DISEÑO DE CONTROLES Y NORMAS DE SEGURIDAD PARA LA EMPRESA QWERTY S.A. QUE GARANTICEN LA PRESERVACIÓN DE LA INTEGRIDAD CONFIABILIDAD Y DISPONIBILIDAD DE LOS ACTIVOS INFORMATIVOS DE LA ORGANIZACIÓN.

JOHANA MARCELA GAITÁN LÓPEZ

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA "UNAD"

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

FUSAGASUGÁ

2020

DISEÑO DE CONTROLES Y NORMAS DE SEGURIDAD PARA LA EMPRESA QWERTY S.A. QUE GARANTICEN LA PRESERVACIÓN DE LA INTEGRIDAD CONFIABILIDAD Y DISPONIBILIDAD DE LOS ACTIVOS INFORMATIVOS DE LA ORGANIZACIÓN.

JOHANA MARCELA GAITÁN LÓPEZ

Proyecto Aplicado como requisito para optar al título de:

Especialista en Seguridad Informática

Director:

Ing. JOEL CARROLL VARGAS M. Sc

Tutor:

Ing. Martin Camilo Cancelado

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA "UNAD"

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

FUSAGASUGÁ

2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Fusagasugá, febrero 2020

DEDICATORIA

A Dios.

Por permitirme llegar hasta este nuevo logro, concederme gozar de buena salud para así lograr mis objetivos, y metas propuestas por iluminarme con su presencia, amor y bondad.

A mi Mama

Por su apoyo incondicional, amor y sus consejos, por la dedicación de motivarme constantemente de lograr lo que me propongo y los valores que me inculco ya que me han permitido ser una persona de bien.

A todas y cada una de las personas que de una u otra forma contribuyeron con mi proceso de aprendizaje.

AGRADECIMIENTOS

Le agradezco a Dios por permitirme culminar una meta más propuesta en mi vida y acompañarme este proceso, por darme la fuerza para continuar y terminar lo que como mucho esfuerzo inicie.

Agradezco a mis padres, esposo e hijos por apoyarme en todo momento; finalmente a mis profesores, tutores y compañeros por toda la confianza, apoyo y dedicación.

Contenido

Tabla de contenido Ilustraciones

Tabla de contenido de Tablas

Tabla de Anexos

GLOSARIO

Activos esenciales: se reconocen como activos esenciales a toda aquella información y equipos que son considerados vitales para el funcionamiento y continuidad de la organización.[1]

Amenaza: es un evento que puede causar daño a una persona o pérdidas materiales[2]

Análisis Cualitativo: se utiliza para clasificar aquellos aspectos los cuales no se dar un tipo de valoración por cantidad.

Análisis Cuantitativo: Este se utiliza con el fin de poder determinar un valor sobre algún activo, como el tipo de inversión que se puede realizar para llevar un análisis, el nivel de afectación que pueda tener una amenaza en un activo entre otros.

Confidencialidad: que la información solo sea accedida por el usuario autorizado.

Disponibilidad: La información esté alcance para el usuario cuando éste la necesite.

Hardware: se define como la parte física de un computador esta incluye los electrónicos subyacentes.

Incidente: se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información.[3]

Integridad: es la garantía de que la información no se encuentra alterada, manipulada por usuarios no autorizados.

Riesgo: este se mide asumiendo una determinada vulnerabilidad frente a cada tipo de peligro; se toma como la probabilidad de que se produzca algún tipo de evento que cause alguna vulnerabilidad que tenga consecuencias negativas

Salvaguarda: Acción genérica que puede producir un riesgo y el mecanismo de salvaguarda como el procedimiento que lo reduce.

---

[1] ISO/IEC 1335-1:204 Tecnología de la información –técnicas de seguridad – gestión de la seguridad en tecnologías de la información y comunicaciones parte 1: conceptos y modelos para la gestión de la seguridad en la tecnología de la información de las comunicaciones.

[2]ISO/IEC 27001. (2005). *Estándar Internacional ISO / IEC 27001*. *2005*, 41. https://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf.

[3] http://www.iso27000.es/sgsi.html

RESUMEN

En el presente trabajo se determinaron los parámetros para la aplicación de controles de seguridad para los activos informáticos y de la información para la Empresa QWERTY S. A.

Dichos controles se realizaron siguiendo la metodología MAGERIT y basados en la norma ISO/IEC 27001 los pasos que se siguieron fueron la definición del estado en el que se encontraba la empresa frente a la seguridad informática, identificación de los activos, comprobación de Riesgos, amenazas a los que estos podían estar expuestos y salvaguardas para de esta manera recomendar un plan de manejo.

Se definió la situación actual de la empresa, identificando los a activos con sus pertinentes amenazas, se procedió a realiza la comprobación de riesgos efectivos sugiriendo las protecciones necesarias las cuales forman parte del plan de implantación.

PALABRAS CLAVE

Amenaza: es un evento que puede causar daño a una persona o pérdidas materiales

Incidente: se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información.

Riesgo: este se mide asumiendo una determinada vulnerabilidad frente a cada tipo de peligro; se toma como la probabilidad de que se produzca algún tipo de evento que cause alguna vulnerabilidad que tenga consecuencias negativas[4]

Salvaguarda: Acción genérica que puede producir un riesgo y el mecanismo de salvaguarda como el procedimiento que lo reduce.

Vulnerabilidad: es cuando una persona o cosa es susceptible a un evento.

[4] Ballesteros, A. (30 de 04 de 2019). Seguridad. Obtenido de http://epn.gov.co/elearning/distinguidos/SEGURIDAD/13_riesgo_amenaza_y_vulnerabilid ad.html

ABSTRACT

In the current settled document, it has been determined the following parameters of security control protocol for computer assets and general information corresponding at the company QWERTY.

These previously mentioned were developed following the MAGERIT methodology and based on ISO / IEC 27001 standards, steps followed for completion have taken into account such as identified current status of the actives, general information safety of the company, appraisal of risks that perhaps the company could have been exposed and safeguard for the proper advice of management plan.

Keywords

Threat: is a phenomenon, substance, human activity or dangerous condition that can cause death, injury or other health impacts, as well as damage to property, loss of livelihoods and services, social and economic disruption, or environmental damage.

Incident: is defined as access, attempt to access, use, disclosure, modification or unauthorized destruction of information.

Safeguard: Generic action that can produce a risk and the safeguard mechanism as the procedure that reduces it.

Vulnerability: are the characteristics and circumstances of a community, system or good that make them susceptible to the harmful effects of a threat.

1. INTRODUCCIÓN

Se debe tener en cuenta que en el ámbito laboral los riesgos informáticos siempre estarán presentes y que estos pueden no solo causar pérdidas económicas en la empresa si no también problemas legales si no son controlados a tiempo y de una forma correcta. Por lo que se hace necesario que las personas y las empresas se tengan que adaptar a este tipo de situaciones y buscar opciones que permitan custodiar de una manera adecuada y segura la información.

La Empresa QWERTY S.A. es una empresa del sector tecnológico que busca el desarrollo Tecnológico en comunidades colombianas a través del uso de tecnologías de información. Debido al volumen de inventario y de clientes externos y colaboradores internos que hacen uso de estas tecnologías se hace necesario la implementación de normas y controles de seguridad para la protección de los activos informáticos.

En el presente trabajo se dio contexto al planteamiento de normas y acciones de seguridad para la protección de los activos informáticos de QWERTY S. A se tomó como referencia los conceptos relacionados con normas y estándares de seguridad, metodologías y herramientas que permitan mitigar y prevenir las consecuencias antes las amenazas.

El proteger la información e implementar controles y normas de seguridad en los activos informáticos debe ser uno de los objetivos planteados por la organización siendo esta un elemento fundamental para la empresa; por este motivo, se ve la necesidad de desarrollar un análisis de los riesgos tecnológicos a los que está expuesta; el cual se llevó a cabo en la empresa QWERTY S. A para de esta manera lograr mantener respaldada la información confidencial de forma segura por lo que se propuso crear un plan de gestión de riesgos para garantizar la continuidad y el logro de la metas y objetivos del negocio.

Debido al volumen de inventario y de clientes externos y de los colaboradores de la organización que hacen uso de sus servicios se recomiendo la implementación de SGSI para el área de informática basándose en la norma ISO/IEC 27001.[5]

[5] LÓPEZ, NEIRA Agustín. & RUIZ, SPOHR Javier. (2020). SGSI Información fundamental sobre el significado y sentido de implantación y mantenimiento de los Sistemas de Gestión de la Seguridad de la Información. 2020, Agosto, de ISO27000.ES Recuperado de https://www.iso27000.es/sgsi.html

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Diseñar un sistema de gestión de seguridad de la información bajo la norma ISO/IEC para el área de informática de la empresa QWERY S.A. que permita establecer normas y procesos de seguridad con el fin de evitar que la información esté en riesgo ante un posible ataque

2.2 OBJETIVOS ESPECÍFICOS

- Identificar los principales inconvenientes de seguridad que presente la empresa.
- Establecer indicadores de gestión para la verificación de seguridad de activos informáticos.
- Plantear un SGSI para el área de informática bajo la norma ISO/IEC 27001 con el fin de poder impartir las mejores prácticas para la empresa QWERTY S. A
- Definir la Aplicabilidad de las metas de la organización con el software (SoA) la cual permitirá llevar el control de las medidas a implementar.

3. PLANTEAMIENTO DEL PROBLEMA

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

QWERY S.A. no tiene implementado un sistema de seguridad biométrico que permita tener control de ingreso y salida de los empleados dentro de estos controles se podría implementar el control por medio de la identificación del uso de las huellas dactilares ya que tiene una efectividad del 99.9%; de igual manera no implementa un monitoreo de entrada y salida de los clientes como el uso de tarjetas con banda magnética que permita autorizar el ingreso a las instalaciones de los clientes y llevar un control de salida de los mismos.

• Los servidores donde se alojan los servicios que albergan los protocolos DHCP, HTTP y la central telefónica de la empresa no se encuentran en un espacio acondicionado para su buen funcionamiento.

• La red de comunicaciones se encuentra configurada en el mismo segmento de red por lo que no se puede garantizar en buen funcionamiento de la misma ya que se generan cuellos de botella debido a la gran demanda de tráfico de red.

• Los equipos de cómputo tienen instalado un sistema de antivirus actualizado, pero dentro de las verificaciones realizadas se evidencia que a estos no se les realiza seguimiento por lo que no se puede garantizar que estén actualizadas y configuradas para brindar la protección que se necesita.

• Debido a que en la oficina de nómina y facturación se atiende una gran de clientes se hace necesario que el ingreso de la información muchas veces sea realizado por personal que se encuentra en capacitación lo que genera un riesgo ya que no se puede garantizar que la información ingresada conserve la integridad y confiabilidad, así como que no haya fuga de información.

• La empresa tiene dentro de sus activos informáticos un firewall Cisco ASA 5505, el cual no cuenta con reglas implementadas para la autorización o denegación de conexiones o transmisión de datos.[6]

Tomando como referencia el método MAGERIT[7] para el desarrollo de esta metodología lo primero que se hizo fue investigar el estado actual de la organización, indagando sobre los procesos, activos informáticos y de esta forma poder identificar los riesgos y vulnerabilidades a los que estaban expuestos los activos; para poder determinar el nivel de riesgos existentes y de esta forma recomendar medidas de seguridad necesarias que podrían formar parte del plan de seguridad de la información.

Para el desarrollo del análisis de riesgo se utilizó a herramienta PILAR[8] la cual sigue la metodología Magerit está, soporta el análisis y gestión de los riesgos de sistemas de información. Así mismo también se hizo uso de herramientas de código libre como: DVWA[9] , Logwatch[10], Nessus[11] Sqlmap[12] y WebScarab[13]

---

[6] https://www.cisco.com/c/en/us/support/security/asa-5505-adaptive-security-appliance/model.html

[7] M. AMUTIO, J. C. (2012.). Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libros I, II y III - . Madrid, España : Eds., MAGERIT.

[8] TOOLS, P. (02 de 02 de 2020). EAR / PILAR. Obtenido de https://www.ar-tools.com/es/index.html

[9] DVWA. (06 de 02 de 2020). Obtenido de http://www.dvwa.co.uk/

[10] Tezer, P. O. (23 de 11 de 2017). Cómo instalar y usar Logwatch Log Analyzer and Reporter en un VPS. Obtenido de https://www.digitalocean.com/community/tutorials/how-to-install-and-use-logwatch-log-analyzer-and-reporter-on-a-vps

[11] Tenable. (02 de 02 de 2020). Nessus. Obtenido de https://www.tenable.com/downloads/nessus

[12] Bernardo Damele AG, M. S. (02 de 02 de 2020). SQLmap Herramienta automática de inyección de SQL y toma de base de datos. Obtenido de http://sqlmap.org/

[13] https://webscarab.apponic.com/

3.1 DEFINICIÓN DEL PROBLEMA

El estado actual en el que se encuentra la empresa QWERTY S.A. es crucial debido a la complejidad del negocio y de los procesos que se deben realizar se evidencia que no cuentan con normas de seguridad definidas; dejando una grave brecha de seguridad, no solo poniendo en riesgo la seguridad física de sus activos sino también de la información que allí se guarda. No se evidencia un control de mantenimiento ni inventario de los equipos.

La empresa no cuenta con un sistema de seguridad biométrico el cual permita llevar un control del ingreso y salida de los colaboradores internos y externos de la organización por lo que no se puede garantizar la seguridad tanto de la planta física como de la información.

No se lleva un control adecuado de las personas que pueden acceder y manipular los activos informáticos por lo tanto se corre el riesgo de que estos equipos sean manipulados y alterada la información que allí contienen.

De igual forma la red no está segmentada por lo que cualquier persona que se conecte a la red de WIFI puede acceder a equipos e información sensible.
Teniendo en cuenta que el software de los equipos esta desactualizado y se hace evidente que los mismo deben ser cambiados por tecnología más nueva; para facilitar las actualizaciones a las últimas versiones de los sistemas operativos y de la misma forma garantizar el buen funcionamiento de los mismos y aplicar las correspondientes salvaguardas QWERTY S.A.

La empresa no cuenta con un diagrama donde se pueda verificar que el cableado cumple las normas mínimas de seguridad; el sistema eléctrico no cuenta con una adecuada canalización y no tienen definida la asignación de puntos de acceso a la red y tomas de la corriente por lo que se considera que no tiene establecidos

estándares de políticas de control como ITILL[14] la cual ayuda a establecer lineamientos para el control, identificación de fallas en los procesos con el fin de mejorar la eficiencia en los mismos y aplicar la mejora continua.

Al igual que otros marcos de administración de TI como COBIT[15] la cual sirve como marco de referencia para implementar las mejores prácticas y estándares en áreas de la organización donde se necesiten mejoras o reformulaciones.

La organización no puede garantizar que los procesos y la información conserve su integridad y esta no se manipulada ya que debido al alto flujo de información que se maneja en la oficina de nómina y facturación muchas veces con practicantes quienes ayudan en este proceso.

Es por esto es recomendable que la empresa QWERTY S. A diseñe un sistema de seguridad de la información que contenga políticas claras sobre el uso y manipulación de los activos informáticos de la empresa.

3.2. FORMULACIÓN DEL PROBLEMA.

La seguridad de la información es un activo esencial para las personas y las organizaciones convirtiéndose esta en un objetivo para los delincuentes ¿**de qué manera se puede proteger la infraestructura y la información de la Empresa QWERTY S. A; es factible que el diseño de controles de seguridad basándose en la norma ISO 27001 sirva para implementar controles que mitiguen y ayuden a reducir los riesgos a los activos informáticos de la empresa**?

[14] E magíster ¿Qué es ITIL, para qué sirve y qué tipos de certificados existen? 27 de 09 de 2019. https://www.emagister.com/ (último acceso: 30 de 03 de 2020).
[15] White, Sarah K. ¿Qué es COBIT? Un marco para la alineación y la gobernanza. 12 de 27 de 2017. https://www.networkworld.es/archive/que-es-cobit-un-marco-para-la-alineacion-y-la-gobernanza (último acceso: 30 de 03 de 2020).

3.3 JUSTIFICACIÓN

Salvaguardar la información de una organización consiste en buscar herramientas que permitan evitar ataques, lo que hace que sea necesario proteger por todos los medios por los que se tenga acceso a la información de la empresa debido a que en los últimos años el incremento del uso de la tecnología e internet va en aumento, así como también la invención de nuevas amenazas.

La empresa QWERTY S.A. es una empresa tecnológica que quiere incursionar en el país pero debido a la cantidad de inventario y de usuarios que se benefician de sus servicio se hace necesario la implementación de un sistema de seguridad de la información cuyo fin es “garantizar que los riesgos de la seguridad de la información sean Identificados, aceptados, manejados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías”. [16]

Ya que es una empresa reconocida en el mercado; esta busca mejorar sus procesos diseñando un el sistema de Seguridad de la información con el fin de optimizar procesos, estableciendo normas de seguridad y de estar forma no solo proteger su infraestructura tecnológica sino también la información.

[16] Isotools.org. (2020). La norma ISO 27001 Aspectos clave de su diseño e implantación. 2020, Agosto, de ISOTools excellence Recuperado de https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

4. MARCO CONCEPTUAL Y TEÓRICO

4.1 Marco de Referencia.

Continuamente surgen reportes en el sector de la seguridad informática y organizaciones encargadas de la seguridad TI, donde se evidencia el incremento del porcentaje de ataques cibernéticos a las organizaciones;

Es muy común apreciar en las noticias que aparecen nuevas amenazas para los sitios web y las aplicaciones en Internet las cuales fueron creadas con el fin de facilitar la investigación y realizar negocios.

Teniendo en cuenta que hoy en día en gran parte las empresas ofrecen y comercializan sus productos en sitios WEB o en aplicaciones basadas en el mismo los riesgos aún son mucho más grandes ya que los delincuentes están al asecho para poder cometer delitos como; ataques con software dañinos como virus, ransomware, phishing; estos tipos de ataques se convierten en principales herramientas para cometer delitos contra la seguridad de la información.

Los riesgos que implican para la privacidad y seguridad a los que están expuestas las personas y las organizaciones crecen exponencialmente al mismo tiempo que la tecnología va avanzando; teniendo presente que este tipo de delitos no se centran solo en organizaciones grandes si no que pueden afectar a todas aquellas que dependan de aplicaciones y sistemas conectados a una red.

Según el informe de “Kaspersky que señala que durante los últimos 12 meses se registraron a diario más de 746.000 infecciones con malware en Latinoamérica” representando una cifra preocupante para las organizaciones que en su gran mayoría son entidades bancarias, por ejemplo, a mediados del 2018 una banda de hackers atacó al Banco de Chile logrando cometer un robo de cerca de 10 millones de dólares.

Este delito fue cometido por medio de un virus el cual obligo a la entidad financiera afectada a desconectar 9 mil estaciones de trabajo en sus sucursales para detener la propagación de un virus, lo cual no fue suficiente ya que este virus fue una distracción para que los delincuentes hicieran incógnitamente transacciones a otras entidades bancarias por grandes sumas de dinero las cuales en su gran mayoría fueron a parar en Hong Kong.

El experto en ciberseguridad de SecPro David Pereira señala que el incremento en el nivel de ciberataques es debido que los delincuentes ya no solo buscan reconocimiento de sus capacidades si no que su fin primordial es lucrasen por lo que las organizaciones no están a salvo y son estas las que se convierten en su principal objetivo.[17]

También se debe tener en cuenta que hoy en día cualquier individuo con acceso a internet y un computador y que posea un mínimo de conocimientos también puede cometer el delito; es por esto que se hace necesario diseñar un sistema de Seguridad de la información para la empresa QWERTY S.A.

Hay que tener en cuenta que en cuestión de seguridad Colombia a diferencia de otros países no esta tan mal según un balance sobre seguridad realizado por Comparitech[18]; plataforma que se especializa en servicios tecnológicos manifiesta en su informe Colombia cuenta con mejor seguridad que países como México, Italia, Grecia y Portugal; para realizar este informe se centraron en siete categorías entre las que se destacan dispositivos móviles infectados con algún tipo de virus.

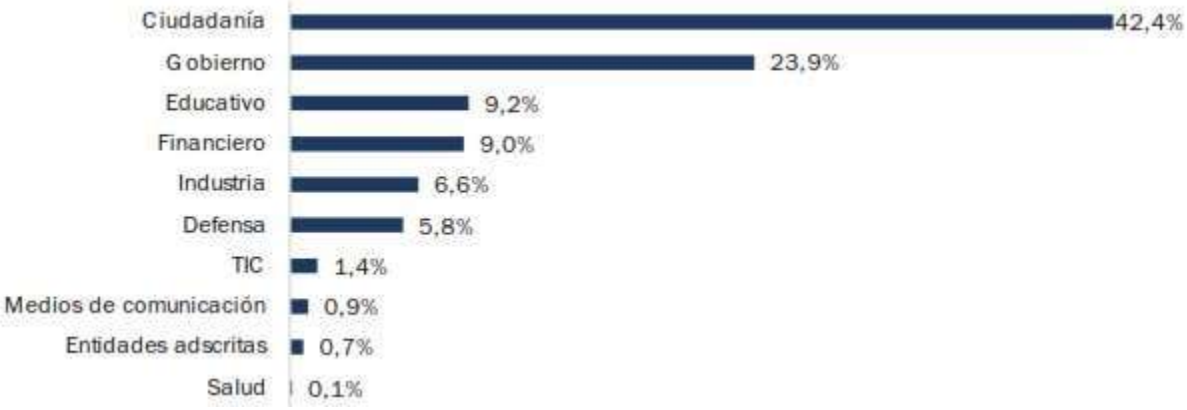
Fortinet, una empresa de **ciberseguridad mundial**, realizo un estudio donde encontró que más del 80% de las organizaciones del país poseen software

[17] TECNÓSFERA. (15 de 08 de 2018). En un segundo se presentan en promedio 9 infecciones con malware. Obtenido de https://www.eltiempo.com/tecnosfera/novedades-tecnologia/aumento-de-ataques-ciberneticos-en-america-latina-en-2018-256078

[18] Profitline. «Actualmente Como se encuentra Colombia en Seguridad Informática.» 26 de 02 de 2019. https://profitline.com.co/actualmente-como-se-encuentra-colombia-en-seguridad-informatica/.

altamente vulnerable, por, lo que recomienda la implementación de plataformas que puedan asegurar la integridad no solo de la información, sino también de la infraestructura digital y de los activos físicos.[19]

Ilustración 1 incidentes digitales en el año 2015 en Colombia



Fuente: colCERT, 2015.

La empresa **Eset**, en una encuesta que realizo a las empresas descubrió que si bien es cierto que hay brechas de seguridad las empresas hoy están haciendo más inversión a software de seguridad.

Las organizaciones ya no solo se centran en proteger su infraestructura física si no también están adoptando medidas de seguridad para proteger la información.

Según el estudio realizado por ESET finalizando el tercer trimestre del año 2016 las tendencias sobre las amenazas de seguridad informática se caracterizan porque su objetivo se centra en apoderarse de sistemas informáticos y bases de datos mediante ataques como el de ransomware; denegación al acceso a datos y sistemas e infectar dispositivos que forman parte de la Internet de las Cosas.[20]

[19] FORTINET. (11 de 2018). Más del 80 por ciento de las compañías en Colombia son vulnerables a ataques informáticos. Recuperado el 10 de 10 de 2019, de https://www.gartner.com/teamsiteanalytics/servePDF?g=/imagesrv/media-products/pdf/fortinet/fortinet-1-5VG5OU4.pdf

[20] tecnology, enjoy safer. «LA SEGURIDAD COMO REHEN TENDENCIAS 2017.» 2017. https://www.welivesecurity.com/wp-content/uploads/2016/12/Tendencias-2017-eset

También debemos tener en cuenta que según las encuestas de Seguridad de la información para las organizaciones para el año 2018 Solo el 15% de las organizaciones manifestaron que cumplen parcialmente las expectativas en temas de seguridad, en su gran mayoría no se atreven a incluir en sus informes incidentes de seguridad.

Las empresas pequeñas con un porcentaje del 23 % no consideran necesario rendir informe Cerca de 4 de 10 compañías orientadas al consumidor (42%) cuenta con un centro de operaciones de seguridad.[21]

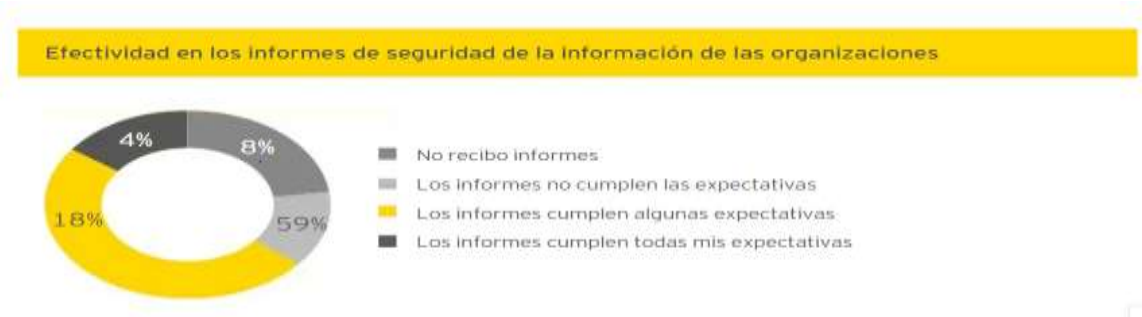
El desafío que tienen hoy en día las empresas lograr avanzar en tres aspectos:

• **Proteger a la empresa**. Para poder proteger la empresa se debe realizar una identificación plena de los activos para poder crear líneas de defensa.

• **Optimizar la ciberseguridad**. Buscar herramientas que permitan optimizar recursos y realizar inversión de tecnologías innovadoras para mejorar la protección ya existente.

• **Impulsar el crecimiento**. Los objetivos de la organización deben ir enfocados al crecimiento de la seguridad de los activos informáticos.

Ilustración 2 Capacidades e incidentes de Seguridad



Fuente: Encuesta-Global-Seguridad-Informacion-2018-19. PDF P-38

[21] INGENIEROS, ACIS ESCUELA DE. «Encuesta-Global-Seguridad-Informacion-2018-19.» 19 de 02 de 2020. https://es.scribd.com/document/423161641/Ey-Encuesta-Global-Seguridad-Informacion-2018-19.

4.2 MARCO CONCEPTUAL

Empresa: es una institución con fines lucrativos donde se pueden desarrollar diferentes actividades, ya sea prestando un servicio o comercializando un producto.

ISO 27001: se considera como la guía donde se pueden encontrar directrices para una buena gestión de la información.

MAGERIT: metodología para análisis de riesgos de una empresa.

Riesgo: este se mide asumiendo una determinada vulnerabilidad frente a cada tipo de peligro; se toma como la probabilidad de que se produzca algún tipo de evento que cause alguna vulnerabilidad que tenga consecuencias negativas.[22]

Amenaza: es un fenómeno, sustancia, actividad humana o condición peligrosa que puede ocasionar la muerte, lesiones u otros impactos a la salud, al igual que daños a la propiedad, la pérdida de medios de sustento y de servicios, trastornos sociales y económicos, o daños ambientales.

Vulnerabilidad: son las características y las circunstancias de una comunidad, sistema o bien que los hacen susceptibles a los efectos dañinos de una amenaza.

Incidente: se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información.[23]

Salvaguarda: Acción genérica que puede producir un riesgo y el mecanismo de salvaguarda como el procedimiento que lo reduce. [24]

Análisis: es el proceso de verificar detalladamente**,** procesos, acciones, etc.

Software: Programa que realiza unas tareas específicas en la empresa.

---

[22] BALLESTEROS, A. (30 de 04 de 2019). Seguridad. Obtenido de http://epn.gov.co/elearning/distinguidos/SEGURIDAD/13_riesgo_amenaza_y_vulnerabilid ad.html

[23] LUJAN, U. N. (30 de 04 de 2019). Incidente informático. Obtenido de http://www.unlu.edu.ar/doc/seginfo/Como_reportar_un_incidente_de_SI

[24] Gestión, S. e. (27 de 04 de 2015). ISO 27001: Funciones y mecanismos de salvaguarda. Obtenido de https://www.pmg-ssi.com/2015/04/iso-27001-funciones-y-mecanismos-desalvaguarda/

SGSI el Sistema de gestión de la seguridad de la información es una guía que permite la integración con todos los procesos que se desarrollan en la organización con el fin de asegurar que se conserve la confidencialidad, integridad y disponibilidad; adaptándose a los objetivos planteados por la organización.

4.3 MARCO LEGAL

En Colombia el cometer delitos informáticos están contemplados bajo la ley 1273, del 2009 denominada “de la protección de la información y de los datos”.

Algunos escritores como Julio Téllez-Valdés (2007), en su libro Derecho Informático, manifiesta que para él; “delito informático está definido desde el punto de vista y conducta en la que el individuo reproduce la acción utilizando las computadoras como instrumento o fin para cometer el ilícito definiéndolo desde un punto de vista típico y atípico lo define como como la utilidad que el atacante le va a dar muy diferente a la persona que posee el activo.[25]

El autor Davara Rodríguez define el delito informático como: “la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevado a cabo utilizando un elemento informático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.”[26]

Para Carlos Sarzana, en su obra Criminalista e tecnología, los crímenes que son perpetrados por medio de una computadora implican cualquier comportamiento que conlleve a cometer el delito en el cual la computadora ha estado involucrada como herramienta para cometerlo[27]

20 V. J. Tellez, «Derecho Informatico,» de *Derecho Informatico* , Mexico , McGrawHill, 1996, p. 281.

[26] Davara Rodríguez, M: A (2015). Manual de Derecho Informático. Pamplona España: Aranzadi

[27] Criminalità E Tecnología En Computers Crime. Rassagna Penitenziaria E Criminología. Nos. 1-2. Año 1. 1979. Roma, Italia. P.53

Como Podemos concluir para estos escritores todo delito informático es aquella manipulación, modificación o alteración de la información contenida en un medio informático; por lo que tanto para Colombia como a nivel mundial surge la necesidad de modificar las leyes y crear una normatividad que pueda regular los delitos según su área y clasificación.

En el año 2009 el legislativo Colombiano modifico el código penal y agrego varios artículos para tipificar los delitos informáticos, este se denominó "De la protección de la información y de los datos", esta normatividad se centra en sancionar a aquella persona o personas que por medio de un computador atente contra las Tecnologías; se determinó que se sancionaría con multas hasta de 1500 salarios mínimos mensuales legales vigentes y penas de prisión de hasta 120 meses.

4.4 Marco Teórico:

Para poder abordar el tema primero debemos saber los conceptos de:

Que es la seguridad de la información: esta es la ejecución y uso de mecanismos (acciones a realizar, como copias de seguridad) que garanticen los tres pilares de la seguridad:

1. **Disponibilidad:** La información esté alcance para el usuario cuando éste la necesite.

2. Confidencialidad: que la información solo sea accedida por el usuario autorizado.

3. Integridad: es la garantía de que la información no se encuentra alterada, manipulada por usuarios no autorizados.[28]

Es decir, que la información se conserve en su estado original para poder cumplir esto se debe fijar políticas que permitan custodiar los activos de la información algunas de estas políticas son:

- Orientar a los colaboradores sobre el uso adecuado de los recursos informáticos

[28] AEC.ES. (03 de 02 de 2020). SEGURIDAD DE LA INFORMACIÓN. Obtenido de https://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

con los que cuenta la empresa.

- Definir las bases para la ejecución de un sistema de seguridad de la información
- Definir su alcance, quienes pueden acceder a este tipo de información.
- Definir metodologías a aplicar.
- Definir el alcance que este va a tener dentro de la empresa entre otras.

4.4.1 ¿Qué es un SGSI y para qué sirve?

"Esta es la sigla que se utilizada para referirse a el sistema de seguridad de la información cuya finalidad es ayudar a establecer políticas y procedimientos en relación a los objetivos y misión de la de la organización, y de esta forma evitar que el nivel de exposición de riesgo a las amenazas y malas prácticas sea menor" [29]

4.4.2 Que compone un SGSI

Ilustración 2 Componentes SGSI

Fuente: www.ISO27000.es P-4

En el primer nivel I tenemos:

Manual de seguridad: en este documento se expone y determina las intenciones,

[29] Alessa, A. (09 de 06 de 2017). SGSI. Obtenido de https://es.slideshare.net/AlessaParedes/sgsi-76786549

el tipo de alcance del manual de seguridad, objetivos, funciones, normas y directrices principales del SGSI.

Nivel 2

Procedimientos: son los documentos que tienen las directrices las cuales garantizan que se realicen de una manera segura la organización y el control de los procesos de seguridad de la información.

Nivel 3

Instrucciones, checklists y formularios: en estos documentos estará plasmado las tareas y las actividades que se llevaran a cabo para asegurar la protección de la información.

Nivel 4

Registros: es la Evidencia la cual queda plasmada en un documento de que la organización si está llevando a cabo la implementación de las normas del SGSI.

En estos de debe especificar el tipo de alcance del SGSI: a que áreas de la organización se va a aplicar y que funciones se van a realizar por cada dependencia.

También deben estar definidos las políticas y objetivos, procedimientos y un informe detallado de riesgos producto de la investigación previa dentro de la empresa.

Por último, el plan de tratamiento de riesgos: este documento define los procedimientos a seguir de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información.

De igual manera deben quedar en archivos todas las documentaciones esto como soporte y evidencia en caso de que se necesite dicha información como soporte o guía para mejorar o aplicar algún tipo de correctivo.[30]

4.4.3 Para qué sirve la implementación del SGSI

El Sistema de Gestión de la Seguridad de la Información (SGSI) sirve como guía para poder definir y establecer políticas orientadas a los procedimientos realizados a los procesos en las organizaciones su finalidad es ayudar a preservar y cumplir los objetivos y metas planteados por la organización.

[30] 27000, I. (02 de 02 de 2020). Sistema de Gestión de la Seguridad de la Información . Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf

Pasos a seguir para su implementación.

• **Plan (planificar):** establecer el SGSI. En este paso es donde se define las políticas, la metodología y el alcance que este va a tener dentro de la organización, de igual manera se realiza la identificación de los activos de la organización y cuáles de estos pueden estar sujetos a riesgos para de esta buscar mitigar los riesgos.

• **Do (hacer):** implementar y utilizar el SGSI. En este punto se debe definir un plan para el tratamiento de los riesgos encontrados y las acciones a implementar con el fin de mitigarlos

• **Check (verificar):** monitorizar y revisar el SGSI. Se realizan procedimientos de verificación y monitorización para identificar y detectar brechas e incidentes de seguridad.

• **Act (actuar):** mantener y mejorar el SGSI. En este punto como tal y ya con los datos arrojados por la investigación previa se procede a implementar el SGSI realizando como tal las acciones correctivas y preventivas en las áreas a asegurar con el fin de ayudar a la consecución de los objetivos planteados por la organización.

