza.

- Mitigar (M): Esta técnica se emplea en el momento que se presenta y se materializa una amenaza.

- Transferir (T): Por medio de esta técnica se pasa parcial o completamente el riesgo a otra empresa, a través de una póliza o de un contrato.

Cuadro 21. Monitoreo

ID RIESGO	RIESGO	TRATAMIENTO				PLAN DE MONITOREO	RESPONSABLE
		A	E	M	T		
VA_001	[E.4] Errores de configuración		X			Auditoria interna de colaboradores	Dependencia de sistemas
VA_002	[E.19] Fugas de información		X			Evaluación periódica de los logs	Dependencia de sistemas
VA_003	[E.20] Vulnerabilidades de los programas			x		Evaluación de los factores ambientales	Dependencia de sistemas
VA_004	[E.1] Errores de los usuarios		x			Auditoria interna de colaboradores	Dependencia de sistemas
VA_005	[E.20] Vulnerabilidades de los programas				x	Evaluación periódica de los logs	Dependencia de sistemas
VA_006	[E.10] Errores de secuencia				x	Evaluación de los factores ambientales	Dependencia de sistemas
VA_007	[E.18] Destrucción de la información		x			Auditoria interna de colaboradores	Dependencia de sistemas
VA_008	[I.5] Deterioro de origen físico o lógico			x		Evaluación periódica de los logs	Dependencia de sistemas
VA_009	[E.1] Errores de los usuarios	x				Evaluación de los factores ambientales	Dependencia de sistemas
VA_010	[E.8] Difusión de software dañino			x		Auditoria interna de colaboradores	Dependencia de sistemas

Cuadro 21. (Continuación)

ID RIESGO	RIESGO	TRATAMIENTO				PLAN DE MONITOREO	RESPONSABLE
		A	E	M	T		
VA_011	[E.20] Vulnerabilidades de los programas			x		Evaluación periódica de los logs	Dependencia de sistemas
VA_012	[E.24] Caída del sistema por el agotamiento de recursos			x		Evaluación de los factores ambientales	Dependencia de sistemas
VA_013	[E.4] Errores de monitorización		x			Auditoria interna de colaboradores	Dependencia de sistemas
VA_014	[A.5] Suplantación de la identidad del usuario		x			Evaluación periódica de los logs	Dependencia de sistemas
VA_015	[E.1] Errores de los usuarios		x			Evaluación de los factores ambientales	Dependencia de sistemas
VA_016	[E.2] Errores del administrador		x			Auditoria interna de colaboradores	Dependencia de sistemas
VA_017	[E.3] Errores de monitorización		x			Evaluación periódica de los logs	Dependencia de sistemas
VA_018	[E.7] Deficiencias en la organización		x			Evaluación de los factores ambientales	Dependencia de sistemas
VA_019	[I.5] Deterioro de origen físico o lógico			x		Auditoria interna de colaboradores	Dependencia de sistemas
VA_020	[A.6] Abuso de privilegios de acceso			x		Evaluación periódica de los logs	Dependencia de sistemas
VA_021	[A.18] Destrucción de la información		x			Evaluación de los factores ambientales	Dependencia de sistemas
VA_022	[E.3] Errores de monitorización		x			Auditoria interna de colaboradores	Dependencia de sistemas
VA_023	[E.18] Destrucción de la información				x	Evaluación periódica de los logs	Dependencia de sistemas
VA_024	[E.19] Fugas de información		x			Evaluación de los factores ambientales	Dependencia de sistemas
VA_025	[I.5] Deterioro de origen físico o lógico				x	Auditoria interna de colaboradores	Dependencia de sistemas
VA_026	[A.6] Abuso de privilegios de acceso			x		Evaluación periódica de los logs	Dependencia de sistemas
VA_027	[A.18] Destrucción de la información					Evaluación de los factores ambientales	Dependencia de sistemas
VA_028	[E.3] Errores de monitorización			x		Auditoria interna de colaboradores	Dependencia de sistemas
VA_029	[E.18] Destrucción de la información	x				Evaluación periódica de los logs	Dependencia de sistemas
VA_030	[E.19] Fugas de información		x			Evaluación de los factores ambientales	Dependencia de sistemas
VA_031	[I.5] Deterioro de origen físico o lógico			x		Auditoria interna de colaboradores	Dependencia de sistemas

Cuadro 21. (Continuación)

ID RIESGO	RIESGO	TRATAMIENTO				PLAN DE MONITOREO	RESPONSABLE
		A	E	M	T		
VA_032	[A.6] Abuso de privilegios de acceso			x		Evaluación periódica de los logs	Dependencia de sistemas
VA_033	[A.18] Destrucción de la información		x			Evaluación de los factores ambientales	Dependencia de sistemas
VA_034	[E.3] Errores de monitorización		x			Auditoria interna de colaboradores	Dependencia de sistemas
VA_035	[E.18] Destrucción de la información		x			Evaluación periódica de los logs	Dependencia de sistemas
VA_036	[E.19] Fugas de información		x			Evaluación de los factores ambientales	Dependencia de sistemas
VA_037	[N.1] Fuego		x			Auditoria interna de colaboradores	Dependencia de sistemas
VA_038	[N.2] Daños por agua		x			Evaluación periódica de los logs	Dependencia de sistemas
VA_039	[I.1] Fuego	x				Evaluación de los factores ambientales	Dependencia de sistemas
VA_040	[I.2] Daños por agua			x		Auditoria interna de colaboradores	Dependencia de sistemas
VA_041	[I.5] Deterioro de origen físico o lógico			x		Evaluación periódica de los logs	Dependencia de sistemas
VA_042	[E.23] Errores de mantenimiento/actualización de equipos			x		Evaluación de los factores ambientales	Dependencia de sistemas
VA_043	[E.25] Perdida de equipos		x			Auditoria interna de colaboradores	Dependencia de sistemas
VA_044	[A.23] Manipulación de equipos		x			Evaluación periódica de los logs	Dependencia de sistemas
VA_045	[I.5] Deterioro de origen físico o lógico				x	Evaluación de los factores ambientales	Dependencia de sistemas
VA_046	[A.6] Abuso de privilegios de acceso				x	Auditoria interna de colaboradores	Dependencia de sistemas
VA_047	[A.18] Destrucción de la información			x		Evaluación periódica de los logs	Dependencia de sistemas
VA_048	[E.3] Errores de monitorización		x			Evaluación de los factores ambientales	Dependencia de sistemas
VA_049	[E.18] Destrucción de la información			x		Auditoria interna de colaboradores	Dependencia de sistemas
VA_050	[E.19] Fugas de información		x			Evaluación periódica de los logs	Dependencia de sistemas
VA_051	[I.5] Deterioro de origen físico o lógico			x		Evaluación de los factores ambientales	Dependencia de sistemas

Cuadro 21. (Continuación)

ID RIESGO	RIESGO	TRATAMIENTO				PLAN DE MONITOREO	RESPONSABLE
		A	E	M	T		
VA_052	[A.6] Abuso de privilegios de acceso		x			Auditoria interna de colaboradores	Dependencia de sistemas
VA_053	[A.18] Destrucción de la información			x		Evaluación periódica de los logs	Dependencia de sistemas
VA_054	[E.3] Errores de monitorización		x			Evaluación de los factores ambientales	Dependencia de sistemas
VA_055	[E.18] Destrucción de la información				x	Auditoria interna de colaboradores	Dependencia de sistemas
VA_056	[E.19] Fugas de información	x				Evaluación periódica de los logs	Dependencia de sistemas
VA_057	[E.1] Errores de los usuarios		x			Evaluación de los factores ambientales	Dependencia de sistemas
VA_058	[E.2] Errores del administrador	x				Auditoria interna de colaboradores	Dependencia de sistemas
VA_059	[E.3] Errores de monitorización			x		Evaluación periódica de los logs	Dependencia de sistemas
VA_060	[E.20] Vulnerabilidades de los programas		x			Evaluación de los factores ambientales	Dependencia de sistemas
VA_061	[E.20] Errores de mantenimiento/actualización de programas		x			Auditoria interna de colaboradores	Dependencia de sistemas
VA_062	[A.8] Difusión de software dañino		x			Evaluación periódica de los logs	Dependencia de sistemas
VA_063	[A.12] Análisis de trafico		x			Evaluación de los factores ambientales	Dependencia de sistemas
VA_064	[A.27] Ocupación enemiga			x		Auditoria interna de colaboradores	Dependencia de sistemas
VA_065	[N.1] Fuego			x		Evaluación periódica de los logs	Dependencia de sistemas
VA_066	[N.2] Daños por agua		x			Evaluación de los factores ambientales	Dependencia de sistemas
VA_067	[I.1] Fuego			x		Auditoria interna de colaboradores	Dependencia de sistemas
VA_068	[I.2] Daños por agua			x		Evaluación periódica de los logs	Dependencia de sistemas
VA_069	[I.5] Deterioro de origen físico o lógico			x		Evaluación de los factores ambientales	Dependencia de sistemas
VA_070	[A.6] Abuso de privilegios de acceso		x			Auditoria interna de colaboradores	Dependencia de sistemas
VA_071	[E.1] Errores de los usuarios	x				Evaluación periódica de los logs	Dependencia de sistemas
VA_072	[E.2] Errores del administrador		x			Evaluación de los factores ambientales	Dependencia de sistemas

Cuadro 21. (Continuación)

ID RIESGO	RIESGO	TRATAMIENTO				PLAN DE MONITOREO	RESPONSABLE
		A	E	M	T		
VA_073	[E.3] Errores de monitorización			x		Auditoria interna de colaboradores	Dependencia de sistemas
VA_074	[E.20] Vulnerabilidades de los programas				x	Evaluación periódica de los logs	Dependencia de sistemas
VA_075	[E.20] Errores de mantenimiento/actualización de programas			x		Evaluación de los factores ambientales	Dependencia de sistemas
VA_076	[A.8] Difusión de software dañino			x		Auditoria interna de colaboradores	Dependencia de sistemas
VA_077	[A.12] Análisis de trafico			x		Evaluación periódica de los logs	Dependencia de sistemas
VA_078	[A.27] Ocupación enemiga			x		Evaluación de los factores ambientales	Dependencia de sistemas
VA_079	[E.1] Errores de los usuarios			x		Auditoria interna de colaboradores	Dependencia de sistemas
VA_080	[E.2] Errores del administrador			x		Evaluación periódica de los logs	Dependencia de sistemas
VA_081	[E.3] Errores de monitorización			x		Evaluación de los factores ambientales	Dependencia de sistemas
VA_082	[E.1] Errores de los usuarios			x		Auditoria interna de colaboradores	Dependencia de sistemas
VA_083	[E.2] Errores del administrador			x		Evaluación periódica de los logs	Dependencia de sistemas
VA_084	[E.3] Errores de monitorización				x	Evaluación de los factores ambientales	Dependencia de sistemas
VA_085	[A.8] Difusión de software dañino				x	Auditoria interna de colaboradores	Dependencia de sistemas
VA_086	[E.20] Errores de mantenimiento/actualización de programas				x	Evaluación periódica de los logs	Dependencia de sistemas
VA_087	[I.5] Deterioro de origen físico o lógico				x	Evaluación de los factores ambientales	Dependencia de sistemas
VA_088	[A.6] Abuso de privilegios de acceso				x	Auditoria interna de colaboradores	Dependencia de sistemas
VA_089	[E.1] Errores de los usuarios				x	Evaluación periódica de los logs	Dependencia de sistemas
VA_090	[E.2] Errores del administrador				x	Evaluación de los factores ambientales	Dependencia de sistemas
VA_091	[E.3] Errores de monitorización			x		Auditoria interna de colaboradores	Dependencia de sistemas
VA_092	[E.20] Vulnerabilidades de los programas		x			Evaluación periódica de los logs	Dependencia de sistemas
VA_093	[E.20] Errores de mantenimiento/actualización de programas		x			Evaluación de los factores ambientales	Dependencia de sistemas
VA_094	[A.6] Abuso de privilegios		x			Auditoria interna de colaboradores	Dependencia de sistemas
VA_095	[A.18] Destrucción de la información		x			Evaluación periódica de los logs	Dependencia de sistemas

Cuadro 21. (Continuación)