4.5 Marco Contextual:

La siguiente investigación se realizará a la empresa **QWERTY S. A** Que tiene como proyecto incursionar en el desarrollo tecnológico de las comunidades colombianas; este tendrá una duración de 4 meses comprendidos en el primer semestre del año 2019. [31]

4.5.1 El Alcance de este será de mejorar la calidad en la prestación del servicio tanto para el cliente interno y externo aplicando un manual de **SGSI** a los procesos, recursos informáticos y tecnológicos con los que cuenta en el área de informática de la empresa **QWERTY S.A** esto con el fin de iniciar adecuadamente la seguridad

[31] Informaticas, O. p. (s.f.). METODOLOGIA PARA LA GESTION DE LA SEGURIDAD INFORMATICA. Obtenido de https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf

de la información su alcance estará destinado a cada Departamento y empleado de la empresa.[32]

4.5.2 QWERTY S.A

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

Para dar soporte tecnológico, la empresa tiene un Departamento de sistemas que se encarga de brindar soporte a toda la infraestructura tecnológica.

En la dependencia de sistemas de la empresa de la organización se tienen tres áreas de trabajo y cada uno con diferentes funciones de acuerdo con el grupo en el cual se cumplen diferentes funciones para proporcionar a los usuarios de la compañía los diferentes servicios de las TI de la empresa.

Ilustración 3 Dependencias

Fuente: Propia

[32] LIZARAZO, L. K. (27 de 08 de 2016). PLANTEAMIENTO DE UN SGSI BASADO EN LA NORMA ISO 27001:. Obtenido de http://polux.unipiloto.edu.co:8080/00003412.pdf

La empresa cuenta con un servicio de internet de 25 Mb para el desarrollo de sus actividades diarias, Para dar respuesta a este requerimiento tecnológico, cuenta con una dependencia de sistemas que brinda soporte a la infraestructura tecnológica 24/7.

Para tener diferentes activos de la información como servidores, impresoras, servidor de archivos –como servicio– firewall, Access point, página web –como servicio– DHCP, software de facturación, equipos de cómputo de usuario final, equipos para gestión del desarrollo tecnológico, puntos de acceso (Hub), Switches, personal técnico de mantenimiento y telefonía IP.

No se evidencia la empresa no tiene sistema de seguridad para el registro de los usuarios que permita verificar y controlar el ingreso y egreso de los clientes tanto internos como externos.

4.5.3 FUNCIONES POR ÁREA

Dentro del análisis que se realizó a la empresa QWERTY S.A esta distribuye las funciones por dependencias Así:

Tabla 1 Funciones por Dependencias

Área de Infraestructura	Se encarga de brinda soporte a la Red de acceso, así como de verificar los diseños de cableado estructurado.
Área de desarrollo	Se encarga de brindar apoyo técnico a las diferentes dependencias de la empresa, así como de Capacitación en el uso de las tecnologías de la informática y telecomunicaciones.

Área de Soporte	La encargada de realizar el mantenimiento y soporte técnico a los computadores que son propiedad de la empresa. Generación de conceptos técnicos de aquellos activos que no se encuentran en óptimas condiciones para su uso. Realiza copias de seguridad de los sistemas de información, bases de datos de las diferentes áreas.

Fuente: Propia

Esta Área no solamente se encarga de las funciones ya definidas, sino que además brinda asistencia para directivos Administrativos y operativos:

Dentro de las funciones que se llevan a cabo esta el apoyar el servicio de correo electrónico institucional garantizando la comunicación efectiva entre los miembros de la entidad, recibir y transferir archivos, así como de llevar acabo las propuestas académicas del programa.

Apoya la gestión y el mantenimiento de los equipos de cómputo de escritorio, móviles, servidores, televisores, softwares operativos y de aplicaciones.

También se encargan de garantizar el servicio de internet. En el anexo C se puede evidenciar el cargo y funciones del Área Informática.

4.5.4 MARCO LEGAL

- **ISO 27000** da las definiciones y los términos estándar para el Sistema de Gestión de Seguridad de la Información. Da la definición y explica el alcance de las demás normas de la familia 27000[33].
- **ISO 27001** indica cuales son los requisitos mínimos que debe tener un SGSI

[33] 27000.es, W. (15 de 03 de 2019). Sistema de Gestión de la Seguridad de la. Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf

para que funcione en una organización. Actualmente es una certificación adoptada por las áreas de TI para garantizar que el activo más importante de la organización se encuentra protegido. [34]

- **LEY 603 DE 2000 "**Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.[35]
- **LEY ESTATUTARIA 1266 DEL 31 DE DICIEMBRE DE 2008** "Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones". [36]
- **LEY 1273 DEL 5 DE ENERO DE 2009** "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".[37]

  LEY 1341 DEL 30 DE JULIO DE 2009

  "Por la cual se definen los principios y conceptos sobre la sociedad de la

---

[34] Excellence, I. (07 de 03 de 2014). ISO 27001 Como implantar políticas de Gestión de un Sistema de Gestión de Seguridad de la Información. Obtenido de https://www.pmg-ssi.com/2014/03/iso-27001-chttps://www.pmg-ssi.com/2014/03/iso-27001-como-implantar-politicas-de-gestion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/

[35] Colombia, E. C. (27 de 07 de 2000). LEY 603 DE 2000. Obtenido de http://derechodeautor.gov.co/documents/10181/182597/603.pdf/42c15f4a-afe5-4339-97ca-a61026450307

[36] ALA/CFT, S. N. (31 de 12 de 2008). Ley Estatutaria 1266 de 2008. Obtenido de https://www.uiaf.gov.co/sistema_nacional_ala_cft/normatividad_sistema/leyes/ley_estatutaria_1266_2008

[37] Colombia, C. d. (05 de 01 de 2009). Ley de Delitos Informáticos en Colombia. Obtenido de https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones".[38]

- **LEY ESTATUTARIA 1581 DE 2012**

  "Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional".[39]

  toda entidad pública o privada, tendrá un de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer las normas adecuados; le brindará al usuario la posibilidad de presentar peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

  Aspectos claves de la normatividad:

1. Cualquier ciudadano tendrá la posibilidad de acceder a su información personal y solicitar la supresión o corrección de la misma frente a toda base de datos en que se encuentre registrado.
2. Establece los principios que deben ser obligatoriamente observados por quienes hagan uso, de alguna manera realicen el tratamiento o mantengan una base de datos con información personal, cualquiera que sea su finalidad.
3. Aclara la diferencia entre clases de datos personales construyendo las bases para la instauración de los diversos grados de protección que deben presentar si son públicos o privados, así como las finalidades permitidas para su utilización.
4. Crea una especial protección a los datos de menores de edad.

---

[38] MinTic. (29 de 07 de 2009). Ley 1341 de 2009. Obtenido de https://www.mintic.gov.co/portal/604/w3-article-3707.html

[39] Republica, C. d. (17 de 10 de 2012). LEY ESTATUTARIA 1581 DE 2012. Obtenido de https://www.sisben.gov.co/Documents/Informaci%C3%B3n/Leyes/LEY%20TRATAMIENTO%20DE%20DATOS%20-%20LEY%201581%20DE%202012.pdf

5. Establece los lineamientos para la cesión de datos entre entidades y los procesos de importación y exportación de información personal que se realicen en adelante.
6. Define las obligaciones y responsabilidades que empresas de servicios tercerizados tales como Call y Contact Center, entidades de cobranza y, en general, todos aquellos que manejen datos personales por cuenta de un tercero, deben cumplir en adelante.
7. Asigna la vigilancia y control de las bases de datos personales a la ya creada Superintendencia Delegada para la Protección de Datos Personales, de la Superintendencia de Industria y Comercio.
8. Crea el Registro Nacional de Bases de Datos.
9. Establece una serie de sanciones de carácter personal e institucional dirigidas a entidades y funcionarios responsables del cumplimiento de sus lineamientos.

DECRETO 1377 DE 2013

Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012."[40]

ASPECTOS GENERALES DE LA LEY 1273 DE 2009

En Colombia fue creada la ley 1273 de 2009 denominada "De la protección de la información y de los datos" el 5 de enero de 2009 por el congreso de la república, por la cual se modifica el código penal y se crea un nuevo mecanismo legal, cuyo objetivo es sancionar todo comportamiento ilícito frente a la comisión de los delitos informáticos en el país.[41]

[40] Camelo, L. (23 de 02 de 2010). Marco legal de Seguridad de la Información en Colombia. Obtenido de http://seguridadinformacioncolombia.blogspot.com/2010/02/marco-legal-de-seguridad-de-la.html

[41] MinTic. (04 de 01 de 2009). Ley 1273 de 2009. Obtenido de https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Estos son los aspectos generales:

Capítulo I De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

1. Acceso abusivo a un sistema informático.
2. Obstaculización ilegitima de sistema informático.
3. Interceptación de datos informáticos.
4. Daño Informático.
5. Uso de software malicioso.
6. Violación de datos personales.
7. Suplantación de Sitios WEB para capturar datos personales.
8. Circunstancias de agravación punitiva.

Atentados informáticos y otras infracciones,

Capítulo 2: De los atentados informáticos y otras infracciones

1. Hurto por medios informáticos y semejantes.
2. Transferencia no consentida de activos. [42]

[42] Colombia, C. d. (05 de 01 de 2009). Ley de Delitos Informáticos en Colombia. Obtenido de https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

5. CAPITULO I

DESARROLLO DEL PROYECTO

5.1 Identificación de los principales inconvenientes de Seguridad de la empresa Qwerty

"MAGERIT es la metodología aplicada que nos sirve como herramienta para conocer las amenazas a los cuales se encuentran expuestos los activos que forman parte de la empresa QWERTY S.A. mediante la implementación de herramientas del análisis de riesgos esta dictamina el tipo de normas y políticas aplicar con el fin de proteger las tecnologías de la información."

Con la utilización de esta metodología lo que se busca es lograr los siguientes objetivos:

• Concientizar a las personas encargadas de los sistemas de información de los riesgos a los que pueden estar expuestos los activos informáticos al darles un uso inadecuado.

• Proponer una metodología para llevar a cabo el análisis de riesgos.

• Especificar y planificar que dimensión tienen las amenazas y de qué forma se pueden mantener bajo control.

• Buscar mecanismos para que la organización este al día y atenta a los procesos de auditoría, certificaciones.

Proceso que se deben llevar a cabo:

I. Catalogar de los activos según su importancia en la organización.
II. Definir el tipo de amenazas a las que puedan estar expuestos los activos.
III. verificar con qué tipo de salvaguardas se cuenta y que tan efectivas son frente una amenaza.
IV. Estimar el porcentaje de riesgo que puede tener una amenaza sobre un activo informático en la organización.
V. Estimar el nivel de riesgo y el porcentaje ponderado de la ocurrencia de un evento.

Técnica de Recolección y Procesamiento de Datos

Para la elaboración de este trabajo se comenzará con el proceso de Observación, lo cual ayudará a extraer y validar la información recolectada durante este proceso,

realizando la debida verificación de los elementos físicos de las diferentes áreas de la empresa, este proceso se iniciara teniendo en cuenta los tiempos de ejecución de cada actividad, de igual forma se realizara un registro de las observaciones hechas verificando que se cumplan las normas de seguridad en cada área.

Adicionalmente se le realiza una entrevista a los empleados de las oficinas con preguntas básicas sobre el conocimiento sobre la seguridad de la información que medidas aplican de estas; con qué frecuencia el área encargada hace el cambio de claves y si saben si estos cuenta con algún programa especializado para llevar el registro y control de las mismas.

También se verificará el estado de los activos informáticos y la dependencia de los mismos, si estos cuentas con las últimas versiones de software y programas al igual del estado en que se encuentra todo esto para poder llegar a la conclusión de que posibles amenazas y riesgos están expuestos los activos informáticos y de esta manera generar un informe para la gerencia con las recomendaciones y medidas pertinentes para cada caso.

5.2. Investigación Aplicada

El propósito de esta es determinar una solución a un problema, enfocándose en buscar diferentes técnicas y alternativas para su solución.[43]

Este tipo de investigación está vinculada a la realización de la investigación pura, lo cual nos servirá de referencia para la elaboración del análisis de riesgos informáticos en la empresa QWERTY S.A este tipo de investigación nos permitirá encontrar una posible solución a los problemas a encontrar.

Como parte del desarrollo de la investigación aplicada, se realizarán algunas actividades como lo son:

[43]Duoc, Bibliotecas. «Definición.» 2018. uoc.cl/biblioteca/crai/definicion-y-proposito-de-la-investigacion-aplicada

- Generación del plan de trabajo y establecimiento de plazos de tiempo: será hará un cronograma de actividades donde se especifican las diferentes actividades a realizar con el fin de alcanzar el objetivo propuesto., se especificarán los tiempos para el desarrollo de las actividades.
- La definición de los objetivos del proyecto y se definirá el alcance del mismo teniendo en cuenta la formulación del problema.
- Se verificará si la empresa en cuestión tiene archivos, para de esta forma poder recolectar información referente a la seguridad informática; tales como documentos de la organización para poder conocer el contexto y el entorno de la empresa su estructura, normas y reglamentación referente al tema.
- Se realizará un reconocimiento del Entorno para poder evaluar los activos, su estado; la infraestructura de las instalaciones para poder medio del análisis de Riesgos poder verificar si cumplen las normas mínimas de seguridad.
- Se identificarán las vulnerabilidades de los activos; así mismo se realizará el respectivo análisis de estas para determinar su origen, por medio de la matriz de valoración de riesgos.
- Después de realizar el respectivo análisis se realizarán sugerencias y recomendaciones para finalmente discutir los resultados.
- Se hará entrega de un informe técnico con los respectivos hallazgos para entregar como resultado el informe a las directivas de la organización.

Dentro de las actividades a desarrollar se aplica un cuestionario basado en la investigación desarrollada por la organización Ernst & Young, ahora también conocida como **EY** es una de las más importantes firmas de servicios profesionales del mundo. El formato del cuestionario se encuentra en el Anexo B del presente documento.

El formulario se aplicó a las tres dependencias del área de sistemas de la empresa QWERY S.A

La aplicación del cuestionario permitirá tener una visión más clara de la situación actual de la organización en cuanto a lo concerniente a la seguridad informática en la empresa.

Este cuestionario se aplicará a las siguientes personas:

- Gerente
- Supervisor de cada área
- Ingenieros Responsable del área de informática
- Jefe de área de soporte

5.2.1 PROCESO

- Elaboración del cuestionario
- Entrevista e inspección de la empresa
- Consolidación de los resultados
- Análisis de los resultados
- Elaboración de informes y plan de acción
- Entrega de resultados

ENTREVISTA E INSPECCIÓN DE LA EMPRESA

El cuestionario fue aplicado a funcionarios de la empresa quienes consideran que es importante darle continuidad al negocio, pero también están la vanguardia del mercado con respecto a la seguridad de la información.

Teniendo cuenta que según la encuesta aplicada por EY solo un 13% de las organizaciones destinan presupuestó con fines a mejorar la seguridad informática en sus empresas la gran mayoría manifestó que parte de su presupuesto era destinado a la imagen corporativa de la empresa mas no al mejoramiento de equipos y tecnología emergente para el mejoramiento de la seguridad de la información en la organización.

Según la información suministrada en la aplicación del cuestionario (Ver anexo B) a diferencia del porcentaje total de inversión de seguridad de la empresas colombiana que según estudios a entre el 2017 y el 2018 la inversión de su presupuesto para invertir en temas de ciberseguridad es solo del 20%[44] del total del

[44] Montes, Sebastián. 08 de 09 de 2018. https://www.larepublica.co/internet-economy/empresas-colombianas-solo-invierten-20-de-presupuesto-en-ciberseguridad-2768645.

presupuesto lo que a diferencia de Qwerty S.A estos solos están destinado un porcentaje entre el 2017 y 2018 de del 6% y 8 % respectivamente, , del total del prepuesto lo que evidencia la gran brecha de seguridad que puede estar presentado la empresa.

A las preguntas relacionadas como si tienen conocimientos sobre la importancia de los activos de la empresa y las medidas de seguridad que se deben tomar respecto a estos; los funcionarios manifiestan que, aunque estos si saben de la importancia de la protección de los activos de la empresa también admiten que en su gran mayoría los empleados no son conscientes de esto.

Reconocen que uno de los mayores activos de las organizaciones es la información, pero debido a las malas prácticas tanto de los altos funcionarios como de los colaboradores internos y externos no se le ha dado la importancia y el manejo que esta merece.

Según la encuesta Global de la organización EY en la siguiente tabla se puede observar el top 10 de la información más codiciada para los delincuentes y las mayores amenazas cibernéticas para para las empresas (según Tabla 2)

Tabla 2 Mayores amenazas cibernéticas

Rating de la Información más valiosa para los criminales	**Principales amenazas de Seguridad**
1. Información clientes (17%)	1. Ingeniería Social Phishing (22%)
2. Información Financiera (12%)	2. Software malicioso Malware (20%)
3. Planes del negocio (12%)	3. Interrupción de operaciones (13%)
4. Información del Consejo (11%)	4. Robo de dinero (12%)
5. Las contraseñas de los clientes (11%)	5. Fraude (10%)
6. Información de Investigación y Desarrollo (9%)	6. Robo de IP (8%)
7. Información sobre fusiones y adquisición de empresas (8%)	7. Correo basura (Spam) (6%)
8. Derechos de Propiedad Intelectual (6%)	8. Ataques al interior de la empresa (5%)
9. Plagio de IP no patentadas (5%)	9. perdida por desastres naturales (2%)
10. Información confidencial de proveedores (5%)	10. Espionaje (2%)

Fuente: Encuesta-Global-Seguridad-Informacion-2018-19. PDF P-23

De la aplicación del cuestionario y de la observación también se logró concluir que las mayores falencias se concentran en:

- los controles de seguridad obsoletos que se aplican en la empresa.

- Imprudencias ocasionadas por los empleados como el no cerrar la sección del usuario, como abrir el correo personal en los computadores de la empresa, el uso sin autorización de medios extraíbles.
- La manipulación del sistema de nómina y facturación por personal que se encuentra en práctica o tienen contratos de aprendizaje.
- También se encontró tiene un cortafuegos que no cumplen con las reglas mínimas de configuración.

Para dar cumplimiento a los objetivos de seguridad de la compañía Qwerty S.A se proponen las siguientes estrategias:

5.2.2. Normas y técnicas de protección de la información.

Se plantean las siguientes normas para la empresa **QWERTY S.A** cuyo fin será garantizar el buen manejo de la información mediante la formulación de un sistema de seguridad SGSI[45]

- Debe definir la postura de la dirección o la gerencia con respecto a la necesidad de proteger la información corporativa Orientando a los funcionarios a la aplicación de la adecuada utilización de los recursos de información. [46]
- La empresa definirá y documentará la aplicación de un sistema de gestión de la calidad y mejoramiento continuo basado en la eficacia de acuerdo con lo establecido en la norma.

[45] Excellence, I. (07 de 03 de 2014). ISO 27001 Como implantar políticas de Gestión de un Sistema de Gestión de Seguridad de la Información. Obtenido de https://www.pmg-ssi.com/2014/03/iso-27001-chttps://www.pmg-ssi.com/2014/03/iso-27001-como-implantar-politicas-de-gestion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/

[46] Castillo, I. M. (03 de 2019). POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN. Obtenido de http://artesaniasdecolombia.com.co/PortalAC/images/politica-seguridad-informacion-proteccion-datos-personales.pdf

- Asegurar la disponibilidad de toda la información necesaria para apoyar la operación y el seguimiento de estos procesos.
- Realizar el seguimiento, medición y análisis de los procesos.
- Implementar los mecanismos necesarios para alcanzar los resultados planificados y la mejora continua de estos procesos.
- Definir la base para la estructura de seguridad de la organización.
- El sistema de gestión de la calidad se basará en normas y objetivos orientados hacia la calidad.
- Se debe implementar un manual de calidad que contenga la descripción de procesos y un mapa de los mismos.
- Asegurar que los documentos que existen en archivo sirvan como guía y se encuentren disponibles, de igual forman que los documentos sean legibles y se puedan identificar de una manera fácil
- Se debe llevar un control de documentos de documentos obsoletos esto con el fin de tener actualizado el archivo de la empresa y no ocupar espacio que puede servir para manejar información vigente.
- Se tendrá en cuenta las normas, leyes y reglamentos vigentes para su implementación.
- Recopilar y analizar los datos apropiados para demostrar la competencia y la eficacia del SGSI y para determinar donde se pueden hacer mejoras y aplicar mejoramiento continuo.

5.2.3 Arquitectura y tecnologías de seguridad

Respecto a esto lo que se observa y se puede concluir en la aplicación del cuestionario es la identificación de algunos elementos que evidentemente causan una brecha de seguridad en la empresa dicha información esta soportada en la respectiva documentación otorgada por la empresa, la revisión del software, licencias, el diagrama de la red y procedimientos y políticas que se manejan:

6. CAPITULO II EVALUACIÓN DE RIESGOS

6.1 Indicadores de gestión para la verificación de seguridad de los activos informáticos.

Se realiza un análisis de riesgos a los activos de la empresa QWERTY S.A según la metodología de MAGERIT

MATRIZ DE RIESGOS ACTIVOS INFORMÁTICOS

- La Empresa Qwerty S.A no presenta documentación que evidencia una evaluación de riesgo posterior a la que se está realizando por lo que no se cuenta con las siguientes salvaguardas:
- Teniendo en cuenta la información suministrada por los colaboradores la empresa no ofrece capacitación a sus empleados respecto a temas de seguridad y el buen uso de las prácticas del manejo de los activos informáticos.
- Debido a la criticidad de la información que se maneja la empresa no cuenta con contratos de confiabilidad, ni pólizas donde transfiere el riesgo a un tercero.
- la compañía no tiene políticas claras y definidas sobre el uso de dispositivos extraíbles (Por ejemplo, USB, CD, DVD entre otros).
- No lleva controles sobre el ingreso de usuarios, creación de contraseñas y control de las mismas.
- No implementan políticas criptográficas para el manejo y transporte de la información considerada critica para la organización.
- Referente a la página web se considera en estado crítico ya que puede presentar Caída del sistema por agotamiento de recursos.
- En cuento a los servidores están sujetos a amenazas como errores de mantenimiento, actualización entre otros.

Salvaguardas de seguridad de la información relacionadas con personas:

- QWERY S.A. no cuenta con un sistema de seguridad biométrico o de monitoreo que permita tener control de ingreso y egreso de los clientes internos y externos.
- Los antecedentes personales de los colaboradores no son verificados.
- La empresa no hace uso de aplicaciones para el control de contraseña.
- Aunque posee manual de funciones es evidente que falta la capacitación hacia los colaboradores.

Salvaguardas de proceso de seguridad de la información:

- Se evidencio que no existen parámetros básicos de seguridad establecidos para socios, clientes y proveedores.
- No tienen documentos donde se evidencien protocolos establecidos para la infraestructura de la organización.
- La compañía no cuenta con un plan de recuperación en lo que se refiere a desastres.

6.2 ANÁLISIS DOFA

Tabla 3 Dofa

Debilidades	Fortalezas
Carencia de un plan que permita el manipular adecuadamente la seguridad de la información.	Se cuenta con buena tecnología
no posee una herramienta que permita clasificar los activos y los riesgos a los que estos están expuestos,	los Directivos de la empresa Qwerty están comprometidos con la protección y continuidad del negocio
no hay evidencia que tengan un registro de incidentes anteriores	Cuenta con lineamientos básicos de seguridad establecidos para los Directivos, clientes y proveedores
La aplicación de salvaguardas y políticas contra riesgo es deficiente.	La página web es un valor agregado al modelo de negocio ya que esta se utiliza para la publicación de información referente al mismo.
no cuenta con un sistema Biométrico o de monitoreo	la organización se preocupa para estar a la vanguardia de otras organizaciones por lo que existe un departamento de desarrollo,
la red no está segmentada	cuenta con una dependencia de sistemas que brinda soporte a la infraestructura tecnológica 24/7
el servidor de archivos puede presentar Fallo del sistema de identificación y autorización	
No existen programas de capacitación sobre políticas y prácticas de seguridad	
Oportunidades	**Amenazas**
Es una empresa del sector tecnológico que busca el desarrollo tecnológico en comunidades colombianas a través del uso de Tecnologías de Información por lo que cuenta con reconocimiento y posición en el mercado	No cumplir con las políticas y lineamientos exigidos por el gobierno nacional en lo que se refiere a la seguridad Informática,

Al ser una organización que cuenta con buena infraestructura tecnológica por lo que puede realizar alianzas estratégicas con otras empresas y proveedores del mercado.	La crisis financiera afecta el poder de adquisición del producto.
Cuenta con márgenes de ganancia amplios por lo que puede incursionar en otros mercados del sector tecnológico y de las telecomunicaciones	los Delitos informáticos cada día van en aumento, así como las herramientas y métodos para cometerlos
Esta incursionado en el mercado de la seguridad de la información por lo que los avances sobre este tema cada vez están más al alcance de la organización.	no cuenta con políticas de confiabilidad por lo que puede haber fuga de información confidencial y critica para la organización,
Las leyes en el país cada vez son más explicitas en lo que se refiere a la seguridad de la información y la penalización de delitos contra las organizaciones y personas esto con el fin de proteger a las organizaciones contra cualquier delito informático.	en Colombia todavía existen vacíos legales que tienen el potencial de ser usados por atacantes para cometer actividades perjudiciales para la organización

Fuente: Propia

A partir de la observación e investigación de pueden determinar que la organización Qwerty tiene las siguientes necesidades:

- Es importante que esta adopte una estrategia que le permita estar al nivel de otras organizaciones que ya implementa la seguridad de la información, por lo que debe adaptarse al mercado adoptando políticas y estrategias referentes a este tema.
- Tiene que cambiar su modelo de negocio en lo que se refiere a seguridad ya que el mercado está adaptándose ambiente normativo en torno a la seguridad de la información
- Administrar de una forma más eficaz los activos informáticos y mejorar, cambiar las salvaguardas tecnológicas ya existentes.

7. ACTIVOS DE LA INFORMACIÓN

Los activos con los que cuenta la empresa **QWERTY S. A**

Tabla 4 Activos Informáticos

Activo	Descripción	ubicación	Cantidad
Servidor de Impresión: Servidor marca Dell en torre PowerEdge T440	Equipo de cómputo que conecta dos impresoras: Destinadas a: Una (1) Impresora HP LaserJet Enterprise serie 600, activo que brinda el servicio para la dependencia de nómina y facturación. Permite la concurrencia de hasta 25 usuarios y el volumen mensual de impresión es de 200 a 25000 páginas	Oficina de nómina y facturación	1
	Una (1) Impresora SMART MultiXpress M4370LX, impresora que ofrece el servicio de escáner e impresión con un ciclo de trabajo de hasta 300000 páginas mensuales con capacidades de red alámbrica e inalámbrica. Impresora destinada para el servicio de directivos y administrativos, practicantes.	Dependencia directiva y administrativa	1

Servidor de archivos FTP: **Servidor marca Dell en torre PowerEdge T130**	Equipo de cómputo que tiene como función el almacenamiento y la administración de los archivos que se están generando en el interior de la organización como son: Digitalización de documento de entrada y de salida, audios generados en reuniones, asambleas y otro tipo de encuentros, video, generados por Directivos y funcionarios. Dentro de las políticas de uso, para este servidor solo pueden tener acceso las personas autorizadas para los fines correspondientes	Oficina antigua de sistemas	1
Página web	Servicio contratado con la empresa Godaddy.com La página web tiene como objeto la publicación de contenido relacionado con el modelo negocio. Está construida a partir del sistema gestor de contenidos dinámicos Joomla versión 2.5 El hospedaje web la infraestructura del servidor es Apache, PHP, MySQL.	Empresa Godaddy	1

Servidor de nómina y facturación **Servidor marca Dell en torre PowerEdge T440** **Características de servidor Apache 2.4.25** **PHP 5.6.30 - 7.1.1 MySQL 5.7.17** **phpMyAdmin 4.6.6**	Plataforma de desarrollo propio. Tiene como función el almacenamiento y la administración de la nómina y facturación de la empresa QWERTY S.A.		2

Servidor DHCP **Servidor marca Dell en torre** **PowerEdge T440**	Servidor que asigna y administra de forma dinámica el direccionamiento dentro de la organización		1
Equipos de cómputo para gestión del desarrollo tecnológico	Equipos de cómputo donde se gestiona información online relacionada con el desarrollo del objeto social Presupuesto • Proveedores • Órdenes de compra • Inventarios	Dependencia de desarrollo tecnológico	3

Cortafuegos Cisco ASA 5505	Sistema de protección	Sistema de seguridad que está protegiendo a la red de datos, de intrusiones que se puedan presentar en la red	1
Equipos de Computo Sistemas operativos win 10 Pro	Equipos destinados para el desarrollo del objeto social	Dependencia de infraestructura	3
Equipos de Computo sistemas operativos win 10 Pro	Equipos destinados para el desarrollo del objeto social	Dependencia de control y seguimiento	10
Equipos de Computo	Equipos destinados para el desarrollo del objeto social	Dependencia de prueba de software	5
Puntos de acceso alámbricos (hub)	Dispositivos de red encargados de la interconexión de la red de datos	Red de datos del centro	4
Switches cisco catalyst 2960	Dispositivos de red encargados de la interconexión de la red de datos	Red de datos del Centro	6
Técnicos de mantenimiento	Personal técnico encargado de realizar el mantenimiento preventivo a los equipos de computo	Departamento de Sistemas	2

Teléfonos IP	Sistema de comunicación a través de teléfonos Voz IP, que comunica las oficinas y departamentos del centro	Dependencias del centro	6
Puntos de acceso	Puntos de acceso al servicio de internet en el campus universitario	Departamento de sistemas	2

Fuente: Escenario2 Enfoque Directivo Administrativo P-4

7.1 identificación de los Activos

Se realiza la identificación y clasificación de activos según la metodología margerit

Activos Informáticos de la Empresa. Los activos de la empresa están definidos en la siguiente tabla. Allí se puede evidencia la utilización de la metodología Margerit para la clasificación de los activos.

Tabla 5 ACTIVOS METODOLOGÍA MARGERIT

CATEGORÍA DEL ACTIVO	NOMBRE DEL ACTIVO
[HW] Equipamiento informático	Servidores: 1. servidor de impresión marca Dell en torre powerEdge T440 2. Servidor de archivos marca Dell en torre powerEdge T130 3. Servidor de nómina y facturación marca Dell en torre powerEdge T440 4. Servidor DHCP marca Dell en torre powerEdge T440 5. servidor FTP PowerEdge T130 6. Firewall cisco ASA 5505 7. Equipos de cómputo sistema operativo Win 10 pro.
[HW] Equipamiento informático	Servidor DHCP Servidor HTTP PBX Servidor de impresión Servidor de nómina y facturación
[SW] Software - Aplicaciones informáticas	Servidor de archivos
[SW] Software - Aplicaciones informáticas	Servidor de registro de nómina y facturación
[S] Servicios	Servidor DHCP
[HW] Equipamiento informático	Firewall
[HW] Equipamiento informático	Equipos de cómputo: 1. gestión de sistema contable 2. Para el sistema de generación de nómina y facturación 3. control de proveedores, órdenes de compra e inventarios
[HW] Equipamiento informático	Puntos de acceso alámbrico (hub)

[HW] Equipamiento informático	Switches
[S] Servicios	Página Web
[P] Personal	Técnicos de mantenimiento
[HW] Equipamiento informático	Teléfonos IP
[COM] Redes de Comunicaciones	Puntos de acceso
[L] Instalaciones	Data Center
[SW] Software - Aplicaciones informáticas	Sistema de registro de nómina y facturación
[SW] Software - Aplicaciones informáticas	Servidor de archivos función almacenamiento y administración de archivos,
[SW] Software - Aplicaciones informáticas	Servidor DHCP administra en forma dinámica el direccionamiento dentro la organización,
[S] Servicios	Página Web
[HW] Equipamiento informático	Teléfonos IP
[HW] Equipamiento informático	Firewall
[S] Servicios y [HW] Equipamiento informático	Correo electrónico Página Web
[HW] Equipamiento informático	Computador

Fuente: Propia

7.2 Valoración de los activos[47]

Para realizar una correcta valoración de los activos se van a tener en cuenta los siguientes criterios que se relacionan a continuación:

Tabla 6 Valorización activos

NIVEL	VALOR	CRITERIO
10	EXTREMO	DAÑO EXTREMADAMENTE GRAVE
9	MUY ALTO	DAÑO MUY GRAVE
6-8	ALTO	DAÑO GRAVE
3-5	MEDIO	DAÑO IMPORTANTE
1-2	BAJO	DAÑO MENOR
0	DESPRECIABLE	IRRELEVANTE

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html

El objetivo de esta actividad es identificar en qué dimensión es valioso el activo, teniendo presente que estos son todos los recursos con los que cuenta la organización para continuar con la operación del negocio.

Esta actividad se lleva a cabo identificando todos los activos que utiliza la empresa tanto en forma digital como física.; y el nivel de afectación que pueda tener la organización en caso de que algo llegara a pasar.

En la siguientes Tablas se puede observar el resultado de la Valoración de activos para la empresa.

Y también el nivel de Probabilidad de impacto y dimensión.