ID RIESGO	RIESGO	TRATAMIENTO				PLAN DE MONITOREO	RESPONSABLE
		A	E	M	T		
VA_096	[A.15] Modificación deliberada de la información		x			Evaluación de los factores ambientales	Dependencia de sistemas
VA_097	[A.22] Manipulación de programas			x		Auditoria interna de colaboradores	Dependencia de sistemas
VA_098	[A.23] Manipulación de equipos			x		Evaluación periódica de los logs	Dependencia de sistemas
VA_099	[A.6] Abuso de privilegios			x		Evaluación de los factores ambientales	Dependencia de sistemas
VA_100	[A.18] Destrucción de la información		x			Auditoria interna de colaboradores	Dependencia de sistemas
VA_101	[A.15] Modificación deliberada de la información		x			Evaluación periódica de los logs	Dependencia de sistemas
VA_102	[A.22] Manipulación de programas		x			Evaluación de los factores ambientales	Dependencia de sistemas
VA_103	[A.23] Manipulación de equipos		x			Auditoria interna de colaboradores	Dependencia de sistemas
VA_104	[A.30] Ingeniería social (picaresca)		x			Evaluación periódica de los logs	Dependencia de sistemas
VA_105	[N.1] Fuego			x		Evaluación de los factores ambientales	Dependencia de sistemas
VA_106	[N.2] Daños por agua				x	Auditoria interna de colaboradores	Dependencia de sistemas
VA_107	[I.1] Fuego				x	Evaluación periódica de los logs	Dependencia de sistemas
VA_108	[I.2] Daños por agua				x	Evaluación de los factores ambientales	Dependencia de sistemas
VA_109	[I.5] Deterioro de origen físico o lógico				x	Auditoria interna de colaboradores	Dependencia de sistemas
VA_110	[A.6] Abuso de privilegios de acceso				x	Evaluación periódica de los logs	Dependencia de sistemas
VA_111	[E.1] Errores de los usuarios				x	Evaluación de los factores ambientales	Dependencia de sistemas
VA_112	[E.2] Errores del administrador			x		Auditoria interna de colaboradores	Dependencia de sistemas
VA_113	[E.3] Errores de monitorización			x		Evaluación periódica de los logs	Dependencia de sistemas
VA_114	[E.20] Vulnerabilidades de los programas			x		Evaluación de los factores ambientales	Dependencia de sistemas
VA_115	[E.20] Errores de mantenimiento/actualización de programas			x		Auditoria interna de colaboradores	Dependencia de sistemas
VA_116	[A.8] Difusión de software dañino			x		Evaluación periódica de los logs	Dependencia de sistemas
VA_117	[A.12] Análisis de trafico		x			Evaluación de los factores ambientales	Dependencia de sistemas
VA_118	[A.27] Ocupación enemiga		x			Auditoria interna de colaboradores	Dependencia de sistemas

Fuente: Autor basado en Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. (Consultado 21 de marzo de 2020) Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

6.4 MANUAL DE SEGURIDAD

Actualmente se incrementa el uso de herramientas informáticas para la comunicación entre personas o empresas aplicadas, con diferentes fines, sean estos económicos o sociales, razón por la cual, el equipo contratado por empresa QWERTY S.A., pone a disposición de los miembros pertenecientes a esta organización, el manual de seguridad y la política de seguridad de la información descrita en el numeral 6.3.1 del presente documento, con el fin de que sirvan como instrumento para minimizar las vulnerabilidades encontradas a través del SGSI diseñado para la compañía, dando a conocer asi la importancia de la información y el cuidado de los activos que pertenecen a QWERTY S.A.

6.4.1 Alcance.

Los lineamientos del siguiente documento estipulan las normas que se deben seguir por parte de todo miembro que pertenenzca o tenga algún tipo de relación con la empresa QWERTY S.A.

Este manual debe revisarse con una periodicidad mínima de una vez al año, o cuando se originen cambios en la entidad que puedan afectar la operación de los servicios TI, o durante las revisiones periódicas que desde la dirección se ejecutan para asegurar la continuidad del sistema.

6.4.2 Objetivos específicos

- Implantar perfiles y responsabilidades a todos los colaboradores de la empresa, verificando el control sobre el acceso a la información de la compañía.

- Implementar sistemas de protección de las buenas prácticas TI a todos los procesos tecnológicos de la empresa.

- Fijar sanciones legales y/o penales a violaciones de seguridad de la información por parte de cualquier persona no autorizada.

6.4.3 Glosario.

AMENAZA: Probabilidad de ocurrencia de hechos que se efectúen en un sitio en especial, causando efectos.

ANTIVIRUS: Programa que se encarga de detectar y en algunas situaciones contener virus informáticos.

CONTRASEÑA: Código secreto que se introduce en una máquina para poder accionar un mecanismo o para acceder a ciertas funciones informáticas.

CIBERSEGURIDAD: Es la protección de los sistemas conectados a Internet, como el hardware, el software y los datos, frente a las amenazas cibernéticas. La práctica es utilizada por individuos y empresas para protegerse contra el acceso no autorizado a centros de datos y otros sistemas computarizados.

REGISTRO: Acción por medio de la cual se mantiene consolidada la información de una empresa.

RIESGO: Posibilidad que se tiene para medir la magnitud de daños que se pueden ocasionar por la explotación de una vulnerabilidad.

VULNERABILIDAD: Es un fallo o debilidad presente en un sistema de información, la cual puede ser explotada poniendo en riesgo la integridad, disponibilidad de los activos de determinada empresa, organización o persona.

6.4.4 Desarrollo general.

- La alta gerencia designa la dependencia responsable de la seguridad de las tecnologías de la información de empresa.

- Todo usuario nuevo en la institución deberá tener una inducción por parte de la dependencia de sistemas, con el fin de darle a conocer las políticas de seguridad de la empresa y los privilegios a los que tiene acceso dependiendo de las funciones del cargo a desempeñar.

6.4.5 Seguridad física y del medio ambiente.

- El cableado de red telemática ira físicamente separado del de la red eléctrica con el fin de evitar interferencias.

- Es obligación de todos los colaboradores proteger los activos de la empresa, informando a la oficina de sistemas cualquier anomalía que ocurra.

- El suministro de energía es exclusivo para los equipos de cómputo, no se puede utilizar para alimentar aparatos que consuman grandes cantidades de energía, debe estar polarizado y contar con UPS para no comprometer la información.

- Se debe implementar un sistema de acceso biométrico el cual ha de ser empleado por todos los colaboradores con el fin de tener identificado el flujo de personas que ingresan a las instalaciones, incluyendo visitantes.

6.4.6 Mantenimiento de equipos.

- Únicamente el personal autorizado por la dependencia de sistemas podrá llevar a cabo el mantenimiento preventivo y correctivo de los equipos informáticos. Los usuarios deberán asegurarse de respaldar en copias o backups la información que consideren relevantes cuando el equipo sea enviado a reparación y borrar aquella sensible que se encuentre en él, previendo así la pérdida involuntaria de esta derivada del proceso de reparación.

- Cualquier falla efectuada en las aplicaciones o sistema por la manipulación errónea de archivos, posterior a su mantenimiento deberá ser notificada y reparada por el personal técnico encargado en dicha función.

- La dependencia de sistemas deberá realizar informes mensuales del estado de los equipos informáticos en donde se relacionará al menos el estado físico y actualizaciones pertinentes del sistema operativo.

6.4.7 Seguridad en las redes de la empresa.

- Implementar firewall en la compañía.

- Es obligatorio el uso de mecanismos de seguridad que se encuentren disponibles para las redes.

- Implementar seguridad por capas en la infraestructura de la red de la compañía, garantizando que, ante un eventual ataque resulta comprometido un nivel, el agresor deberá traspasar otra capa de seguridad para vulnerar los sistemas.

- La dependencia de sistemas deberá cambiar contraseñas de los router, cada vez que el proveedor de servicios de internet tenga conocimiento de ellas.

- Verificar que todos los dispositivos pertenecientes a la red se encuentren configurados y actualizados según las recomendaciones del fabricante.

- Servidores que se encuentren con problemas de configuración o de hardware deberán ser aislados y custodiados.

- Los servidores se deben instalar en sitios con condiciones ambientales óptimas según las especificaciones de los fabricantes.

- Se deben bloquear los dispositivos informáticos cuando el o los funcionario(s) o colaborador(es) no se encuentren frente a estos.

- Cuando un funcionario o colaborador de la empresa QWERTY S.A. se encuentre trabajando en un sitio fuera de la planta física de la compañía es necesario el uso de una red privada virtual o VPN.

- No se permite el uso de equipos informáticos ajenos a la compañía en la red de la empresa.

- Se debe establecer control mediante la asociación de direcciones MAC.

6.4.8 Seguridad en internet.

- El uso del correo electrónico proporcionado por la empresa es únicamente para realizar comunicaciones de interés al cargo y las funciones que tenga cada colaborador.

- Toda la información que sea enviada a través de correo electrónico debe ser encriptada y se debe verificar que el receptor tenga facultades para recibir la información.

- Se deben implementar proxys con el fin de evitar que funcionarios o colaboradores ingresen a páginas web que no sean útiles para el desarrollo de sus funciones.

- La oficina de sistemas debe semalmente brindar informacion a colaboradores sobre diferentes tipos de ataques cibernéticos especificando como evitarlos y que hacer en caso de ser victima de estos.

- Queda prohibido el uso de aplicaciones que permitan evadir los controles de seguridad informática implementados en la empresa

- Evitar la descarga de imágenes, sonido y video; más cuando estos provienen de sitios gratuitos.

- El acceso a páginas Web con contenido inapropiado se encuentra restringido. Sin embargo, si por la naturaleza del cargo se requiere el acceso a páginas de acceso contralado, se debe solicitar a la Mesa de Ayuda adjuntando la aprobación y justificación por parte del jefe inmediato.

- Cada colaborador es responsable del adecuado manejo de los usuarios de autenticación y contraseñá a la hora de ingresar a los diferentes sistemas de información que consulte en internet.

6.4.9 Seguridad de la información.

- Gestionar el acceso a la informacion dependiendo del cargo y funciones de cada colaborador dentro de la empresa.

- Utilizar en todos los equipos informáticos de QWERTY S.A. un antimalware.

- Realizar seguimiento al programa antimalware verificando asi el estado de actualización.

- Se permite únicamente el uso de CD, DVD, USB, tarjetas SD o cualquier tipo de memoria flash que proporcione la dependencia de sistemas, donde la información allí contenida debe ser cifrada o encriptada.

- Los puestos de trabajo que se encuentran en la compañía deben permanecer limpios de documentación, no deben existir hojas que contengan información.

- Es obligación de la dependencia de sistemas y el equipo técnico clasificar en confidencial, privada y pública la información de la empresa QWERTY S.A. de acuerdo al nivel de impacto que tendria sobre la compañía la posible pérdida de la misma.

- No se deben instalar programas en los equipos informáticos sin autorización de la dependencia de sistemas.

- No se permite el uso de información de la compañía QWERTY S.A. en equipos informáticos que no pertenezcan a esta.

- Realizar backup de toda la información de la compañía la cual debe ser alojada en un servidor separado de la empresa.

- Se deben realizar backups diarios de la informacion que fue modificada en el día.

6.4.10 Excepciones. No hay excepciones en los lineamientos establecidos.

6.4.11 Control de cambios.

Cuadro 22. Control de cambios

Versión	Fecha de entrada en vigencia	Naturaleza del cambio
Versión 1.0	Falta por aprobación por parte de la alta dirección de QWERTY S.A.	Inicio de la normativa

Fuente: Autor

6.4.12 Sanciones. Incurrirá en proceso penal quien se encuentre culpable de robo, daño voluntario a un bien de la empresa, divulgación de información reservada o confidencial.

El anterior manual de seguridad de la información debe ser conocido y aplicado por todos los miembros de la compañía QWERTY S.A.

7. CONCLUSIONES

- Se identifica la situación actual de la empresa QWERTY S.A a través de las estrategias implementadas para la recolección de datos, reconociéndose así el objetivo del negocio, la estructura de la compañía, cargos y funciones de los colaboradores y los activos tecnológicos con sus respectivas características y ubicaciones, lo cual permite contextualizar la realidad de la empresa y tener insumos para realizar un análisis de riesgos y con previa aprobación por parte de la alta dirección establecer las medidas a tomar por medio del sistema de gestión de seguridad de la información a desarrollar y reducir el riesgo ante posibles ataques cibernéticos.

- Se siguieron las indicaciones de la metodología MAGERIT para realizar la evaluación de bienes de la empresa y del sistema de control interno de la organización, permitiendo así efectuar un análisis de riesgos, vulnerabilidades, amenazas y salvaguardas, encontrándose 118 vulnerabilidades, de las cuales el 4% van a ser aceptadas, el 47.45% controladas, el 36.44% evitadas, el 10.16% investigadas y el 1.69% mitigadas; esta decisión se toma de acuerdo a los parámetro establecidos por la alta dirección donde se comparó el posible daño causado por cada vulnerabilidad versus el costo que al implementar el control requiere, de igual manera se le recalca a la gerencia de QWERTY S.A. la importancia de generar un ambiente seguro de trabajo, mediante la educación de los colaboradores en ataques cibernéticos y estableciendo políticas de seguridad y manual de usuario.

- Se desarrolla un plan de monitoreo de la compañía en cada una de las 118 vulnerabilidades encontradas a través del análisis de riesgos realizado por medio de la metodología MAGERIT, pero debido a que la empresa entra en una restructuración económica, según lo informa la alta gerencia, este plan de monitoreo no se puede efectuar en este momento, pero si se logran establecer las políticas de seguridad, las cuales permiten determinar quién es el responsable de realizar cada una de las actividades, para así lograr minimizar los riesgos de un posible ataque cibernético.

- Se establece un manual de seguridad informática en concordancia con las políticas de seguridad diseñadas para la empresa, donde se plasman algunos códigos de buenas prácticas TI, como son, seguridad de sistemas operativos, seguridad de redes, seguridad de bases de datos y seguridad de servidores. Teniendo como soporte el apoyo de la alta dirección de la compañía y siguiendo las recomendaciones de la norma ISO/IEC 27001:2013.

- Se ratifica que la ciberseguridad es de gran relevancia en la actualidad, ya que todo procedimiento o acción que se realice en un dispositivo sea celular, computador, tablet, router, servidor o cualquier otro equipo perteneciente a la infraestructura TI es vulnerable a diferentes tipos de ataques, por ende es imprecindible la implementación de acciones que permiten minimizar los riesgos ante delicuentes informáticos.

- Se establecen acciones en ciberseguridad, que se encuentran estipuladas como buenas practicas TI, siendo estas, el no abrir un mensaje de procedencia sospechosa, no descargar contenido multimedia de páginas de dudosa reputación, participar en capacitaciones sobre como prevenir ataques por ingeniería social, mantener los software actulizados, ser conciente de las vulnerabilidades de los programas utilizados, realizar configuraciones a los terminales según la recomendación del fabricante, entre otras; por ende es de vital importancia acatar estas buenas practicas TI no solo en la vida laboral sino en el dia a dia de cada persona.

RECOMENDACIONES

- Implementar un sistema de control biométrico para tener registro y alertas oportunas que indiquen las personas que ingresan a las instalaciones.

- Profundizar en las fichas técnicas de los activos informáticos de la empresa QWERTY S.A., con el fin de indagar acerca de vulnerabilidades que tienen intrínsecamente cada uno de los equipos utilizados.

- Realizar informes mensuales sobre el estado de los equipos de cómputo relacionando tanto el estado físico como lógico con el fin de identificar posibles vulnerabilidades y llevar control sobre actualizaciones de software de cada uno.

- Ubicar los servidores en lugares que sean custodiados, aislados y en condiciones ambientales recomendadas por los fabricadores.

BIBLIOGRAFÍA

ACADEMY. Plan de tratamiento de riesgos. [En línea]. [Consultado 7 de mayo de 2019]. España. Advisera., Disponible en: https://advisera.com/27001academy/es/documentation/plan-de-tratamiento-deriesgos/

AGESIC. Indicadores para un SGSI guía metodológica. [En línea]. [Consultado 7 de mayo de 2019]. gub.uyy Uruguay. 2016., Disponible en: https://www.agesic.gub.uy/innovaportal/file/7004/1/anexo-iv_indicadores.pdf

BARRACUDA. Email Spoofing. [En línea]. [Consultado 19 de marzo de 2020] 2011 Disponible en: https://www.barracuda.com/glossary/email-spoofing

BORGHELLO Cristian. Criptología. [En línea]. [Consultado 19 de marzo de 2020] Disponible en: https://www.segu-info.com.ar/criptologia/criptologia.html

CIOSPAIN. Las metodologías de gestión de proyectos más populares. [En línea]. [Consultado 7 de mayo de 2019]. España., Disponible en: https://www.ciospain.es/gobierno-ti/las-metodologias-de-gestion-de-proyectosmas-Populares

CLOUDFLARE. What is IP Spoofing? [En línea]. [Consultado 19 de marzo de 2020] 2011 Disponible en: https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/

CUERVO Sara. Implementación iso 27001. [En línea]. [Consultado 7 de mayo de 2019]. España., Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/64827/10/scuervoTFM0617presentaci%C3%B3n.pdf

FRUHLINGER Josh. ¿Qué es la seguridad de la red? [En línea]. [Consultado 19 de marzo de 2020] Network world.2018., Disponible en: https://www.networkworld.es/seguridad/que-es-la-seguridad-de-la-red

GARCIA, Manuel; QUISPE, Carlos y RÁEZ, Luis. Mejora continua en la calidad de los procesos. [En línea]. [Consultado 9 mayo de 2019 Industria data revista de investigación. Lima. 2003 P.5., Disponible en: https://www.redalyc.org/pdf/816/81606112.pdf

GERENCIE. Auditoria interna. [En línea]. [Consultado 7 de mayo de 2019]. Disponible en: https://www.gerencie.com/auditoria-interna.html

GOBIERNO DE ESPAÑA. ISO/IRC 27001: PDCA. [En línea]. [Consultado 9 mayo de 2019] Ministerio de Educación, Cultura y Deporte. España, Disponible en: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/isoirc_27001_pdca.html

GOBIERNO DE ESPAÑA. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. [Consultado 19 de marzo de 2020] Ministerio de Educación, Cultura y Deporte. España, Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

INSIGNIA. Amenaza. [En línea]. [Consultado 19 de marzo de 2020] 2017. Disponible en: https://blog.elinsignia.com/2017/11/28/tipos-de-amenazas-informaticas/

INSTITUTO NACIONAL DE CIBERSEGURIDAD. Tecnologías biométricas aplicadas a la ciberseguridad. [En línea]. [Consultado 19 de marzo de 2020] Madrid. Gobierno de España. p 4., Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf

INTECO. Implantación de un SGSI en la empresa. [En línea]. [Consultado 8 de mayo de 2019]. INTECO. 2014. p 3., Disponible en:https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

ISO27000. Sistema de Gestión de la Seguridad de la Información. [En línea]. [Consultado 19 de marzo de 2020] ISO27000. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

ISOTOOLS. Acciones preventinas o correctivas en el SG-SST. [En línea]. ISOTOOLS excellence 2016., [Consultado 7 de mayo de 2019]. Disponible en: https://www.isotools.org/2016/11/22/acciones-preventivas-correctivas-sg-sst/

ISOTOOLS. ISO 27001 2013: Pasos a seguir en una evaluación de riesgos. [En línea]. [Consultado 7 de mayo de 2019]. ISOTools Excellence. 2016., Disponible en: https://www.pmgssi.com/2016/05/iso-27001-2013-pasos-seguir-evaluacion-riesgos/

ISOTOOLS. ISO 27001: Evaluacion y tratamiento de riesgos en 6 pasos. [En línea]. [Consultado 7 de mayo de 2019]. ISOTools Excellence. 2016., Disponible en: https://www.isotools.org/2017/06/18/evaluacion-de-riesgos-segun-iso-27001/

MENDOZA Miguel, ¿Qué es una declaración de aplicabilidad [SoA] y para que MENDOZA Miguel. ¿Cómo definir el alcance del SGSI?. [En línea]. [Consultado 7 de mayo de 2019]. Mexico welivesecurity. 2018., Disponible en: https://www.welivesecurity.com/laes/2018/01/09/definir-alcance-sgsi/

MINTIC. Elaboración de la politica general de seguridad y privacidad de la informacion. [En línea]. [Consultado 7 de mayo de 2019]. Bogotá Ministerio de Tecnologías de la Información y las Comunicaciones. 2016., 8 p. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

MOZ://A. Seguridad de Sitios Web. [En línea]. [Consultado 19 de marzo de 2020] Disponible en: https://developer.mozilla.org/es/docs/Learn/Server-side/Primeros_pasos/seguridad_sitios_web

NORMAS ISO. ISO 20000 CALIDAD DE LOS SERVICIOS TI. [En línea]. [Consultado 19 de marzo de 2020] Normas ISO. España, Disponible en: https://www.normas-iso.com/iso-20000/

NUEVA ISO 9001:2015. 9.3 Revisión por la dirección. [En línea]. [Consultado 7 de mayo de 2019]. Escuela Europea de Excelencia. Santiago de Chile. 2013., Disponible en: https://www.nueva-iso-9001-2015.com/9-3-revision-por-la-direccion/

PEREZ-ROCA. Jesus; PEREIRA. Jose. Firewall. [En línea]. [Consultado 19 de marzo de 2020] p 4., Disponible en: http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/06%20-%20Firewalls%20%5Bupdated%5D.pdf

RAFFINO Maria. Servidor web. [En línea]. [Consultado 19 de marzo de 2020] Argentina. concepto.de. 2019., Disponible en: https://concepto.de/servidor-web/

RODRIGUEZ María. 3 Razones para implementar un plan de capacitación en sus empresas. [En línea]. [Consultado 7 de mayo de 2019]. España., Disponible en: https://blog.acsendo.com/3-razones-para-implementar-un-plan-de-capacitacion-ensu-empresa/

ROMERO CASTRO, Martha Irene, *et al.* Introducción a la seguridad informática y el análisis de vulnerabilidades. [En línea]. [Consultado 19 de marzo de 2020] Alicante. Universidad estatal del sur de Manabi. 2018. p 15., Disponible en: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

ROMERO, Martha, *et al.* Introducción a la seguridad informática y el análisis de vulnerabilidades. [En línea]. [Consultado 19 de marzo de 2020] Alicante. Universidad estatal del sur de Manabi. 2018. p 41., Disponible en: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

SEGOVIA Antonio. ¿Qué es la ISO 27001?. [En línea]. [Consultado 7 de mayo de 2019]. España. Advisera., Disponible en: https://advisera.com/27001academy/es/que-es-iso-27001/

SEGOVIA Antonio. Beneficios de ISO 27001: Como obtener el apoyo de la dirección. [En línea]. [Consultado 7 de mayo de 2019]. España. Advisera., Disponible en: https://advisera.com/27001academy/wpcontent/uploads/sites/5/2015/06/ISO_27001_Benefits_How_To_Obtain_Management_Support4_ES_presentation_deck.pdf

SGSI. ISO/IEC 27005. Gestión de riesgos de la Seguridad la Información. [En línea]. [Consultado 19 de marzo de 2020]. ISOTools Excellence.2014., Disponible en: https://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/

SGSI. ISO/IEC 27005. ISO 27005: ¿Cómo identificar los riesgos?. [En línea]. [Consultado 19 de marzo de 2020] ISOTools Excellence.2014., Disponible en: https://www.pmg-ssi.com/2017/01/iso-27005-como-identificar-los-riesgos/

SINERAY. Concepto de seguridad y sus estándares. [En línea]. [Consultado 19 de marzo de 2020] Disponible en: http://sistoperasinequi.blogspot.com/2016/06/concepto-de-seguridad-y-sus-estandares.html

sirve?. [En línea]. [Consultado 7 de mayo de 2019]. Mexico welivesecurity. 2015., Disponible en: https://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/

SISCA. ¿Qué es un control de acceso?. [En línea]. [Consultado 19 de marzo de 2020] Caracas. 2015., Disponible en: http://sisca.co/nosotros-sisca-sistemas-integrales-de-seguridad/

VILLALOBOS Johnny. PRINCIPIOS BÁSICOS DE SEGURIDAD EN BASES DE DATOS. [En línea]. [Consultado 19 de marzo de 2020] Disponible en:https://revista.seguridad.unam.mx/numero-12/principios-basicos-de-seguridad-en-bases-de-datos