[47] D. Espinosa, J. M. (12 de 2014). GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN CON. Obtenido de http://web.usbmed.edu.co/usbmed/fing/v5n2/pdf/Articulo_Gestion_Riesgo_Seguridad_Infor macion

Tabla 7 Valorización Activos Qwerty S.A

Tipo de activo	Nombre de activo	Bajo	Medio	Alto
Equipamiento - hardware	Computadoras de escritorio Win 10 pro			
	portatiles S.O win 10 pro			
	Antenas			
	Cableado			
	Internet			
	LAN			
	Switches			
	Router			
	Sistema de vigilancia			
	Telefonía PBX			
	WIFI			
	Cd y discos duros			
	Medios de impresión			
	1. servidor de impresión marca Dell en torre powerEdge T440 2. Servidor de archivos marca Dell en torre powerEdge T130 3. Servidor de nómina y facturación marca Dell en torre powerEdge T440 4. Servidor DHCP marca Dell en torre powerEdge T440 5. Servidor FTP PowerEdge T130 6. Firewall cisco ASA 5505			
Equipamiento - software	Correo electrónico			
	Sistema de Registro de nómina y Facturación			
	Antivirus			
	Ofimática			
	Otros softwares			
	Sistema operativo			
Equipamiento Auxiliar	Sistema de alimentación ininterrumpida			
	Equipos de climatización			
Instalaciones	Data center			
	Cuartos de red			
Personal	Administradores			

	Equipo de desarrollo de aplicaciones y Proyectos			
	Equipo soporte			

Fuente: Propia

7.3 Dimensiones

A fin de poder determinar el impacto que tendría un incidente de seguridad sobre la organización, se tendrán en cuenta las siguientes dimensiones de la seguridad[48]

Dimensiones en las cuales el activo se vuelve relevante:

[D] disponibilidad

[I] integridad de los datos

[C] confidencialidad de los datos

[A] autenticidad de los usuarios y de la información

[T] trazabilidad del servicio y de los datos[49]

Fuente: http://administracionelectronica.gob.es/ctt/verPestanaDescargas.htm?idIniciativa=184#.U48C7Pl_tO4

7.3.1 Dimensiones de Hardware

Tabla 8 Criterios de Valorización

VALOR		CRITERIO
10	Muy Alto	Impacto muy grave a la organización
7-9	Alto	Impacto grave a la organización
4-6	Medio	Impacto importante a la organización
1-3	Bajo	Impacto menor a la organización
0	Despreciable	Irrelevante a efectos prácticos

Fuente: https://www.pilar-tools.com/doc/magerit/v2/cat-es-v11.pdf P-19

[48] ccn-cert.cni. (19 de 04 de 2020). ANEXO I Categorías de los sistemas ANEXO I Categorías de los sistemas\2. Dimensiones de la seguridad. Obtenido de https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1068

[49] Magerit-versión 3.0 Metodología de análisis Y gestión de Riesgos de Sistemas de información , Libro I-Método , https://www.ccn-cert.eni.es/publico/herramientas/pilar5/magerit/c, p 40

Tabla 9 Dimensiones de Hardware

	HARDWARE																			
	SERVIDORES					COMPUTADORES PERSONALES					EQ DE COMUNICACIONES					RESPALDOS				
Amenaza vs Dimensión	[D]	[I]	[A]	[C]	[T]	[D]	[I]	[A]	[C]	[T]	[D]	[I]	[A]	[C]	[T]	[D]	[I]	[A]	[C]	[T]
Fuego	10					10					10					10				
Terremoto	10					10					10					10				
Inundaciones											6									
Caída del sistema por sobrecarga						8					8					8				
Corte del suministro eléctrico	8					6					6					6				
Condiciones inadecuadas de temperatura o humedad	6																			
Errores de configuración		5										6								
Desconexión física o lógica	8					2					8				8					
Agotamiento de recursos	6																			
Fuga de información	10																			
Acceso no autorizado			9						8					9				5		
spam						6	5													
Malware	8	8																		
phishing						5	5													
spyware		8					5													
robo	10					8					10					10				

Fuente: Propia

7.3.2 Dimensiones de Software

Tabla 6 Dimensiones de Software

	SOFTWARE																									
	INTERNET					RREO ELECTRONI					SISTEMA FINANCIERO Y ADMINISTRATIV					VIRTUALIZACIÓN					ALMACENAMIENTO BASE DE DATOS				
Amenaza vs Dimesion	[D]	[I]	[A]	[C]	[T]	[D]	[I]	[A]	[C]	[T]	[D]	[I]	[A]	[C]	[T]	[D]	[I]	[A]	[C]	[T]	[D]	[I]	[A]	[C]	[T]
Fuego	10					10					8					10					8				
Terremoto	10					10					8					10					8				
Inundaciones																									
Caída del sistema por sobrecarga	8					8					8					8					8				
Corte del suministro eléctrico	6					6					6					6					6				
Condiciones inadecuadas de temperatura o humedad																									
Errores de configuración							7								7		7								
Desconexión física o lógica	10					8										8					9				
Agotamiento de recursos																					8				
Fuga de información																									
Acceso no autorizado									9										8				8	8	
spam																									
Malware																									
phishing									6																
spyware									6																
robo																									

Fuente: Propia

7.3.3. Dimensiones del Personal

Tabla 7 Dimensiones del Personal

	PERSONAL														
	EQUIPO DE DESARROLLO					ADMINISTRADORES					EQUIPO DE TÉCNICO				
Amenaza vs Dimensión	[D]	[I]	[A]	[C]	[T]	[D]	[I]	[A]	[C]	[T]	[D]	[I]	[A]	[C]	[T]
Fuego	10					10					10				
Terremoto	10					10					10				
Inundaciones															
Caída del sistema por sobrecarga															
Corte del suministro eléctrico															
Condiciones inadecuadas de temperatura o humedad															
Errores de configuración															
Desconexión física o lógica															
Agotamiento de recursos															
Fuga de información		10		10					10					10	
Acceso no autorizado		10		10					10					10	
spam															
Malware															
phishing															
spyware															
robo															

Fuente: Propia

7.3.4 Dimensiones Equipamiento Auxiliar

Tabla 8 Dimensiones Equipamiento Auxiliar

	EQUIPAMIENTO AUXILIAR														
	CABLEADO ELÉCTRICO					EQUIPOS DE CLIMATIZACIÓN					GENERADORES ELÉCTRICOS				
Amenaza vs Dimensión	[D]	[I]	[A]	[C]	[T]	[D]	[I]	[A]	[C]	[T]	[D]	[I]	[A]	[C]	[T]
Fuego	10					10					10				
Terremoto	10					10					10				
Inundaciones	8					8					8				
Caída del sistema por sobrecarga															
Corte del suministro eléctrico															
Condiciones inadecuadas de temperatura o humedad						10					10				
Errores de configuración															
Desconexión física o lógica	10														
Agotamiento de recursos															
Fuga de información															
Acceso no autorizado															
spam															
Malware															
phishing															
spyware															
robo	10					10					10				

Fuente: Propia

7.3.5 Dimensiones Instalaciones

Tabla 9 Dimensiones Instalaciones

	INSTALACIONES														
	UPS					CUARTO DE RED					CENTRO DE DATOS				
Amenaza vs Dimensión	[D]	[I]	[A]	[C]	[T]	[D]	[I]	[A]	[C]	[T]	[D]	[I]	[A]	[C]	[T]
Fuego	10					10					10				
Terremoto	10					10					10				
Inundaciones	8					9					9				
Caída del sistema por sobrecarga						8					8				
Corte del suministro eléctrico						8					8				
Condiciones inadecuadas de temperatura o humedad											8				
Errores de configuración															
Desconexión física o lógica						10					10				
Agotamiento de recursos						5					5				
Fuga de información															
Acceso no autorizado						8					8				
spam															
Malware															
phishing															
spyware															
robo	10														

Fuente: Propia

Tabla 10 Tabla de Impacto y dimensión

IDENTIFICACIÓN DEL ACTIVO			CALIFICACIÓN		EVALUACIÓN
ÍTEM	CATEGORÍA DEL ACTIVO	NOMBRE DEL ACTIVO	PROBABILIDAD	IMPACTO	TIPO DE IMPACTO Dimensión [Disponibilidad, Integridad, Confidencialidad]
1	[HW] Equipamiento informático	Servidores: 1. servidor de impresión 2. Servidor de archivos 3. Servidor de registro y control académico 4. Servidor DHCP 5. Servidor FTP Firewall Equipos de cómputo.	3-Posible	4-Mayor	Disponibilidad
2	[HW] Equipamiento informático	Servidor DHCP Servidor HTTP PBX Servidor de	3-Posible	4-Mayor	Disponibilidad

		impresión Servidor de nómina y facturación			
3	[SW] Software - Aplicaciones informáticas	Servidor de archivos	3-Posible	2-Menor	Confidencialidad e Integridad
4	[SW] Software - Aplicaciones informáticas	Servidor de registro de nómina y facturación	4-Probable	3-Moderado	Integridad y Disponibilidad
5	[S] Servicios	Servidor DHCP	2-Improbable	4-Mayor	Disponibilidad, Confidencialidad e Integridad

6	[HW] Equipamiento informático	Firewall	3-Posible	4-Mayor	Disponibilidad, Confidencialidad e Integridad
7	[HW] Equipamiento informático	Equipos de cómputo: 1. gestión de sistema contable 2. Para el sistema de generación de nómina y facturación 3. Control de proveedores, órdenes de compra e inventarios.	3-Posible	2-Menor	Disponibilidad

8	[HW] Equipamiento informático	Puntos de acceso alámbrico (hub)	2-Improbable	2-Menor	Disponibilidad
9	[HW] Equipamiento informático	Switches	2-Improbable	4-Mayor	Disponibilidad, Confidencialidad e Integridad
10	[S] Servicios	Página Web	4-Probable	4-Mayor	Disponibilidad
11	[P] Personal	Técnicos de mantenimiento	3-Posible	2-Menor	Disponibilidad
12	[HW] Equipamiento informático	Teléfonos IP	2-Improbable	2-Menor	Disponibilidad
13	[COM] Redes de Comunicaciones	Puntos de acceso	3-Posible	3-Moderado	Disponibilidad
14	[L] Instalaciones	Data Center	3-Posible	5-Catastrófico	Integridad y confidencialidad
15	[SW] Software - Aplicaciones informáticas	Sistema de registro y control académico	4-Probable	3-Moderado	Integridad
16	[SW] Software - Aplicaciones informáticas	Servidor de archivos función almacenamiento y administración de archivos.	3-Posible	2-Menor	Disponibilidad
17	[SW] Software - Aplicaciones informáticas	Servidor DHCP administra en forma dinámica el direccionamiento dentro la organización.	4-Probable	3-Moderado	Integridad
18	[S] Servicios	Página Web	3-Posible	4-Mayor	Disponibilidad, Confidencialidad e Integridad

19	[HW] Equipamiento informático	Teléfonos IP	4-Probable	2-Menor	Confidencialidad
20	[HW] Equipamiento informático	Firewall	3-Posible	4-Mayor	Disponibilidad, Confidencialidad e Integridad
21	[S] Servicios y [HW] Equipamiento informático	Correo electrónico Página Web Biblioteca Virtual	4-Probable	4-Mayor	Disponibilidad
22	[HW] Equipamiento informático	Computador	3-Posible	2-Menor	Disponibilidad

Fuente: Propia

8. AMENAZAS

El proceso de caracterización de las Amenazas se hizo por medio de la metodología aplicada donde su objetivo era poder determinar el nivel de riesgo a los que estaban expuestos los activos de la empresa.

Se llegó a la conclusión de que estos están expuesto a un nivel de riesgo considerable debido a las falencias de acuerdo al manejo que se les ha dado, según la matriz de riesgo se contempla riesgos críticos, importantes y apreciables, en cuento a la clasificación de las amenazas se encontraron amenazas en todas las clasificaciones de la caracterización de las Amenazas.

Una de las más preocupantes es la manipulación de personal no vinculado directamente a la empresa en la oficina de nómina y facturación ya que están expuesto a que la información pierda la integridad, confiabilidad y disponibilidad que esta necesita, así como que pueda haber robo y filtración de información crítica para la organización.

De igual forma al verificar el nivel de valorización de las amenazas se puede observar que mucho activo de la cuenta con un de valor de Degradación y Probabilidad de Ocurrencia dan niveles de Alta y Muy Alta, por lo que es importante hacer énfasis en este problema en el momento de rendir el informe

Caracterización de las Amenazas se realiza según metodología Margerit capítulo 5 “del Catálogo de los Elementos”

- Mapa de Riesgos
- Caracterización de las Amenazas
- Identificación de las Amenazas
- Valoración de Amenazas por Activos

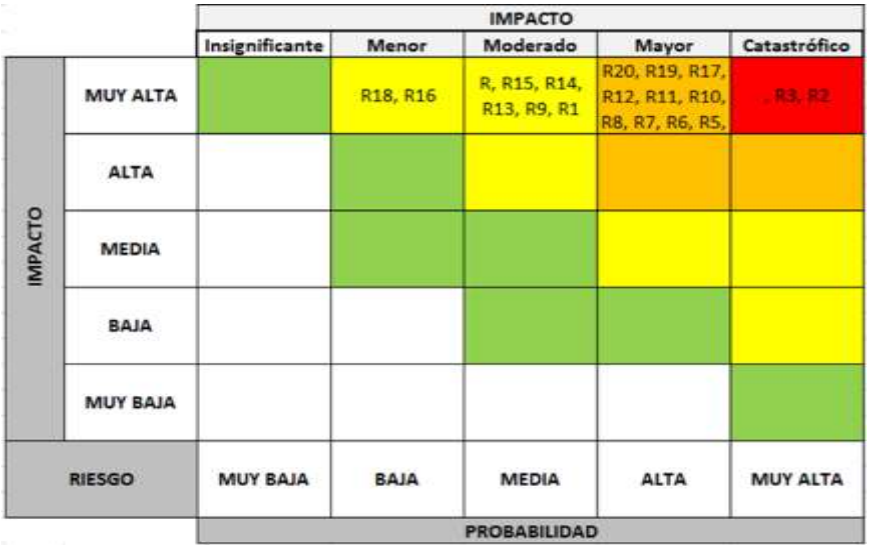
Se observa el mapa de calor, en el cual las zonas de riesgo derivan del producto de los valores de impacto y probabilidad, dando como resultado un mapa de calor y sus respectivas zonas de riesgo.

Tabla 11 Estimación de Riesgos

Nombre	Riesgo	AUTENTICIDAD	TRAZABILIDAD	ONFIDENCIALIDA	INTEGRIDAD	DISPONIBILIDAD	VALOR
[S] [www] Página Web	IMPORTANTE	9	20	20	20	20	18
[D] [Info] Información de nómina y facturación	CRITICO	20	25	25	25	25	24
MEDIA [Printed] Material impreso	IMPORTANTE	9	25	20	25	20	20
[HW][print] impresora HP laser Una (1) Impresora HP LaserJet Enterprise serie 600	APRECIABLE	25	9	9	9	25	15
[HW][print] Impresora SMART MultiXpress M4370LX,	APRECIABLE	25	9	9	9	25	15
[HW] [pc] Equipos de cómputo para el sistema de regi	IMPORTANTE	15	20	20	20	20	19
[HW][ipphone] telefonos de voz ip	APRECIABLE	25	9	9	9	15	13
[SW][prp] Sistemas contables	CRITICO	20	25	25	25	25	24
[SW][av] Antivirus	CRITICO	20	25	20	20	20	21
[HW][data] Servidor de impresión	CRITICO	20	25	25	25	25	24
[HW][data] Servidor DHCP	CRITICO	20	25	25	25	25	24
[HW][data] Servidor de Nómina y facturación	CRITICO	20	25	25	25	25	24
[P][adm] Administrador del sistema	CRITICO	4	25	25	25	25	21
[P][des] Desarrolladores	APRECIABLE	4	25	15	15	15	15
[P][op]Operadores	CRITICO	25	25	20	25	20	23
[P][ue] Usuarios Externos	BAJO	25	9	4	4	4	9
[P][ui] Usuarios Internos	BAJO	25	9	4	4	4	9
[AUX]Archivadores	CRITICO	25	25	25	25	20	24
[D][log] Registro en la Aplicación	CRITICO	25	25	25	25	25	25
[HW][firewall] Cisco ASA 5505	APRECIABLE	20	4	9	15	20	14
[D][password] contraseñas de ingreso al sistema	IMPORTANTE	20	25	25	15	15	20
[D][source]Aplicativo de Resgistro y control	CRITICO	20	25	20	25	20	22
[D][file]registro de información	CRITICO	FALSO	20	20	25	25	23
[D][file] Recibos de pago	IMPORTANTE	FALSO	20	20	20	20	20
[COM][LAN] Red local	IMPORTANTE	FALSO	20	20	20	20	20

Fuente: Propia

Mapa de Riesgos

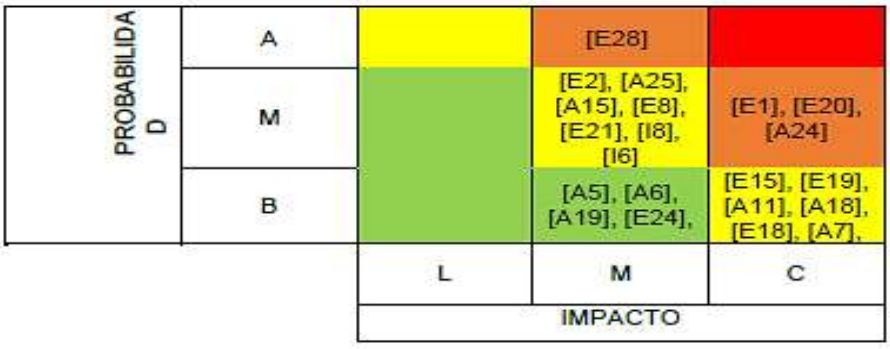


Se observa el mapa de calor, en el cual las zonas de riesgo derivan del producto de los valores de impacto y probabilidad, dando como resultado un mapa de calor y sus respectivas zonas de riesgo.

ANÁLISIS: con la ayuda de la herramienta matriz de Riesgos se puede evidenciar que Al no tener personal de planta y permitir que personal que no está incorporado directamente a la organización ayude en el área de nómina y facturación se evidencia que hay áreas críticas de la empresa generando graves consecuencias, presentándose una alta probabilidad de errores de digitación de datos lo que compromete y garantiza la confiabilidad de los datos almacenados.

Análisis de Riesgos Grupo de Activos

- **[SW]** Software – Aplicaciones informáticas
- **[Prp]:** Aplicación académica de educación virtual.
- **[Av]:** Antivirus.
- **[Www]**: Página Web



Análisis: A pesar de que la empresa QWERTY S.A cuenta con un software de antivirus, a este no se le realiza el seguimiento adecuado en cuanto a mantenimiento y actualizaciones, lo que puede conllevar a pérdida de información a causa de virus, botnets, ransomware, etc.

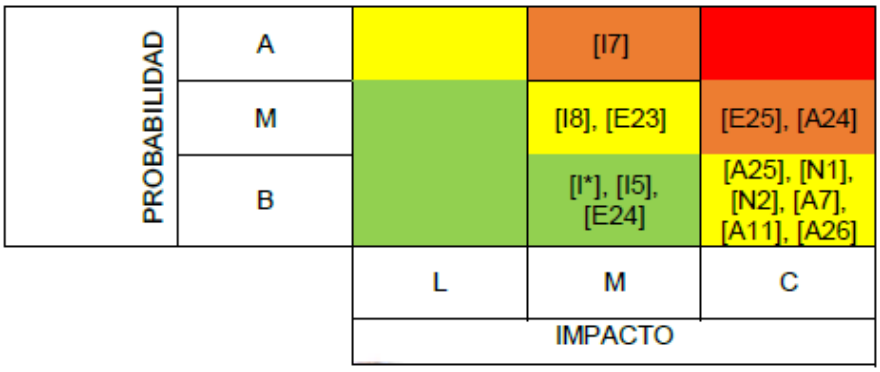
También se evidencia que al no tener un el suficiente personal de planta en el área de facturación y nomina se deba recurrir a personal en capacitación, lo que aumenta el riesgo de modificación de la información, errores del usuario y suplantaciones de identidad.

Otro punto a tener en cuenta es que por falta de mantenimientos y de actualizaciones en los sistemas, se puede aprovechar este tipo de vulnerabilidades para realizar ataques como denegación del servicio, a través de la explotación de vulnerabilidades; se están utilizando protocolo s como HTTP que no son seguros ya que se necesitan la creación de certificados de autenticación.

Análisis de Riesgos Grupo de Activos

- **[HW]** Equipamiento Informático – Servidores y dispositivos
- **[host]:** grandes equipos (servidores)

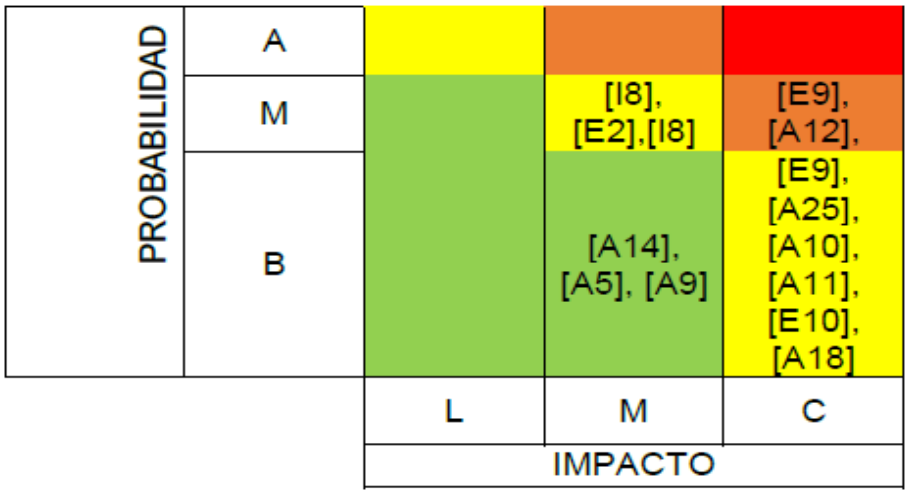
- **[pc]:** informática personal
- **[print]**: medios de impresión
- **[Switch]**: conmutadores
- **[router]**: encaminadores
- **[wap]**: punto de acceso inalámbrico



Análisis: una vulnerabilidad es la empresa QWERTY S.A presenta es que no tiene un sistema de seguridad biométrico o cámaras de monitoreo que permita tener control sobre el ingreso de sus instalaciones. Los servidores donde se alojan los servicios DHCP, HTTP y PBX no están ubicados encuentran en un espacio donde cuente con un sistema de ventilación en óptimas condiciones, teniendo en cuenta que esto puede generar un riesgo al recalentarse los equipos se puede producir un corto circuito generando incendios, perdida de equipos u otro tipo de eventos que puedan dañar los medios donde se almacena información.

Análisis de Riesgos Grupo de Activos

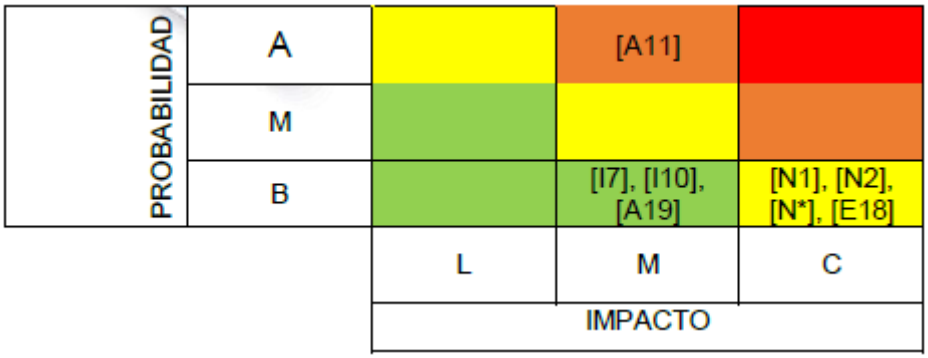
- **[COM]** Redes de Comunicaciones
- **[PSTN]:** red telefónica
- **[Wifi]:** red inalámbrica



Análisis: teniendo en cuenta que la empresa no posee ningún tipo de segmentación en su red, se puede llevar a cabo análisis de tráfico a través de programas fáciles de adquirir y gratuitos como wireshark; los computadores no cuentan con un programa que impida la instalación de este tipo de programas.

Análisis de Riesgos Grupo de Activos

- **[Media]** Soportes de información
- **[Printed]:** material impreso



Análisis: Al no tener un sistema de seguridad definido con el que se pueda llevar el control del personal que entra y sale de las instalaciones de la institución se puede presentar que personas ajenas a la misma puedan robar información, manipularla afectando la integridad y confiabilidad de la misma.

Las amenazas están clasificadas en cuatro grupos:

8.1 Caracterización de las Amenazas

- **[50]Caracterización de las amenazas**
- [N] Desastres Naturales
- [I] De origen industrial
- [E] Errores y fallos no intencionados
- [A] Ataque intencionados)[51]
-

8.2 Identificación de las amenazas[52]

El objetivo de esta tarea:

Identificar las amenazas relevantes sobre cada activo en anexo D Se evidencia la clasificación de los activos y la caracterización de las mismas realizada en la herramienta PILAR 5.2.9 [53]

---

[50] T.*, C. H. (2019). AMENAZAS INFORMÁTICAS Y. Obtenido de file:///C:/Users/JOHANAJANUS/Downloads/965-Texto%20del%20art%C3%ADculo-33752-10-20180126.pdf

[51] Cert, C. (10 de 2012). *TÍTULO: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Recuperado el 05 de 03 de 2020, de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

[52] (Excellence, ISO 27001: Amenazas y vulnerabilidades, 2015)

[53] https://www.pilar-tools.com/download/stable_es.html

8.3 Valoración de las amenazas[54]

Tabla 12 Valoración de Amenaza por Activo

IDENTIFICACIÓN DEL ACTIVO			IDENTIFICACIÓN DE RIESGO	
ITEM	**CATEGORÍA DEL ACTIVO**	**NOMBRE DEL ACTIVO**	**AMENAZA**	**ZONA DE RIESGO**
1	[HW] Equipamiento informático	Servidores: 1. servidor de impresión 2. Servidor de archivos 3. Servidor de registro y control académico 4. Servidor DHCP 5. Servidor FTP Firewall Equipos de cómputo.	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	E-Extremo
2	[HW] Equipamiento informático	Servidor DHCP Servidor HTTP PBX Servidor de impresión Servidor de nómina y facturación	[I.7] Condiciones inadecuadas de temperatura o humedad	E-Extremo
3	[SW] Software - Aplicaciones informáticas	Servidor de archivos	[A.11] Acceso no autorizado	M-Media
4	[SW] Software - Aplicaciones informáticas	Servidor de registro de nómina y facturación	[E.21] Errores de mantenimiento / actualización de programas (software)	A-Alta

[54] Magerit-versión 3.0 Metodología de análisis Y gestión de Riesgos de Sistemas de información, Libro I-Método, https://www.ccn-cert.eni.es/publico/herramientas/pilar5/magerit/c, p 40

5	[S] Servicios	Servidor DHCP	[E.2] Errores del administrador	A-Alta
6	[HW] Equipamiento informático	Firewall	[A.7] Uso no previsto	E-Extremo
7	[HW] Equipamiento informático	Equipos de cómputo: 1. gestión de sistema contable 2. Para el sistema de generación de nómina y facturación 3. Control de proveedores, órdenes de compra e inventarios.	[I.5] Avería de origen físico o lógico	M-Media
8	[HW] Equipamiento informático	Puntos de acceso alámbrico (hubo)	[A.23] Manipulación de los equipos	B-Baja
9	[HW] Equipamiento informático	Switches	[E.2] Errores del administrador	A-Alta
10	[S] Servicios	Página Web	[E.24] Caída del sistema por agotamiento de recursos	E-Extremo
11	[P] Personal	Técnicos de mantenimiento	[E.2] Errores del administrador	M-Media
12	[HW] Equipamiento informático	Teléfonos IP	[I.6] Corte del suministro eléctrico	B-Baja
13	[COM] Redes de Comunicaciones	Puntos de acceso	[I.8] Fallas servicios de comunicaciones	A-Alta
14	[L] Instalaciones	Data Center	[A.11] Acceso no autorizado	E-Extremo

15	[SW] Software - Aplicaciones informáticas	Sistema de registro y control académico	[E.1] Errores de los usuarios	A-Alta
16	[SW] Software - Aplicaciones informáticas	Servidor de archivos función almacenamiento y administración de archivos.	[E.18] Destrucción de información	M-Media
17	[SW] Software - Aplicaciones informáticas	Servidor DHCP administra en forma dinámica el direccionamiento dentro la organización.	[A.9] [Re-]encaminamiento de mensajes	A-Alta
18	[S] Servicios	Página Web	[A.22] Manipulación de programas.	M-Media
19	[HW] Equipamiento informático	Teléfonos IP	[A.14] Interceptación de información (escucha)	A-Alta
20	[HW] Equipamiento informático	Firewall	Difusión de software dañino	E-Extremo
21	[S] Servicios y [HW] Equipamiento informático	Correo electrónico Página Web Biblioteca Virtual	No hay comunicación con el Hosting.	E-Extremo
22	[HW] Equipamiento informático	Computador	Difusión de software dañino	M-Media

Fuente: Propia

8.4 Valoración de las Amenazas

Los objetivos planteados son:

- Analizar la frecuencia con la que se presentan las amenazas en lo que se refieren a los activos de la empresa.

- Qué grado de degradación se presenta a causa de una amenaza sobre el activo.[55]

Tabla 13 Degradación *de Valor la Amenaza*

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

Tabla 14 Probabilidad de ocurrencia de

CS	CASI SEGURO	A diario
MA	MUY ALTO	una Vez al año
P	POSIBLE	mensualmente
PP	POCO PROBABLE	cada Varios años
MB	MUY POCO FRECUENTE	siglos
MR	MUY POCO FRECUENTE	rara vez

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

[55]Publica, Ministerio de Hacienda y Administración. «Magerit 3.0 Proyectos de análisis de riesgos.» 10 de 2012. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html (último acceso: 05 de 03 de 2020); P-28 (127)

Tabla 15 VALORIZACIÓN DE AMENAZAS

ACTIVOS	AMENAZAS	PROBABILIDAD	[D]	[I]	[C]	[A]	[T]
SISTEMA OPERATIVO	[I.5] Avería de origen físico o lógico	MA - CS	2	5	6	6	
	[E.1] Errores de los usuarios	M - P	2				
	[E.8] Difusión de software dañino	A - MA		7		6	
	[E.20] Vulnerabilidades de los programas (software)	M - P	1				
	[E.21] Errores de mantenimiento / actualización de programas (software)	MA - CS	2		4		
	[A.7] Uso no previsto	B - PP	1		8		

ACTIVOS	AMENAZAS	PROBABILIDAD	[D]	[I]	[C]	[A]	[T]
PAGINA WEB	[E.1] Errores de los usuarios	A - P	0				
INTERNET	[A.7] Uso no previsto	B -PP	6				1
	[I.5] Avería de origen físico o lógico	A - MA	1	6	8		
	[E.20] Vulnerabilidades de los programas (software)	A - MA	1			10	8
	[E.21] Errores de mantenimiento / actualización de programas (software)	A - MA	0	7			
	[A.5] Suplantación de la identidad del	A - P	0	10	10	10	10

ACTIVOS	AMENAZAS	PROBABILIDAD	[D]	[I]	[C]	[A]	[T]
SERVIDOR DE BASE DE DATOS	[N.1] Fuego	A - MA	2	10	10	6	6
	[N.2] Daños por agua	A - P	2	10	10	0	8
	[N.*] Desastres naturales	M - P	2	10	10	3	8
	[I.3] Contaminación medioambiental	A - MA	2	6	6	6	
	[I.5] Avería de origen físico o lógico	MA - CS	4	9	9	3	1
	[I.7] Condiciones inadecuadas de temperatura o humedad	A - MA	4	9	9		
	[E.2] Errores del administrador del sistema / de la seguridad	M - P	1	8	8		
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	MA – CS	1	6	6		
	[A.11] Acceso no autorizado	A - MA	2	8	8	8	
	[A.23] Manipulación del hardware	A - MA	1		6		

ACTIVOS	AMENAZAS	PROBABILIDAD	[D]	[I]	[C]	[A]	[T]
COMPUTADORAS DE ESCRITORIO	[N.2] Daños por agua	M - P	0	10	10		9
	[N.*] Desastres naturales	M - PP	1	8			
	[I.*] Desastres industriales	M - PP	1	8			
	[I.5] Avería de origen físico o lógico	A - P	4	8	8	8	7
	[I.7] Condiciones inadecuadas de temperatura o humedad	M -P	0	6			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A - MA	3	8	8		2
	[E.24] Caída del sistema por agotamiento de recursos	A - MA	1	8	8		
	[A.6] Abuso de privilegios de acceso	A - P	1	8	7	7	4
	[A.7] Uso no previsto	A –P	1		3		1

ACTIVOS	AMENAZAS	PROBABILIDAD	[D]	[I]	[C]	[A]	[T]
MEDIOS DE IMPRESIÓN	[I.5] Avería de origen físico o lógico	MA - MA	2				1
	[I.7] Condiciones inadecuadas de temperatura o humedad	M -P	0				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	MA - CS	1				1
	[A.11] Acceso no autorizado	A - P	2				3

ACTIVOS	AMENAZAS	PROBABILIDAD	[D]	[I]	[C]	[A]	[T]
ANTIVIRUS	[E.8] Difusión de software dañino	A - MA		7	7	8	
	[E.20] Vulnerabilidades de los programas (software)	A - P	1		6		
	[E.21] Errores de mantenimiento / actualización de programas (software)	A - MA	0				

ACTIVOS	AMENAZAS	PROBABILIDAD	[D]	[I]	[C]	[A]	[T]
SWITCHES	[N.1] Fuego	M -P	1	7	7	7	4
	[N.2] Daños por agua						
	[N.*] Desastres naturales	M - PP	1	7	7	7	5
	[I.3] Contaminación medioambiental	M -PP	1	7	7		
	[I.5] Avería de origen físico o lógico	M - MA	3	7	7	7	5
	[I.7] Condiciones inadecuadas de temperatura o humedad	M - P	1	4	4	4	2
	[A.11] Acceso no autorizado	A - P	0				
	[I.8] Fallo de servicios de comunicaciones	A - MA	3	7	7	7	2
	[E.9] Errores de [re-]encaminamiento	A -P	3	7	7	7	2
	[E.15] Alteración de la información	A - P	0	10	10	10	7
	[E.19] Fugas de información	A - MA	0	10	10	10	7
	[A.7] Uso no previsto	M -P	1	7	7		1
	[A.9] [Re-]encaminamiento de mensajes	A-P	1				
	[A.10] Alteración de secuencia	A - P	1				
	[A.12] Análisis de tráfico	M - P	1				
	[A.14] Interceptación de información (escucha)	A - MA	0	7	8		5

ACTIVOS	AMENAZAS	PROBABILIDAD	[D]	[I]	[C]	[A]	[T]
EDIFICIO	[N.1] Fuego	MB - PP	1	9	9	9	9
	[N.2] Daños por agua	MB - PP	1	9	9	9	9
	[N.*.1] Tormentas	B – MB	0	9	9		9
	[N.*.4] Terremotos	MB - MR	0	9	9		6
	[N.*.9] Tsunamis	0 - 0	0				
	[N.*.11] Calor extremo	0 - 0	0				
	[I.*] Desastres industriales	MB - MR	0				
	[A.27] Ocupación enemiga	MB - MR	0		10		

ACTIVOS	AMENAZAS	PROBABILIDAD	[D]	[I]	[C]	[A]	[T]
WIFI	[I.8] Fallo de servicios de comunicaciones	MA - CS	0				2
	[E.9] Errores de [re-]encaminamiento	A - MA	0				

ACTIVOS	AMENAZAS	PROBABILIDAD	[D]	[I]	[C]	[A]	[T]
LAN	[I.8] Fallo de servicios de comunicaciones	A - MA	1				5
	[E.9] Errores de [re-]encaminamiento	MB - MR	1				5
	[E.10] Errores de secuencia	MB - MB	0				
	[A.5] Suplantación de la identidad del usuario	B - PP	1	10	10	10	5
	[A.9] [Re-]encaminamiento de mensajes	MB - MB	0				
	[A.10] Alteración de secuencia	MB - MR	1				
	[A.11] Acceso no autorizado	M - P	0				

ACTIVOS	AMENAZAS	PROBABILIDAD	[D]	[I]	[C]	[A]	[T]
CABLEADO	[I.3] Contaminación medioambiental	0 - MR					1
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB - MR					2
SISTEMA DE VIGILANCIA	[I.3] Contaminación medioambiental	MB – MR	0	5	8		
	[I.7] Condiciones inadecuadas de temperatura o humedad						
SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA	[I.3] Contaminación medioambiental	P – P	0				

ACTIVOS	AMENAZAS	PROBABILIDAD	[D]	[I]	[C]	[A]	[T]
PERSONAL	[E.28.1] Enfermedad	M - P	1				2
	[E.28.2] Huelga	MB – MR	0		3		
	[A.29] Extorsión	MB - MR	0	7	7		
	[A.30] Ingeniería social (picaresca)	0 - 0	0				

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html-p28

9. CAPITULO 3 SALVAGUARDAS

Planteamiento del SGSI del manual de seguridad de la información

9.1. Tipo de Salvaguardas

Tabla 20 Tipo de Salvaguardas

Efecto	Tipo
Preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
Acotan la degradación	[IM] minimizado ras [CR] correctivas [RC] recuperativas
Consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

***Fuente**: Magerit. V 3.0 Libro 1*

9.1.2. Salvaguardas Activos esenciales

Se entiende como activos esenciales aquellos activos que son primordiales para el buen funcionamiento de la organización, lo que quiere decir que en caso de daño o pérdida estaría afectado directamente el funcionamiento de la empresa.[56]

[56] IBID. Magerit. V 3.0 Libro II, p 7

Tabla 16 Salvaguardas Activos Esenciales

Código Activo	Activo	Código Activo	Nombre activo	Tipo de Protección	Des. Salvaguarda
[vr]	Datos vitales	[I_ Proyectos]	Protección de la información de los Proyectos	PREVENTIVAS (PR)	la Aplicación de Políticas enfocadas al manejo y uso de la información, así como a la protección de la misma y de todos los activos informáticos, limitación de acceso y asignación de privilegios
				RECUPERACIÓN (RC)	Realización de copias de seguridad Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación a los colaboradores de la importancia del buen manejo de la información

				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas
		[Info]	Información la nómina de trabajadores, Facturación, Certificados laborales, archivo de hojas de vida, Base de datos.	PREVENTIVAS (PR)	la Aplicación de Políticas enfocadas al manejo y uso de la información, así como a la protección de la misma y de todos los activos informáticos, limitación de acceso y asignación de privilegios
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.