ANEXOS

ANEXO A. ENCUESTA – VERIFICACIÓN DE SEGURIDAD INFORMÁTICA

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A5	Políticas de seguridad de la información			
A5.1	Directrices de gestión de la seguridad de la información			
A5.1.1	Políticas para la seguridad de la información	Cumple parcialmente	¿Existe una clara evidencia de un marco / estructura / jerarquía global razonablemente diseñada y administrada? ¿Las políticas son razonablemente completas y cubren todos los riesgos de información y áreas de control relevantes? ¿Cómo se autorizan, comunican, comprenden y aceptan las políticas? ¿Están formalmente obligados a cumplir todos los trabajadores y, en su caso, sus empleadores? ¿Hay acuerdos adecuados de cumplimiento y refuerzo? ¿Hay referencias cruzadas a buenas prácticas (como ISO27k, NIST SP800, CSC20 y otras normas y directrices relevantes)? ¿Están las políticas bien escritas, legible, razonable y viable? ¿Incorporan controles adecuados y suficientes? ¿Cubren todos los activos de información esenciales, sistemas, servicios, etc.? ¿Cuán madura es la organización en esta área?	Cumple parcialmente pese a que no existen como tal políticas escritas Existe clara evidencia de jerarquía en la empresa ya que hay varias dependencias entre las que se encuentra la de sistemas.
A5.1.2	Revisión de las políticas para la seguridad de la información	No cumple	¿Todas las políticas tienen un formato y estilo consistentes? ¿Están todos al día, habiendo completado todas las revisiones debidas? ¿Se han vuelto a autorizar y se han distribuido?	
A6	Organización de la seguridad de la información			
A6.1	Organización interna			
A6.1.1	Roles y responsabilidades en seguridad de la información	Cumple parcialmente	¿Se le da suficiente énfasis a la seguridad y al riesgo de la información? ¿Hay apoyo de la administración? ¿Existe un foro de alta gerencia para analizar el riesgo de la información y las políticas, los riesgos y los problemas de seguridad? ¿Los roles y las responsabilidades están claramente definidos y asignados a personas adecuadamente capacitadas? ¿Tiene cada rol responsabilidad específica con respecto al riesgo y la seguridad de la información? ¿Hay suficiente presupuesto para las actividades de seguridad y riesgo de la información? ¿Hay coordinación dentro de la organización entre las unidades de negocio? ¿Funciona efectivamente en la práctica? ¿Existe una conciencia y un apoyo adecuados para la estructura de riesgo y seguridad de la información?	Existe apoyo por parte de la administración

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A6.1.2	Segregación de tareas	No cumple	¿Son los deberes / funciones segregados entre roles o individuos cuando sea relevante para reducir la posibilidad de incompetencia, negligencia y actividades inapropiadas? ¿Se utiliza una matriz tipo RACI para mantener la identificación para cada tarea? Responsable | Accionable | Consultad | Informe ¿Existe una política que cubra la segregación de deberes? ¿Cómo llegan las decisiones con respecto a tal segregación? ¿Quién tiene la autoridad para tomar tales decisiones? ¿Se realiza un seguimiento regular de las actividades y los registros de auditoría?	
A6.1.3	Contacto con las autoridades	No cumple	¿Hay disponible una lista de detalles de contacto para las autoridades reguladoras u otras autoridades y organismos que podrían necesitar ser contactados en caso de consultas, incidentes y emergencias? ¿Quién es el responsable de contactar a las autoridades y en qué punto de un incidente / evento se realiza este contacto y cómo? ¿La lista es actual y correcta? ¿Hay un proceso de mantenimiento?	
A6.1.4	Contacto con grupos de interés especial	No cumple	¿Hay un contacto regular, con grupos especiales de interés, foros y listas de correo profesionales en riesgo de la información y la seguridad, tales como los capítulos locales de ISACA, ISC 2, ISSA, ISO27k? ¿Se comparte información sobre amenazas emergentes, nuevas tecnologías de seguridad, buenas prácticas de seguridad, advertencias tempranas de alertas y advertencias, vulnerabilidades recientemente descubiertas y disponibilidad de parches?	
A6.1.5	Seguridad de la información en la gestión de proyectos	No cumple	¿Se identifican y abordan los riesgos de la información y los requisitos de seguridad en todas las etapas de todos los proyectos, incluidos todos los tipos de proyectos relacionados con la información, los nuevos desarrollos y los cambios / mejoras en los sistemas, aplicaciones y procesos existentes? ¿La etapa del proyecto incluye actividades apropiadas?	
A6.2	Los dispositivos móviles y el teletrabajo			
A6.2.1	Política de dispositivos móviles	No cumple	¿Existen política y controles seguridad relacionados con los usuarios móviles? ¿Se distinguen los dispositivos personales de los empresariales? ¿Cómo se mantienen y controlan los sistemas portátiles para garantizar que estén actualizados sobre las definiciones de antivirus y los parches de seguridad? ¿Se emplean soluciones de MDM y soluciones MAM para controlar las aplicaciones, el acceso y el cifrado completo de disco?	

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A6.2.2	Teletrabajo	No cumple	¿Los controles de seguridad para el teletrabajo son equivalentes a los de los lugares de trabajo de oficina? ¿Existen disposiciones adecuadas para la autenticación del usuario (2FA), la seguridad de la red (Always-on-VPN), antivirus, copias de seguridad, parches, registro de seguridad y monitoreo, encriptación y continuidad del negocio?	
A7	Seguridad relativa a los recursos humanos			
A7.1	Antes del empleo			
A7.1.1	Investigación de antecedentes	No cumple	¿El proceso de evaluación previa al empleo toma en cuenta las leyes y regulaciones relevantes de privacidad y empleo? ¿Se hace en la empresa o se subcontrata a un tercero? Si se subcontrata a un tercero, ¿Se han revisado sus procesos y se han considerado aceptables? ¿Se hace contacto de referencias y una verificación de antecedentes, según corresponda durante el proceso de selección? ¿Existen procesos de selección mejorados para los trabajadores en roles críticos? ¿Cómo se logra todo esto? ¿Hay un proceso documentado, consistente y repetible, que sea propiedad y mantenido por RRHH?	
A7.1.2	Términos y condiciones del empleo	No cumple	¿Están claramente definidos los términos y condiciones de empleo? ¿Se hace distinción entre profesionales de la seguridad, los administradores de redes / sistemas de TI, los gerentes, los auditores y los trabajadores en general? ¿Se identifican responsabilidades específicas relacionadas con el riesgo y la seguridad de la información de acuerdo con la naturaleza de los roles? ¿Se mantienen registros para probar que los trabajadores entendieron, reconocieron y aceptaron sus obligaciones de seguridad de la información?	
A7.2	Durante el empleo			
A7.2.1	Responsabilidades de gestión	No cumple	¿Existe un programa de concientización / educación sobre la seguridad de la información dirigido a la gerencia? ¿Se hace de forma regular y está a día? ¿El contenido y la naturaleza / formato / estilo de la información y las actividades de sensibilización son adecuados? ¿Los gerentes reciben el conocimiento y la capacitación apropiados específicamente sobre su riesgo clave de información y roles y responsabilidades relacionados con la seguridad? ¿Se provee información sobre la postura, estrategias y políticas de seguridad de la información de la organización?	

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	No cumple	¿Están las competencias necesarias y los requisitos de capacitación / concienciación para los profesionales de seguridad de la información y otros con funciones y responsabilidades específicas identificadas explícitamente? ¿Existe un programa estructurado de sensibilización y capacitación sobre seguridad de la información para todos los tipos de trabajadores? ¿Existe una estrategia o plan de comunicación, que incluya folletos, carteles, correos electrónicos, gestión de aprendizaje online, cuestionarios, concursos, videos, redes sociales y otros métodos? ¿Se cubren los requisitos legales, reglamentarios, contractuales, políticos, responsabilidad personal, responsabilidades generales, puntos de contacto y otros recursos? ¿Se actualiza el contenido para reflejar los riesgos de la información en evolución, como las amenazas emergentes, las vulnerabilidades recientemente identificadas y los incidentes, y los cambios, como las políticas nuevas / revisadas? ¿Hay exámenes y ejercicios periódicos para verificar el nivel de conocimiento? ¿Hay acciones de seguimiento para cualquiera que tenga problemas en dichas pruebas?	
A7.2.3	Proceso disciplinario	No cumple	¿Existe un proceso disciplinario para incidentes de seguridad de la información, violaciones a la privacidad, piratería informática, fraude y espionaje industrial por parte de los trabajadores? ¿Cómo se informa a los trabajadores sobre el proceso, incluidas las expectativas de la organización y sus derechos? ¿Está esto cubierto por contratos y acuerdos, capacitación inicial y conocimiento continuo? ¿Se actualiza el proceso de forma regular?	
A7.3	Finalización del empleo o cambio en el puesto de trabajo			
A7.3.1	Responsabilidades ante la finalización o cambio	No cumple	¿Existen políticas de revisión, estándares, procedimientos, directrices y registros relacionados con la seguridad de la información para los trabajadores que se mueven lateral o verticalmente dentro de la organización? ¿Se tienen en cuenta las promociones, degradaciones, cambios de roles, nuevas responsabilidades, nuevas prácticas de trabajo, renuncias, despidos? ¿Se tiene en cuenta la recuperación de los activos de información (documentos, datos, sistemas), las llaves, la eliminación de los derechos de acceso?	
A8	Gestión de activos			
A8.1	Responsabilidad sobre los activos			

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A8.1.1	Inventario de activos	Cumple	¿Hay un inventario de activos de la información? ¿Contiene la siguiente información? • Datos digitales • Información impresa • Software • Infraestructura • Servicios de información y proveedores de servicios • Seguridad física • Relaciones comerciales • Las personas ¿A quién pertenece el inventario? ¿Cómo se mantiene el inventario en una condición razonablemente completa, precisa y actualizada a pesar de los cambios de equipo / personal, nuevos sistemas, negocios y cambios de TI? ¿Es suficientemente detallado y está estructurado adecuadamente?	
A8.1.2	Propiedad de los activos	Cumple parcialmente	¿Los activos tienen propietario de riesgo? ¿Los activos tienen responsable técnico? ¿Cómo se asigna la propiedad poco después de crear o adquirir los activos críticos? ¿Cómo se etiquetan los activos? ¿Cómo se informa ante incidentes de seguridad de la información que los afectan?	
A8.1.3	Uso aceptable de los activos	Cumple parcialmente	¿Existe una política sobre el uso aceptable de los recursos tecnológicos, como el correo electrónico, la mensajería instantánea, el FTP, las responsabilidades de los usuarios, etc.? ¿Cubre el comportamiento del usuario en Internet y en las redes sociales? ¿Se permite el uso personal de los activos de la empresa? En caso afirmativo, ¿En qué medida y cómo se controla / asegura esto? ¿Se describe de forma explícita lo qué constituye un uso inapropiado? ¿Se distribuye esta información a toda la empresa? ¿El uso de la criptografía cumple con todas las leyes, acuerdos / contratos y normativas relevantes?	
A8.1.4	Devolución de activos	Cumple parcialmente	¿Existe un procedimiento para recuperar los activos tras una baja o despido? ¿Es un procedimiento automatizado o manual? Si es manual, ¿Cómo se garantiza que no haya desvíos? ¿Cómo se abordan los casos en los que los activos no han sido devueltos?	
A8.2	Clasificación de la información			
A8.2.1	Clasificación de la información	Cumple parcialmente	¿Existen políticas de revisión, estándares, procedimientos, directrices y registros asociados relacionados con la clasificación de la información? ¿La clasificación es impulsada por obligaciones legales o contractuales? ¿La clasificación se basa en los requisitos de confidencialidad, integridad y disponibilidad? ¿Se utilizan marcas apropiadas en los activos en función de la clasificación de la información que contienen? ¿El personal conoce los requisitos de seguridad correspondientes para el manejo de materiales clasificados?	

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A8.2.2	Etiquetado de la información	Cumple parcialmente	¿Existe un procedimiento de etiquetado para la información tanto en forma física como electrónica? ¿Está sincronizado con la política de clasificación de la información? ¿Cómo se garantiza el correcto etiquetado? ¿Cómo se garantiza que solo aquellos con permisos de acceso aprobados accedan a la información de la clasificación relevante? ¿Cómo se garantiza que no haya acceso no autorizado? ¿Se revisan los niveles de clasificación en intervalos predefinidos?	
A8.2.3	Manipulado de la información	Cumple parcialmente	Más allá de A.8.2.1 ¿Están los niveles de clasificación adecuadamente asignados a los activos? ¿Se considera los gimiente? Método de etiquetado, transferencia, almacenamiento, manejo de medios extraíbles, eliminación de medios electrónicos y físicos, divulgación, intercambio, intercambio con terceros, etc.	
A8.3	Manipulación de los soportes			
A8.3.1	Gestión de soportes extraíbles	No cumple	¿Existe un registro de activos completo y actualizado de CD / DVD, almacenamiento USB y otros medios extraíbles? ¿Los medios extraíbles están debidamente etiquetados y clasificados? ¿Los medios se mantienen y almacenan de forma adecuada? ¿Hay controles apropiados para mantener la confidencialidad de los datos almacenados?	
A8.3.2	Eliminación de soportes	No cumple	Más allá de A.8.3.1 ¿Existen una política específica y documentación de obligaciones contractuales, legales o reglamentarias para la eliminación de los medios? ¿Se documenta la aprobación en cada etapa para la eliminación de los medios? ¿Los datos que aún deben conservarse se copian en otros medios y se verifican antes de su eliminación? ¿Se tiene en cuenta los periodos de retención? ¿Los datos particularmente confidenciales se eliminan de forma segura (borrado criptográfico, desmagnetización o destrucción física)?	
A8.3.3	Soportes físicos en tránsito	No cumple	¿Se utiliza un transporte o servicio de mensajería confiable? ¿Se utiliza un mecanismo de cifrado adecuado durante el proceso de transferencia? ¿Se verifica la recepción por el destino?	
A9	Control de acceso			
A9.1	Requisitos de negocio para el control de acceso			

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A9.1.1	Política de control de acceso	Cumple parcialmente	¿Existe una política de control de acceso? ¿Es consistente con la política de clasificación? ¿Hay una segregación de deberes apropiada? ¿Existe un proceso documentado de aprobación de acceso? ¿El proceso de aprobación requiere que se involucre el propietario del sistema o la información en cuestión?	
A9.1.2	Acceso a las redes y a los servicios de red	Cumple parcialmente	¿Se asegura que el acceso VPN e inalámbrico es supervisado, controlados y autorizado? ¿Se utiliza autenticación de múltiples-factor para acceso a redes, sistemas y aplicaciones críticas, especialmente para los usuarios privilegiados? ¿Cómo monitoriza la red para detectar acceso no autorizado? ¿Los controles de seguridad de la red son evaluados y probados regularmente (Pentesting)? ¿La organización mide la identificación y los tiempos de respuesta ante incidentes?	
A9.2	Gestión de acceso de usuario			
A9.2.1	Registro y baja de usuario	Cumple parcialmente	¿Se utiliza un ID de usuario únicos para cada usuario? ¿Se genera en función a una solicitud con aprobaciones y registros apropiados? ¿Se deshabilitan los ID de usuario de forma inmediata tas una baja o despido? ¿Existen una comunicación eficiente ente la Administración de Seguridad y Recursos Humanos? ¿Existe una revisión / auditoría periódica para identificar y deshabilitar los ID de usuario redundantes? ¿Se eliminan los ID deshabilitados después de confirmar que ya no son necesarios? ¿Qué impide que los ID de usuario sean reasignados a otros usuarios?	
A9.2.2	Provisión de acceso de usuario	Cumple parcialmente	¿El acceso a sistemas y servicios de información se basa en las necesidades del negocio? ¿Se garantiza que todo acceso que se concede se ajuste a las políticas de control de acceso y segregación de funciones? ¿Existe un registro documental de la solicitud y aprobación de acceso?	
A9.2.3	Gestión de privilegios de acceso	No cumple	¿Hay un proceso para realizar revisiones más frecuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios? ¿Se genera un ID de usuario separado para otorgar privilegios elevados? ¿Se ha establecido una caducidad para los ID de usuario con privilegios? ¿Se controlan las actividades de los usuarios privilegiados de forma más detallada?	

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Cumple parcialmente	¿Se implementan controles técnicos, como la longitud mínima de la contraseña, reglas de complejidad, cambio forzado de contraseñas en el primer uso, autenticación de múltiples factores, datos biométricos, contraseñas compartidas etc.? ¿Se verifica rutinariamente si hay contraseñas débiles? ¿Se requiere confirmar la identidad de los usuarios antes de proporcionarles contraseñas temporales nuevas? ¿Se transmite dicha información por medios seguros? ¿Se generan contraseñas temporales suficientemente fuertes? ¿Se cambian las contraseñas por defecto de los fabricantes? ¿Se recomienda a los usuarios usar el software adecuado de protección de contraseñas? ¿Se almacenen de forma cifrada las contraseñas en sistemas, dispositivos y aplicaciones?	
A9.2.5	Revisión de los derechos de acceso de usuario	Cumple parcialmente	¿Se hace una revisión periódica y documentada de los derechos de acceso de los usuarios en sistemas y aplicaciones? ¿Participan en dicha revisión los "propietarios" para verificar cambios en las funciones de los usuarios? ¿Se revisan los derechos de acceso para usuarios con privilegios de forma más exhaustiva y frecuente?	
A9.2.6	Retirada o reasignación de los derechos de acceso	Cumple	¿Existe un proceso de ajuste de derechos de acceso? ¿Tiene en cuenta empleados, proveedores y contratistas al finalizar o cambiar su empleo, contrato o acuerdo? ¿Incluye el acceso físico a las instalaciones y el acceso lógico a la red? En casos en los que se usan credenciales compartidas, ¿Se cambian las contraseñas cuando ocurren ceses o despidos de empleados que las usan?	
A9.3	Responsabilidades del usuario			
A9.3.1	Uso de la información secreta de autenticación	Cumple parcialmente	¿Cómo se asegura la confidencialidad de las credenciales de autenticación? ¿Existe un proceso de cambio de contraseñas en caso de ser comprometida? ¿Existen controles de seguridad relativas a las cuentas compartidas?	
A9.4	Control de acceso a sistemas y aplicaciones			
A9.4.1	Restricción del acceso a la información	Cumple parcialmente	¿Existen controles de acceso adecuados? ¿Se identifican los usuarios de forma individual individuales? ¿Cómo se definen, autorizan, asignan, revisan, gestionan y retiran los derechos de acceso, los permisos y las reglas asociadas?	

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A9.4.2	Procedimientos seguros de inicio de sesión	No cumple	¿Se muestra una pantalla de advertencia en el proceso de inicio de sesión para disuadir el acceso no autorizado? ¿Cómo se autentican las identidades de usuario durante el proceso de inicio de sesión? ¿Se utiliza autenticación multifactor para sistemas / servicios / conexiones remotas críticas a través de VPN s etc.? ¿La información de inicio de sesión solo se valida una vez imputadas las credenciales? ¿Las contraseñas no válidas desencadenan demoras o bloqueos, entradas de registro y alertas / alarmas? ¿Se registran los inicios de sesión exitosos? ¿Se transmiten las contraseñas de modo seguro mediante el uso de cifrado?	
A9.4.3	Sistema de gestión de contraseñas	Cumple parcialmente	¿Los sistemas requieran una fortaleza de contraseñas establecidos en las políticas y estándares corporativos? ¿Las reglas tienen en cuenta lo siguiente? • Longitud mínima de la contraseña • Evitan la reutilización de un número específico de contraseñas • Imponen reglas de complejidad (mayúsculas, minúsculas, números, símbolos, etc.) • Requiere el cambio forzado de contraseñas en el primer inicio de sesión • Esconde la contraseña durante la imputación ¿Se almacenan y transmiten de forma segura (cifrado)?	
A9.4.4	Uso de utilidades con privilegios del sistema	Cumple parcialmente	¿Quién controla los servicios privilegiados? ¿Quién puede acceder a ellos, bajo qué condiciones y con qué fines? ¿Se verifica que estas personas necesidad comercial para otorgar el acceso según su roles y responsabilidades? ¿Existe un proceso auditable de aprobación, y cada instancia de su uso está registrado? ¿Se tiene en cuenta la segregación de tareas?	
A9.4.5	Control de acceso al código fuente de los programas	Cumple parcialmente	¿El código fuente se almacena en una o más bibliotecas de programas fuente o repositorios? ¿El entorno es seguro, con un acceso adecuado, control de versiones, monitoreo, registro, etc.? ¿Cómo se modifica el código fuente? ¿Cómo se publica y se compila el código? ¿Se almacenan y revisan los registros de acceso y cambios?	
A10	Criptografía			
A10.1	Controles criptográficos			
A10.1.1	Política de uso de los controles criptográficos	No cumple	¿Existe una política que cubra el uso de controles criptográficos? ¿Cubre lo siguiente? • Los casos en los que información debe ser protegida a través de la criptografía • Normas que deben aplicarse para la aplicación efectiva • Un proceso basado en el riesgo para determinar y especificar la protección requerida • Uso de cifrado para información almacenada o transferida • Los efectos de cifrado en la inspección de contenidos de software • Cumplimiento de las leyes y normativas aplicables ¿Se cumple con la política y requerimientos de cifrado?	

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A10.1.2	Gestión de claves	No cumple	¿La política de criptografía abarca todo el ciclo de vida de la gestión de claves (de principio a fin)? ¿Se protege el equipo utilizado para generar, almacenar y archivar claves criptográficas? ¿Se generan claves diferentes para sistemas y aplicaciones? ¿Se evitan claves débiles? ¿Existen reglas sobre cambio / actualización de claves (ej. autorizar, emitir, comunicar e instalar claves)? ¿Se hacen copias de respaldo de las claves? ¿Se registran las actividades clave de gestión? ¿Cómo se cumplen todos estos requisitos?	
A11	Seguridad física y del entorno			
A11.1	Áreas seguras			
A11.1.1	Perímetro de seguridad física	Cumple parcialmente	¿Las instalaciones se encuentran en una zona de riesgo? ¿Se definen los perímetros de seguridad (edificios, oficinas, redes informáticas, habitaciones, armarios de red, archivos, salas de máquinas, etc.)? ¿El techo exterior, las paredes y el suelo son de construcción sólida? ¿Están todos los puntos de acceso externos adecuadamente protegidos contra el acceso no autorizado? ¿Las puertas y ventanas son fuertes y con cerradura? ¿Se monitorea los puntos de acceso con cámaras? ¿Existe un sistema de detección de intrusos y se prueba periódicamente?	
A11.1.2	Controles físicos de entrada	Cumple parcialmente	¿Se utilizan sistemas de control de acceso adecuados (ej. Tarjetas de proximidad, biométrico, cerraduras de seguridad, monitorización CCTV, detección de intrusos)? ¿Hay procedimientos que cubran las siguientes áreas? • Cambio regular código de acceso • Inspecciones de las guardias de seguridad • Visitantes siempre acompañados y registrados en el libro de visitantes • Registro de movimiento de material • Entrada a áreas definidas del edificio según roles y responsabilidades (acceso a CPD, salas de comunicación y otras áreas críticas) ¿Se utiliza autenticación multi-factor de autenticación (ej. Biométrico más el código PIN)? ¿Se requiere para las áreas críticas? ¿Existe un registro de todas las entradas y salidas?	
A11.1.3	Seguridad de oficinas, despachos y recursos	Cumple parcialmente	¿Están los accesos (entrada y salida) de las instalaciones físicamente controlas (ej. Detectores de proximidad, CCTV)? ¿Son proporcionados los controles de seguridad utilizados para salvaguardar las oficinas, salas e instalaciones con respecto a los riesgos? ¿Se tiene en cuenta los activos de información almacenados, procesados o utilizados en dichas ubicaciones?	
A11.1.4	Protección contra las amenazas externas y ambientales	Cumple parcialmente	¿Qué tipo de protecciones existen contra el fuego, el humo, inundaciones, rayos, intrusos, vándalos, etc.? ¿Existe un procedimiento de recuperación de desastres? ¿Se contemplan sitios remotos?	

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A11.1.5	El trabajo en áreas seguras	Cumple parcialmente	¿Se verifican al final del día las oficinas, las salas de informática y otros lugares de trabajo? ¿Se hace un análisis para evaluar que los controles adecuados están implementados? Controles de acceso físico Alarmas de intrusión Monitoreo de CCTV (verificar la retención y frecuencia de revisión) Se prohíbe el uso de equipos fotográficos, video, audio u otro tipo de grabación Políticas, procedimientos y pautas ¿Cómo se asegura que la información de carácter sensible permanece confidencial a personal autorizado?	
A11.1.6	Áreas de carga y descarga	Cumple parcialmente	¿Las entregas se hacen en un área segura con control de acceso y limitado a personal autorizado? ¿Se verifica que el material recibido coincide con un número de pedido autorizado? ¿Se registran los detalles de la recepción de material según las políticas y procedimientos de adquisición, gestión de activos y seguridad?	
A11.2	Seguridad de los equipos			
A11.2.1	Emplazamiento y protección de equipos	Cumple parcialmente	¿Las TIC y el equipo relacionado se encuentran en áreas adecuadamente protegidas? ¿Las pantallas de los equipos de trabajo, las impresoras y los teclados están ubicados o protegidos para evitar la visualización no autorizada? ¿Existen controles para minimizar los siguientes riesgos de amenazas físicas y medioambientales? • Agua / inundación • Fuego y humo • Temperatura, humedad y suministro eléctrico • Polvo • Rayos, electricidad estática y seguridad del personal ¿Se prueban estos controles periódicamente y después de cambios importantes?	
A11.2.2	Instalaciones de suministro	Cumple parcialmente	¿El sistema UPS proporciona una potencia adecuada, confiable y de alta calidad? ¿Hay una capacidad de UPS adecuada para abarcar todos los equipos esenciales durante un período de tiempo suficiente? ¿Hay un plan de mantenimiento pare los UPS y generadores en acuerdo con las especificaciones del fabricante? ¿Son probados con regularidad? ¿Hay una red de suministro eléctrico redundante? ¿Se realizan pruebas de cambio? ¿Se ven afectados los sistemas y servicios? ¿Hay sistemas de aire acondicionado para controlar entornos con equipos críticos? ¿Están ubicados apropiadamente? ¿Hay una capacidad adecuada de A / C para soportar la carga de calor? ¿Hay unidades redundantes, de repuesto o portátiles disponibles? ¿Hay detectores de temperatura con alarmas de temperatura?	