				CONCIENCIACIÓN (AW)	Capacitación a los colaboradores de la importancia del buen manejo de la información
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas

[classified]	Datos	[E_S_Licenciador]	Ejecutable software licenciador	PREVENTIVAS (PR)	la Aplicación de Políticas enfocadas al manejo y uso de la información, así como a la protección de la misma y de todos los activos informáticos, limitación de acceso y asignación

					de privilegios
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación a los colaboradores de la importancia del buen manejo de la información
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de
		[D_ Históricos]	Historial de los Proyectos radicados		Aplicación y cumplimiento de las buenas prácticas.
				ELIMINACIÓN (EL)	Políticas para la creación,

	eliminación y manejo de contraseñas
PREVENTIVAS (PR)	Políticas de seguridad dirigidas al personal de la empresa que tiene acceso, manejo y uso de la información.
RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
CONCIENCIACIÓN (AW)	Capacitación a los colaboradores de la importancia del buen manejo de la información
ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimien

					to de las buenas prácticas.
		[Proyectos]	Documentación proyectos	PREVENTIVAS (PR)	la Aplicación de Políticas enfocadas al manejo y uso de la información, así como a la protección de la misma y de todos los activos informáticos, limitación de acceso y asignación de privilegios
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación a los colaboradores de la importancia del buen manejo de

					la información
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
[classified]		[I_Normativa]	Normatividad (Normas locales, nacionales)	PREVENTIVAS (PR)	la Aplicación de Políticas enfocadas al manejo y uso de la información, así como a la protección de la misma y de todos los activos informáticos, limitación de acceso y asignación de privilegios

				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación a los colaboradores de la importancia del buen manejo de la información
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
[per]	Datos de Carácter personal	[I_ Contabilidad]	Información financiera	PREVENTIVAS (PR)	la Aplicación de

			de la Empresa		Políticas enfocadas al manejo y uso de la información, así como a la protección de la misma y de todos los activos informáticos, limitación de acceso y asignación de privilegios
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación a los colaboradores de la importancia del buen manejo de la información

				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.

Fuente: Propia

9.1.3 Salvaguardas Datos, Información

Los datos son un bien preciado de la organización ya que son estos los que permiten la continuidad del negocio permitiendo prestar sus servicios.

La información es un activo el cual es almacenado en equipos o soportes de información; estos pueden estar almacenados en ficheros o bases de datos por lo es de vital importancia tomar medidas que permitan salvaguardar esta información.[57]

Tabla 17 Salvaguardas Datos/Información

Código Activo	Activo	Código Activo	Nombre activo	Tipo de Protección	Des. Salvaguarda
[files]	Ficheros	[A proyectos]	Archivos de proyectos	PREVENTIVAS (PR)	la Aplicación de Políticas enfocadas al manejo y uso de la información, así como a la protección de la misma y de todos los activos informáticos, limitación de acceso y

[57] IBIT. Magerit. V 3.0 Libro II, p 8

					asignación de privilegios
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación a los colaboradores de la importancia del buen manejo de la información
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas
		[A Clientes]	Archivos de Clientes	PREVENTIVAS (PR)	la Aplicación de Políticas enfocadas al manejo y uso de la información, así como a la protección de la misma y de todos los activos informáticos, limitación de acceso y asignación de privilegios

				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el Manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación a los colaboradores de la importancia del buen manejo de la información
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas
		[A Contabilidad]	Archivos financieros	PREVENTIVAS (PR)	la Aplicación de Políticas enfocadas al manejo y uso de la información, así como a la protección de la misma y de todos los activos informáticos, limitación de acceso y asignación de privilegios

				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW))	Capacitación a los colaboradores de la importancia del buen manejo de la información
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas.

		[A_ Informes y Licencias]	Archivos de Informes y licencias expedidas	PREVENTIVAS (PR)	La Aplicación de Políticas enfocadas al manejo y uso de la información, así como a la protección de la misma y de todos los activos informáticos, limitación de acceso y asignación de privilegios.
				RECUPERACIÓN (RC)	Copias de Seguridad, y Resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW))	Capacitación a los colaboradores de la importancia del buen manejo de

					la información
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas.
	Copias de Respaldo	[A_Copias de Seguridad]	Archivo de Copias de Seguridad	PREVENTIVAS (PR)	Políticas de seguridad enfocadas al personal que tiene acceso, manejo y uso de la información.

[Backus]				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación a los colaboradores de la importancia del buen manejo de la información
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas.

[Conf.]	información Configuración	[D_ Configuración ser]	configuración de servicios, servidores y equipos	PREVENTIVAS (PR)	Políticas de seguridad enfocadas al personal que tiene acceso, manejo y uso de la información.

[Conf.]	Datos de Configuración	[D_Configuracion_ser]	Datos de configuración de servidores y equipos	RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación al personal de la importancia del buen manejo de la información.
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación

					y cumplimiento de las buenas prácticas.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas.
				DETECCIÓN (DC)	Utilización de herramientas que permitan mitigar y detener todo tipo de amenazas. Como WAFS, IDS, DMZ
				CORRECCIÓN(CR)	Políticas del manejo de incidentes que permitan corregir y prevenir futuros problemas.
[int]	Datos de gestión interna	[D_GestionProy ectos]	Datos de Gestión de proyectos radicados	PREVENTIVAS (PR)	Políticas de seguridad dirigidas al personal que tiene

					acceso, manejo y uso de la información.
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el Manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación al personal de la
					Importancia del buen manejo de la información.
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				ELIMINACIÓN (EL)	Políticas para la creación,

					eliminación y manejo de contraseñas.
[password]	credenciales de autenticación	[Pass_usuarios]	Contraseñas de acceso Colaboradores	PREVENTIVAS (PR)	Políticas de seguridad enfocadas al personal que tiene acceso, manejo y uso de la información.
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW))	Capacitación al personal de la importancia del buen manejo de la información.
				ADMINISTRATIVAS (AD)	Divulgación del manual de

					seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas.
				MONITORIZACIÓN (MN)	Políticas de monitorización para la mitigación de incidentes y disminución de impacto.

Fuente: Propia

9.1.4 Salvaguardas Claves Criptográficas

Este tipo de salvaguardas se utiliza para proteger información considerada como esencial para la organización.

Este proceso se realiza por medio de la utilización de herramientas que permiten cifrar la información.

Categorización de la información según su importancia políticas de cifrado y aplicación de métodos criptográficos.

Tabla 18 Salvaguardas Claves Criptográficas

Código Activo	Activo	Código Activo	Nombre activo	Tipo de Protección	Des. Salvaguarda
[Keys]	Claves de cifrado	[CC_ Aplicaciones s_bancarias]	Claves de cifrado para aplicaciones de Bancos e información considerada sensible.	PREVENTIVAS (PR)	Categorización de la información según su importancia políticas de cifrado y aplicación de métodos criptográficos.
				MINIMIZACIÓN (IM)	Detención de los servicios en caso de presentarse un incidente, aplicación del plan de contingencia.
				CORRECTIVAS (CR)	Gestión de incidentes, Políticas del manejo de incidentes que permitan corregir y prevenir futuros problemas.
				MONITORIZACIÓN (MN)	Registro de Descargas y aplicaciones utilizadas.
				DETENCIÓN (DC)	Utilización de herramientas que permitan mitigar y detener todo tipo de

					amenazas. Como WAFS, IDS, DMZ, firewall,
[Keys]	Claves de cifrado	protección de la información	[info], [encrypt], [authentication], [com], [shared_secret], [channel], [verification], [x509], [disk]	PREVENTIVAS (PR)	Categorización de la información según su importancia políticas de cifrado y aplicación de métodos criptográficos.
				MINIMIZACIÓN (IM)	Detención de los servicios en caso de presentarse un incidente, aplicación del plan de contingencia.
				CORRECTIVAS (CR)	Gestión de incidentes, Políticas del manejo de incidentes que permitan corregir y prevenir futuros problemas.
				MONITORIZACIÓN (MN)	Registro de Descargas y aplicaciones utilizadas.

				DETENCIÓN (DC)	Utilización de herramientas que permitan mitigar y detener todo tipo de amenazas. Como WAFS, IDA, DMZ, firewall,

Fuente: Propia

9.1.5 Salvaguardas Servicios

En este tipo de salvaguardas se tienen en cuenta servicios en internet, correo electrónico accesos remotos, asignación de privilegios entre otros por lo que las salvaguardas asignadas van enfocadas a la eficacia en la utilización de estos recursos.

Tabla 19 Salvaguardas Servicios

Código Activo	Activo	Código Activo	Nombre activo	Tipo de Protección	Des. Salvaguarda
[ext]	usuarios externos	[Ext] a usuarios externos.	Servicios prestados a Colaboradores Externos.	PREVENTIVAS (PR)	Clasificación de la información considerada como confidencial. Políticas de seguridad que garanticen la confiabilidad de la información, Gestión de privilegios
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo

					de metidos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación al personal de la importancia del buen manejo de la información.
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
[int]	Interno (colaboradores de la organización)	[int] interno (a usuarios de la propia organización)	Servicios prestados a los colaboradores de la organización.	PREVENTIVAS (PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios.
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación al personal de la importancia del buen manejo de la información.
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y

					cumplimiento de las buenas prácticas.
				MONITORIZACIÓN (M	Registro y control de descargas y aplicaciones utilizadas

[www]	World wide web	[S Internet]	INTERNET	PREVENTIVAS (PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios.
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación al personal de la importancia del buen manejo de la información.
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				MONITORIZACIÓN(Mn)	Registro de aplicaciones utilizadas de y

					control de descargas.
[email]-[edi]	Intercambio Correo Electrónico	[S-Email]; [S-edi] intercambio electrónico de datos	Correo electrónico para uso de los colaboradores de la organización.	PREVENTIVAS (PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios.
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación al personal de la importancia del buen manejo de la información.
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				MONITORIZACIÓN (Mn)	Registro de aplicaciones utilizadas y control de descargas.

[file]-[ftp]	Almacenamiento y transferencia	[S_A_Base de Datos]; transferen	Base de Datos, Almacenamiento de la	PREVENTIVAS (PR)	Clasificación de la información en este caso catalogada como confidencial.

	de Ficheros	cia ficheros.	Información.		Políticas de seguridad, Gestión de privilegios.
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación al personal de la importancia del buen manejo de la información.
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				MONITORIZACIÓN (Mn)	Registro de aplicaciones utilizadas y control de descargas.
				DETECCIÓN (DC)	Utilización de herramientas que permitan mitigar y detener todo tipo de amenazas. Como WAFS, IDS, DMZ, firewall,
[ipm]-[idm]	Gestión de privilegios y de identidades	[Privilegios], [G_ gestión de identidades]	Políticas del manejo Control y asignación de privilegios de acuerdo	PREVENTIVAS (PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios.
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.

			al perfil dentro de la empresa; así como un monitoreo de acceso remoto.	CONCIENCIACIÓN (AW)	Capacitación al personal de la importancia del buen manejo de la información. Descargas.
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas, Id de usuarios.
				DETENCIÓN (DC)	Utilización de herramientas que permitan mitigar y detener todo tipo de amenazas. Como WAFS, Id, DMZ, firewall,
				MONITORIZACIÓN(Mn)	Registro de aplicaciones utilizadas y control de

[telnet]	Acceso remoto	[telnet] acceso remoto a cuenta local	Servicio de acceso remoto para los colaboradores de la organización.	PREVENTIVAS (PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios.
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.

				CONCIENCIACIÓN (AW)	Capacitación al personal de la importancia del buen manejo de la información.
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas.
[pki]-[anon]	usuarios anónimos y claves publicas	PKI - infraestructura de clave pública; anónimo (sin requerir identificación del usuario)	Administración y control de generación de claves públicas, verificación de ingreso de usuarios sin identificación.	PREVENTIVAS (PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios.
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación al personal de la importancia del buen manejo de la información.
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas, Id de usuarios.

Fuente: Propia

9.1.6 Salvaguardas Software y Aplicaciones Informáticas

Estas salvaguardas se enfatizan en proteger y analizar todas aquellas aplicaciones que transforman los datos permitiendo la explotación de la información para la prestación de los servicios.[58]

Tabla 20 [SW] Software - Aplicaciones informáticas

Código Activo	Activo	Código Activo	Nombre activo	Tipo de Protección	Des. Salvaguarda
[App]-[www]- [file]-[ts]	Servidores	[Server_App], [www] servidor de presentación; [file] servidor de ficheros, [ts] servidor de terminales	Servidor de aplicaciones y otros para dar continuidad a la operación de la empresa.	PREVENTIVAS (PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios.
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación al personal de la importancia del buen manejo de la información.

[58] IBIT., Magerit. V 3.0 Libro II, p 10

				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				MONITORIZACIÓN (Mn)	Registro de y control de descargas.
				DETENCIÓN (DC)	Utilización de herramientas que permitan mitigar y detener todo tipo de amenazas. Como WAFS, IDS, DMZ, firewall,
				CORRECTIVAS(CR)	Políticas de manejo de gestión de Incidentes.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas, Id de creación de los usuarios.

[dbms]	Gestión de bases de datos	[S_Base Datos]	Gestión de las bases de datos propiedad de la empresa.	PREVENTIVAS (PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad,

					Gestión de privilegios.
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación al personal de la importancia del buen manejo de la información.
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				MONITORIZACIÓN (Mn)	Registro de y control de descargas.
				DETENCIÓN (DC)	Utilización de herramientas que permitan mitigar y detener todo tipo de amenazas. Como WAFS, IDS, DMZ, firewall,
				CORRECTIVAS (CR)	Políticas de manejo de

					gestión de Incidentes.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas, ld de creación de los usuarios.
[office]	Ofimática	[office] ofimática	Office 2010	PREVENTIVAS(PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios.
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación al personal de la importancia del buen manejo de la información.
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación

					y cumplimiento de las buenas prácticas.
				MONITORIZACIÓN (Mn)	Registro de aplicaciones utilizadas y control de descargas.
				DETENCIÓN (DC)	Utilización de herramientas que permitan mitigar y detener todo tipo de amenazas. Como WAFS, IDS, DMZ, firewall,
				CORRECTIVAS(CR)	Políticas de manejo de gestión de Incidentes.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas, ld de creación de los usuarios.

[os]	sistema operativo	[Os]-sistema operativo	Win 10 Pro	PREVENTIVAS (PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad,

					Gestión de privilegios.
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación al personal de la importancia del buen manejo de la información.
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				MONITORIZACIÓN(Mn)	Registro de utilización de aplicaciones y control de descargas.
				DETECCIÓN(DC)	Utilización de herramientas que permitan mitigar y detener todo tipo de amenazas. Como WAFS, IDS,

					DMZ, firewall,
				CORRECTIVAS(CR)	Políticas de manejo de gestión de Incidentes.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas, Id de creación de los usuarios.
[av]	[av] antivirus	antivirus	sistema de antivirus	PREVENTIVAS (PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios.
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación al personal de la

					importancia del buen manejo de la información.
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				MONITORIZACIÓN(Mn)	Registro de y control de descargas.
				DETECCIÓN(DC)	Utilización de herramientas que permitan mitigar y detener todo tipo de amenazas. Como WAFS, IDS, DMZ, firewall,
				CORRECTIVAS(CR)	Políticas de manejo de gestión de Incidentes.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas, Id de creación de los usuarios.

Fuente: Propia

9.1.7 Salvaguardas de Equipos Informáticos

Salvaguardas aplicadas a los medios os medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.

Tabla 21 Salvaguardas de equipos informáticos.

Código Activo	Activo	Código Activo	Nombre activo	Tipo de Protección	Des. Salvaguarda
[host]	Servidores	[Aplicaciones]-[S_Database]	Servidores	PREVENTIVAS (PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios.
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación al personal de la importancia del buen manejo de la información.
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.

				MONITORIZACIÓN(Mn)	Registro de y control de descargas.
				DETECCIÓN(DC)	Utilización de herramientas que permitan mitigar y detener todo tipo de amenazas. Como WAFS, IDS, DMZ, firewall,
				CORRECTIVAS(CR)	Políticas de manejo de gestión de Incidentes.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas, Id de creación de los usuarios.

[mid]-[Pc]	Equipos que son fáciles de transportar.	[PC_trabajadores]-[PC_portatiles]	Equipos de mesa y portátiles.	PREVENTIVAS (PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios.
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el

					manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación al personal de la importancia del buen manejo de la información.
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				MONITORIZACIÓN(Mn)	Registro de y control de descargas.
				DETECCIÓN(DC)	Utilización de herramientas que permitan mitigar y detener todo tipo de amenazas. Como WAFS, IDS, DMZ, firewall,
				CORRECTIVAS(CR)	Políticas de Manejo de gestión de incidentes.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas, Id de creación

					de los usuarios.

[print]-[ipphone]-[pabx]-[scan]-[crypto]	Equipos de impresión	[E Impresoras], centralita telefónica, teléfono IP, escáneres dispositivos criptográficos	Impresoras, teléfono IP, central telefónica, escáneres, dispositivos criptográficos	PREVENTIVAS (PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios.
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación al personal de la importancia del buen manejo de la información.
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				MONITORIZACIÓN(Mn)	Registro de y control de descargas.

				DETECCIÓN(DC)	Utilización de herramientas que permitan mitigar y detener todo tipo de amenazas. Como WAFS, IDS, DMZ, firewall,
				CORRECTIVAS(CR)	Políticas de manejo de gestión de Incidentes.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas.
[bp]-[network]-[hub]-[switch]-[router]-[bridge]-[firewall][wap]-[modem]-[switch]	Equipos de red	dispositivo de frontera, soporte de la red, módems, concentradores conmutadores, en caminadores, pasarelas cortafuegos punto de acceso inalámbrico	Equipos de red	PREVENTIVAS (PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios.
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación al personal de la importancia del buen manejo de la información.

				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				MONITORIZACIÓN(Mn)	Registro de y control de descargas.
				DETECCIÓN(DC)	Utilización de herramientas que permitan mitigar y detener todo tipo de amenazas. Como WAFS, IDS, DMZ, firewall,
				CORRECTIVAS(CR)	Políticas de manejo de gestión de Incidentes.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas.

[bp]-[network]-[hub]-[switch]-[router]-[bridge]-[firewall][wap]-[modem]-[switch]	Equipos de red	dispositivo de frontera, soporte de la red, módems, concentradores conmutadores, en caminadores	Equipos de red	PREVENTIVAS (PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios.

		, pasarelas cortafuegos punto de acceso inalámbrico		RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación al personal de la importancia del buen manejo de la información.
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				MONITORIZACIÓN(Mn)	Registro de y control de descargas.
				DETECCIÓN(DC)	Utilización de herramientas que permitan mitigar y detener todo tipo de amenazas. Como WAFS, IDS, DMZ, firewall,
				CORRECTIVAS(CR)	Políticas de manejo de gestión de Incidentes.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas.

Fuente: Propia

9.1.8 Salvaguardas comunicaciones

Salvaguardas enfocadas a la protección de los equipos que ayudan al transporte de datos de un sitio a otro.

Tabla 22 Salvaguardas de Comunicaciones

Código Activo	Activo	Código Activo	Nombre activo	Tipo de Protección	Des. Salvaguarda
[wifi]	Red inalámbrica	[R_wifi]	Red Inalámbrica	PREVENTIVAS(PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios.
				MINIMIZACIÓN (IM)	Detención de los servicios en caso de presentarse un incidente, aplicación del plan de contingencia.
				CORRECTIVAS(CR)	Políticas de manejo de gestión de Incidentes.
				DISUASIÓN (DR)	Implementación de Sistemas de Seguridad, Guardias de seguridad
[LAN]	Red local	[R_Local]	LAN	PREVENTIVAS (PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad,

					Gestión de privilegios.
				MINIMIZACIÓN (IM)	Detención de los servicios en caso de presentarse un incidente, aplicación del plan de contingencia.
				CORRECTIVAS(CR)	Políticas de manejo de gestión de Incidentes.
				DISUASIÓN(DR)	Implementación de Sistemas de Seguridad, Guardias de seguridad

[Internet]	Internet	[Internet]	Servicio Internet	PREVENTIVAS (PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios.
				MINIMIZACIÓN (IM)	Detención de los servicios en caso de presentarse un incidente, aplicación del plan de contingencia.
				CORRECTIVAS(CR)	Políticas de manejo de gestión de Incidentes.
				DISUASIÓN(DR)	

					Implementación de Sistemas de Seguridad, Guardias de seguridad

Fuente: Propia

9.1.7 Salvaguardas Soportes de Información y almacenamiento electrónico

Salvaguardas para los dispositivos físicos que permiten almacenar información de manera permanente.

Tabla 23 Salvaguardas almacenamiento electrónico.

Código Activo	Activo	Código Activo	Nombre activo	Tipo de Protección	Des. Salvaguarda
[electrónica]-[disk]-[vdisk]-san]-[cd]-[USB]-[DVD]-[ic].	Medios de almacenamiento electrónico.	Electrónicos, discos normales y virtuales, almacenamiento en red; cederrón, memorias USB, DVD, tarjetas inteligentes.	Medios de almacenamiento electrónico.	PREVENTIVAS (PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios.
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación al personal de la importancia

					del buen manejo de la información.
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				MONITORIZACIÓN(Mn)	Registro de y control de descargas.
				DETECCIÓN(DC)	Utilización de herramientas que permitan mitigar y detener todo tipo de amenazas. Como WAFS, IDS, DMZ, firewall,
				CORRECTIVAS(CR)	Políticas de manejo de gestión de Incidentes.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas.

9.1.8 Salvaguardas Soportes de Información y almacenamiento no electrónico

Tabla 24 Salvaguardas de Soportes de Información _almacenamiento no electrónico

Código Activo	Activo	Código Activo	Nombre activo	Tipo de Protección	Des. Salvaguarda
[non_electronic]-[printed]-[tape]-	Medios de almacenamiento no electrónico.	Documentación de proyecto; carpetas de informes, carpetas de contabilidad, varios.	Medios de almacenamiento no electrónico.	PREVENTIVAS (PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios.
				RECUPERACIÓN (RC)	Copias de Seguridad, y resguardo de las mismas en sitios seguros, así como el manejo de métodos de cifrado.
				CONCIENCIACIÓN (AW)	Capacitación al personal de la importancia del buen manejo de la información.
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				MONITORIZACIÓN(Mn)	Registro de y control de descargas.

				DETECCIÓN(DC)	Utilización de herramientas que permitan mitigar y detener todo tipo de amenazas. Como WAFS, IDS, DMZ, firewall,
				CORRECTIVAS(CR)	Políticas de manejo de gestión de Incidentes.
				ELIMINACIÓN (EL)	Políticas para la creación, eliminación y manejo de contraseñas.

Fuente: Propia

9.1.9 Salvaguardas de Equipamiento auxiliar

Salvaguardas para otros equipos que sirven de soporte a los sistemas de información.

Tabla 25 Salvaguardas de Equipamiento auxiliar

Código Activo	Activo	Código Activo	Nombre activo	Tipo de Protección	Des. Salvaguarda
[printed]-[power]-[ups]-[gen]-[ac]-[cabling] -[wire]-[fiber]-[robot]	Sistemas de Alimentación interrumpida, fuentes de alimentación sistemas de alimentaci	Computadores, todos los activos físicos de la organización,	Ups, computadores.	PREVENTIVAS(PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios.
				CONCIENCIACIÓN (AW)	

	ón; ininterrumpida generadores eléctricos, equipos de climatización. Cableado cable eléctrico fibra óptica.				
				ADMINISTRATIVAS (AD)	Implementación de Sistemas de Seguridad, Guardias de seguridad
				DISUASIÓN (DR)	

[suplly]	Suministros esenciales	Esenciales	Suministros esenciales	PREVENTIVAS (PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios.
				CONCIENCIACIÓN (AW)	Capacitación al personal de la importancia del buen manejo de la información.

				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
				DISUASIÓN (DR)	Implementación de Sistemas de Seguridad, Guardias de seguridad
Mobiliario	M_Mobiliario	Mobiliario: Estantes, armarios, escritorios, archivadores, etc.	Mobiliario	PREVENTIVAS (PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios.
				CONCIENCIACIÓN (AW)	Capacitación al personal de la importancia del buen manejo de la información.
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimient

					o de las buenas prácticas.
				DISUASIÓN (DR)	Implementación de Sistemas de Seguridad, Guardias de seguridad

Fuente: Propia

9.1.9 Salvaguardas de Instalaciones

Tabla 26 Salvaguardas Instalaciones

Código Activo	Activo	Código Activo	Nombre activo	Tipo de Protección	Des. Salvaguarda
[building]	Edificio	[E_empresa]	Instalaciones de la empresa QWERTY S. A	DISUASIÓN (DR)	Implementación de Sistemas de Seguridad, Guardias de seguridad
				DETENCIÓN (DC)	Sistema de detección de incendios.

Fuente: Propia

9.1.10 Salvaguardas Personal

Tabla 27 Salvaguardas personal

Código Activo	Activo	Código Activo	Nombre activo	Tipo de Protección	Des. Salvaguarda
[ui]-[ue]	Usuarios internos, externos	[E personal]	Personal de recepción, área técnica, archivo y	CONCIENCIACIÓN (AW)	Capacitación al personal de la importanci

			administrativa.		a del buen manejo de la información.
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
[adm]-[op]-[com]	Administrad ores de sistemas	operadores, administradores de sistemas, administradores de comunicaciones,	Administrador de sistemas	CONCIENCIACIÓN (AW)	Capacitación al personal de la importancia del buen manejo de la información.
				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.
	subcontratas,	[E personal]	Personal, proveedore	CONCIENCIACIÓN (AW)	Capacitación al

	proveedores		s de la empresa		personal de la importancia del buen manejo de la información.
[sub]-[prov.]				ADMINISTRATIVAS (AD)	Divulgación del manual de seguridad y verificación de aplicación y cumplimiento de las buenas prácticas.

Fuente: Propia

9.2 Caracterización de las Salvaguardas [59]

En esta etapa del proceso se evaluarán las medias para minimizar el riesgo y en lo posible eliminarlo, en algunos casos estas medidas serán tecnológicas, procedimentales o físicas, para el estudio de la empresa **QWERTY S.A** se tendrán

- Etapa uno POTENCIAL
- Etapa dos SITUACIÓN ACTUAL
- Etapa tres OBJETIVO[60]

[59] España, G. d. (10 de 2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid: © Ministerio de Hacienda y Administraciones Públicas. Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libroiii-tecnicas/file.html

[60]Magerit-versión 3.0 Metodología de Análisis y Gestión De Riesgos de los Sistemas de Información Libro 1-Metodo, p 31

Hay que tener en cuenta que en lo que se refiere a seguridad informática la organización se encuentra bastante vulnerables, en ese orden de ideas es evidente que la empresa no cuenta con salvaguardas que son de importancia para su organización dentro de los puntos importantes se logró determinar que la empresa no cuenta con un plan de contingencia definido para desastres.

No tiene medidas de seguridad que garanticen la seguridad física de la empresa ya que no cuenta con sistemas de seguridad biométricos para la identificación y control del personal que laboran en la empresa como de los visitantes y clientes que se benefician de sus servicios.

Los equipos donde reportan la información importante no se encuentran en el espacio adecuado puesto que estos no cuentan con las condiciones de climatización óptimas, se debe tener en cuenta que los servidores están expuesto a todo tipo de ataques ya que estos no están en una red segmentada si no están compartiendo una misma red.

En cuento a los equipos y la protección de la red a pesar de que cuentan con un cortafuego Cisco ASA 5505 este no está configurado de la mejor manera y tampoco se lleva un registro de control de actualización del mismo.

Frente a si se lleva un control o registro de quien tiene acceso o no a los equipos la situación podemos decir que es crítica ya que debido al gran flujo de información y personas que se atiende en el área de facturación y nomina muchas veces son las personas que se encuentran en capacitación quienes brindan apoyo y soporte por lo que no se puede garantizar la integridad y

[58] IBID., Magerit. V 3.0 Libro 1, p 32

confiabilidad de la información así como que esta no se pueda filtrar perder o manipular.

9.2.1 Identificación De Las Salvaguardas

Protecciones generales H Protecciones Generales - H. IA Identificación y autenticación - H.AC Control de acceso lógico

Esta salvaguarda se seleccionó porque según los observado cualquier persona tiene acceso a los activos de la información incluso los más importantes, dejando en exposición a los mismos, entre los activos que se pueden encontrar en amenaza está la información, como lo son todo tipo de software, infraestructura tecnológica, redes y comunicaciones, el objetivo principal es proteger los pilares de la seguridad de la información: Disponibilidad, Integridad, Confidencialidad y Autenticidad.

Se busca contrarrestar las siguientes amenazas:

- Fallos provocados por los usuarios, voluntarios e involuntarios[61]
- Fallos de la persona que ejerce el rol de administrador del sistema de la seguridad en algunas ocasiones por exceso de confianza al no tomar todas las precauciones necesarias.
- Propagación de software malicioso
- Alteración de la información (Principio de Integridad)
- Fugas de información (Principio de Confidencialidad)
- Vulnerabilidad de sistemas operativos y aplicaciones
- Falta de actualizaciones de seguridad para todo tipo de software
- Suplantación del usuario (Principio de autenticidad)
- Dejar roles que pueden tener un abuso de privilegios de acceso
- Ingresos no autorizados.

[61] Turmero, P. (01 de 04 de 2019). *Administración del control de accesos, adecuado a los sistemas de información.* Obtenido de https://www.monografias.com/trabajos102/administracion-delcontrol-accesos-adecuado-sistemas-informacion/administracion-del-control-accesosadecuado-sistemas-informacion.shtml

- Suministrar información y Manipulación de hardware

9.2.1.2 Herramienta contra el código dañino [62]

La empresa **QWERTY S.A** tiene herramientas contra código dañino como lo es un antivirus, pero no ofrece todas las garantías necesarias ya que es un antivirus gratuito y no siempre está actualizado facilitando la propagación de virus, troyanos rasonware[63], etc. Por tal motivo se escogieron las siguientes salvaguardas:

- Adquirir un antivirus de pago anual por su licenciamiento el cual cuente con módulos especializados como antivirus, antispyware, antimalware.
- Se definió con el proveedor que el programa será actualizado regularmente
- A diario se actualizará automáticamente la base de datos.
- Se verifican los programas y servicios de arranque del sistema, para identificar programas innecesarios consumiendo recursos y servicios anómalos que pueden ser potenciales.

Las siguientes salvaguardas serán aplicadas al software (aplicaciones) y buscan prevenir las siguientes amenazas: Propagación de software malicioso y Aseguramiento la disponibilidad de la información.

Dentro de las salvaguardas que se tendrán en cuenta están:

- Tomar medidas de protección frente ataques de denegación de servicio (DOS)
- Procedimientos Operativos
- Tomar medidas frente a ataques originados al interior de la empresa.

---

[62] Mieres, J. (30 de 04 de 2009). Herramientas para evitar ataques. Obtenido de https://www.welivesecurity.com/wp-content/uploads/2014/01/herramientas_evitar_ataques_informaticos.pdf

[63] ES-ET. (04 de 2019). GUÍA DE RANSOMWARE. Obtenido de https://www.welivesecurity.com/wpcontent/uploads/2017/11/guia-ransomware.pdf

9.2.1.3 Protección de las aplicaciones (software)

Para este ítem se seleccionaron las siguientes salvaguardas ya que la empresa no cuenta con unos controles de seguridad definidos como son:

- Elaborar procedimientos para realizar copias de seguridad y restauración de las copias de seguridad.
- Elaborar técnicas para la manipulación adecuada de las aplicaciones
- Elaborar directrices para el cumplimiento de las responsabilidades ante las aplicaciones
- Controlar la instalación y manipulación de software por parte de los usuarios.
- Crear perfiles de seguridad únicos para garantizar solo el acceso adecuado a las aplicaciones y equipos tecnológicos, evitando propagación de software malicioso.
- Proteger los ficheros de datos de la aplicación
- Proteger los ficheros de configuración
- Controlar todas las actualizaciones del software, para asegurar que los que poseen estén desactualizados o tengan errores de configuración para de esta forma prevenir cualquier vulnerabilidad.

9.2.1.4 Protección de los equipos (hardware)

Las siguientes salvaguardas son las adecuadas para la protección de los equipos:

- Elaborar normatividad sobre el manejo correcto de los recursos tecnológicos
- Elaborar procedimientos de manejo y uso de la infraestructura tecnológica.
- Crear perfiles de seguridad únicos para minimizar amenazas como errores que se puedan presentar en la administración del sistema como lo pueden llegar a hacer uso y acceso no autorizado, asegurando de esta manera la integridad y confidencialidad de la información.

9.2.1.5 Protección de las comunicaciones

Se han elegido las siguientes salvaguardas para minimizar riesgos:

- Se deben definir roles de seguridad que sean únicos con el fin garantizar la integridad en la empresa y para hacer frente amenazas como: Manipulación de la información, Uso y acceso no autorizado, fuga de la información.
- Elaborar normatividad para el manejo correcto de los recursos de red.
- Establecer mecanismos de control de filtrado de la navegación.
- Establecer mecanismos de control para la comprobación de tráfico entrante y saliente, asegurando los servicios de red
- Establecer herramienta de inspección de contenidos en internet con filtros actualizados.
- Examinar la configuración de los navegadores para que éstos no sean manipulados por los usuarios.
- Establecer herramientas de filtrado de correo electrónico que permita identificar phishing, virus, spam.
- Deshabilitar las “cookies” en los navegadores
- Contar con registros de la navegación en internet por usuario
- Elaborar normatividad sobre el uso adecuado de los servicios Internet
- Establecer herramientas de monitoreo del trafico

Todos estos controles nos permiten mitigar las vulnerabilidades que pueden ocasionar el acceso no autorizado y ataques desde el exterior de la empresa.