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A11.2.3	Seguridad del cableado	Cumple	¿Hay protección física adecuada para cables externos, cajas de conexiones? ¿Se separa el cableado de suministro eléctrico del cableado de comunicaciones para evitar interferencias? ¿Se controla el acceso a los paneles de conexión y las salas de cableado? ¿Existen procedimientos adecuados para todo ello?	
A11.2.4	Mantenimiento de los equipos	Cumple	¿Se asigna personal cualificado para realizar el mantenimiento de los equipos (infraestructura y dispositivos de red, equipos de trabaja, portátiles, equipos de seguridad y servicios tales como detectores de humo, dispositivos de extinción de incendios, HVAC, control de acceso, CCTV, etc.)? ¿Hay programas de mantenimiento y registros / informes actualizados? ¿Se aseguran los equipos?	
A11.2.5	Retirada de materiales propiedad de la empresa	Cumple	¿Existen procedimiento relativos al traslado de activos de información? ¿Hay aprobaciones o autorizaciones documentadas en los niveles apropiados? ¿Existe un control para limitar el traslado de activos de información mediante el uso de unidades de almacenamiento externo? ¿Existe un procedimiento para rastrear movimientos de activos de alto valor o alto riesgo?	
A11.2.6	Seguridad de los equipos fuera de las instalaciones	Cumple parcialmente	¿Existe una “política de uso aceptable” que cubra los requisitos de seguridad y “obligaciones” con respecto al uso de dispositivos móviles o portátiles que se utilizan desde casa o en ubicaciones remotas? ¿Contempla el almacenamiento seguro de los dispositivos, uso cifrado y uso de conexiones seguras? ¿Existen controles para asegura todo esto? ¿Cómo se les informa a los trabajadores sobre sus obligaciones? ¿Se les da suficiente apoyo para alcanzar un nivel aceptable de seguridad?	
A11.2.7	Reutilización o eliminación segura de equipos	Cumple	¿Cómo evita la organización que se revele la información almacenada en equipos tras su reasignación o eliminación? ¿Se utiliza cifrado fuerte o borrado seguro? ¿Se mantienen registros adecuados de todos los medios que se eliminan? ¿La política y el proceso cubren todos los dispositivos y medios de TIC?	
A11.2.8	Equipo de usuario desatendido	Cumple	¿Se suspenden / finalizan las sesiones a aplicaciones para evitar la pérdida de datos o la corrupción? ¿Se define un tiempo de inactividad adecuado los riesgos de acceso físico no autorizado? ¿Se protegen los bloqueos de pantalla con contraseña? ¿Se aplica a todos los servidores, equipos de trabajo, portátiles, teléfonos y otros dispositivos TIC? ¿Cómo se verifica el cumplimiento?	

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Cumple parcialmente	¿Existen políticas, normas, procedimientos y directrices para mantener las zonas de trabajo limpias y despejadas? ¿Funciona en la práctica? ¿Todos los dispositivos informáticos tienen un salvapantallas o bloqueo con contraseña que los empleados usan cuando se alejan de sus dispositivos? ¿Se activa automáticamente tras de un tiempo inactivo definido? ¿Se mantienen las impresoras, fotocopiadoras, escáneres despejados?	
A12	Seguridad de las operaciones			
A12.1	Procedimientos y responsabilidades operacionales			
A12.1.1	Documentación de procedimientos operacionales	Cumple parcialmente	¿Existen procedimientos para las operaciones de TI, sistemas y gestión de redes, gestión de incidencias, la administración de TI, seguridad de TI, seguridad física, gestión de cambios, etc.? ¿Existe un conjunto completo de procedimientos de seguridad y cuándo se revisaron por última vez? ¿Los procesos son razonablemente seguros y están bien controlados? ¿Los roles y responsabilidades están bien definidos y se capacita adecuadamente al personal? ¿Se tienen en cuenta los cambios, configuraciones, versiones, capacidad, rendimiento, problemas, incidentes, copias de seguridad, almacenamiento, restauración, registros de auditoría, alarmas / alertas, endurecimiento, evaluaciones de vulnerabilidad, parches, configuración / actualizaciones de antivirus, encriptación, etc.)? ¿Los procedimientos están siendo revisados y mantenidos rutinariamente, autorizados / ordenados, compartidos y usados?	
A12.1.2	Gestión de cambios	Cumple parcialmente	¿Existe una política de gestión de cambios? ¿Existen registros relacionados a la gestión de cambios? ¿Se planifican y gestionan los cambios? ¿Se evalúan los riesgos potenciales asociados con los cambios? ¿Los cambios están debidamente documentados, justificados y autorizados por la administración?	
A12.1.3	Gestión de capacidades	Cumple parcialmente	¿Existe una política de gestión de capacidad? ¿Existen registros relacionados a la gestión de capacidad? ¿Incluye aspectos tales como las SLA, seguimiento de las métricas relevantes (ej. uso de la CPU, almacenamiento y errores de página, capacidad de la red, demanda de RAM, la capacidad de aire acondicionado, espacio de rack, la utilización, etc.), alarmas / alertas en niveles críticos, la planificación hacia adelante? ¿Se basa la prioridad en asegurar el rendimiento y la disponibilidad de servicios críticos, servidores, infraestructura, aplicaciones, funciones en un análisis de riesgos?	

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	Cumple parcialmente	¿Se segregan entornos de TIC de desarrollo, prueba y operacionales? ¿Cómo se logra la separación a un nivel de seguridad adecuado? ¿Existen controles adecuados para aislar cada entorno (ej. redes de producción, redes utilizadas para el desarrollo, redes de pruebas, la gestión)? ¿Se tienen acceso a través de perfiles de usuario debidamente diferenciados para cada uno de estos entornos? ¿Cómo se promueve y se lanza el software? ¿Se aplica la gestión de cambios a la autorización y migración de software, datos, metadatos y configuraciones entre entornos en cualquier dirección? ¿Se tiene en cuenta el riesgo de la información y los aspectos de seguridad que incluye el cumplimiento de privacidad si los datos personales se mueven a entornos menos seguros? ¿Se identifica un responsable de garantizar que el software nuevo / modificado no interrumpa las operaciones de otros sistemas o redes?	
A12.2	Protección contra el software malicioso (malware)			
A12.2.1	Controles contra el código malicioso	Cumple parcialmente	¿Existen políticas y procedimientos asociados a controles antimalware? ¿Se utilizan listas blancas o negras para controlar el uso de software autorizado y no autorizado? ¿Cómo se compila, gestiona y mantiene la lista y por quién? ¿Hay controles de antivirus de “escaneado en acceso” y “escaneo programático” en todos los dispositivos relevantes, incluidos servidores, portátiles, ordenadores de sobremesa y dispositivos integrados / IoT? ¿Se actualiza el software antivirus de forma automática? ¿Se general alertas accionables tras una detección? ¿Se toma acción de forma rápida y apropiada para minimizar sus efectos? ¿Cómo se gestionan las vulnerabilidades técnicas? ¿Existe una capacitación y una concienciación apropiada que cubra la detección, el informe y la resolución de malware para usuarios, gerentes y especialistas de soporte? ¿Existe un mecanismo de escalación para incidentes graves?	
A12.3	Copias de seguridad			

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A12.3.1	Copias de seguridad de la información	Cumple parcialmente	¿Existen políticas y procedimientos asociados a las copias de seguridad? ¿Existe un mandato basado en el riesgo para un registro preciso y completo de copias de seguridad cuya política de retención y frecuencia reflejen las necesidades del negocio? ¿Las copias de seguridad cubren los datos y metadatos, sistema y programas de aplicación y los parámetros de configuración de copias de seguridad para todos los sistemas, incluyendo servidores, ordenadores de sobremesa, teléfonos / sistemas de red, sistemas de gestión de red, portátiles, sistemas de control, sistemas de seguridad, etc.? ¿Los medios de respaldo están físicamente protegidos / asegurados al menos al mismo nivel que los datos operacionales? ¿Las copias de seguridad se almacenan en ubicaciones adecuadas, protegiendo contra desastres físicos y acceso indebido? ¿Se mantienen copias off-line para evitar una propagación de ransomware catastrófica? ¿Las copias de seguridad se prueban regularmente para garantizar que puedan restaurar? ¿Hay una clara adherencia a principios de confidencialidad, integridad y disponibilidad?	
A12.4	Registros y supervisión			
A12.4.1	Registro de eventos	Cumple parcialmente	¿Existen políticas y procedimientos para el registro de eventos? ¿Se monitorean y registran de manera consistente y segura todos los sistemas clave incluido el registro de eventos en sí? ¿Se registra lo siguiente? • cambios en los ID de usuario • permisos y controles de acceso • actividades privilegiadas del sistema • intentos de acceso exitosos y fallidos • inicio de sesión y cierre de sesión • identidades y ubicaciones de dispositivos • direcciones de red, puertos y protocolos • instalación de software • cambios a las configuraciones del sistema • uso de utilidades y aplicaciones del sistema • archivos accedidos y el tipo de acceso • filtros de acceso web ¿Quién es responsable de revisar y hacer un seguimiento de los eventos informados? ¿Cuál es el periodo de retención de eventos? ¿Existe un proceso para revisar y responder adecuadamente a las alertas de seguridad?	
A12.4.2	Protección de la información del registro	No cumple	¿Los registros se almacenan / archivan en un formato seguro o mecanismo de control no-editable? ¿El acceso a los registros es adecuadamente controlado, autorizado y monitoreado? ¿Quién tiene o podría obtener acceso a leer / escribir / eliminar registros de eventos? ¿Hay suficiente capacidad de almacenamiento dado el volumen de registros que se generan y los requisitos de retención? ¿Existen copias de seguridad de los registros?	