9.2.1.6. Protección de los soportes de información

Para resguardad los activos informáticos se han seleccionados las siguientes salvaguardas:

- Resguardar en depósitos cerrados
- Elaborar normatividad relacionada a la defensa cifrada de los contenidos

9.2.1.7. Protección de los elementos auxiliares

Para asegurar la disponibilidad se establecerá:

- Seguir las advertencias del fabricante o proveedor para garantizar la vida del producto.
- Asegurar que los equipos se encuentren en las condiciones de temperatura adecuados para su correcto funcionamiento.

9.2.1.8. Seguridad física – Protección de las instalaciones

- Elaborar normatividad de seguridad física para las instalaciones.

- Contar con un área específica para la infraestructura tecnológica, restringiendo su acceso.
- Asegurar el perímetro de la empresa con sensores de movimiento y CCTV.

9.2.1.9. Salvaguardas relativas al personal

Se recomienda la creación de las siguientes normas de seguridad:

- Creación de normas y procedimientos para él personas directo o Subcontratado, estableciendo deberes, derechos y responsabilidades.
- Elaborar normatividad de cumplimiento obligatorio para el desempeño de las funciones de cada cargo.
- Elaborar procedimientos de seguridad, respuesta ante emergencias.

9.2.3 Valoración de las salvaguardas

Tabla 28 .Niveles de Madurez

Eficacia	Nivel	Madurez	Estado
0%	L0	inexistente	inexistente
10%	L1	inicial/ad hoc	iniciado
50%	L2	reproducible, pero intuitivo	parcialmente realizado
90%	L3	proceso definido	en funcionamiento
95%	L4	gestionado y medible	monitorizado
100%	L5	optimizado	mejora continua

Fuente: Margerit libro III

Para este Ítem se definió que hay varias salvaguardas consideradas importantes ya que en muchos casos no son consideradas ni aplicadas dentro de la organización; teniendo en cuenta que al realizar la evaluación se evidencia que los niveles de madurez no cuentan con un plan de contingencia antes posible desastres.

Otro hallazgo es que no tienen definido un plan de simulacro en caso de presentarse una eventualidad.

Otro hallazgo es que no se realizan periódicamente copias de seguridad, teniendo en cuenta que hay practicantes ayudando en el área de facturación y nomina que tienen acceso a esta base de datos y pueden manipular la información.

Los equipos Informáticos asignados a los empleados no cuentan están asegurados ni muchos menos asignados a una sola persona, por lo que se corre el riesgo de que estos puedan sustraer información confidencial y de carácter sensible para la organización.

Aunque la organización cuenta con un Firewall de calidad este no está configurado de la manera correcta para que proteja las redes de la empresa, así como no se puede garantizar el agotamiento de recursos ya que la red no está segmentada por lo que todo se encuentra en un mismo segmento.

En el Anexo E denominado Evaluación de salvaguardas se puede se realizan la Identificación de las Salvaguardas y la Valoración de las Salvaguardas.

9.3 IMPACTO

De acuerdo al estudio realizado a los activos de la empresa QWERTY S.A los que mayor riesgo presentan actualmente son:

• Los servidores donde se alojan los servicios que albergan los protocolos DHCP, HTTP y la central telefónica de la empresa el PBX se encuentran en un espacio donde no se cumplen condiciones de climatización óptimas.

Estos están expuestos a acceso no autorizado y fallas eléctricas ya que la empresa no cuenta con un diagrama donde se pueda verificar que el cableado cumple las normas mínimas de seguridad; el sistema eléctrico no cuenta con una adecuada canalización y no tienen definida la asignación de puntos de acceso a la red y tomas de la corriente por lo que se considera que no tiene establecidos estándares de políticas de control como ITILL la cual ayuda a establecer lineamientos para el control, identificación de fallas en los procesos con el fin de mejorar la eficiencia en los mismos y aplicar la mejora continua.

Al igual que otros marcos de administración de TI como COBIT la cual sirve como marco de referencia para implementar las mejores prácticas y estándares en áreas de la organización donde se necesiten mejoras o reformulaciones.

• La configuración de la red de comunicaciones se encuentra en el mismo segmento de red por lo que no se puede garantizar en buen funcionamiento de la misma ya que se generan cuellos de botella debido a la gran demanda de trabajo.

• Aunque los equipos de cómputo cuentan con sistemas de antivirus actualizado, no se hace un seguimiento a sus actualizaciones o estado.

• Debido al alto flujo de personas en la oficina de nómina y facturación, el ingreso de la información al sistema en ocasiones la diligencia personal que se encuentra realizando prácticas de otras dependencias o contratos de aprendizaje; esto implica que no se pueda garantizar la integridad, confiabilidad y disponibilidad de la información.

• Aunque existe un firewall Cisco ASA 5505, este no cuenta con reglas implementadas para la autorización o denegación de conexiones o transmisión de datos.

• Los computadores para el uso personal de los colaboradores están expuestos a ataques de malware.

• Los servidores donde está alojada la información financiera y administrativa están expuesta a acceso indebido.

• Las bases de datos están expuestas a ingreso no autorizado y agotamiento de recursos.

• El correo electrónico, El internet y el Cableado eléctrico debido a la desconexión física o lógica.

En el Anexo F, se evidencia el Impacto el cual viene definidos por el Impacto Potencial, el Impacto Residual Acumulado y la Estimación del Riesgo[64], lo que lleva a determinar el estado actual de la organización y de esta forma poder implementar el informe a las directivas.

Este informe determinara las vulnerabilidades, amenazas y riesgos de seguridad a los que está expuesta la empresa.

9.4 TOTALIDAD DE LAS VULNERABILIDADES Y AMENAZAS ENCONTRADAS[65]

CONSOLIDADO DE AMENAZAS

[64] CCN-CERT. (10 de 2012). *versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html, P -9

[65] IBIT, Capitulo 5 Amenazas, Margerit libro II

Tabla 29 Vulnerabilidades Datos/información

[D] DATOS/INFORMACIÓN

ACTIVOS	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Códigos fuentes, contratos, ficheros Copias de Seguridad de los Sistemas de Información, información online, proveedores órdenes de compra, inventarios, información de nómina facturación, información proyectos,	[A.11] Acceso no autorizado	5	100%	100 %	100%	0%	0%
	[A.15] Modificación deliberada de la información	5	0%	100 %	0%	100 %	0%
	[A.18] Destrucción de información	5	100%	0%	0%	0%	0%
	[A.19] Divulgación de información	5	0%	0%	100%	0%	0%
	[A.3] Manipulación de los registros de actividad (log)	5	0%	100 %	0%	0%	100%
	[A.5] Suplantación de la identidad del usuario	5	75%	75%	75%	0%	0%
	[A.6] Abuso de privilegios de acceso	5	100%	100 %	100%	0%	0%
	[E.1] Errores de los usuarios	50	0%	50%	0%	0%	0%
	[E.14] Escapes de información	10	0%	50%	50%	0%	0%
	[E.15] Alteración accidental de la información	5	0%	50%	0%	0%	0%

	[E.18] Destrucción de información	5	100%	0%	0%	0%	0%
	[E.19] Fugas de información	5	0%	0%	100%	0%	0%
	[E.2] Errores del administrador	5	50%	50%	75%	0%	0%
	[E.3] Errores de monitorización (log)	5	100%	0%	0%	0%	100%
	[E.4] Errores de configuración	10	20%	0%	0%	0%	0%

Fuente: Propia

[S] SERVICIOS

Tabla 29 Vulnerabilidades Servicios

ACTIVOS	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Correo electrónico, gestión de identidades, servicios internos, almacenamiento, transferencia de archivos, servicio de acceso remoto, claves públicas,	[A.10] Alteración de secuencia	5	0%	100 %	0 %	100 %	0 %
	[A.13] Repudio	5	0%	0%	0 %	50%	0 %
	[A.24] Denegación de servicio	5	100%	0%	0 %	0%	0 %
	[E.24] Caída del sistema por agotamiento de recursos2	50	100%	0%	0 %	0%	0 %

Fuente: Propia

[SW] SOFTWARE

Tabla 30 Vulnerabilidades Software

ACTIVOS	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Servidores almacenamiento y administración de archivos que se generan el interior de la organización, administración de nómina y facturación, equipos de cómputo y desarrollo	[I.5] Avería de origen físico o lógico	5	75%	75%	75%	0%	75%
	[A.22] Manipulación de programas	5	0%	50%	50%	0%	0%
	[A.7] Uso no previsto	5	75%	75%	75%	75%	0%
	[A.8] Difusión de software dañino	5	5%	5%	5%	0%	0%
	[A.9] [Re-]encaminamiento de mensajes	5	50%	0%	0%	0%	0%
	[E.1] Errores de los usuarios	10	5%	5%	5%	0%	0%
	[E.2] Errores del administrador	10	50%	50%	50%	0%	0%
	[E.20] Vulnerabilidades de los programas (software)	10	50%	75%	75%	0%	0%
	[E.8] Difusión de software dañino	8	8%	8%	8%	0%	0%

[HW] HARDWARE

Tabla 31 Vulnerabilidades Hardware

ACTIVOS	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Computadoras de escritorio que utilizan en la empresa, computadoras portátiles que utilizan en la empresa,	[I.1] Fuego	5	100%	0%	0%	0%	0%
	[A.23] Manipulación de los equipos	5	0%	75%	0%	0%	20%
	[A.25] Robo	5	100%	0%	0%	0%	0%
	[E.23] Errores de mantenimiento / actualización de	5	75%	0%	0%	0%	0%

dispositivos de respaldo, escáner, firewall, impresoras, puntos de acceso inalámbricos, routers, servidores, switch.	equipos (hardware)						
	[E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
	[I.2] Daños por agua	5	100%	0%	0%	0%	0%
	[I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
	[I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%

Fuente: Propia

[COM] COMUNICACIONES

Tabla 32 Salvaguardas Comunicaciones

ACTIVOS	AMENAZA	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Conectividad inalámbrica, internet, red de área local, PBX	[E.9] Errores de [re-]encaminamiento	5	0%	20%	0%	0%	0%
	[A.12] Análisis de tráfico	5	0%	50%	50%	0%	0%
	[A.14] Interceptación de información (escucha)	5	0%	0%	100%	0%	0%

Fuente: Propia

[AUX] EQUIPO AUXILIAR

Tabla 33 Equipamiento Auxiliar

ACTIVOS	AMENAZA	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Cableado eléctrico, fibra óptica, fuente de alimentación, rack, sistema de alimentación ininterrumpida.	[A.26] Ataque destructivo	5	100%	0%	0%	0%	0%

Fuente: Propia

[L] INSTALACIONES

Tabla 34 Instalaciones

ACTIVOS	AMENAZA	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Oficinas	[I.11] Emanaciones electromagnéticas	5	20%	0%	0%	0%	0 %

Fuente: Propia

[P] PERSONAL

Tabla 35 Personal

ACTIVOS	AMENAZA	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Área administrativa, área de desarrollo, área de soporte,	[E.28] Indisponibilidad del personal	10	50%	0%	0%	0%	0%
	[E.7] Deficiencias en la organización	5	75%	0%	0%	0%	0%

Fuente: Propia

9.5 RIESGO INHERENTE.

El riesgo inherente hace referencia que es propio en cada actividad y que no puede ser eliminado; en este caso la información, es uno de los activos que más está en riesgo ya que en muchas ocasiones el área de nómina y facturación se vale de practicantes para ayudar al ingreso de la misma.

En la siguiente tabla se puede observar el riesgo inherente de acuerdo a la categoría del riesgo, la probabilidad de que suceda y el impacto muestran resultados bastantes críticos al interior de la empresa.

Tabla 36. Riesgo Inherente de acuerdo a la categoría del riesgo, la probabilidad de que suceda y el impacto

[A.5] Suplantación de la identidad del usuario	Operativo	Posible	Crítica	Moderado
[A.6] Abuso de privilegios de acceso	Administrativo	Ocasional	Crítica	Moderado
[A.7] Uso no previsto	Estratégico	Constante	Menor	Moderado
[A.8] Difusión de software dañino	Operativo	Ocasional	Mayor	Alto
[A.9] [Re-]encaminamiento de mensajes	Estratégico	Posible	Insignificante	Bajo
[E.1] Errores de los usuarios	Operativo	Constante	Crítica	Alto
[E.14] Escapes de información	Financiero	Posible	Mayor	Alto
[E.15] Alteración accidental de la información	Operativo	Moderado	Crítica	Alto
[E.19] Fugas de información	Estratégico	Ocasional	Catastrófico	Crítica
[E.2] Errores del administrador	Estratégico	Ocasional	Crítica	Moderado

Fuente: Propia

9.6 PUNTOS CRÍTICOS DEL RIESGO INHERENTE

Tabla 37 Puntos Críticos

Nombre del Riesgo	Categoría del Riesgo	Probabilidad	Impacto	Riesgo Inherente
[A.15] Modificación deliberada de la información	Operativo	Constante	Crítica	Alto
[A.18] Destrucción de información	Operativo	Ocasional	Catastrófico	Crítica
[A.25] Robo	Estratégico	Ocasional	Mayor	Alto
[A.26] Ataque destructivo	Operativo	Posible	Catastrófico	Crítica
[A.8] Difusión de software dañino	Operativo	Ocasional	Mayor	Alto
[E.1] Errores de los usuarios	Operativo	Constante	Crítica	Alto
[E.19] Fugas de información	Estratégico	Ocasional	Catastrófico	Crítica
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Estratégico	Constante	Mayor	Crítica
[E.7] Deficiencias en la organización	Operativo	Constante	Crítica	Alto
[E.9] Errores de [re-]encaminamiento	Estratégico	Ocasional	Catastrófico	Crítica
[I.1] Fuego	Operativo	Posible	Catastrófico	Crítica
[I.5] Avería de origen físico o lógico	Financiero	Ocasional	Mayor	Alto

Fuente: Propia

Según los resultados arrojados por el estudio aplicado a los activos de la empresa QWERTY la gran mayoría de estos están en riesgo de poner la continuidad del negocio en peligro, por lo que se recomienda implementar el sistema de gestión de seguridad informática de forma urgente.

En la siguiente tabla se puede observar el plan de tratamiento de Riesgos a implementar

9.7 PLAN DE TRATAMIENTO DEL RIESGO

Tabla 38 Plan de Tratamiento de Riesgo

No.	Activos de Información	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades	Plan de Tratamiento							
					Transferir	Aceptar	Mitigar	Si el plan de tratamiento es MITIGAR, Indique el control aplicar a partir de la norma ISO 27001			Descripción de la aplicación del control	Eliminar
1	[SW] SOFTWARE	[www] Página Web	[A11] Acceso no autorizado	No se tienen copias de seguridad de las configuraciones. Pérdida de la disponibilidad del activo debido a la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.			X	A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Las políticas deben ser definidas para poder implementar un procedimiento que establezca la forma de realizar las revisiones periódicas de cuentas privilegiadas. Se tienen usuarios privilegiados para otorgar niveles de acceso.	

No.	Activos de Información	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades	Plan de Tratamiento							
					Transferir	Aceptar	Mitigar	Si el plan de tratamiento es MITIGAR, Indique el control aplicar a partir de la norma ISO 27001			Descripción de la aplicación del control	Eliminar
	[HW] EQUIPAMENTO INFORMÀTICO	2	[E1] Errores de los usuarios	Configuración inadecuada del servidor de red.			X	A13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	Se debe realizar la segmentación de la red y dejar información documentada del procedimiento para la definición de los segmentos de red y sus reglas para establecer también el procedimiento de gestión de servicios de red.	

No.	Activos de Información	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades	Plan de Tratamiento							
					Transferir		Mitigar	Si el plan de tratamiento es MITIGAR, Indique el control aplicar a partir de la norma ISO 27001			Descripción de la aplicación del control	Eliminar
3	[HW] EQUIPAMENTO INFORMÀTICO	[host] Servidor de Archivos	[E2] Errores del administrador	Configuración inadecuada en los ficheros del servidor.			X	A13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	Se cuenta con el procedimiento de transferencia de información.	
4	[HW] EQUIPAMENTO INFORMÀTICO	[host] Servidor de Registro y facturación de nómina.	[E1] Errores de los usuarios	Personal no calificado que accede al sistema			X	A12.4.2	Protección de la información de facturación y nómina.	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	No se cuenta con controles de acceso biométrico. Se deben implementar controles físicos como cámaras de seguridad, controles de acceso biométrico, CCTV, etc.	

No.	Activos de Información	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades	Plan de Tratamiento							
					Transferir	Aceptar	Mitigar	Si el plan de tratamiento es MITIGAR, Indique el control aplicar a partir de la norma ISO 27001			Descripción de la aplicación del control	Eliminar
5	[HW] EQUIPAMENTO INFORMÀTICO	[host] Servidor DHCP	[E21] Errores de mantenimiento / actualización de programas (software)	Configuración inicial inadecuada o deficiente			X	A11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	Los servidores DHCP, HTTP y PBX se encuentran en un espacio donde no se cumplen condiciones de climatización óptimas. Se deben implementar mecanismos como sensores de humedad y de calor, deshumidificadores, cables anti flama, sistemas de refrigeración certificados, entre otros. Se deben implementar controles físicos como cámaras de seguridad, controles de acceso biométrico, CCTV, etc.	

No.	Activos de Información	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades	Plan de Tratamiento							
					Transferir	Aceptar	Mitigar	Si el plan de tratamiento es MITIGAR, Indique el control aplicar a partir de la norma ISO 27001			Descripción de la aplicación del control	Eliminar
6	[HW] EQUIPAMENTO INFORMÀTICO	[firewall] Cortafuegos	[A11] Acceso no autorizado	Políticas insuficientes o inadecuadas			X	A12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	A pesar de que se cuenta con un sistema antivirus y cortafuegos, estos están mal configurados o no se les realizan las actualizaciones requeridas. Se debe implementar un procedimiento de actualización y mantenimiento de las aplicaciones que dan soporte a la seguridad.	
7	[HW] EQUIPAMENTO INFORMÀTICO	[mid] Computador	[A5] Suplantación de la identidad del usuario	Defectos de origen o fallas presentadas durante el funcionamiento del activo			X	A11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a	La empresa Qwerty no cuenta con un sistema de seguridad biométrico o de monitoreo que permita tener control sobre la zona derecha del Centro.	

No.	Activos de Información	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades	Plan de Tratamiento							
					Transferir	Aceptar	Mitigar	Si el plan de tratamiento es MITIGAR, Indique el control aplicar a partir de la norma ISO 27001			Descripción de la aplicación del control	Eliminar
										personal autorizado.	Se deben implementar controles físicos como cámaras de seguridad, controles de acceso biométrico, CCTV, etc.	
8	[COM] REDES DE COMUNICACIONES	Puntos de acceso inalámbrico (hub)	[I8] Fallo de servicios de comunicaciones	Ubicación del activo sin protección			X	A9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	La red no se encuentra Segmentada por lo que se debe realizar la adecuación de la misma y dejar información documentada del procedimiento para la definición de los segmentos de red y sus reglas.	

No.	Activos de Información	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades	Plan de Tratamiento							
					Transferir		Mitigar	Si el plan de tratamiento es MITIGAR, Indique el control aplicar a partir de la norma ISO 27001			Descripción de la aplicación del control	Eliminar
9	[COM] REDES DE COMUNICACIONES	[switch] Switches	[I8] Fallo de servicios de comunicaciones	Configuraciones insuficientes o inadecuadas			X	A9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	La red no se encuentra Segmentada por lo que se debe realizar la adecuación de la misma y dejar información documentada del procedimiento para la definición de los segmentos de red y sus reglas.	

No.	Activos de Información	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades	Plan de Tratamiento							
					Transferir		Mitigar	Si el plan de tratamiento es MITIGAR, Indique el control aplicar a partir de la norma ISO 27001			Descripción de la aplicación del control	Eliminar
10	[P] PERSONAL	[op] Técnicos de Mantenimiento	[A23] Manipulación de los equipos	Personal desactualizado en el uso de herramientas y con falta de compromiso			X	A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	En los contratos con los proveedores se cuenta con los requisitos de seguridad que deben cumplir.	

No.	Activos de Información	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades	Plan de Tratamiento							
					Transferir		Mitigar	Si el plan de tratamiento es MITIGAR, Indique el control aplicar a partir de la norma ISO 27001			Descripción de la aplicación del control	Eliminar
11	[COM] REDES DE COMUNICACIONES	[iPhone] Teléfono IP	[I8] Fallo de servicios de comunicaciones	Requerimientos mínimos de energía para su funcionamiento			X	A13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	Se debe realizar la segmentación de la red y dejar información documentada del procedimiento para la definición de los segmentos de red y sus reglas para establecer también el procedimiento de gestión de servicios de red.	

No.	Activos de Información	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades	Plan de Tratamiento							
					Transferir	Aceptar	Mitigar	Si el plan de tratamiento es MITIGAR, Indique el control aplicar a partir de la norma ISO 27001			Descripción de la aplicación del control	Eliminar
12	[HW] EQUIPAMENTO INFORMÁTICO	[com] Puntos de Acceso	[A4] Manipulación de la configuración	Puntos expuestos a desconexiones			X	A11.2.3	Seguridad en el cableado.	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	Todo el cableado del Centro se encuentra protegido y con las medidas de acuerdo a la legislación vigente.	
13	[COM] REDES DE COMUNICACIONES	[L] Data Center	[E1] Errores de los usuarios	Insuficientes o inadecuados sistemas de identificación y autorización.			X	A9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	Se tienen políticas de control de acceso a activos que contienen información crítica	

No.	Activos de Información	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades	Plan de Tratamiento							
					Transferir	Aceptar	Mitigar	Si el plan de tratamiento es MITIGAR, Indique el control aplicar a partir de la norma ISO 27001			Descripción de la aplicación del control	Eliminar
14	[D] DATOS	Sistema de Registro y control académico	[A5] Suplantación de la identidad del usuario	Personal no calificado que accede al sistema			X	A9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	El nivel de acceso está definido por política de control de acceso.	
15	[HW] EQUIPAMENTO INFORMÁTICO	[os] Windows 10 Pro	[E20] Vulnerabilidades de los programas (software)	Deficientes actualizaciones de programas ya reparados por el fabricante.			X	A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	Se deben dejar claro cuáles son los roles asignados para cada uno los integrantes del sistema	
16	**[P] PERSONAL**	[P][adm] Administrador del Sistema	[E2] Errores del administrador	Mala configuración y/o parametrización de los sistemas de información de la dependencia			X	A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de	El acceso se basa en las necesidades y políticas de control de acceso que hay definidas.	

No.	Activos de Información	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades	Plan de Tratamiento							
					Transferir	Aceptar	Mitigar	Si el plan de tratamiento es MITIGAR, Indique el control aplicar a partir de la norma ISO 27001			Descripción de la aplicación del control	Eliminar
										usuarios para todos los sistemas y servicios.		
17	**[P] PERSONAL**	[P][des] Desarrolladores	[A10] Alteración de secuencia	Errores en la programación de códigos y alteración del sistema			X	A.14.2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	Solo el personal autorizado en el área de sistemas puede hacer desarrollo de aplicaciones.	
18	**[P] PERSONAL**	[P] [op] Operadores	[A6] Abuso de privilegios de acceso	Falta de control de perfiles y permisos de usuarios. Debido al alto flujo en la oficina de Registro y Control Académico, la alimentación de la información en el sistema, en ocasiones la diligencia personal de			X	A12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	

No.	Activos de Información	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades	Plan de Tratamiento							
					Transferir	Aceptar	Mitigar	Si el plan de tratamiento es MITIGAR, Indique el control aplicar a partir de la norma ISO 27001			Descripción de la aplicación del control	Eliminar
				prácticas de otras dependencias.								
19	**[P] PERSONAL**	[P] [ue] Usuarios externos	[A11] Acceso no autorizado	Perdida de elementos físicos de las instalaciones			X	A11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	La empresa Qwerty no cuenta con un sistema de seguridad biométrico o de monitoreo que permita tener control sobre la zona derecha del Centro. Se deben implementar controles físicos como cámaras de seguridad, controles de acceso biométrico, CCTV, etc.	

No.	Activos de Información	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades	Plan de Tratamiento							
					Transferir		Mitigar	Si el plan de tratamiento es MITIGAR, Indique el control aplicar a partir de la norma ISO 27001			Descripción de la aplicación del control	Eliminar
14	[D] DATOS	Sistema de Registro y control académico	[A5] Suplantación de la identidad del usuario	Personal no calificado que accede al sistema			X	A9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	El nivel de acceso está definido por política de control de acceso.	
15	[HW] EQUIPAMENTO INFORMÀTICO	[os] Windows 10 Pro	[E20] Vulnerabilidades de los programas (software)	Deficientes actualizaciones de programas ya reparados por el fabricante.			X	A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	Se deben dejar claro cuáles son los roles asignados para cada uno los integrantes del sistema	
16	**[P] PERSONAL**	[P][adm] Administrador del Sistema	[E2] Errores del administrador	Mala configuración y/o parametrización de los sistemas de información de la dependencia			X	A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de	El acceso se basa en las necesidades y políticas de control de acceso que hay definidas.	

No.	Activos de Información	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades	Plan de Tratamiento							
					Transferir		Mitigar	Si el plan de tratamiento es MITIGAR, Indique el control aplicar a partir de la norma ISO 27001			Descripción de la aplicación del control	Eliminar
										usuarios para todos los sistemas y servicios.		
17	**[P] PERSONAL**	[P][des] Desarrolladores	[A10] Alteración de secuencia	Errores en la programación de códigos y alteración del sistema			X	A.14.2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	Solo el personal autorizado en el área de sistemas puede hacer desarrollo de aplicaciones.	
18	**[P] PERSONAL**	[P] [op] Operadores	[A6] Abuso de privilegios de acceso	Falta de control de perfiles y permisos de usuarios. Debido al alto flujo en la oficina de Registro y Control Académico, la alimentación de la información en el sistema, en ocasiones la diligencia personal de			X	A12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	

No.	Activos de Información	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades	Plan de Tratamiento							
					Transferir	Aceptar	Mitigar	Si el plan de tratamiento es MITIGAR, Indique el control aplicar a partir de la norma ISO 27001			Descripción de la aplicación del control	Eliminar
20	**[P] PERSONAL**	[P] [ui] Usuarios internos	[A11] Acceso no autorizado	Pérdida de la disponibilidad debido a equivocaciones de personas con responsabilidades de instalación y operación			X	A7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	No se cuenta con un proceso definido. Se debe definir el alcance, los objetivos y procedimientos del mismo.	
21	**[SW] SOFTWARE**	[SW] [av] Antivirus	[E21] Errores de mantenimiento / actualización de programas (software)	Aunque los equipos de cómputo cuentan con sistemas de antivirus actualizado, no se hace un seguimiento a sus actualizaciones o estado.			X	A12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Establecer un indicador para el seguimiento de la gestión de incidentes de seguridad asociados a códigos maliciosos y generar las acciones de mejora requeridas.	

Fuente: Propia

9.8 IDENTIFICACIÓN DE RIESGOS

Tabla 38 Tabla de riesgos [P] Personal

RIESGOS	CATEGORIA	VULNERABILIDAD	AMENAZAS	RECURSOS AFECTADOS	CAUSAS	CONTROLES INTERNOS	TRATAMIENTO DE LOS RIESGOS	ACCIONES
Desconocimiento de las políticas de Seguridad	Control de Información	Políticas de seguridad	Difusión de la información confidencial o hurto de la misma con fines diferentes a los establecidos	SI	Manipulación de contenidos confidenciales por terceros	PSI.	Practica de seguridad de la información	Capacitar al personal que efectúe el tratamiento de datos personales.

Fuente: Propia

Tabla 39 17 Tabla de Riesgos [D] Datos- Información

RIESGOS	CATEGORIA	VULNERABILIDAD	AMENAZAS	RECURSOS AFECTADOS	CAUSAS	CONTROLES INTERNOS	TRATAMIENTO DE LOS RIESGOS	ACCIONES
Destrucción de la información	Seguridad Lógica	Backup	Perdida de la información por falta de respaldo	Imagen institucional y toma de decisiones	Perdida de la Información	Copias de seguridad de la información.	Actividades para la ejecución de respaldos de información para prevenir la pérdida de información.	Respaldo de información
Adecuación y mantenimiento	Hardware	Instalación de UPS	Perdida de la información sin respaldo y daño a los equipos.	Retraso en los procesos	Falta de plan de mantenimiento	Perímetro de seguridad física.	Realizar un registro de los medios de almacenamiento de los datos personales	planes de recuperación de información inmediata y cubrimiento de equipos
Virus	Servicios	Instalación de Programas a todos los usuarios	Exponen el ingreso de software dañinos	Daño de la información y conectividad	Ataque a los sistemas por falta de actualización de antivirus	Controles contra el código malicioso.	Constante actualización de antivirus	Instalación de antivirus

Fuente: Propia

Tabla 39 Tabla de Riesgos Activos

RIESGOS	CATEGORIA	VULNERABILIDAD	AMENAZAS	RECURSOS AFECTADOS	CAUSAS	CONTROLES INTERNOS	TRATAMIENTO DE LOS RIESGOS	ACCIONES
Manipulación de terceros a información confidencial y privilegiada	Software	Fallas en los sistemas operativos	Perdida de programas e información valiosa, que afectan al software de facturación y contable	la Imagen Institucional de la Empresa	Mal manejo de los permisos de acceso	Privacidad y protección de informacion personal.	Realizar capacitaciones para la reducción de riesgos en cuanto a las políticas de seguridad	Capacitaciones a funcionarios de las políticas
Hurto de información	Personal	Suplantación de usuarios.	Utilización de información privilegiada para fines inadecuado	Imagen Institucional	Desconocimiento de políticas de seguridad	Seguridad de Recursos Humanos	Practica de seguridad de la información	Capacitar al personal que efectúe el tratamiento de datos personales.
Acceso no autorizado a información	Hardware	Acceso no autorizado	Manipulación de información de reserva	SI	Privilegio no adecuado en accesos	Política de control de accesos.	Practica de seguridad de la información	Capacitar al personal que efectúe el tratamiento de datos personales.
Errores de Usuarios	Servidor de Correo	Contraseñas fáciles de descifrar	El poco cambio de contraseñas y la utilización de algunas sin seguridad que se conviertan en fáciles de adivinar	SI	Usurpación de Usuario para el acceso a información	Política de uso de los controles criptográficos.	Protección mediante medios criptográficos e impedir el acceso a usuarios no autorizados	Técnicas y recomendaciones para el manejo de contraseñas
Mantenimiento de Software	Equipos Activos	Configuración de Servidores	Penetración a los sistemas desde cualquier ventana abierta	Desastre por la alteración de la información	Manipulación de contenidos confidenciales por terceros	Adquisición, desarrollo y mantenimiento de Sistemas.	Actualizar las medidas de seguridad y garantizar los SI	Mantenimiento continuo y actualizaciones de software autorizados

Fuente: Propia

10. CAPITULO V APLICABILIDAD DE LA SOA

POLÍTICAS DE SEGURIDAD DE LOS ACTIVOS DE LA INFORMACIÓN Y ALCANCES DEL SGSI PARA LA EMPRESA QWERTY S.A

Se elabora el Manual de Políticas y Procedimientos de Seguridad de la Información (PSI) definidas por la Empresa Qwerty S.A, para la elaboración de este se toman como base las leyes y demás regulaciones aplicables, la norma ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013.

Las políticas incluidas en este manual son parte fundamental para la implementación del sistema de gestión de seguridad de la información de la Empresa QWERTY S.A, cuyo único fin serán los controles, procedimientos y directrices que permitirán la aplicación de buenas normas y prácticas para el manejo de los activos informáticos de la organización.

Este manual contendrá todos los aspectos administrativos y normas que deben cumplir todos los directivos, colaboradores y clientes de la organización; Anexo D

De común acuerdo se plantea la prohibición de la reproducción total o parcial de los documentos clasificados como confidenciales, así como de asumir la responsabilidad por el deterioro ocasionado adrede de los mecanismos informáticos, software, cableado de datos, suministro eléctrico, o cualquier activo de la empresa.

Se implementarán políticas y lineamientos de seguridad que obliguen a mantener la información de en un entorno seguro. Las cuáles será difundida a todos los directivos y colaboradores d la empresa; así como los Planes de Continuidad del Negocio y Recuperación de Desastres.

10.1. DOMINIOS Y CONTROLES APLICABLES

Se establecen los siguientes controles de seguridad establecidos en la metodología de análisis y evaluación de riesgos MAGERIT y los controles del Anexo A del estándar ISO/IEC 27001:2013 (ver Anexo A de este documento)

Seleccionar los controles dentro del proceso de implementación del Sistema de Gestión de Seguridad de la Información – SGSI

Referencias normativas: La ISO/IEC 27000, es referenciada parcial o totalmente en el documento y es indispensable para su aplicación.

Términos y definiciones: Para los propósitos de este documento se aplican los términos y definiciones presentados en la norma ISO/IEC 27000.

En Anexo G se describen los Dominios y controles de acuerdo a los activos informáticos existentes en la empresa.

En el Anexo H: Requisitos de la Norma ISO/IEC 27001:2013 se exponen los resultados del nivel de conformidad y cumplimiento de estos requisitos.