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A12.4.3	Registros de administración y operación	Cumple parcialmente	Hay responsables identificados para la administración de acceso privilegiado al análisis de eventos (SIEM)? ¿Cómo se recogen, almacenan y aseguran, analizan los registros? ¿Existen limitaciones a la capacidad de dichas personas para interferir con los registros o, al menos, no sin generar alarmas de seguridad?	
A12.4.4	Sincronización del reloj	Cumple parcialmente	¿Existen políticas, arquitecturas o procedimientos relativos a la sincronización del reloj del sistema su precisión? ¿Hay un tiempo de referencia definido (ej. Reloj atómicos, GPS o NTP)? ¿El método para sincronizar relojes con la referencia cumple con los requisitos comerciales, de seguridad, operacionales, legales, regulatorios y contractuales? ¿Está implementado en todo el entorno TI, incluidos los sistemas de monitoreo tales como CCTV, sistemas de alerta, mecanismos de control de acceso, sistemas de auditoría y registro, etc.? ¿Existe una configuración de respaldo para la referencia de tiempo?	
A12.5	Control del software en explotación			
A12.5.1	Instalación del software en explotación	Cumple parcialmente	¿Existe una política acerca de la instalación de software? ¿Se asegura que todo software instalado es probado, aprobado, permitido y mantenido para su uso en producción? ¿Se verifica que ya no se utiliza software sin soporte (firmware, sistemas operativos, middleware, aplicaciones y utilidades)? ¿Se hace esta verificación en ordenadores de sobremesa, portátiles, servidores, bases de datos, etc.? ¿Existen controles para evitar instalaciones de software, excepto por administradores capacitados y autorizados? ¿Existe un monitoreo y alerta para detectar instalaciones de software no aprobadas? ¿Existe un control de cambio y aprobación adecuado para la aprobación de software?	
A12.6	Gestión de la vulnerabilidad técnica			

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A12.6.1	Gestión de las vulnerabilidades técnicas	Cumple parcialmente	¿Existe una política la gestión de vulnerabilidades técnicas? ¿Cómo se escanean los sistemas para detectar vulnerabilidades de forma automatizada? ¿Cómo responde la organización ante vulnerabilidades técnicas descubiertas en equipos, servidores, aplicaciones, dispositivos de red y otros componentes? ¿Existen procesos adecuados para verificar los inventarios de los sistemas e identificar si las vulnerabilidades divulgadas son relevantes? ¿Se ha realizado una evaluación integral de riesgos de los sistemas TIC? ¿Se han identificado los riesgos y se han tratado apropiadamente, se han priorizado según el riesgo? ¿Se identifican cambios tales como amenazas emergentes, vulnerabilidades conocidas o sospechadas, y consecuencias o impactos comerciales en evolución? ¿Los parches son evaluados por su aplicabilidad y riesgos antes de ser implementados? ¿Los procesos para implementar parches urgentes son adecuados? ¿Se emplea una administración automatizada de parches? ¿Existen registros de aprobación o rechazo de implementación de parchas asociado a vulnerabilidades (aceptación de riesgo) en los niveles de administración adecuados?	
A12.6.2	Restricción en la instalación de software	Cumple parcialmente	¿La instalación software en los sistemas está limitada personal autorizado con privilegios de sistema adecuados? ¿Los privilegios de instalación están divididos en categorías y permiten instalar tipos de sistemas específicos? ¿Los controles se aplican a parches, copias de seguridad y descargas de la web, así como a instalaciones de sistemas, servidores, etc.?	
A12.7	Consideraciones sobre la auditoria de sistemas de información			
A12.7.1	Controles de auditoría de sistemas de información		¿Existe una política que requiera auditorias de seguridad de la información? ¿Existe un programa definido y procedimientos para auditoría? ¿Las auditorías se planifican cuidadosamente y se acuerdan para minimizar el riesgo de interrupciones en los procesos comerciales? ¿Se define el alcance de la auditoría en coordinación con la administración? ¿El acceso a las herramientas de auditoría de sistemas están controladas para evitar el uso y acceso no autorizado?	
A13	Seguridad de las comunicaciones			
A13.1	Gestión de la seguridad de las redes			

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A13.1.1	Controles de red	Cumple parcialmente	¿Existen políticas de redes físicas e inalámbricas? ¿Existe una separación de la administración de las operaciones de sistemas y la de infraestructuras de red? ¿Existe un mecanismo de registro i monitorización de la red y los dispositivos que se conectan ella? ¿Hay un sistema de autenticación para todos los accesos a la red de la organización? ¿El sistema limita el acceso de personas autorizadas a aplicaciones / servicios legítimos? ¿Los usuarios se autentican adecuadamente al inicio de sesión? ¿Cómo se autentican los dispositivos de red? ¿Existe una segmentación de red adecuada usando cortafuegos, VLAN, VPN, etc.? ¿Se controlan los puertos y servicios utilizados para funciones de administración de sistemas?	
A13.1.2	Seguridad de los servicios de red	Cumple parcialmente	¿Se gestionan, clasifican y protegen los servicios de red de forma adecuada? ¿Existe un monitoreo de servicios de red? ¿Se mantiene un derecho a auditar servicios de red gestionados por terceros (contratos, SLA y requisitos de informes de gestión)? ¿Se emplean mecanismos de autenticación en la red, cifrado de tráfico de red? ¿Se hace una revisión periódica de las configuraciones de cortafuegos, IDS / IPS, WAF, DAM?	
A13.1.3	Segregación en redes	Cumple parcialmente	¿Existe una política de segmentación de red? ¿Qué tipo de segmentación existe? ¿Es basada en la clasificación, los niveles de confianza, dominios (público, escritorios, servidor, funciones, etc.)? ¿Cómo se monitorea y controla la segregación? ¿Se segmenta la red inalámbrica de la red física? ¿Y la red de invitados? ¿Hay controles adecuados entre ellos? ¿Cómo se controla la segmentación con proveedores y clientes? ¿La seguridad es adecuada dados los riesgos y el apetito de riesgo de la organización?	
A13.2	Intercambio de información			

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A13.2.1	Políticas y procedimientos de intercambio de información	Cumple parcialmente	¿Existen políticas y procedimientos relacionados con la transmisión segura de información? ¿Contempla mecanismos como correo electrónico, FTP y otras aplicaciones de transferencia de datos y protocolos Web (ej. Los grupos / foros, Dropbox y servicios en la nube similares), WiFi y Bluetooth, CD / DVD, almacenamiento externo USB, mensajería, etc.? ¿Está basado en la clasificación de la información? ¿Existen controles de acceso adecuados para esos mecanismos? ¿Cómo se implementa el uso de criptografía para los mecanismos aceptados (ej. TLS, cifrado de correo electrónico, ZIP codificados)? ¿Se sigue el principio de confidencialidad y privacidad? ¿Existen un programa de concientización, capacitación y cumplimiento?	
A13.2.2	Acuerdos de intercambio de información	Cumple parcialmente	Más allá de A.13.2.1 ¿Qué tipos de comunicaciones se implementan las firmas digitales? ¿Qué tipo de responsabilidades se asocian a la perdida, corrupción o divulgación de datos? ¿Existe una identificación y sincronización de los niveles de clasificación de información de todas las partes involucradas? ¿Cómo se mantiene una cadena de custodia para las transferencias de datos?	
A13.2.3	Mensajería electrónica	Cumple parcialmente	¿Existe una política de mensajería que cubra controles de intercambio de datos por comunicación de red, incluyendo correo electrónico y FTP / SFTP, etc.? ¿Hay controles de seguridad adecuados (ej. cifrado de correo electrónico, la autenticidad, la confidencialidad y la irrenunciabilidad de mensajes, etc.)? ¿Existen controles de seguridad para la interacción con sistemas Internet, Intranet relacionados con foros y tableros de anuncios electrónicos?	
A13.2.4	Acuerdos de confidencialidad o no revelación	Cumple parcialmente	¿Existen acuerdos de confidencialidad? ¿Han sido revisados y aprobados por el Departamento Legal? ¿Cuándo fueron revisados por última vez (periódicos o basados en cambios)? ¿Han sido aprobados y firmados por las personas adecuadas? ¿Existen sanciones adecuadas y acciones esperadas en caso de incumplimiento y / o beneficios por el cumplimiento (ej. una bonificación de rendimiento)?	
A14	Adquisición, desarrollo y mantenimiento de los sistemas de información			
A14.1	Requisitos de seguridad en los sistemas de información			

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Cumple parcialmente	¿Existen políticas, procedimientos y registros relacionados al análisis de requisitos de seguridad para la adquisición de sistemas y software? ¿Existen procedimientos para analizar riesgos, requisitos funcionales y técnicos, arquitectura de seguridad, las pruebas de seguridad y la certificación de sistemas y desarrollo? ¿Son estos procedimientos obligatorios para todos los nuevos desarrollos y cambios en los sistemas existentes (ej. Actualizaciones de sistema operativo / aplicaciones en las actualizaciones, cambios de criptografía, etc.) ¿Se aplican estos controles para sistemas / software comercial, incluidos los productos "a medida" o personalizados?	
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Cumple parcialmente	¿La organización usa o proporciona aplicaciones web de comercio electrónico? ¿Se verifican los aspectos de seguridad como control de acceso y autenticación de usuarios, integridad de datos y la disponibilidad del servicio? ¿Contiene controles tales como validación de datos de entrada, validación de procesamiento, encriptación, autenticación de mensajes e irrenunciabilidad? ¿Se fuerza https? ¿Los sitios web públicos están siendo monitoreados (ej. eventos, vulnerabilidades, etc.)? ¿Se analizan y documentan las amenazas de forma rutinaria? ¿Existe una gestión de incidentes y cambios para tratarlos?	
A14.1.3	Protección de las transacciones de servicios de aplicaciones	Cumple parcialmente	Más allá de A.14.1.2 ¿Las transacciones se realizan y almacenan en un entorno interno seguro o expuesto a internet? ¿Se protege la información mediante el uso de protocolos seguros, cifrado, firma electrónica, etc.? ¿Cumplen con todos los requisitos legales, regulatorios y de cumplimiento?	
A14.2	Seguridad en el desarrollo y en los procesos de soporte			
A14.2.1	Política de desarrollo seguro	Cumple parcialmente	¿Existe una política de desarrollo seguro que abarque la arquitectura de seguridad? ¿Los entornos de desarrollo usan repositorios seguros con control de acceso, seguridad y control de cambios? ¿Los métodos de desarrollo incluyen pautas de programación segura? ¿Se capacita a los desarrolladores para que tengan el conocimiento adecuado acerca de las prácticas seguras de programación?	

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A14.2.2	Procedimiento de control de cambios en sistemas	Cumple parcialmente	¿Existen políticas, procedimientos y registros relacionados de la gestión de cambios? ¿Incluyen planificación y prueba de cambios, evaluaciones de impacto (incluido el riesgo de información y aspectos de seguridad, más los impactos de no cambiar), verificaciones de instalación y procedimientos de retroceso / reversión? ¿Incluye un procedimiento para cambios de emergencia? ¿Se aplica los cambios significativos en equipos informáticos y de telecomunicaciones? ¿Los cambios en el sistema están debidamente documentados, justificados y autorizados por la administración?	
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Cumple parcialmente	¿Se requiere una validación / evaluaciones de riesgo y, si es necesario, recertificación de sistemas tras actualizaciones / mantenimiento, parches, cambios sistema operativo, actualizaciones de aplicaciones y cambios de cifrado? ¿Hay registros de estas actividades?	
A14.2.4	Restricciones a los cambios en los paquetes de software	Cumple parcialmente	¿Se hacen cambios a paquetes software adquiridos? ¿Se verifica que los controles originales no han sido comprometidos? ¿Se obtuvo el consentimiento y la participación del proveedor? ¿El proveedor continúa dando soporte tras los cambios? ¿Se exploró la posibilidad de obtener actualizaciones de programas estándar por parte de los proveedores? ¿Se hace una comprobación de compatibilidad con otro software en uso?	
A14.2.5	Principios de ingeniería de sistemas seguros	Cumple parcialmente	¿Se siguen principios de SDLC que incluye controles de seguridad? ¿Se capacita a los desarrolladores para que tengan el conocimiento adecuado acerca de las prácticas seguras de programación?	
A14.2.6	Entorno de desarrollo seguro	Cumple	¿Se aíslan los entornos de desarrollo? ¿Cómo se desarrolla, prueba y lanza el software? ¿Quién es responsable de garantizar que el software nuevo / modificado no interrumpa otras operaciones? ¿Se realizan comprobaciones de antecedentes de los desarrolladores? ¿Tienen que cumplir con un NDA? ¿Cuáles son los reglamentos y los requisitos de cumplimiento que afectan el desarrollo? ¿Cómo se protegen los datos de prueba de la divulgación y dónde están almacenados?	
A14.2.7	Externalización del desarrollo de software	Cumple parcialmente	Más allá de A.14.2.6 ¿Se tienen en cuanta los siguientes aspectos cuando el desarrollo es lleva a cabo por un tercero? • Los acuerdos de licencia, la propiedad del código y los derechos de propiedad intelectual • Requisitos contractuales para prácticas seguras de diseño, desarrollo y prueba • Acceso al código fuente si el código ejecutable necesita ser modificado • Controles de prueba de seguridad de aplicaciones • Evaluación de vulnerabilidad y tratamiento	

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A14.2.8	Pruebas funcionales de seguridad de sistemas	Cumple parcialmente	Más allá de A.14.2.7 ¿Existe un procedimiento de pruebas y verificación para sistemas nuevos y actualizados? ¿Tiene en cuenta acuerdos de licencia, propiedad del código y propiedad intelectual?	
A14.2.9	Pruebas de aceptación de sistemas	Cumple parcialmente	¿Se efectúan pruebas de seguridad antes de la introducción de nuevos sistemas en la red? ¿Las pruebas replican situaciones y entornos operativos realistas? ¿Los defectos relacionados con la seguridad son tratados antes de que el producto sea certificado / aprobado? ¿Hay pruebas de aceptación del usuario (UAT) antes del lanzamiento al entorno operativo? ¿Se actualizan los controles de resiliencia y recuperación tras incidentes para reflejar los sistemas nuevos, modificados y retirados?	
A14.3	Datos de prueba			
A14.3.1	Protección de los datos de prueba	Cumple	¿Se utilizan mecanismos para proteger datos de prueba como la seudonimización, enmascaramiento, datos falsos, borrado, etc.? ¿Existe un mecanismo de verificación y aprobación para el uso de datos no protegidos para pruebas? ¿Existen registros de estas actividades?	
A15	Relación con proveedores			
A15.1	Seguridad en las relaciones con proveedores			
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	No cumple	¿Existen políticas, procesos, prácticas y registros relacionados con la gestión de relaciones con proveedores que involucran servicios de TI? ¿Incluyen servicios de nube, logística, servicios públicos, recursos humanos, médicos, financieros, legales y otros servicios subcontratados de alto riesgo? ¿Los contratos y acuerdos abordan lo siguiente? • Arreglos de gestión de relaciones, incluyendo el riesgo de la información y los aspectos de seguridad, la métrica, el rendimiento, problemas, rutas de escalada • Información / propiedad intelectual, y obligaciones / limitaciones derivadas • Rendición de cuentas y responsabilidades relacionadas con el riesgo y la seguridad de la información • Requisitos legales y normativos, como el cumplimiento certificado de ISO 27001 • Identificación de controles físicos y lógicos • Gestión de eventos, incidentes y desastres incluyendo evaluación, clasificación, priorización, notificación, escalado, gestión de respuesta y aspectos de continuidad del negocio • Habilitación de seguridad de los empleados y concienciación • Derecho de auditoría de seguridad por parte de la organización ¿Existe una obligación contractual de cumplimento? ¿Los proveedores de servicios externos son monitoreados rutinariamente y auditados para cumplir con los requisitos de seguridad?	