En el anexo K se establece el manual de normas y políticas de Seguridad para la empresa Qwerty S. A

10.2. LISTAS DE CHEQUEO

Se elabora las listas de chequeo para verificación del cumplimiento de los controles de acuerdo a la norma ISO/IEC 27001:2013 para determinar el nivel de cumplimiento; El cual se encontrará en el Anexo I

10.3 ANÁLISIS DE LA SITUACIÓN ACTUAL Y RECOMENDACIÓN DE APLICABILIDAD ISO/IEC 27001:2013

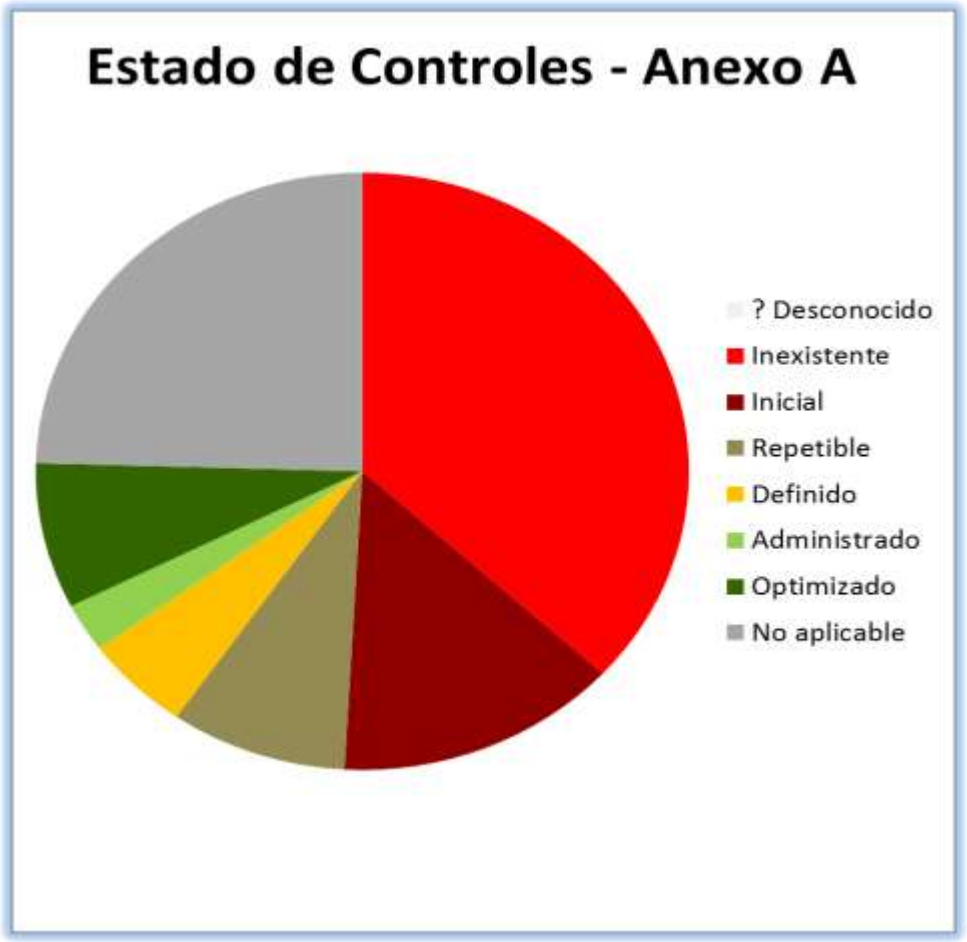
Se relacionan los controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001:2013 que contiene controles para la implementación de medidas de protección de la información; Así como en la siguiente tabla se relaciones los niveles de aplicabilidad de la norma ISO Anexo J

Tabla 40 niveles de aplicabilidad de la norma ISO

Estado	Significado	Proporción de requerimientos SGSI	Proporción de Controles de Seguridad de la Información
? Desconocido	No ha sido verificado	100%	0%
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	0%	37%
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.	0%	14%
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	0%	9%
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.	0%	5%
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	0%	3%
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	0%	8%
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.	0%	25%
	Total	100%	100%

Fuente: Propia.

Tabla 41 Estado de Aplicabilidad de los controles



Fuente: Propia

10.4 DECLARACIÓN DE APLICABILIDAD SOA

La Declaración de Aplicabilidad, (SoA), es un componente fundamental para la implementación del Modelo de Seguridad y Privacidad de la Información.

En el Anexo H definido como Declaración De Aplicabilidad SOA presenta la declaración los controles que son relevantes para el SGSI de la Empresa Qwerty S.A.

11. RESULTADOS E IMPACTOS ESPERADOS

RESULTADO/PRODUCTO ESPERADO	INDICADOR	BENEFICIARIO
Entrega del diseño del plan de seguridad de la información para la empresa QWERTY S.A. que contenga políticas y recomendaciones a aplicar en cada una de sus dependencias.	1	**QWERTY S. A**
Entrega del documento que permita definir la Aplicabilidad de las metas de la organización con su software (SoA[66]) la cual permitirá llevar el control de las medidas a implementar.	1	**QWERTY S. A**

[66] Data, P. (02 de 02 de 2020). Arquitectura Orientada a Servicios (SOA). Obtenido de https://www.powerdata.es/soa

12. CRONOGRAMA

1. CRONOGRAMA DE ACTIVIDADES				
ACTIVIDAD	MES 1	MES 2	MES 3	MES 4
levantamiento de la información				
Identificación de los activos y Dependencias entre ellos.				
Verificación del estado de los activos				
Identificación de las amenazas				
Valoración de las amenazas				
Identificación de las salvaguardas pertinentes				
Valoración de las salvaguardas				
Evaluación del impacto de las amenazas sobre los activos				
Estimación del riesgo				

12.1. RECURSOS NECESARIOS

1. RECURSOS NECESARIO		
RECURSO	**DESCRIPCIÓN**	**PRESUPUESTO**
Equipo Humano	Profesional en el área de la Ingeniería de sistemas con una experiencia mínima de 2 años.	$4.000.0000
Equipos y Software	• Características destacadas • Procesador: Intel Core i7 • Memoria RAM: 12GB • Tamaño de la pantalla: 15.6 pulgadas • Disco duro HDD: No aplica • Unidad de estado sólido SSD: • Herramientas a utilizar	$3.799.000

	PILAR[67] • DVWA[68], Logwatch[69], Nessus[70] Sqlmap[71] y WebScarab[72] las cuales son herramientas de código libre.	
Viajes y Salidas de Campo	Realizar las visitas a cada una de las oficinas con las que cuenta la empresa.	$200.000
Materiales y suministros	Fotocopias e impresiones entre otros.	$ 100.000
Recursos	Los recursos utilizados serán propios.	
TOTAL$ $ 8.099000		

[67] EAR. (06 de 02 de 2019). Obtenido de https://www.ar-tools.com/es/tools/pilar_basic/v74/download.html

[68] DVWA. (02 de 02 de 2020). Damn Vulnerable Web Application. Obtenido de http://www.dvwa.co.uk/

[69] Tezer, P. O. (23 de 11 de 2017). Cómo instalar y usar Logwatch Log Analyzer and Reporter en un VPS. Obtenido de https://www.digitalocean.com/community/tutorials/how-to-install-and-use-logwatch-log-analyzer-and-reporter-on-a-vps

[70] Tenable. (02 de 02 de 2020). Nessus. Obtenido de https://www.tenable.com/downloads/nessu

[71] Bernardo Damele AG, M. S. (02 de 02 de 2020). SQLmap Herramienta automática de inyección de SQL y toma de base de datos. Obtenido de http://sqlmap.org/

[72] ReYDeS. (16 de 09 de 2014). Proyecto OWASP WebScarab. Obtenido de http://www.reydes.com/d/?q=Proyecto_OWASP_WebScarab

13. CONCLUSIONES Y RECOMENDACIONES

13.1 CONCLUSIONES

1. La finalidad de este proyecto aplicado es determinar la importancia de establecer normas y políticas que determinen el correcto manejo de la seguridad informática para ayudar a la organización a cumplir sus metas dentro de estas darle continuidad al negocio y garantizar la integridad, confiabilidad e integridad de la información.

2. Con la elaboración de este proyecto aplicado se lograron identificar los principales inconvenientes de seguridad que presenta la empresa Qwerty S: A se utilizaron herramientas como la observación directa, la aplicación de un cuestionario donde aplicado a algunos colaboradores de la organización ayudo a determinar qué áreas de la empresa se encuentran más en riesgo de presentar algún tipo de vulnerabilidad; este proceso sirvió para poder tener mayor claridad para poder definir el punto de partida para el desarrollo del SGSI.

3. Con la utilización de la metodología MAGERIT se lograron establecer los indicadores de gestión lo cual sirvió para identificar las amenazas a las que pueden estar expuestos los activos de la información de la organización Qwerty S. A se llegó a esta conclusión mediante el desarrollo y aplicación del análisis de riesgo cualitativo esto se hizo mediante un análisis de riesgos cualitativo, permitiendo identificar el nivel de madurez en la seguridad con el que contaba la empresa.

4. Con los datos recogidos mediante el tipo de análisis se permitió identificar las amenazas y así mismo poder recomendar los controles y políticas aplicar los cuales serán consignados en el planteamiento del SGSI para la empresa.

5. El análisis de riesgos, la definición de políticas de seguridad, la declaración de aplicabilidad y aplicabilidad de los controles conforma el diseño del SGSI bajo la norma ISO/IEC 27001 tiene su único fin en garantizar la integridad, disponibilidad y confiabilidad de la información.; La aplicación de (SoA) permitirá crear un sistema escalable para impulsar el rendimiento, reducción de costos de TI y mejorar los procesos de la organización

13.2 RECOMENDACIONES

1. De acuerdo al estudio realizado se recomienda la difusión de plan de seguridad cuyo único fin será la capacitación de las buenas prácticas y normas del manejo de la información.
2. Se debe garantizar el compromiso por cada uno de los Directivos y colaboradores con la difusión y la aplicación del manual de Seguridad de la información.
3. Áreas como las donde se alojan los equipos deben contar con las adecuaciones de acuerdos a las normas establecidas por la ley y las entidades encargadas de supervisar.
4. Se sugiere realizar verificaciones periódicas que garanticen que todos los sistemas operativos estén actualizados.
5. Se recomienda implementar un sistema biométrico que permita tener control sobre la entrada y salida de personal a la organización.
6. Después de realizar las respectivas verificaciones a los activos informáticos se les recomienda a los directivos de la empresa la aplicación de controles y normas las cuales se pueden encontrar en el Anexo G.
7. Se recomienda implementar un sistema que permita llevar el control de los clientes,
8. Es importante que se segmente la red no solo para que esta sea más segura si no para que tenga un mejor funcionamiento y no se congestione.

REFERENCIAS BIBLIOGRÁFICAS

AEC, A. E. Seguridad De La Información. {En línea} {06 de Abril del 2019} Disponible en: https://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

27000, I. Sistema de Gestión de la Seguridad de la Información, {en línea} {02 de Febrero del 2020}. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

27000. es, W. Sistema de Gestión de la Seguridad de la Información {en línea} {15 de Marzo del 2019}. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

AEC.ES. Seguridad De La Información. {En línea} {03 de febrero del 2020}. Disponible en: https://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

ALA/CFT, S. N. Ley Estatutaria 1266 de 2008. {En línea} {31 de Diciembre del 2008}. Disponible en: https://www.uiaf.gov.co/sistema_nacional_ala_cft/normatividad_sistema/leyes/ley_estatutaria_1266_2008

ALESSA, A. SGSI. {En línea} {09 de Junio del 2017} Disponible en: https://es.slideshare.net/AlessaParedes/sgsi-76786549

AMÉRICA ECONOMIA.COM. La fuga de información es una de las razones por las que las empresas pierden más dinero. {En línea}{27 de Julio del 2014}. Disponible en : https://mba.americaeconomia.com/articulos/notas/la-fuga-de-informacion-es-una-de-las-razones-por-las-que-las-empresas-pierden-mas-di

BERNARDO DAMELE Ag, M. S. SQLmap Herramienta automática de inyección de SQL y toma de base de datos. {En línea} {02 de Febrero del 2020}. Disponible en: http://sqlmap.org/

CAMELO, L. Marco legal de Seguridad de la Información en Colombia. {En línea} {23 de Febrero del 2010} Disponible en: http://seguridadinformacioncolombia.blogspot.com/2010/02/marco-legal-de-seguridad-de-la.html

CASTILLO, I. M. Política General De Seguridad De La Información {En línea}. {03 de Marzo del 2019}. Disponible en: http://artesaniasdecolombia.com.co/PortalAC/images/politica-seguridad-informacion-proteccion-datos-personales.pdf

CCN, c. Margerit - Libro II - Catálogo de Elementos. {En línea} {10 de Octubre del 2012}. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

CCN-CERT. Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información {En línea} {10 de Octubre del 2012}. Disponible en https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html

CCN, Cert.Cni. ANEXO I Categorías de los sistemas ANEXO I Categorías de los sistemas\2. Dimensiones de la seguridad. {En línea} {19 de Abril del 2020}. Disponible en: https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1068

CERT, C, TÍTULO: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. {En línea} {05 de Marzo del 2020}, Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

COLOMBIA, C. ley de Delitos Informáticos en Colombia {En línea} {. 05 de Enero del 2009}. Disponible en: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

COLOMBIA, E. C. LEY 1273 DE 2009. {En línea} {05 de Enero del 2009}. Disponible en: http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf

COLOMBIA, E. C. LEY 603 DE 2000. {En línea} {27 de Julio del 2000}. Disponible en: http://derechodeautor.gov.co/documents/10181/182597/603.pdf/42c15f4a-afe5-4339-97ca-a61026450307

COMUNICACIÓN, I. N. Inteco. Obtenido de Implantación de un SGSI en la empresa: {En línea} {16 de Marzo del 2019} Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

COURSEWARE. Marco Contextual.{ en línea } { 27 de Agosto 2019 } Disponible en : Obtenido de http://courseware.url.edu.gt/Facultades/Facultad%20de%20Ciencias%20Econ%C3%B3micas/T%C3%A9cnicas%20B%C3%A1sicas%20de%20Investigaci%C3%B3n/Segundo%20ciclo%202010/Marco%20de%20referencia/01%20Marco%20de%20referencia/marco_contextual.html

CUERVO, C. y. Política de seguridad del SGSI. {En línea} {04 Abril del 2019}. Disponible en:

https://www.caroycuervo.gov.co/recursos/6.1.POLITICA_DE_SEGURIDAD_ICC_0.pdf

D. ESPINOSA, J. M... Gestión Del Riesgo En La Seguridad De La Información Con. {En Línea} {12 de Diciembre del 2014} Disponible en: http://web.usbmed.edu.co/usbmed/fing/v5n2/pdf/Articulo_Gestion_Riesgo_Seguridad_Informacion

DATA, Arquitectura Orientada a Servicios (SOA). {En línea} {02 de Febrero del 2020}. Obtenido de https://www.powerdata.es/soa

DUOC, B. {En línea} {2018}. Definición. Disponible en: uoc.cl/biblioteca/crai/definicion-y-proposito-de-la-investigacion-aplicada

DUOC, B. {En línea} {2018}. Definición. Disponible en: uoc.cl/biblioteca/crai/definicion-y-proposito-de-la-investigacion-aplicada

DUOC, B. {En línea} {2018}. Definición. Disponible en: uoc.cl/biblioteca/crai/definicion-y-proposito-de-la-investigacion-aplicada

DVWA. Damn Vulnerable Web Application {En Línea} {02 de Febrero del 2020}. Disponible en: http://www.dvwa.co.uk/

DVWA. {En línea} {06 de febrero del 2020} Disponible en: http://www.dvwa.co.uk/

EAR. {En línea} {06 de Febrero de 2019}. Disponible en: https://www.ar-tools.com/es/tools/pilar_basic/v74/download.html

ES-ET. Guía De Ransomware. {En línea} {Abril del 2019} Disponible en: https://www.welivesecurity.com/wp-content/uploads/2017/11/guia-ransomware.pdf

ESPAÑA, G. d. . MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid: © Ministerio de Hacienda y Administraciones Públicas. {En línea} {Abril del 2019}. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html

ESTEBAN, E. J. SGSI: Gestión y Seguridad. {En línea} {Abril del 2007} disponible en: http://secugest.blogspot.com/2007/04/sgsi-gestion-y-seguridad.html

EXCELLENCE, I. ISO 27001: Amenazas y vulnerabilidades {En Línea} {06 de Abril del 2015} Disponible en: https://www.pmg-ssi.com/2015/04/iso-27001-amenazas-y-vulnerabilidades/

EXCELLENCE, I. ISO 27001 Como implantar políticas de Gestión de un Sistema de Gestión de Seguridad de la Información. {En línea} {07 de Marzo del 2014}.

Disponible en: https://www.pmg-ssi.com/2014/03/iso-27001-chttps://www.pmg-ssi.com/2014/03/iso-27001-como-implantar-politicas-de-gestion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/

FORTINET. Más del 80 por ciento de las compañías en Colombia son vulnerables a ataques informáticos. {En línea} {Noviembre del 2018} Disponible en: https://www.gartner.com/teamsiteanalytics/servePDF?g=/imagesrv/media-products/pdf/fortinet/fortinet-1-5VG5OU4.pdf

FORTINET. Más del 80 por ciento de las compañías en Colombia son vulnerables a ataques informáticos. {En línea} {Noviembre del 2018} https://www.gartner.com/teamsiteanalytics/servePDF?g=/imagesrv/media-products/pdf/fortinet/fortinet-1-5VG5OU4.pdf

GONZÁLEZ, S. F. Diagnostico Y Actualización Del Sistema De Gestión De. {En línea} {28 de 05 de 2013}. Disponible en: http://repository.ucatolica.edu.co:8080/bitstream/10983/866/2/Mantenimiento%20y%20Actualizacion%20de%20un%20sistema%20de%20gestion%20de%20seguridad%20de%20la%20informacion%20para%20ventas.pdf

GONZÁLEZ, W, Técnicas De Recolección De Datos. {En línea}. {13 de 05 de 2009}.Disponible en: http://recodatos.blogspot.com/2009/05/tecnicas-de-recoleccion-de-datos.html

HUERTA, A. Análisis de riesgos con MAGERIT en el ENS (II). {En línea}{26 de 04 de 2012}. Obtenido de https://www.securityartwork.es/2012/04/26/analisis-de-riesgos-con-magerit-en-el-ens-ii/

HUERTA, A. {En línea} {26 de Abril del 2012}. https://www.securityartwork.es/2012/04/26/analisis-de-riesgos-con-magerit-en-el-ens-ii/. Obtenido de https://www.securityartwork.es/2012/04/26/analisis-de-riesgos-con-magerit-en-el-ens-ii/

INFORMÁTICAS, O. p. (s.f.). Metodología Para La Gestión De La Seguridad Informática. {En línea} {Agosto del 2013} Disponible en: https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf

INGENIEROS, A. E. (Encuesta-Global-Seguridad-Informacion-2018-19 {En línea} 19 de Febrero del 2020). Disponible en: https://es.scribd.com/document/423161641/Ey-Encuesta-Global-Seguridad-Informacion-2018-19

ISO, N. ISO 27001 Gestión De La Seguridad De La Información {En línea} {02 de Febrero de 2020}. Obtenido de https://www.normas-iso.com/iso-27001/

ISO, S. Sistemas de Gestión de Riesgos y Seguridad. {En línea} { Marzo del 2019). Disponible en: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

LEBET, G. Técnicas De Recolección De Datos. {En línea} {Abril del 2019} https://gabriellebet.files.wordpress.com/2013/01/tecnicas-de-recoleccic3b3n4.pdf

LIZARAZO, L. K. Planteamiento De Un SGSI Basado En La Norma ISO 27001:{} En línea} (27 de 08 de 2016). {27 de 08 de 2016}. Disponible en: http://polux.unipiloto.edu.co:8080/00003412.pdf

M. AMUTIO, J. C. Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libros I, II y III - . Madrid, España: Eds., MAGERIT {En línea} {2012} Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789

MARQUES, L. Mapa de los ataques cibernéticos en Latinoamérica. {En línea} {11 de Febrero del 2019). Disponible en : http://blog.f-secure.com/es/mapa-de-los-ataques-ciberneticos-en-latinoamerica-2018/

MIERES, J. Herramientas para evitar ataques. {En línea} {30 de Abril del 2009}. Obtenido de https://www.welivesecurity.com/wp-content/uploads/2014/01/herramientas_evitar_ataques_informaticos.pdf

MINISTERIO DE HACIENDA Y ADMINISTRACIÓN PÚBLICA. {En Línea} {2020} Obtenido de Margerit -V3 libro 1: https://es.scribd.com/document/337634447/2012-Magerit-v3-libro1-metodo-es-NIPO-630-12-171-8-pdf

MINTIC. Ley 1273 de 2009. {En línea} {04 de Enero del 2009} Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

MINTIC, Ley 1341 de 2009. {En línea}. {29 de Julio del 2009}. Disponible en https://www.mintic.gov.co/portal/604/w3-article-3707.html

MONTES, S. {En línea} {08 de 09 de 2018} Disponible en. https://www.larepublica.co/internet-economy/empresas-colombianas-solo-invierten-20-de-presupuesto-en-ciberseguridad-2768645

MONTES, S. Empresas colombianas solo invierten 20% de presupuesto en ciberseguridad {En Línea} {08 de Septiembre de 2018}. Disponible en: https://www.larepublica.co/internet-economy/empresas-colombianas-solo-invierten-20-de-presupuesto-en-ciberseguridad-2768645

NEGOCIOS, T. p. Qué es un ciberataque y qué tipos existen. {En línea} {03 de 02 de 2020}. Disponible en:

https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-un-ciberataque-y-que-tipos-existen/

PAREDES, M. A. Sistema de Gestión de la Seguridad de la información SGSI {En línea}. {09 de 06 de 2017} Disponible en: https://es.slideshare.net/AlessaParedes/sgsi-76786549

PROFITLINE. Actualmente Como se encuentra Colombia en Seguridad Informática. {En línea} {26 de Febrero del 2019}. Disponible en: https://profitline.com.co/actualmente-como-se-encuentra-colombia-en-seguridad-informatica/

PUBLICA, M. d. Magerit 3.0 Proyectos de análisis de riesgos {En línea} {05 de Marzo del 2020}, Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

REPUBLICA, C. d. LEY ESTATUTARIA 1581 DE 2012. {En línea} {17 de 10 de 2012} Disponible en: https://www.sisben.gov.co/Documents/Informaci%C3%B3n/Leyes/LEY%20TRATAMIENTO%20DE%20DATOS%20-%20LEY%201581%20DE%202012.pdf

REYDES. Proyecto OWASP WebScarab. {En línea} {16 de 09 de 2014}. Disponible en: http://www.reydes.com/d/?q=Proyecto_OWASP_WebScarab

T.*, C. H. AMENAZAS INFORMÁTICAS Y. [En línea} {2019}. Disponible en: file:///C:/Users/JOHANAJANUS/Downloads/965-Texto%20del%20art%C3%ADculo-3375-2-10-20180126.pdf

TECNOLOGY, e. s. La Seguridad Como Rehén Tendencias 2017 {En línea} {Diciembre del 2017} Disponible en: https://www.welivesecurity.com/wp-content/uploads/2016/12/Tendencias-2017-eset.pdf

TECNOSFERA. En un segundo se presentan en promedio 9 infecciones con malware. {En línea} (15 de Agosto del 2018). Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/aumento-de-ataques-ciberneticos-en-america-latina-en-2018-256078

TENABLE. Nessus. {En Línea} {02 de Febrero del 2020). Disponible en: https://www.tenable.com/downloads/nessus

TEZER, P. O. Cómo instalar y usar Logwatch Log Analyzer and Reporter en un VPS. {En línea} {23 de 11 de 2017}. Disponible en: https://www.digitalocean.com/community/tutorials/how-to-install-and-use-logwatch-log-analyzer-and-reporter-on-a-vps

TOOLS, Pear / Pilar. {En linea}. {02 de Febrero de 2020}. Disponible en: https://www.ar-tools.com/es/index.html

TURMERO, P. Administración del control de accesos, adecuado a los sistemas de información. {En línea} {01 de Abril del 2019}. Disponible en: https://www.monografias.com/trabajos102/administracion-del-control-accesos-adecuado-sistemas-informacion/administracion-del-control-accesos-adecuado-sistemas-informacion.shtml

UNAD. (Propuesta para el desarrollo de la alternativa de grado. Universidad Nacional Abierta y a distancia Obtenido de Escenario2_EnfoqueDirectivoAdministrativo.pdf

VALDEZ DELGADO, Andrés Israel Manual de procedimientos e higiene. {En línea} {2015}. Disponible en: https://dspace.ups.edu.ec/bitstream/123456789/10260/1/UPS-GT001284.pdf

ANEXO A ISO 27001:2013

1. OBJETIVO DE CONTROL Y CONTROLES

Anexo Norma ISO27001:2013

ISO27001:2013 - ANEXO A		
OBJETIVOS DE CONTROL Y CONTROLES		
A.5. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN.	A.5.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información.	A.5.1.1. Políticas para la Seguridad de la Información. Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.
	Objetivo. Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.	A.5.1.2. Revisión de las Políticas para seguridad de la información. Las Políticas para Seguridad de la Información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas.
A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	A.6.1. Organización Interna.	A.6.1.1. Seguridad de la Información Roles y Responsabilidades. Se deben definir y asignar todas las responsabilidades de la seguridad de la información.

	Objetivo. Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación del SGSI.	A.6.1.2. Separación de deberes. Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.
		A.6.1.3. Contacto con las autoridades. Se debe mantener contactos apropiados con las autoridades pertinentes.
		A.6.1.4. Contacto con grupos de interés especial. Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
		A.6.1.5. Seguridad de la información en Gestión de Proyectos. La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de proyecto,
	A.6.2. Dispositivos Móviles y Teletrabajo.	A.6.2.1. Política para dispositivos móviles. Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
	Objetivo. Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.	A.6.2.2. Teletrabajo. Se deben implementar una política y medidas de seguridad de soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.

A.7. SEGURIDAD DE LOS RECURSOS HUMANOS.	A.7.1. Antes de asumir el empleo.	A.7.1.1. Selección. Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
	Objetivo. Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	A.7.1.2. Términos y condiciones del empleo. Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información.
	A.7.2. Durante la ejecución del empleo.	A.7.2.1. Responsabilidades de la Dirección. La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.
	Objetivo. Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.	A.7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información. Todos los empleados de la organización y donde sea pertinente, los contratistas deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
		A.7.2.3. Proceso disciplinario. Se debe contar con un proceso formal y comunicado para emprender acciones contra

		empleados que hayan cometido una violación a la seguridad de la información.
	A.7.3. Terminación y cambio de empleo.	A.7.3.1. Terminación o cambio de responsabilidades de empleo. Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.
	Objetivo. Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.	
A.8. GESTIÓN DE ACTIVOS.	A.8.1. Responsabilidad por los Activos.	A.8.1.1. Inventario de Activos. Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
	Objetivo. Identificar los activos organizacionales y definir las responsabilidades de protección apropiada.	A.8.1.2. Propiedad de los activos. Los activos mantenidos en el inventario deben ser propios.
		A.8.1.3. Uso Aceptable de los Activos. Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
		A.8.1.4. Devolución de Activos. Todos los empleados y usuarios de partes externas deben devolver todos los activos de la

		organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
	A.8.2. Clasificación de la Información.	A.8.2.1. Clasificación de la Información. La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
	Objetivo. Asegurar que la organización recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.	A.8.2.2. Etiquetado de la Información. Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
		A.8.2.3. Manejo de Activos. Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
	A.8.3. Manejo de medios de soporte.	A.8.3.1. Gestión de medios de Soporte Removibles. Se deben implementar procedimientos para la gestión de medios de soporte removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
	Objetivo. Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.	A.8.3.2. Disposición de los medios de soporte. Se debe disponer en forma segura de los medios de soporte cuando ya no se requieran, utilizando procedimientos formales.
		A.8.3.3. Transferencia de medios de soporte físicos. Los medios que contienen información se deben proteger

		contra acceso no autorizado, uso indebido o corrupción durante el transporte.
A.9. CONTROL DE ACCESO.	A.9.1. Requisitos del Negocio para Control de Acceso.	A.9.1.1. Política de Control de Acceso. Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
	Objetivo. Limitar el acceso a información y a instalaciones de procesamiento de información.	A.9.1.2. Acceso a redes y a servicios en red. Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
	A.9.2. Gestión de Acceso de Usuarios.	A.9.2.1. Registro y cancelación del registro de usuarios. Se debe implementar un proceso formal de registro y de cancelación del registro para posibilitar la asignación de los derechos de acceso.
	Objetivo. Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.	A.9.2.2. Suministro de acceso de usuarios. Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
		A.9.2.3. Gestión de derechos de acceso privilegiado. Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
		A.9.2.4. Gestión de información de autenticación secreta de usuarios. La asignación de información de autenticación secreta se debe controlar por medio de un procedimiento de gestión formal.

		A.9.2.5. Revisión de los derechos de acceso de usuarios. Los dueños de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.
		A.9.2.6. Cancelación o ajuste de los derechos de acceso. Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procedimiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
	A.9.3. Responsabilidades de los usuarios.	A.9.3.1. Uso de información secreta. Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
	Objetivo. Hacer que los usuarios rindan cuentas por la custodia de su información de autenticación.	
	A.9.4. Control de Acceso a Sistemas y Aplicaciones.	A.9.4.1. Restricción de acceso a información. El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
	Objetivo. Prevenir el uso no autorizado de sistemas y aplicaciones.	A.9.4.2. Procedimiento de Conexión Segura. Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de conexión segura.

		A.9.4.3. Sistema de Gestión de Contraseñas. Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.
		A.9.4.4. Uso de programas utilitarios privilegiados. Se debe restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.
		A.9.4.5. Control de Acceso a Códigos Fuente de Programas. Se debe restringir el acceso a códigos fuente de programas.
A.10. CRIPTOGRAFÍA	A.10.1. Controles Criptográficos.	A.10.1.1. Política sobre el uso de controles Criptográficos. Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para protección de información.
	Objetivo. Asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información.	A.10.1.2. Gestión de Claves. Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas, durante todo su ciclo de vida.
A.11. SEGURIDAD FÍSICA Y AMBIENTAL.	A.11.1. Áreas Seguras.	A.11.1.1. Perímetro de Seguridad Física. Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.

	Objetivo. Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	A.11.1.2. Controles Físicos de entrada. Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
		A.11.1.3. Seguridad de oficinas, salones e instalaciones. Se debe diseñar y aplicar seguridad física a oficinas, salones e instalaciones.
		A.11.1.4. Protección contra amenazas externas y ambientales. Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
		A.11.1.5. Trabajo en áreas seguras. Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
		A.11.1.6. Áreas de despacho y carga. Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
	A.11.2. Equipos.	A.11.2.1. Ubicación y protección de los equipos. Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros

		ambientales y las posibilidades de acceso no autorizado.
	Objetivo. Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	A.11.2.2. Servicios Públicos de soporte. Los equipos se deben proteger de fallas de potencia y otras interrupciones causadas por fallas en los servicios públicos de soporte.
		A.11.2.3. Seguridad del cableado. El cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptaciones, interferencia o daño.
		A.11.2.4. Mantenimiento de equipos. Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
		A.11.2.5. Retiro de Activos. Los equipos, información o software no se deben retirar de su sitio sin autorización previa.
		A.11.2.6. Seguridad de equipos y activos fuera del predio. Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de los predios de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichos predios.
		A.11.2.7. Disposición segura o reutilización de equipos. Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software con licencia haya

		sido retirado o sobre escrito en forma segura antes de su disposición o reusó.
		A.11.2.8. Equipos sin supervisión de los usuarios. Los usuarios deben asegurarse de que el equipo sin supervisión tenga la protección apropiada.
		A.11.2.9. Política de escritorio limpio y pantalla limpia. Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.
A.12. SEGURIDAD DE LAS OPERACIONES.	A.12.1. Procedimientos operacionales y responsabilidades.	A.12.1.1. Procedimientos de operación documentadas. Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan.
	Objetivo. Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.	A.12.1.2. Gestión de Cambios. Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
		A.12.1.3. Gestión de Capacidad. Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.

		A.12.1.4. Separación de los ambientes de desarrollo, ensayo y operación. Se deben separar los ambientes de desarrollo, ensayo y operativos, para reducir los riesgos de acceso o cambios no autorizados al ambiente operacional.
	A.12.2. Protección contra códigos maliciosos.	A.12.2.1. Controles contra códigos maliciosos. Se deben implementar controles de detección, de prevención y de recuperación, combinarlos con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
	Objetivo. Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.	
	A.12.3. Copias de Respaldo.	A.12.3.1. Copias de respaldo de la información. Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
	Objetivo. Proteger contra la pérdida de datos.	
	A.12.4. Registro y Seguimiento.	A.12.4.1. Registro de eventos. Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepcionales, fallas y eventos de seguridad de la información.
	Objetivo. Registrar eventos y generar evidencia.	A.12.4.2. Protección de la información de registro. Las instalaciones y la información de

		registro se deben proteger contra alteración y acceso no autorizado.
		A.12.4.3. Registros del administrador y del operador. Las actividades del administrador y del operador del sistema se deben registrar y los registros se deben proteger y revisar con regularidad.
		A.12.4.4. Sincronización de relojes. Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.
	A.12.5. Control de Software Operacional.	A.12.5.1. Instalación de software en sistemas operativos. Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
	Objetivo. Asegurarse de la integridad de los sistemas operacionales.	
	A.12.6. Gestión de vulnerabilidad técnica.	A.12.6.1. Gestión de las vulnerabilidades técnicas. Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
	Objetivo. Prevenir el aprovechamiento de las vulnerabilidades técnicas.	A.12.6.2. Restricciones sobre la instalación de Software. Se debe establecer e implementar el reglamento de instalación de

		software por parte de los usuarios.
	A.12.7. Consideraciones sobre auditorías de sistemas de información.	A.12.7.1. Controles sobre auditorías de Sistemas de Información. Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
	Objetivo. Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.	
A.13. SEGURIDAD DE LAS COMUNICACIONES.	A.13.1. Gestión de Seguridad de Redes.	A.13.1.1. Controles de redes. Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
	Objetivo. Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.	A.13.1.2. Seguridad de los servicios de red. Se deben identificar los mecanismos de seguridad y los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.
		A.13.1.3. Separación en las redes. Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
	A.13.2. Transferencia de información.	A.13.2.1. Políticas y procedimientos de transferencia de información. Se debe contar con políticas, procedimientos y

		controles de transferencia formales para proteger la transferencia de información, mediante el uso de todo tipo de instalaciones de comunicaciones.
	Objetivo. Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	A.13.2.2. Acuerdos sobre transferencia de información. Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.
		A.13.2.3. Mensajes electrónicos. Se debe proteger apropiadamente la información incluida en los mensajes electrónicos.
		A.13.2.4. Acuerdos de confidencialidad o de no divulgación. Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.	A.14.1. Requisitos de seguridad de los sistemas de información.	A.14.1.1. Análisis y especificación de requisitos de seguridad de la información. Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.

	Objetivo. Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que prestan servicios sobre redes públicas.	A.14.1.2. Seguridad de servicios de las aplicaciones en redes públicas. La información involucrada en servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
		A.14.1.3. Protección de transacciones de servicios de aplicaciones. La información involucrada en las transacciones de servicios de aplicaciones se debe proteger para prevenir la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes. La divulgación no autorizada y la duplicación o reproducción de mensajes no autorizados.
	A.14.2. Seguridad en los procesos de desarrollo y de soporte.	A.14.2.1. Política de desarrollo seguro. Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas a los desarrollos dentro de la organización.
	Objetivo. Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	A.14.2.2. Procedimiento de control de cambios en sistemas. Los cambios a los sistemas dentro del ciclo de vida de desarrollo de software y de sistemas a los desarrollos dentro de la organización.

		A.14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones. Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y poner a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad organizacionales.
		A.14.2.4. Restricciones sobre los cambios de paquetes de software. Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
		A.14.2.5. Principios de construcción de sistemas de seguros. Se deben establecer, documentar y mantener principios para la organización de sistemas seguros, y aplicarlos a cualquier trabajo de implementación de sistemas de información.
		A.14.2.6. Ambiente de desarrollo seguro. Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
		A.14.2.7. Desarrollo contratado externamente. La organización debe supervisar y hacer seguimiento de la actividad de

		desarrollo de sistemas subcontratados.
		A.14.2.8. Pruebas de seguridad de sistemas. Durante el desarrollo se deben llevar a cabo ensayos de funcionalidad de la seguridad.
		A.14.2.9. Pruebas de aceptación de sistemas. Para los sistemas de información nuevos, actualizaciones y nuevas versiones se deben establecer programas de ensayo y criterios relacionados.
	A.14.3. Datos de ensayo.	A.14.3.1. Protección de datos de ensayo. Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.
	Objetivo. Asegurar la protección de los datos usados para ensayos.	
A.15. RELACIONES CON LOS PROVEEDORES.	A.15.1. Seguridad de la información en las relaciones con los proveedores.	A.15.1.1. Política de seguridad de la información para las relaciones con proveedores. Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.
	Objetivo. Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.	A.15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores. Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que puedan tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.

		A.15.1.3. Cadena de suministro de tecnología de información y comunicación. Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
	A.15.2. Gestión de la prestación de servicios de proveedores.	A.15.2.1. Seguimiento y revisión de los servicios de los proveedores. Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
	Objetivo. Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.	A.15.2.2. Gestión de cambios a los servicios de los proveedores. Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de los riesgos.
A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.	A.16.1. Gestión de incidentes y mejoras en la seguridad de la información.	A.16.1.1. Responsabilidades y procedimientos. Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

	Objetivo. Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidad.	A.16.1.2. Informe de eventos de seguridad de la información. Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.
		A.16.1.3. Informe de debilidades de seguridad de la información. Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que se observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
		A.16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.
		A.16.1.5. Respuesta a incidentes de seguridad de la información. Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
		A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información. El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.

		A.16.1.7. Recolección de evidencia. La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO.	A.17.1. Continuidad de seguridad de la información	A.17.1.1. Planificación de la continuidad de la seguridad de la información. La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres.
	Objetivo. La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.	A.17.1.2. Implementación de la continuidad de la seguridad de la información. La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
		A.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información. La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que los válidos y eficaces durante situaciones adversas.
	A.17.2. Redundancia	A.17.2.1. Disponibilidad de instalaciones de procesamiento de información. Las instalaciones de procesamiento de información se deben

		implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
	Objetivo. Asegurarse de la disponibilidad de instalaciones de procesamiento de información.	
A.18. CUMPLIMIENTO.	A.18.1. Cumplimiento de requisitos legales y contractuales.	A.18.1.1. Identificación de los requisitos de legislación y contractuales aplicables. Se deben identificar, documentar y mantener actualizados explícitamente todos los requisitos legislativos estatutarios, de reglamentación y contractuales pertinentes, y el enfoque de la organización para cada sistema de información y para la organización.
	Objetivo. Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.	A.18.1.2. Derechos de Propiedad Intelectual. Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software licenciados.
		A.18.1.3. Protección de registros. Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
		A.18.1.4. Privacidad y protección de la información identificable personalmente. Se deben asegurar la privacidad y

		la protección de la información identificable personalmente, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.
		A.18.1.5. Reglamentación de Controles Criptográficos. Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos
	A.18.2. Revisiones de seguridad de la información	A.18.2.1. Revisión independiente de la seguridad de la información. El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, la política, los procesos y los procedimientos para seguridad de la información se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
	Objetivo. Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimiento organizacionales.	A.18.2.2. Cumplimiento con las políticas y normas de seguridad. Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad.

		A.18.2.3. Revisión del Cumplimiento Técnico. Los Sistemas de información se deben revisar con regularidad para determinar el cumplimiento con las políticas y normas de seguridad de la información.[73]

Anexo B

Anexo 1 Cuestionario

2. Cuestionario Aplicado

Cuestionario

Fecha: _____

Nombre: _____

Cargo: _____

Las preguntas del siguiente formulario son de tipo cerrado y selección múltiple

Información General

1. ¿Sabe usted si la empresa implementa medidas de seguridad de la información?

a. si

b. no

c. c no sabe

2. sabe que prepuesto es destinado para temas de seguridad en la empresa.

[73] STANDARDIZATION., I. O. (2013). Information Technology. Security Techniques. Information Security Management Systems. Requirements. Geneva, ISO P-15 Obtenido de http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

a. Entre 1.000.000 a 10.000.000

b. 11.000.000 a 20.000.000

c. 21.000.000 a 30.000.000

d. Más de 30 millones de pesos

e. No sabe.

3. Cuáles son los activos más importantes de la empresa

a. Si

b. No

c. No sabe

4. Tiene conocimiento si la organización toma medidas de seguridad ante amenazas de terceros.

a. Si

b. No

c. No sabe

5. Sabe que versión de sistemas operativos tienen instalados los equipos.

a. Si

b. No

c. No sabe

6. Tiene conocimiento de si los programas instalados como antivirus y licencias de funcionamiento están al día.

a. Si

b. No

c. No sabe

d.

7. Tiene conocimientos si se tiene aplicadas políticas de seguridad.

a. Si

b. No

c. No sabe

8. Tiene conocimiento si se realizan copias de seguridad.

a. Si

b. No

c. No sabe

9. Se restringe los accesos a páginas como a las redes sociales YouTube, Amazon, Netflix entre otras.

a. Si

b. No

c. No se

10. Se cuentan con manuales e instructivos de procedimientos

a. Si

b. No

c. No sabe

11. El personal de la organización se encuentra debidamente identificado.

a. Si

b. No

c. No sabe

12. sabe si laguna vez se han reportado incidentes de seguridad.

a. Si

b. No

c. No sabe

13. Tiene conocimiento sobre las funciones y políticas asignadas a su cargo

a. Si

b. No

c. No sabe

14. ¿Sabe usted si se cuentan con políticas sobre el manejo y cambio de usuarios y contraseñas de acceso al sistema?

a. Si

b. No

c. No sabe

ANEXO C

3. CARGOS Y FUNCIONES DEL ÁREA INFORMÁTICA

Anexo 2 Cuestionario Aplicado

Brinda soporte al área encargada de la generación de usuarios y contraseñas.

Verifica que el departamento de generar el proceso de nómina y facturación pueda cumplir con las tareas asignadas como la generación de recibos de pagos, creación, almacenamiento de archivos, generación de los certificados laborales.

Desde la dependencia de Sistemas, la asistencia que ofrece se divide así:

Asistencia para directivos, administrativos y operativos:

Apoya el servicio de correo electrónico institucional: servicio que está contratado con Google, este servicio busca

- Comunicación con otros miembros de la entidad
- Compartir archivos
- Recibir comunicados oficiales
- Brindar espacio de almacenamiento ilimitado
- Dar prioridad a las actividades propuestas por el desarrollo académico del programa

Apoyo en la gestión y mantenimiento de activos informáticos: servicio que cumple la función de mantener en optimo desempeño servicios tecnológicos como:

- Equipos de cómputo de escritorio, móviles y servidores, televisores, video proyectores
- Software operativo y aplicativo
- Servicio de Internet
- Todo el equipamiento que se requiera para ayudar a dar cumplimiento al objeto social.

Apoyo en la gestión de usuarios y contraseñas: Servicio que se enfoca en la gestión de usuarios y contraseñas usadas en las diferentes aplicaciones enfocadas en apoyar el desarrollo académico de la comunidad educativa:

- Correo electrónico
- Sistema de gestión de calidad

Apoyo a la dependencia de nómina y facturación: En la dependencia de nómina y facturación se desarrollan las siguientes tareas:

- Generación de nómina de trabajadores
- Generación de recibos de pago
- Creación, alimentación y custodia de Hojas de vida
- Control del seguimiento al talento humano
- Generación certificados laborales y relacionados con el modelo de negocio

ANEXO D

4. LA CLASIFICACIÓN DE LOS ACTIVOS Y LA CARACTERIZACIÓN

Anexo D la clasificación de los activos y la caracterización

CLASIFICACION ACTIVO	ACTIVOS	AMENAZAS POR ACTIVOS
	COMPUTADOR PERSONAL	[A.6] Abuso de privilegios de acceso
		[A.7] Uso no previsto
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)
		[E.24] Caída del sistema por agotamiento de recursos
		[I.*] Desastres industriales
		[I.5] Avería de origen físico o lógico
		[I.7] Condiciones inadecuadas de temperatura o humedad
		[N.*] Desastres naturales
		[N.2] Daños por agua
		[A.10] Alteración de secuencia
		[A.11] Acceso no autorizado
		[A.12] Análisis de tráfico

Equipamiento Hardware	Equipo de comunicaciones	[A.14] Interceptación de información (escucha)
		[A.5] Suplantación de la identidad del usuario
		[A.7] Uso no previsto
		[A.9] [Re-]encaminamiento de mensajes
		[E.1] Errores de los usuarios
		[E.10] Errores de secuencia
		[E.15] Alteración de la información
		[E.19] Fugas de información
		[E.9] Errores de [re-]encaminamiento
		[I.3] Contaminación medioambiental
		[I.5] Avería de origen físico o lógico
		[I.7] Condiciones inadecuadas de temperatura o humedad
		[I.8] Fallo de servicios de comunicaciones
		[N.*] Desastres naturales
		[N.1] Fuego
		[N.2] Daños por agua
	Activos de Respaldo	[A.11] Acceso no autorizado
		[A.15] Modificación de la información
		[A.19] Revelación de información
		[E.15] Alteración de la información
		[E.19] Fugas de información
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)
		[I.5] Avería de origen físico o lógico
		[I.7] Condiciones inadecuadas de temperatura o humedad
	Servidores	[A.11] Acceso no autorizado
		[A.23] Manipulación del hardware
		[E.2] Errores del administrador del sistema / de la seguridad
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)
		[I.3] Contaminación medioambiental
		[I.5] Avería de origen físico o lógico
		[I.7] Condiciones inadecuadas de temperatura o humedad
		[N.*] Desastres naturales
		[N.1] Fuego
		[N.2] Daños por agua

Equipamiento Software	Almacenamiento Base de Datos	[A.10] Alteración de secuencia
		[A.11] Acceso no autorizado
		[A.5] Suplantación de la identidad del usuario
		[A.9] [Re-]encaminamiento de mensajes
		[E.10] Errores de secuencia
		[E.9] Errores de [re-]encaminamiento
Equipamiento de software		[I.8] Fallo de servicios de comunicaciones
	Correo Electronico	[A.10] Alteración de secuencia
		[A.11] Acceso no autorizado
		[A.5] Suplantación de la identidad del usuario
		[A.9] [Re-]encaminamiento de mensajes
		[E.10] Errores de secuencia
		[E.9] Errores de [re-]encaminamiento
		[I.8] Fallo de servicios de comunicaciones
	Internet	[A.5] Suplantación de la identidad del usuario
		[A.7] Uso no previsto
		[E.20] Vulnerabilidades de los programas (software)
		[E.21] Errores de mantenimiento / actualización de
		I.5] Avería de origen físico o lógico
	Sistemas Financieros contables y Administrativos	[A.7] Uso no previsto
		[A.8] Difusión de software dañino
		[E.1] Errores de los usuarios
		[E.20] Vulnerabilidades de los programas (software)
		[E.21] Errores de mantenimiento / actualización de programas (software)
		[E.8] Difusión de software dañino
		[I.5] Avería de origen físico o lógico
	Virtualización	[A.10] Alteración de secuencia
		[A.11] Acceso no autorizado
		[A.5] Suplantación de la identidad del usuario
		[A.9] [Re-]encaminamiento de mensajes
		[E.10] Errores de secuencia
		[E.9] Errores de [re-]encaminamiento
		[I.8] Fallo de servicios de comunicaciones

Equipamiento Auxiliar	Cableado	[A.6] Abuso de privilegios de acceso
		[A.7] Uso no previsto
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)
		[E.24] Caída del sistema por agotamiento de recursos
		[I.*] Desastres industriales
		[I.3] Contaminación medioambiental
		[I.5] Avería de origen físico o lógico
		[I.7] Condiciones inadecuadas de temperatura o humedad
		[N.*] Desastres naturales
		[N.2] Daños por agua
	Equipo de Climatizacion	[A.6] Abuso de privilegios de acceso
		[A.7] Uso no previsto
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)
		[E.24] Caída del sistema por agotamiento de recursos

Equipamiento Auxiliar		[I.*] Desastres industriales
		[I.3] Contaminación medioambiental
		[I.5] Avería de origen físico o lógico
		[I.7] Condiciones inadecuadas de temperatura o humedad
		[N.*] Desastres naturales
		[N.2] Daños por agua
	Generadores Eléctricos	[A.6] Abuso de privilegios de acceso
		[A.7] Uso no previsto
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)
		[E.24] Caída del sistema por agotamiento de recursos
		[I.*] Desastres industriales
		[I.3] Contaminación medioambiental
		[I.5] Avería de origen físico o lógico
		[I.7] Condiciones inadecuadas de temperatura o humedad
		[N.*] Desastres naturales
		[N.2] Daños por agua
	UPS	[A.11] Acceso no autorizado
		[A.23] Manipulación del hardware
		[E.2] Errores del administrador del sistema / de la seguridad
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)
		[I.3] Contaminación medioambiental
		[I.5] Avería de origen físico o lógico
		[I.7] Condiciones inadecuadas de temperatura o humedad
		[N.*] Desastres naturales
		[N.1] Fuego
		[N.2] Daños por agua

Instalaciones	Centro de Datos	[A.27] Ocupación enemiga
		[I.*] Desastres industriales
		[N.*.1] Tormentas
		[N.*.11] Calor extremo
		[N.*.4] Terremotos
		[N.*.9] Tsunamis
		[N.2] Daños por agua
		[N.1] Fuego
	Cuarto de Equipos	[A.27] Ocupación enemiga
		[I.*] Desastres industriales
		[N.*.1] Tormentas
		[N.*.11] Calor extremo
		[N.*.4] Terremotos
		[N.*.9] Tsunamis
		[N.2] Daños por agua
		[N.1] Fuego
Area Personal	Equipos Administradores	[A.29] Extorsión
		[A.30] Ingeniería social (picaresca)
		[E.28.1] Enfermedad
		[E.28.2] Huelga
	Equipos Area de Desarrollo	[A.29] Extorsión
		[A.30] Ingeniería social (picaresca)
		[E.28.1] Enfermedad
		[E.28.2] Huelga
	Equipos Técnico	[A.29] Extorsión
		[A.30] Ingeniería social (picaresca)
		[E.28.1] Enfermedad

Tabla 14 Identificación de Amenazas

Identificación de Amenazas a cada uno de los activos

Fuente: realizado en PILAR 5.2.9

ANEXO E

5. EVALUACIÓN DE SALVAGUARDAS

Anexo E Evaluación de Salvaguardas

Riesgos	Salvaguardas	Actual	Objetivo
Incendio, inundaciones Terremoto	Instalación de sistemas contra incendio	L3	L4
	Instalación de alarmas contra incendio	L3	L4
	Uso y mantenimiento de extintores	L4	L5
	Desarrollo de plan de emergencia ante incendios	L2	L3
	Desarrollo de plan de contingencia ante desastres	L0	L3
	Realizar simulacros de forma periódica	L0	L3
	Almacenar las cintas de respaldo en otra oficina	L3	L3
Falla de generador eléctrico	Mantenimiento semanal de generador eléctrico	L4	L5
Falla de equipos de climatización	Mantenimiento de equipos de climatización	L4	L5
	Adquirir nuevos equipos de climatización	L1	L3
Agotamiento de recursos	Mantenimiento preventivo de servidores y robot de cinta	L3	L4
	Revisión de directiva de copias de seguridad de forma regular	L0	L3
	Monitoreo de recursos de los equipos críticos	L3	L4

Desconexión Física o lógica	Asegurar los equipos de comunicaciones y servidores en armarios cerrados	L1	L3
Robo	Uso de cables de seguridad para computadores de personal y portátiles	L0	L3
Virus	Instalación de antivirus en servidores	L3	L4
	Instalación de antivirus en equipos de personal	L4	L4
	Actualizar periódicamente las firmas del antivirus	L4	L4
Malware	Instalación de antimalware en servidores	L0	L3
	Instalación de antimalware en equipos de personal	L0	L3
Errores de configuración	Realizar pruebas de actualizaciones previo a la instalación	L1	L3
	Pruebas periódicas del cortafuegos	L0	L3
Acceso no autorizado	Establecer controles de acceso físico	L3	L4
	Analizar directivas de cortafuegos con regularidad	L1	L3
	Implementación de sistema de detección de intrusos	L0	L3
	Asignar cuentas para la administración de sistemas	L1	L3
	Utilizar autenticación multifactor para conexión remota	L0	L3
	Implementar control de cuarentena en VPN	L0	L3
	Implementar directivas de contraseñas complejas	L2	L4
	Implementar controles avanzados de gestión de cuentas	L2	L4
Fuga de información	Implementar cifrado de datos	L2	L3
	Contratar personal responsable de la seguridad	L0	L4
	Solicitar historial de personal antes de ser contratado	L2	L3
	Dar charlas al personal referente a la seguridad	L1	L3

Tabla 1 Evaluación de Salvaguardas

Anexo 3 Impacto

6. IMPACTO

6.1. IMPACTO POTENCIAL

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

Impacto Residual Acumulado.

El impacto acumulado se calcula con los datos de impacto acumulado sobre un activo y salvaguardas apropiadas para las amenazas sobre dicho activo.

6.2 ESTIMACIÓN DEL RIESGO

6.2.1. Riesgo Potencial. Es al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener la probabilidad de ocurrencia. Los riesgos se muestran con la siguiente escala según su valor:

6.2.2. Riesgo Residual Es al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como eficacia de las salvaguardas actualmente desplegadas.

6.2.3. Riesgo Residual Acumulado. La estimación de riesgo residual acumulado nos indica la medida que las amenazas que afectan a los activos de orden superior que dependen de dicho activo.

Posteriormente se debe hacer una descripción del área informática o departamento de sistemas identificando los activos informáticos, los procesos que se realiza dentro del área y los servicios que presta a las demás áreas de la organización.

Finalmente se debe determinar las vulnerabilidades, amenazas y riesgos de seguridad del área informática o departamento de sistemas en cada uno de los activos informáticos categorizados de acuerdo al activo donde se presentan (talento humano, hardware, seguridad física, redes de datos, sistemas operativos,

bases de datos, seguridad lógica, entre otros) y se debe entregar un cuadro con las categorías de los activos, las vulnerabilidades, amenazas de seguridad encontrados en dicha organización.[74]

escalas		
impacto	probabilidad	riesgo
MA: muy alto	**MA:** prácticamente seguro	**MA:** crítico
A: alto	**A:** probable	**A:** importante
M: medio	**M:** posible	**M:** apreciable
B: bajo	**B:** poco probable	**B:** bajo
MB: muy bajo	**MB:** muy raro	**MB:** despreciable

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html P-28

Los impactos que se muestran con la siguiente escala según su valor:

[5]: Muy alto
[4]: Alto
[3]: medio
[2]: Bajo
[1]: Muy bajo

Los riesgos se muestran con la siguiente escala según su valor:

[5]: Crítico
[4]: Importante
[3]: Apreciable
[2]: Bajo
[1]: Despreciable

[74] ccn-cert.cni. (10 de 2012). *Margerti-libro I .* Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Activos	Amenaza	Impacto Potencial	Impacto Actual	Impacto Objetivo	Riesgo Potencial	Riesgo Actual
Servidores	Incendio	5	4	3	4	4
	Terremoto	5	4	3	4	4
	Robo	4	3	2	4	4
	Acceso no autorizado	4	3	2	5	5
	Falla de generador eléctrico	4	3	2	5	5
Equipos de comunicaciones	Incendio	5	3	3	4	4
	Terremoto	5	3	3	4	4
	Robo	4	4	3	4	4
	Acceso no autorizado	4	4	2	5	5
	Desconexión Física o lógica	4	4	2	5	4
	Falla de generador eléctrico	4	4	2	5	4
Robot de cintas	Incendio	5	3	3	4	4
	Terremoto	5	3	3	4	4
	Robo	4	3	2	5	4
Computador de personal	Incendio	5	4	3	4	4
	Terremoto	5	4	3	4	4
	Robo	4	4	2	5	4
	Malware	4	4	2	5	5
Sistemas financieros y administrativos	Incendio	5	4	3	4	4
	Terremoto	5	4	3	4	4
	Acceso no autorizado	4	4	2	5	6
	Acceso no autorizado	4	4	2	5	5
	Desconexión física o lógica	4	4	2	5	4

Almacenamiento – bases de datos	Agotamiento de recursos	4	4	3	5	5	

Correo electrónico	Incendio	5	3	3	4	4	3
	Terremoto	5	3	3	4	4	3
	Acceso no autorizado	4	3	2	5	5	3
	Desconexión física o lógica	4	6	2	5	5	3
Virtualización	Incendio	5	4	3	4	4	3
	Terremoto	5	4	3	4	4	3
	Acceso no autorizado	4	3	2	5	5	3
	Desconexión física o lógica	4	3	2	5	5	3
Internet	Incendio	5	4	3	4	4	3
	Terremoto	5	4	3	4	4	3
	Desconexión física o lógica	4	3	2	5	5	3
Red alámbrica	Incendio	5	4	3	4	4	3
	Terremoto	5	4	3	4	4	3
Red alámbrica	Incendio	5	4	3	4	4	3
	Terremoto	5	4	3	4	4	3
Enlace con proveedor	Incendio	5	4	3	4	4	3
	Terremoto	5	4	3	4	4	3
	Desconexión física o lógica	4	3	2	5	4	3
UPS	Incendio	5	4	3	4	4	3
	Terremoto	5	4	2	4	4	3
	Falla de equipos de climatización	4	4	2	5	5	4

Generador eléctrico	Incendio	5	4	3	4	4	3
	Terremoto	5	4	3	4	4	3
Equipos de climatización	Incendio	5	4	3	4	4	3
	Terremoto	5	4	3	4	4	3
	Falla de equipos de climatización	4	4	2	5	5	4
Cableado eléctrico	Incendio	5	4	3	4	4	3
	Terremoto	5	4	3	4	4	3
	Desconexión física o lógica	4	3	2	5	5	3
Centro de datos	Incendio	5	4	3	4	4	3
	Terremoto	5	4	3	4	4	3
	Acceso no autorizado	4	3	2	5	4	3
Cuarto de rack	Incendio	5	4	3	4	4	3
	Terremoto	5	4	3	4	4	3
	Acceso no autorizado	4	3	2	5	4	3
Equipo de desarrollo	Incendio	5	4	3	4	4	3
	Terremoto	5	4	3	4	4	3
	Fuga de información	4	3	2	5	5	3
Equipo técnico	Incendio	5	4	3	4	4	3
	Terremoto	5	4	3	4	4	3
	Fuga de información	4	3	2	5	5	3
Administradores	Incendio	5	4	3	4	4	3
	Terremoto	5	4	3	4	4	3
	Fuga de información	4	3	2	5	5	3

De acuerdo a la tabla anterior se realiza la evaluación de impacto y riesgo que puedan tener cada amenaza de los activos de la empresa Qwerty S.A. según la evaluación del impacto potencial, actual y objetivo se pueden determinar el tipo de salvaguardas a implementar cuyo único objetivo será la mitigación y prevención de los riesgos asociados a los activos informáticos.

Adicionalmente se debe poner a consideración el implementar control sobre el impacto residual que se pueda generar y tipo de riesgo residual esto para tenerlo en cuenta en nuevo estudio.[75]

[75] ccn-cert.cni. (10 de 2012). Margerti-libro I. Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

ANEXO G

7. DOMINIOS Y CONTROLES

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	X			Se adopta este control, es un requisito establecido en la norma, por lo que se debe definir un conjunto de políticas para la Seguridad de la Información, aprobadas por la Dirección, publicadas y comunicadas a los empleados y partes externas pertinentes como parte esencial del SGSI
A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su			x	La política puede ser ajustada de acuerdo a las variaciones en la institución o en las partes interesadas.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		conveniencia, adecuación y eficacia continuas.				
A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.		x		Se deben dejar claro cuáles son los roles asignados para cada uno los integrantes del sistema
A6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	x			Enfatizando en la importancia que tienen dentro del SGSI

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.			x	La organización no tiene contacto directo con ninguna autoridad competente
A6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad		x		No se especifica, pero es claro que no comparte información con grupos de interés, ni tampoco está recibiendo notificaciones de seguridad, parches y vulnerabilidades
A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.		x		No incluye el componente de seguridad en el proceso de planeación y administración de proyectos

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.		X		No se tiene segmentación en la red que permita tener un control en las conexiones inalámbricas. Se recomienda realizar la segmentación y establecer políticas y medidas para el uso de dispositivos móviles
A6.2.2	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.			x	No se tiene segmentación en la red que permita tener un control en las conexiones inalámbricas. Se recomienda realizar la segmentación y establecer políticas y medidas de seguridad para el uso de dispositivos móviles

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.			x	Se deben definir los requisitos que debe cumplir el personal de planta, contratistas y pasantes, se deben incluir elementos de seguridad de la información en la definición del perfil del cargo. Este proceso debe ser revisado por el área encargada.
A7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades		X		Este proceso debe ser verificado y controlado por el área de Talento Humano para la poder llevar un control de las obligaciones y responsabilidades específicas frente a la seguridad de la información dentro de los perfiles tanto para servidores de planta

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		y las de la organización en cuanto a la seguridad de la información.				como para contratistas de apoyo. Se debe dejar claro cláusulas que responsabilicen a las personas implicada en caso del mal manejo del uso de la información.
A7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.		x		Se debe formular un procedimiento sobre dar de alta a usuarios dentro de los diferentes sistemas de información que maneje la dependencia. Formato de asistencia proceso inducción y reinducción, material usado en el proceso.
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en			x	no aplica

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.				
A7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.		X		No se cuenta con un proceso definido. Se debe definir el alcance, los objetivos y procedimientos del mismo.
A7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen		X		Se debe realizar la suscripción de cláusulas de confidencialidad y no divulgación de la información del área de Registro y Matrícula, se debe definir un periodo mínimo de un (1)

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.				año después de la desvinculación o terminación del contrato. Esto debe ser estipulado desde un principio.
A8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	X			Se realiza la identificación de activos y se documenta
A8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.	X			Todos los activos de información tienen un propietario

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	X			Se tienen establecidas algunas reglas de acceso a los activos de información.
A8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	x			Existen procedimientos para la devolución de activos en general

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	X			Se cuenta con una clasificación de información de nivel crítico y con reglas para el acceso a ella.
A8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.			x	Implementar el procedimiento de etiquetado de la información.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	X			Se tienen especificadas las formas de acceso a algunos recursos de información, de acuerdo a la clasificación de la información, así por ejemplo al servidor FTP que sirve de almacenamiento de material fotográfico, solo pueden acceder las personas autorizadas
A8.3.1	Gestión de medio removibles	Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.			x	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando			x	Se debe establecer un procedimiento de disposición final de los medios para evitar que se tenga acceso a la información que puedan tener por personal no autorizado.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		procedimientos formales.				
A8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.		X		Se debe definir un procedimiento de protección de medios
A9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	X			Se tienen políticas de control de acceso a activos que contienen información crítica

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.		X		La red no se encuentra Segmentada por lo que se debe realizar la adecuación de la misma y dejar información documentada del procedimiento para la definición de los segmentos de red y sus reglas.
A9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	X			Se cuenta con registro de usuarios y nivel de acceso a la información, se debe implementar el procedimiento de cancelación de registro de usuarios.
A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de	X			El acceso se basa en las necesidades y políticas de control de acceso que hay definidas.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		acceso para todo tipo de usuarios para todos los sistemas y servicios.				
A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado		X		Las políticas deben ser definidas para poder implementar un procedimiento que establezca la forma de realizar las revisiones periódicas de cuentas privilegiadas. Se tienen usuarios privilegiados para otorgar niveles de acceso.
A9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	X			El acceso a los sistemas de información se realiza por medio de usuarios y contraseñas que deben cumplir con unas especificaciones de longitud mínima y de características específicas.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.		X		Se debe establecer un procedimiento de revisión de derechos de acceso
A9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.		X		Se debe establecer un procedimiento de revisión de derechos de acceso

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	X			El acceso a los sistemas de información se realiza por medio de usuarios y contraseñas que deben cumplir con unas especificaciones de longitud mínima y de características específicas.
A9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.				El nivel de acceso está definido por política de control de acceso.
A9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un	X			El acceso a información restringida se realiza por medio de autenticación y con niveles de acceso establecidos, garantizando que solo la persona autorizada tenga acceso a la información. Se debe realizar el procedimiento de acceso seguro.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		proceso de ingreso seguro.				
A9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	X			El ingreso a los sistemas de información y correo electrónico se realiza mediante contraseñas
A9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	X			El acceso a las aplicaciones se realiza por las personas autorizadas solamente

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.	X			Solo los desarrolladores del Centro tienen acceso al código fuente
A10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.		x		no tiene
A10.1.2	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.		x		no tiene

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.		X		Se debe implementar un sistema de seguridad físico con mecanismos que le permitan al centro tener control sobre su perímetro, como cámaras de seguridad, CCTV, entre otros.
A11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.		x		El Centro no cuenta con un sistema de seguridad biométrico o de monitoreo que permita tener control sobre la zona derecha del Centro. Se deben implementar controles físicos como cámaras de seguridad, controles de acceso biométrico, CCTV, etc.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.		X		El Centro no cuenta con un sistema de seguridad biométrico o de monitoreo que permita tener control sobre la zona derecha del Centro. Se deben implementar controles físicos como cámaras de seguridad, controles de acceso biométrico, CCTV, etc.
A11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.		X		Los servidores DHCP, HTTP y PBX se encuentran en un espacio donde no se cumplen condiciones de climatización óptimas.
A11.1.5	Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	x			Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
A11.1.6	Áreas de carga, despacho y acceso público	Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por			x	No aplica

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.				
A11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.		X		Los servidores DHCP, HTTP y PBX se encuentran en un espacio donde no se cumplen condiciones de climatización óptimas. Se deben implementar mecanismos como sensores de humedad y de calor, deshumidificadores, cables anti-flama, sistemas de refrigeración certificados, entre otros. Se deben implementar controles físicos como cámaras de seguridad, controles de acceso biométrico, CCTV, etc.
A11.2.2	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones	X			Se cuenta con una UPS que proporciona 20 minutos de autonomía, se está en proceso de compra de otros ups para el área de registro y control.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		causadas por fallas en los servicios de suministro.				
A11.2.3	Seguridad en el cableado.	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	X			Todo el cableado del Centro se encuentra protegido y con las medidas de acuerdo a la legislación vigente.
A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	X			Se realizan los mantenimientos correctivos y preventivos. Procedimiento de mantenimiento a equipos implementado.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa		X		Se debe implementar el procedimiento de retiro de activos
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.		x		no existe
A11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de			x	no aplica

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.				
A11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	x			Se da cumplimiento con el compromiso del Centro
A11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de		x		no existe

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		pantalla limpia en las instalaciones de procesamiento de información.				
A12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.		X		Faltan algunos procedimientos por documentar.
A12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.		x		no existe

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A12.1.3	Gestión de capacidad	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.			x	no aplica
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.			x	no aplica

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	x			A pesar de que se cuenta con un sistema antivirus y cortafuegos, estos están mal configurados o no se les realizan las actualizaciones requeridas. Se debe implementar un procedimiento de actualización Y mantenimiento de las aplicaciones que dan soporte a la seguridad.
A12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	X			El área de sistemas se encarga del respaldo de la información de los servidores virtuales y de los sistemas de información.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	X			Se cuenta con los logos de los servidores, logos del cliente de antivirus y registro de actividades en el firewall
A12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.		X		No se cuenta con controles de acceso biométrico. Se deben implementar controles físicos como cámaras de seguridad, controles de acceso biométrico, CCTV, etc.
A12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben	X			Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		proteger y revisar con regularidad.				
A12.4.4	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	X			Se tienen los sistemas de información sincronizados con el servidor donde se alojan.
A12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en	X			Se tienen separadas sesiones en los computadores, solo puede instalar software el personal de sistemas con clave de administrador.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		sistemas operativos.				
A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.			x	Procedimiento de reporte de incidentes y vulnerabilidades de seguridad.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	x			Solo el personal de soporte técnico puede instalar software con usuario y clave de administrador. Para instalar software los usuarios deben hacer la solicitud al área de sistemas quien evalúa si se puede o no realizar la instalación.
A12.7.1	Controles de auditorías de sistemas de información	Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.		x		Se deben definir controles y parámetros para realizar las auditorias y poder llevar un control con eso se puede implementar un plan de mejora continua.
A13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en		X		Se debe controlar de forma adecuada el firewall y controlar las actualizaciones del antivirus.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		sistemas y aplicaciones.				
A13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.		X		Se debe realizar la segmentación de la red y dejar información documentada del procedimiento para la definición de los segmentos de red y sus reglas para establecer también el procedimiento de gestión de servicios de red.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.		X		La configuración de la red de comunicaciones se encuentra en el mismo segmento. Se debe realizar la segmentación de la red y separar los servicios. Se debe realizar el procedimiento de segmentación de red.
A13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	X			Se cuenta con el procedimiento de transferencia de información.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.				
A13.2.3	Mensajería Electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	X			El riesgo se transfiere y es el proveedor el que realiza la protección de la información de la mensajería electrónica.
A13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para		X		Se debe realizar el procedimiento de confidencialidad y no divulgación de la información.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		la protección de la información.				
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	X			Se tiene el procedimiento de desarrollo de software y de gestión de cambios.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe		X		Se debe realizar la gestión debida en el firewall y en la red del Centro.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.				
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de	X			Se tienen controles criptográficos de acuerdo a la legislación y el procedimiento de transferencia de información. Políticas de acceso al servidor FTP.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		mensajes no autorizada.				
A.14.2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	X			Solo el personal autorizado en el área de sistemas puede hacer desarrollo de aplicaciones.
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	X			Se cuenta con el procedimiento de gestión de cambios.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	X			Se cuenta con el procedimiento de pruebas a sistemas de información y aplicaciones.
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	X			Se cuenta con el procedimiento de desarrollo de software. Solo los desarrolladores pueden hacer cambios, aprobados previamente por Gestión de cambios y se deben dejar documentados.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	X			Se cuenta con el procedimiento de desarrollo de software.
A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo	X			Se cuenta con ambientes separados entre desarrollo, pruebas y producción.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		el ciclo de vida de desarrollo de sistemas.				
A.14.2.7	Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	X			Procedimiento de seguimiento a desarrollos por terceros
A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	X			Se cuenta con el procedimiento de pruebas a sistemas de información y aplicaciones.
A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para	X			Se cuenta con el procedimiento de pruebas a sistemas de información y aplicaciones.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		aceptación y criterios de aceptación relacionados.				
A.14.3.1	Protección de datos de prueba	Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	X			Solo los desarrolladores tienen acceso a los datos de prueba, están custodiados en un servidor virtual del área de sistemas.
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	X			En los contratos con los proveedores se cuenta con los requisitos de seguridad que deben cumplir.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	X			En los contratos con los proveedores se cuenta con los requisitos de seguridad que deben cumplir.
A15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de	X			En los contratos con los proveedores se cuenta con los requisitos de seguridad que deben cumplir.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		suministro de productos y servicios de tecnología de información y comunicación.				
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	X			Se realiza el seguimiento y evaluación a los servicios prestados por los proveedores de acuerdo al cronograma establecido para tal fin
A15.2.2	Gestión del cambio en los servicios de los proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de	X			Se tiene el procedimiento de control del cambio con los proveedores.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la evaluación de los riesgos.				
A16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	X			Se tiene establecidos los roles y responsabilidades dentro del SGSI.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	X			Procedimiento de reporte de incidentes y vulnerabilidades de seguridad.
A16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	X			Procedimiento de reporte de incidentes y vulnerabilidades de seguridad.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	X			Se analizan los incidentes reportados y se toman las decisiones pertinentes, queda soportado en actas de reuniones.
A16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	X			A los incidentes presentados se les da tratamiento de acuerdo a lo establecido.
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o	X			Se cuenta con una carpeta compartida donde se colocan todos los casos documentados con la solución dada.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		impacto de incidentes futuros.				
A16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.		X		Se debe establecer el procedimiento de recolección y mantenimiento de evidencias.
A17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en	X			Se cuenta con el procedimiento Gestión de la Continuidad de la Seguridad.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		situaciones adversas, por ejemplo, durante una crisis o desastre.				
A17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	X			Se cuenta con el procedimiento Gestión de la Continuidad de la Seguridad.
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de	X			Se realizan revisiones de acuerdo al cronograma establecido.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.				
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	X			Se cuenta con servicios de respaldo que pueden garantizar la disponibilidad de las aplicaciones y servicios.
A18.1.1	Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el	X			Se tiene identificada la legislación que aplica a la organización.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.				
A18.1.2	Derechos propiedad intelectual (DPI)	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.		x		Es obligación de la Organización asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.		x		Se deben definir políticas claras y en donde los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada.
A18.1.4	Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.	X			Se tienen políticas de control de acceso a activos que contienen información crítica

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.		x		Se está incumpliendo con legislación y reglamentación pertinentes, se debe implementar controles criptográficos.
A18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos		X		No se ha realizado aun la primera revisión.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
		planificados o cuando ocurran cambios significativos.				
A18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.		x		El área encargada debe revisar regularmente el cumplimiento del de los procesos de información con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.