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A15.1.2	Requisitos de seguridad en contratos con terceros	No cumple	¿Los contratos o acuerdos formales con proveedores cubren lo siguiente? • Gestión de las relaciones, incluyendo riesgos • Cláusulas de confidencialidad vinculantes • Descripción de la información que se maneja y el método de acceder a dicha información • Estructura de la clasificación de la información a usar • La Inmediata notificación de incidentes de seguridad • Aspectos de continuidad del negocio • Subcontratación y restricciones en las relaciones con otros proveedores • Aspectos de personal y RRHH (ej. Rendimiento, antecedentes, "robo de empleados", etc.)	
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	No cumple	Más allá de A.15.1.1 y A.15.1.2 ¿Cómo se validan los requisitos de seguridad de los productos o servicios adquiridos? ¿Cómo se logra una capacidad de recuperación cuando productos o servicios críticos son suministrados por terceros? ¿Se puede rastrear el origen del producto o servicio?	
A15.2	Gestión de la provisión de servicios del proveedor			
A15.2.1	Control y revisión de la provisión de servicios del proveedor	No cumple	¿Existe una monitorización de servicios y quien responsable de esta actividad? ¿Se llevan a cabo reuniones de revisión del servicio, con qué frecuencia? ¿Se generan informes y / o métricas relacionadas a las reuniones y las decisiones tomadas? ¿Las reuniones abarcan riesgos, incidentes, políticas, cumplimiento e informes de auditoría? ¿Existen cláusulas de penalización o de bonificación en el contrato relacionadas con el riesgo de la información?	
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	No cumple	¿Cómo se comunican cambios en los servicios relacionados con la información, servicios adicionales o cambios en la forma en que se prestan los servicios contratados? ¿Cómo se comunican cambios en las políticas y requerimientos legales de la organización? ¿Se actualizan los acuerdos relacionados con los cambios?	
A16	Gestión de incidentes de seguridad de la información			
A16.1	Gestión de incidentes de seguridad de la información y mejoras			

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A16.1.1	Responsabilidades y procedimientos	Cumple parcialmente	¿Existen políticas, procedimientos e ITT´s para la gestión de incidentes? ¿Qué cubre? • I plan de respuesta a incidentes • Puntos de contacto para la notificación de incidentes, seguimiento y evaluación • Monitoreo, detección y reporte de eventos de seguridad • Asignación y escalado de incidentes (N1 > N2) incluyendo las respuestas de emergencia y la continuidad de negocio • Método de recolección de evidencias y pruebas forenses digitales • Revisión post-evento de seguridad y procesos de aprendizaje / mejora ¿Existen evidencias de la notificación de incidentes, registro, clasificación, asignación de resolución, la mitigación y la confirmación de cierre?	
A16.1.2	Notificación de los eventos de seguridad de la información	Cumple parcialmente	¿Cómo se informan los eventos de seguridad de la información? ¿Son conscientes los trabajadores de la necesidad de informar de inmediato y lo hacen? ¿Se crean informes de seguimiento de los incidentes? Desde la detección a la resolución. ¿Qué pasa con esos informes?	
A16.1.3	Notificación de puntos débiles de la seguridad	Cumple parcialmente	Más allá de A.16.1.2 ¿Existe una obligación contractual por parte de los empleados para reportar cualquier tipo de ocurrencia inusual? ¿Las políticas prohíben explícitamente a los trabajadores 'verificar', 'explorar', 'validar' o 'confirmar' vulnerabilidades a menos que estén expresamente autorizados para hacerlo?	
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	Cumple parcialmente	¿Qué tipos de eventos se espera que informen los empleados? ¿A quién informan? ¿Cómo se evalúan estos eventos para decidir si califican como incidentes? ¿Hay una escala de clasificación? ¿Hay un proceso de clasificación y / o escalamiento para priorizar los incidentes graves? ¿En qué se basa?	
A16.1.5	Respuesta a incidentes de seguridad de la información	Cumple parcialmente	¿Cómo se recolecta, almacena y evalúa la evidencia? ¿Hay una matriz de escalación para usar según sea necesario? ¿Hay medios para comunicar información de tales incidentes a las organizaciones internas y externas pertinentes? ¿Se documentan las acciones tomadas para resolver y finalmente cerrar un incidente?	
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	Cumple parcialmente	¿Existe un proceso de evaluación / investigación para identificar incidentes de impacto recurrentes? ¿Se aprovecha la información obtenida de la evaluación de incidentes para evitar recurrencias? Además, ¿Se está utilizado para formación y concienciación? ¿La organización cuenta con un proceso de gestión de incidentes relativamente maduro? ¿Se está aprendiendo de forma proactiva de incidentes, mejorando los conocimientos de riesgo y los controles de seguridad?	

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A16.1.7	Recopilación de evidencias	Cumple parcialmente	¿La recolección de evidencias de hace de forma competente en la empresa o por terceros especializados y capacitados en esta área? ¿Haya personal capacitado, competente y confiable con herramientas adecuadas y procesos definidos para el rol? (cadena de evidencia rigurosamente mantenida, evidencia asegurada en almacenamiento, herramientas y técnicas) ¿Quién decide emprender un análisis forense, y en qué criterio se base? ¿Existen obligaciones relacionadas con la jurisdicción, las diferentes normas forenses y los requisitos legales asociados?	
A17	Aspectos de seguridad de la información para la gestión de la continuidad de negocio			
A17.1	Continuidad de la seguridad de la información			
A17.1.1	Planificación de la continuidad de la seguridad de la información	Cumple parcialmente	¿Cómo se determinan los requisitos de continuidad del negocio? ¿Existe un plan de continuidad de negocio? ¿Existen un diseño adecuado de "alta disponibilidad" para sistemas de TI, redes y procesos críticos? ¿Se identifica el impacto potencial de los incidentes? ¿Se evalúan los planes de continuidad del negocio? ¿Se llevan a cabo ensayos de continuidad?	
A17.1.2	Implementar la continuidad de la seguridad de la información	Cumple parcialmente	¿Los planes tienen plazos definidos para restaurar servicios tras una interrupción? ¿Los planes tienen en cuenta la identificación y el acuerdo de responsabilidades, la identificación de pérdidas aceptables, la implementación de procedimientos de recuperación y restauración, la documentación de procedimientos y las pruebas regulares? ¿La planificación de la continuidad es consistente e identifica las prioridades de restauración? ¿Tienen los miembros de los equipos de recuperación / gestión de crisis / incidentes conocimiento de los planes y tienen claro sus roles y responsabilidades? ¿Los controles de seguridad son adecuados en los sitios de recuperación de desastres remotos?	
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Cumple parcialmente	¿Existe un método de pruebas del plan de continuidad? ¿Con qué frecuencia se llevan a cabo dichas pruebas? ¿Hay evidencia de las pruebas reales y sus resultados? ¿Se han identificado deficiencias?, ¿Se han remediado? y ¿Se han vuelto a probar hasta que los resultados sean satisfactorios?	
A17.2	Redundancias			
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	Cumple parcialmente	¿Cómo se identifican los requisitos de disponibilidad de servicios? ¿Se tienen en cuenta la capacidad de recuperación, la capacidad de rendimiento, el balanceo de carga? ¿Se tienen en cuenta servicios poco fiables, equipos, instalaciones, servidores, aplicaciones, enlaces, funciones, y la organización en sí? ¿Los controles clave de seguridad de la información están implementados y son funcionales en los sitios de recuperación de desastres?	

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A18	Cumplimiento			
A18.1	Cumplimiento de los requisitos legales y contractuales			
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Cumple parcialmente	¿Existe una política acerca del cumplimiento de requisitos legales? LOPD, GDPR, etc. ¿Se mantiene un registro o base de datos de cumplimiento enumerando todas las obligaciones, expectativas legales, reglamentarias y contractuales aplicables? ¿Hay una persona encargada de mantener, usar y controlar el registro? ¿Cómo se logra y se garantiza el cumplimiento? ¿Existen controles adecuados para cumplir con los requisitos?	
A18.1.2	Derechos de Propiedad Intelectual (DPI)	Cumple parcialmente	¿Existen políticas y procedimientos relativos a la adquisición, el uso y licencias de propiedad intelectual, gestión de licencias y cumplimiento?	
A18.1.3	Protección de los registros de la organización	Cumple parcialmente	¿Existe una política que contemple lo siguiente? Clasificación, categorización, períodos de retención y medios de almacenamiento permitidos. ¿Se almacenan las firmas digitales de forma segura? ¿Se contempla la posibilidad de destrucción, falsificación y acceso no autorizado? ¿Se verifica periódicamente la integridad de los registros? ¿Se utilizan medios de almacenamiento de larga duración para el almacenamiento a largo plazo?	
A18.1.4	Protección y privacidad de la información de carácter personal	No cumple	¿Hay un mecanismo para instruir al personal en el manejo de información de carácter personal? ¿Hay un responsable de privacidad en la organización? ¿Es el responsable conocedor de la información de carácter personal que es recopilado, procesado y almacenados por la organización? ¿Cuáles son los controles de acceso a información de carácter personal? ¿Cuál es el nivel de acceso y roles (de personal) que tienen acceso a estos activos?	
A18.1.5	Regulación de los controles criptográficos	No cumple	¿Existe una política que cubra actividades relacionadas con importación / exportación de material criptográfico? ¿Estas actividades cumplen con los requisitos legales y reglamentarios?	
A18.2	Revisiones de la seguridad de la información			
A18.2.1	Revisión independiente de la seguridad de la información	No cumple	¿Están las prioridades de implementación de controles alineadas con los riesgos a activos de información? ¿Los requisitos de auditoría de sistemas son cuidadosamente planificados, autorizados, implementados y controlados para minimizar los riesgos? ¿Están los objetivos y el alcance de auditoria autorizados por la gerencia? ¿Está adecuadamente controlado el acceso a las herramientas / software de auditoría del sistema de información? ¿Se documentan los hallazgos de auditoría y las actuaciones para solventarlos?	
A18.2.2	Cumplimiento de las políticas y normas de seguridad	No cumple	¿Cómo garantizar que todos los procedimientos de seguridad dentro de un área de responsabilidad se llevan a cabo correctamente? ¿Se hace una verificación periódica?	

Anexo A. (Continuación)

NÚMERO	CONTROL	ESTADO	PREGUNTAS	COMENTARIOS
A18.2.3	Comprobación del cumplimiento técnico	No cumple	¿Se llevan a cabo escaneos de vulnerabilidades de red y pruebas de Pentesting regulares? ¿Las pruebas son realizadas por profesionales debidamente cualificados, competentes y confiables? ¿Cómo informa, analiza y utilizan los resultados de dichas pruebas? ¿La prioridad de tratamiento se basa en un análisis de riesgos? ¿Hay evidencias de medidas tomadas para abordar los problemas identificados?	

Fuente: Autor basado en Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. (Consultado 23 de marzo de 2020) Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html