CODIFICACIÓN	TITULO	DESCRIPCIÓN	SI	NO	NO APLICA	JUSTIFICACIÓN
A18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.		x		Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Anexo 4 Dominios y Controles

Anexo H.

8. REQUISITOS DE LA NORMA ISO/IEC 27001:2013.

Anexo 5 Requisito de la Norma ISO/IEC 27001:2013

REQUISITO	CONTEXTO DE LA EMPRESA	CUMPLE	CONTEXTO	RECOMENDACIONES A IMPLEMENTAR
4.1	CONOCIMIENTO DE LA EMPRESA Y DE SU CONTEXTO	SI	Los colaboradores conocen la información de la organización misión, visión y objetivos para dar continuidad al negocio.	Se recomienda la implementación de políticas enfocadas a la creación de un Departamento de Tecnología Informática que se adapte a las necesidades de la
4.2	COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS	SI	Las dependencias de la empresa entienden de la necesidad del buen funcionamiento de sus recursos para poder continuar con la actividad sin interrupciones de la empresa	Coordinar con las áreas de la organización la aplicación de normas y políticas para la protección de la información de la empresa
4.3	DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA	SI	Hay que diseñar un SGSI para toda la empresa en general	Se debe divulgar a todos los colaboradores de la organización los objetivos para que esta manera se pueda establecer compromisos y responsabilidades. Se debe concientizar al personal de la importancia de aplicación de
4.4	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	NO	Actualmente no se tiene implementado un SGSI.	Diseño y planeación SGSI su finalidad es el mejoramiento continuo y de esta forma lograr un nivel de aceptación de riesgos mínimos. Este manual estará basado en la

Tabla 18. Requisito de la Norma Liderazgo.

REQUISITO	LIDERAZGO	CUMPLE	CONTEXTO	RECOMENDACIONES A IMPLEMENTAR
5.1	LIDERAZGO Y COMPROMISO	SI	La empresa sabe de la importancia de la implementación del SGSI y del valor agregado que le dará a la empresa.	Se debe establecer una comunicación directa y efectiva con los colaboradores y con todas aquellas personas que tengan vínculos comerciales con la misma. Donde se vea
5.2	POLÍTICA	NO	No se tiene una política de seguridad de la información documentada.	Ajustar las políticas generales y detalladas del SGSI que sean de alcance para la empresa y que sean públicamente accesibles a
5.3	ROLES, RESPONSABILIDADES. Y AUTORIDADES EN LA	SI	Los roles y responsabilidades están asignadas.	Es recomendable que se documente los roles y responsabilidades asignadas en base a la seguridad de la información

Tabla 19. Requisito de la Norma Planificación.

REQUISIT	PLANIFICACIÓN	CUMPL	CONTEXTO	RECOMENDACIONES A
6.1	ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDAD	NO	La empresa no cuenta con un plan de contingencia en caso de presentar un incidente de seguridad	Se debe manejar un plan de contingencia que guía para poder manejar incidentes futuros en caso de que se llegaran a presentar sirvan de
6.1.1	GENERALIDADES	SI	Existen todas las condiciones para aplicar el SGSI.	Se cuenta con la disponibilidad de directivos y colaboradores

6.1.2	VALORACIÓN DE RIESGOS DE LA SEGURIDAD DE	NO	No existe una metodología claramente definida que clasifique, analice, evalúe. Así como un análisis de riesgos	Después de realizar diferentes metodologías se llegó a la conclusión que la mejor metodología para aplicar es la Magerit
6.1.3	TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE	NO	Se tiene la matriz de riesgos del Proceso de Gestión del Desarrollo Tecnológico, debe complementarse con los riesgos	El desarrollo de este proceso sirvió para definir los controles a implementar y el tratamiento que se les debe dar
6.2	OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN	NO	No están documentados los objetivos de la seguridad de la información.	Definir los objetivos de la seguridad de la información y establecer la forma de alcanzarlos comprometiendo a los colaboradores.

Tabla 20. Requisito de la Norma ISO/IEC 27001:2013. Soporte.

REQUISIT	SOPORTE	CUMPLE	CONTEXTO	RECOMENDACIONES A
7.1	RECURSOS	NO	La empresa no posee documentación anterior al proceso que se está	La empresa debe tener la disposición y los recursos necesarios para iniciar con el desarrollo del SGSI.
7.2	COMPETENCIA	SI	La persona contratada debe es idónea y cuenta con los conocimientos necesarios para la implementación del Plan de seguridad Informática	Se debe Capacitar a los colaboradores al igual que contratar personas certificadas en la implementación un SGSI con la norma ISO 27001:2013.
7.3	TOMA DE CONCIENCIA	NO	Se debe dejar políticas y normas definidas de confidencialidad y los empleados emplean algunas técnicas de seguridad	Divulgación de las normas y políticas de la protección de la información

7.4	COMUNICACIÓN	NO	Aunque existen medios de comunicación no se están aplicando normas y buenas prácticas de utilización	Se deben buscar mecanismos efectivos para la divulgación del manual de seguridad.
7.5	INFORMACIÓN DOCUMENTAD	-	-	-
7.5.1	GENERALIDADES	NO	No hay evidencia de que se lleve registro de normas o políticas referentes a un SGSI	De realizo un análisis de riesgos donde con los resultados arrojados de documentos bajo la norma ISO
7.5.2	CREACIÓN Y ACTUALIZACIÓN	NO	No se actualizan los documentos del SGSI ya que no hay uno implementado.	Actualizar los documentos del SGSI y del estándar ISO 27001:2013 cada vez que se considere necesario.
7.5.3	CONTROL DE LA INFORMACIÓN DOCUMENTAD	NO	No existe ya que antes de este análisis no había un plan de seguridad de la información.	Se debe documentar todo tipo de incidente que pueda comprometer la integridad, confiabilidad y disponibilidad de la información

Tabla 21. Requisito de la Norma Operación.

REQUISITO	OPERACIÓN	CUMPLE	CONTEXTO	RECOMENDACIONES A IMPLEMENTAR
8.1	PLANIFICACIÓN Y CONTROL OPERACIONAL	NO	No tiene implementados controles definidos.	Establecer los procesos necesarios para planear, implementar, mantener y mejorar el SGSI.
8.2	VALORACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	NO	No existe una valoración de riesgos informáticos.	Establecer un esquema de clasificación de riesgos informáticos que permita analizarlos y valorarlos para determinar los controles a implementar con el fin de

8.3	TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA	NO	No existe un plan para el tratamiento de riesgos.	Documentar el plan de tratamiento de riesgos informáticos.

Tabla 22. Requisito de la Norma ISO/IEC 27001:2013. Evaluación del Desempeño.

REQUISITO	EVALUACIÓN DEL	CUMPLE	CONTEXTO	RECOMENDACIONES A IMPLEMENTAR
9.1	SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN	NO	No se tienen definidos	Establecer normas que permitan para realizar el seguimiento, medición, análisis y evaluación de los procesos y controles de seguridad del SGSI
9.2	AUDITORIA INTERNA	NO	No existen registros de auditorías anteriores	Se debe llevar una planificación de un plan de auditoría interna que permita medir el estado de la seguridad de la información en base al estándar ISO 27001:2013.
9.3	REVISIÓN POR LA DIRECCIÓN	NO	No está documentado un plan de la revisión del SGSI por parte de la dirección.	Documentar y planear a intervalos regulares una revisión al SGSI de forma general, se debe actualizar y adaptar según la situación de la empresa

Tabla 23. Requisito de la Norma ISO/IEC 27001:2013. Mejora.

REQUISITO	10 MEJORA	CUMPLE	CONTEXTO	RECOMENDACIONES A IMPLEMENTAR
10.1	NO CONFORMIDADES Y ACCIONES	NO	No está documentada la forma de cómo tratar a las no	Se deben definir políticas claras que permitan llevar correcciones y mejorar a aquellas inconformidades al SGSI

10.2	MEJORA CONTINUA	NO	No se tiene el SGSI implementado.	Proponer un plan de mejora continua a todos los procesos, así como la aplicación de buenas prácticas al manejo de la

9. LISTA DE CHEQUEO

Anexo 6 Lista de Chequeo

CONTROL	NOMBRE DEL CONTROL	DESCRIPCION DEL CONTROL	APLICA SI/NO	JUSTIFICACIÓN	OBSERVACIONES
A.5.1.1	Políticas para la seguridad de la información	*Control*: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	NO		se deben deficnir politicas y normas claras para el buen manejo de la informacion,
A.5.1.2	Revisión de las políticas para la seguridad de la información	*Control*: Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúa.	NO		Estas politicas deben ser somentidas a mejora continua esto con el fin de que estan actualizados a los cambios que se pueden presentar en la organización.
A.6.1.1	Roles y responsabilidades para la seguridad de la información	*Control*: Se debe definir y asignar todas las responsabilidades de la seguridad de la información	SI	Se responsabiliza a los colaboradores y usuarios del manejo de la informacion.	

Organización de la Seguridad de la Información					
A.6.1.2	Separación de deberes	*Control*: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	NO		
A.6.1.3	Contacto con las autoridades	*Control*: Se debe mantener contacto apropiados con las autoridades pertinentes	NO		La empresa esta en la obligacion de informar sobre cualquier tipo de eventualidad que se present y ponga en riesgo la seguridad de la informacion
A.6.1.4	Contacto con grupos de interés especial	*Control*: Se debe mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	NO		

A.6.1.5	Seguridad de la Información en la gestión de proyectos	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	SI	La entidad cuenta con los reglamentos técnicos para la gestión de los mismos.	
A.6.2.1	Políticas para dispositivos moviles	Control: Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	SI	El departamento de desarrollo WEB cuenta con las herramientas, para el desarrollo de aplicaciones que permitan llebvar un control sobre herramientas a utilizar en los dispositivos mobiles propiedad de la empresa.	
A.6.2.2	Teletrabajo	Control: Se debe implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	NO		

Seguridad de los recursos humanos.					
A.7.1.1	Selección.	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	NO		Este tipo de seguridad se debe implementar en cada una de las oficinas y dependencias donde se maneje recursos humanos y técnicos.
A.7.1.2	Técnicas y condiciones de empleo.	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	SI	A cada colaborador se le asigna un manual de funciones que debe cumplir con los reglamentos de Contro Interno.	
A.7.2.1	Responsabilidades de la dirección	*Control*: La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	NO		aunque saben de la seguridad de la informacion no estan aplicando normas y politicas para el manajo de la informacion y de los activos informaticos,

A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y donde sea pertinente, los contratistas, deben recibir la educación y formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	NO		la empresa debe capacitar a sus colaboradores en temas de seguridad, asi como incentivarlos a realizar certificaciones sobre estos temas.
A.7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	SI	el departamento encargado de emitir las normas y saciones en caso de que un colaborar cometa algun tipo de falta,	
A.7.3.1	Terminación o cambio de responsabilidades de empleo.	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o	SI	se informa por anticipado la temrinacion del contrato según la ley.	

Gestión de activos					
A.8.1.1	Inventario de activos	*Control*: Se deben identificar los activos asociados con la información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	SI	se lleva inventario de Activos, para que permita realizar los cambios pertinenentes en casi de tener la necesidad de dar de baja a un equipo,	
A.8.1.2	propiedad de los activos	*Control*: Los activos mantenidos en el inventario deben tener un propietario.	SI	se deja soporte de facturas y licencias para llevar control de los inventarios,	
A.8.1.4	Devolución de activos	*Control*: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	SI	llevar inventario de los activos asignados a los colaboradores	
A.8.2.1	Clasificación de la Información	*Control*: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	NO		

A.8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la	SI	poseen etiquetas con un numero de identicacion asi como el numero de las licencias y version de SO	
A.8.2.3	Manejo de activos	Control: Se debe desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	NO		
A.8.3.1	Gestión de medios removibles	Control: Se debe implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	NO		
A.8.3.2	Disposición de los medios	Control: Se debe disponer de forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	NO		
A.8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	NO		

Control de acceso					
A.9.1.1	Política de control de acceso	*Control* : Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	SI	el administrador del sistema es quien asigna privilegios, permiso y puede acceder a las bases de datos.	
A.9.1.2	Acceso a redes y a servicios en red	*Control* : Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	SI	tienes controles de acceso pero la red no esta segmentada.	
A.9.2.1	Registro y cancelación del registro de usuarios.	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	SI	Se deben aplicar politicas mas definidas sobre la creacion de usuarios y eliminacion de los mismos,	
A.9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para *todos los sistemas y servicios.*	NO		
A.9.2.3	Gestión de derecho de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	NO		

A.9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	NO		
A.9.2.5	Revisión de los derechos de acceso de usuarios.	Control: Los propietarios de los activos deben revisar los derechos de acceso de usuarios, a intervalos regulares.	NO		
A.9.2.6	Retiro o ajuste de los derecho de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o			
A.9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticidad secreta.	NO		La Empresa debe asignar un protocolo de seguridad respecto a la responsabilidad y confiabilidad de los datos que maneja el usuario interno.
A.9.4.1	Restricción de acceso a la información.	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con las políticas de control de acceso.	NO		Los accesos de la Información debe manejarse con confiabilidad del administrador del sistema.

A.9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiera la política de control de acceso, el acceso al sistema y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	NO		
A.9.4.3	Sistema de gestión de contraseñas	*Control* : Los sistemas de gestión de contraseña deben ser interactivos y deben asegurar la calidad de las contraseñas.	NO		
A.9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente l uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	NO		
A.9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.	NO		

Criptografía					
A.10.1.1	Política sobre el uso de controles criptográficos.	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	NO		deben implemtar politicas de criptografia y tranferencia de la informacion para poder garantizar la integridad, confiabilidad y disponibilidad de la información.
A.10.1.2	Gestión de llaves.	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	NO		creación de normas y politicas de genercion de llaves publicas y privadas.

Seguridad física y del entorno					
A.11.1.1	Perímetro de seguridad física	*Control*: Se debe definir y usar perímetro de seguridad, y usarlo para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	NO		se debe mejorar el sistema de seguridad con el que cuenta la empresa.
A.11.1.2	Controles de acceso físicos	*Control*: Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.	SI	El área se encuentra protegida	Se debe mejorar la seguridad para la proteccion de la empresa ya que no cuentan con un sistema de control y salida
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	*Control*: Se debe diseñar y ampliar seguridad física a oficinas, recintos e instalaciones.	NO		Se debe aplicar un sistema que permita garantizar la seguridad física de los equipos de cómputo.
A.11.1.4	Protección contra amenazas externas y ambientales	*Control*: Se debe diseñar y ampliar protección física contra desastres naturales, ataques maliciosos o accidentes.	SI	El edificio donde funciona la Empresa cuenta con un buen aislamiento por lo tanto evita el riesgo de inundación	
A.11.1.5	Trabajo en áreas seguras	*Control*: Se deben diseñar y ampliar procedimientos para trabajo en áreas seguras.	NO		

A.11.1.6	Áreas de despacho y carga	*Control* : Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlo de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	NO		no aplica
A.11.2.1	Ubicación y protección de los equipos	*Control* : Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	NO		Se debe implementar un sistema de protección y aislamiento en los equipos de informática y servidores
A.11.2.3	Seguridad del cableado	*Control* : El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra intercepciones, interferencia o	SI	el sistema de cableado no cumple con los estandares adecuados.	
A.11.2.4	Mantenimiento de equipos	*Control* : Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	NO		Hay equipos que no estan al dia con las configuraciones y actualizaciones.

A.11.2.5	Retiro de activos	*Control* : Los equipos, información o software no se deben retirar de un sitio sin autorización previa.	SI	Solo el área encargada es quien le puede dar de baja a un activo despues de realizar las validaciones	
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	SI	Los Equipos se encuentran en el área de informática.	
A.11.2.7	Disposición segura o reutilización de equipos.	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o	NO		
A.11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	NO		
A.11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	SI	Generalmente los equipos se mantienen en un buen aspecto de limpieza y orden interno.	

Seguridad de las Operaciones					
A.12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	NO		
A.12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	NO		
A.12.1.3	Gestión de capacidad	*Control*: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	NO		
A.12.1.4	Separación de los ambientes de desarrollo, pruebas, y operaciones	Control: Se deben separar los ambientes de desarrollo, prueba y operaciones, para reducirlos riesgos de acceso o cambios no autorizados al ambiente de operación.	NO		

A.12.2.1	Controles contra códigos maliciosos	*Control*: Se deben implementar controles de detención, de prevención y recuperación, combinado con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	NO		
A.12.3.1	Respaldo de la información	*Control*: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	SI	Se hace copia de seguridad a los sistema de información	
A.12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	NO		
A.12.4.2	Protección de la información de registro	Control: La instalaciones y la información de registro se deben proteger contra alteraciones y acceso no autorizado.	NO		
A.12.4.3	Registro del administrador y del operador.	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	NO		

12.4.4	Sincronización de relojes.	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	NO		
A.12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	NO		
A.12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los SI que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para	NO		
A.12.6.2	Restricciones sobre la instalación de software.	Control: Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	SI	solo el departmanto encargado puede realizar instalacion de software en los equipos de la organización.	
A.12.7.1	Controles de auditorías de SI.	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	NO		

Seguridad de las comunicaciones					
A.13.1.1	Controles de redes.	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	NO		
A.13.1.2	Seguridad de los servicios de red.	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contrate externamente.	NO		
A.13.1.3	Separación en las redes.	Control: Los grupos de servicios de información, usuarios y SI se deben separar en las redes.	NO		
A.13.2.1	Políticas y procedimientos de transferencia de información.	Control: Se debe contar con políticas, procedimiento y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	NO		

A.13.2.2	Acuerdos sobre transferencia de información.	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	NO		
A.13.2.3	Mensajería electrónica.	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	NO		
A.13.2.4	Acuerdos de confidencialidad o de no divulgación.	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	NO		

Adquisición, desarrollo y mantenimiento de Sistemas					
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información.	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos SI o para mejoras a los SI existentes.	NO		
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas.	Control: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	NO		
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: La información involucrada de las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la	NO		
A.14.2.1	Política de desarrollo seguro.	Control: Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	NO		

A.14.2.2	Procedimientos de control de cambios en sistemas.	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante uso de procedimientos formales de control de cambio.			
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación.	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	NO		
A.14.2.4	Restricciones en los cambios a los paquetes de software.	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	NO		
A.14.2.5	Principios de construcción de los sistemas seguro.	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguro, y aplicarlos a cualquier actividad de implementación de SI.	NO		
A.14.2.6	Ambiente de desarrollo seguro.	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguro para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	NO		

A.14.2.7	Desarrollo contratado externamente.	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	NO		
A.14.2.8	Pruebas de seguridad de sistemas.	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	NO		
A.14.2.9	Prueba de aceptación de sistemas.	Control: Para los SI nuevos, actualizaciones y nuevas versiones, se deben establecer programa de prueba para aceptación y criterios de aceptación relacionados.	NO		
A.14.3.1	Protección de datos de prueba.	Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	NO		

Relación con los proveedores					
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores.	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y se deben documentar.	NO		Se debe implementar un Politicas que permita mejorar los requisitos para mejorar los riesgos en la información
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores.	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	NO		
A.15.1.3	Cadena de suministro de tecnología de información y comunicación.	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	NO		
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores.	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	NO		Se debe realizar una auditoria en la administración para verificar el alcance del mismo
A.15.2.2	Gestión de cambios en los servicios de los proveedores.	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la	NO		

Gestión de incidentes de seguridad de la información					
A.16.1.1	Responsabilidades y procedimiento	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	NO		
A.16.1.2	Reporte de eventos de seguridad de la información.	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	NO		
A.16.1.3	Reporte de debilidades de seguridad de la información.	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y SI de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	NO		
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información	NO		
A.16.1.5	Respuesta a incidentes de seguridad de la información.	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo procedimientos documentados.	NO		se debe aplicar ya que en caso de una eventualidad de hace necesrio la implmentacion de un plan de acción inmediata

A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información.	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	NO		Se debe implementar un sistema que permita de forma inmediata solucionar incidentes en los SI dentro de la Empresa.
A.16.1.7	Recolección de evidencia.	Control: La organización definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	NO		
A.17.1.1	Planificación de la continuidad de la seguridad de la información.	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	NO		
A.17.1.2	Implementación de la continuidad de la seguridad de la información.	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	NO		la empresa debe mejorar sus proceso por medio de la mejora continua de los procesos que se ejecutan dentro de la Organización.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	NO		
A.17.2.1	Disponibilidad de instalaciones de procesamiento de	Control: Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	NO		

Cumplimiento					
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para	NO		
A.18.1.2	Derechos de propiedad intelectual.	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	NO		
A.18.1.3	Protección de registros.	Control: Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	NO		politicas que permitan cumplir con la proteccion de los registros de los procesos , requisitos legislativos, etc.
A.18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	NO		Se deben implmentar controles criptograficos,

A.18.2.1	Revisión independiente de la seguridad de la información.	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran Cambios significativos.	NO		
A.18.2.2	Cumplimiento con las políticas y normas de seguridad.	Control: Los directores deben revisar con regularidad el cumplimiento de procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	NO		
A.18.2.3	Revisión del cumplimiento técnico.	Control: Los SI se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	NO		se debe implementar un conograma que permita llevar el control de este tipo de actividades.

A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y donde sea pertinente, los contratistas, deben recibir la educación y formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	NO		La entidad no cuenta con los recursos para las acapacitaciones del personal adscrito a la Entidad.
A.7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	SI	El departamento jurídico es el encargado de aunar esfuerzos para cumplir con este requisito en la Entidad	
A.7.3.1	Terminación o cambio de responsabilidades de empleo.	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o	SI	La Entidad informa con anticiopación los posibles sucesos y cambios que se presenten en cada una de las áreas.	

ANEXO J

10 DECLARACIÓN DE APLICABILIDAD (SOA)

TIPO	*Codificación*	*TITULO*	*Descripción*	*si*	*no*	*no aplica*	*Declaración de Aplicabilidad*
C	A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	X			Se adopta este control, es un requisito establecido en la norma, por lo que se debe definir un conjunto de políticas para la Seguridad de la Información, aprobadas por la Dirección, publicadas y comunicadas a los empleados y partes externas pertinentes como parte esencial del SGSI
C	A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.			x	La política puede ser ajustada de acuerdo a las variaciones en la institución o en las partes interesadas.

C	A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.		x		Se deben dejar claro cuáles son los roles asignados para cada uno los integrantes del sistema.
C	A6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	x			Enfatizando en la importancia que tienen dentro del SGSI
C	A6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.			x	La organización no tiene contacto directo con ninguna autoridad competente
C	A6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad		x		No se especifica, pero es claro que no comparte información con grupos de interés, ni tampoco está recibiendo notificaciones de seguridad, parches y vulnerabilidades

C	A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.		x		No incluye el componente de seguridad en el proceso de planeación y administración de proyectos
C	A6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.		X		No se tiene segmentación en la red que permita tener un control en las conexiones inalámbricas. Se recomienda realizar la segmentación y establecer políticas y medidas para el uso de dispositivos móviles
C	A6.2.2	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.			x	No se tiene segmentación en la red que permita tener un control en las conexiones inalámbricas. Se recomienda realizar la segmentación y establecer políticas y medidas de seguridad para el uso de dispositivos móviles

C	A7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.			x	Se deben definir los requisitos que debe cumplir el personal de planta, contratistas y pasantes, se deben incluir elementos de seguridad de la información en la definición del perfil del cargo. Este proceso debe ser revisado por el área encargada.
C	A7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.		X		Este proceso debe ser verificado y controlado por el área de Talento Humano para la poder llevar un control de las obligaciones y responsabilidades específicas frente a la seguridad de la información dentro de los perfiles tanto para servidores de planta como para contratistas de apoyo. Se debe dejar claro cláusulas que

							responsabilicen a las personas implicada en caso del mal manejo del uso de la información.
C	A7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.		x		Se debe formular un procedimiento sobre dar de alta a usuarios dentro de los diferentes sistemas de información que maneje la dependencia. Formato de asistencia proceso inducción y reinducción, material usado en el proceso.
C	A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.			x	no aplica

C	A7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.		X		No se cuenta con un proceso definido. Se debe definir el alcance, los objetivos y procedimientos del mismo.
C	A7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.		X		Se debe realizar la suscripción de cláusulas de confidencialidad y no divulgación de la información del área de facturación y nomina, se debe definir un periodo mínimo de un (1) año después de la desvinculación o terminación del contrato. Esto debe ser estipulado desde un principio.
C	A8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un	X			Se realiza la identificación de activos y se documenta

			inventario de estos activos.				
C	A8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.	X			Todos los activos de información tienen un propietario
C	A8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	X			Se tienen establecidas algunas reglas de acceso a los activos de información.
C	A8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	x			Existen procedimientos para la devolución de activos en general
C	A8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales,	X			Se cuenta con una clasificación de información de nivel

			valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.				crítico y con reglas para el acceso a ella.
C	A8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.			x	Implementar el procedimiento de etiquetado de la información.
C	A8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	X			Se tienen especificadas las formas de acceso a algunos recursos de información, de acuerdo a la clasificación de la información, así por ejemplo al servidor FTP que sirve de almacenamiento de material fotográfico, solo pueden acceder las personas autorizadas

C	A8.3.1	Gestión de medio removibles	Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.			x	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
C	A8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.			x	Se debe establecer un procedimiento de disposición final de los medios para evitar que se tenga acceso a la información que puedan tener por personal no autorizado.
C	A8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.		X		Se debe definir un procedimiento de protección de medios
C	A9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	X			Se tienen políticas de control de acceso a activos que contienen información crítica

C	A9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.		X		La red no se encuentra Segmentada por lo que se debe realizar la adecuación de la misma y dejar información documentada del procedimiento para la definición de los segmentos de red y sus reglas.
C	A9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	X			Se cuenta con registro de usuarios y nivel de acceso a la información, se debe implementar el procedimiento de cancelación de registro de usuarios.
C	A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	X			El acceso se basa en las necesidades y políticas de control de acceso que hay definidas.

C	A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado		X		Las políticas deben ser definidas para poder implementar un procedimiento que establezca la forma de realizar las revisiones periódicas de cuentas privilegiadas. Se tienen usuarios privilegiados para otorgar niveles de acceso.
C	A9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	X			El acceso a los sistemas de información se realiza por medio de usuarios y contraseñas que deben cumplir con unas especificaciones de longitud mínima y de características específicas.
C	A9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.		X		Se debe establecer un procedimiento de revisión de derechos de acceso

C	A9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.		X		Se debe establecer un procedimiento de revisión de derechos de acceso
C	A9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	X			El acceso a los sistemas de información se realiza por medio de usuarios y contraseñas que deben cumplir con unas especificaciones de longitud mínima y de características específicas.
C	A9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.				El nivel de acceso está definido por política de control de acceso.

C	A9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	X			El acceso a información restringida se realiza por medio de autenticación y con niveles de acceso establecidos, garantizando que solo la persona autorizada tenga acceso a la información. Se debe realizar el procedimiento de acceso seguro.
C	A9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	X			El ingreso a los sistemas de información y correo electrónico se realiza mediante contraseñas
C	A9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	X			El acceso a las aplicaciones se realiza por las personas autorizadas solamente
C	A9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.	X			Solo los desarrolladores del Centro tienen acceso al código fuente

C	A10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.		x		no tiene
C	A10.1.2	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.		x		no tiene
C	A11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.		X		Se debe implementar un sistema de seguridad físico con mecanismos que le permitan al centro tener control sobre su perímetro, como cámaras de seguridad, CCTV, entre otros.
C	A11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se		x		La empresa Qwerty S.A. con un sistema de seguridad biométrico o de monitoreo que permita tener control sobre la zona derecha

			permite el acceso a personal autorizado.				del Centro. Se deben implementar controles físicos como cámaras de seguridad, controles de acceso biométrico, CCTV, etc.
C	A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.		X		La Empresa Qwerty no cuenta con un sistema de seguridad biométrico o de monitoreo que permita tener control sobre la zona derecha del Centro. Se deben implementar controles físicos como cámaras de seguridad, controles de acceso biométrico, CCTV, etc.
C	A11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.		X		Los servidores DHCP, HTTP y PBX se encuentran en un espacio donde no se cumplen condiciones de climatización óptimas.
C	A11.1.5	Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	x			Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.

C	A11.1.6	Áreas de carga, despacho y acceso público	Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.			x	no aplica
C	A11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.		X		Los servidores DHCP, HTTP y PBX se encuentran en un espacio donde no se cumplen condiciones de climatización óptimas. Se deben implementar mecanismos como sensores de humedad y de calor, deshumidificadores, cables anti-flama, sistemas de refrigeración certificados, entre otros. Se deben implementar controles físicos como cámaras de seguridad,

							controles de acceso biométrico, CCTV, etc.
C	A11.2.2	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	X			Se cuenta con una UPS que proporciona 20 minutos de autonomía, se está en proceso de compra de otros ups para el área de registro y control.
C	A11.2.3	Seguridad en el cableado.	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	X			Todo el cableado de la empresa se encuentra protegido y con las medidas de acuerdo a la legislación vigente.
C	A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su	X			Se realizan los mantenimientos correctivos y preventivos. Procedimiento de

			disponibilidad e integridad continuas.				mantenimiento a equipos implementado.
C	A11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa		X		Se debe implementar el procedimiento de retiro de activos
C	A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.		x		no existe
C	A11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes			x	no aplica

			de su disposición o reúso.				
C	A11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	x			Se da cumplimento con el compromiso de la empresa
C	A11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.		x		no existe
C	A12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.		X		Faltan algunos procedimientos por documentar.
C	A12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las		x		no existe

			instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.				
C	A12.1.3	Gestión de capacidad	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.			x	no aplica
C	A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.			x	no aplica
C	A12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los	x			A pesar de que se cuenta con un sistema antivirus y cortafuegos, estos están mal configurados o no se les realizan las actualizaciones requeridas.

			usuarios, para proteger contra códigos maliciosos.				Se debe implementar un procedimiento de actualización y mantenimiento de las aplicaciones que dan soporte a la seguridad.
C	A12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	X			El área de sistemas se encarga del respaldo de la información de los servidores virtuales y de los sistemas de información.
C	A12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	X			Se cuenta con los logs de los servidores, logs del cliente de antivirus y registro de actividades en el firewall
C	A12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.		X		No se cuenta con controles de acceso biométrico. Se deben implementar controles físicos como cámaras de seguridad,

							controles de acceso biométrico, CCTV, etc.
C	A12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	X			Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.
C	A12.4.4	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	X			Se tienen los sistemas de información sincronizados con el servidor donde se alojan.
C	A12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	X			Se tienen separadas sesiones en los computadores, solo puede instalar software el personal de sistemas con clave de administrador.

C	A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.			x	Procedimiento de reporte de incidentes y vulnerabilidades de seguridad.
C	A12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	x			Solo el personal de soporte técnico puede instalar software con usuario y clave de administrador. Para instalar software los usuarios deben hacer la solicitud al área de sistemas quien evalúa si se puede o no realizar la instalación.
C	A12.7.1	Controles de auditorías de sistemas de información	Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y		x		Se deben definir controles y parámetros para realizar las auditorias y poder llevar un control con eso se

			acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.				puede implementar un plan de mejora continua.
C	A13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.		X		Se debe controlar de forma adecuada el firewall y controlar las actualizaciones del antivirus.
C	A13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.		X		Se debe realizar la segmentación de la red y dejar información documentada del procedimiento para la definición de los segmentos de red y sus reglas para establecer también el procedimiento de gestión de servicios de red.
C	A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de		X		La configuración de la red de comunicaciones se encuentra en el mismo segmento. Se debe realizar la

			información se deben separar en las redes.				segmentación de la red y separar los servicios. Se debe realizar el procedimiento de segmentación de red.
C	A13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	X			Se cuenta con el procedimiento de transferencia de información.
C	A13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.				
C	A13.2.3	Mensajería Electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	X			El riesgo se transfiere y es el proveedor el que realiza la protección de la información de la mensajería electrónica.

C	A13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.		X		Se debe realizar el procedimiento de confidencialidad y no divulgación de la información.
C	A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	X			Se tiene el procedimiento de desarrollo de software y de gestión de cambios.
C	A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades		X		Se debe realizar la gestión debida en el firewall y en la red del Centro.

			fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.				
C	A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	X			Se tienen controles criptográficos de acuerdo a la legislación y el procedimiento de transferencia de información. Políticas de acceso al servidor FTP.
C	A.14.2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	X			Solo el personal autorizado en el área de sistemas puede hacer desarrollo de aplicaciones.

C	A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	X			Se cuenta con el procedimiento de gestión de cambios.
C	A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	X			Se cuenta con el procedimiento de pruebas a sistemas de información y aplicaciones.
C	A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	X			Se cuenta con el procedimiento de desarrollo de software. Solo los desarrolladores pueden hacer cambios, aprobados previamente por Gestión de cambios y se deben dejar documentados.

C	A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	X			Se cuenta con el procedimiento de desarrollo de software.
C	A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	X			Se cuenta con ambientes separados entre desarrollo, pruebas y producción.
C	A.14.2.7	Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	X			Procedimiento de seguimiento a desarrollos por terceros

C	A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	X			Se cuenta con el procedimiento de pruebas a sistemas de información y aplicaciones.
C	A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	X			Se cuenta con el procedimiento de pruebas a sistemas de información y aplicaciones.
C	A.14.3.1	Protección de datos de prueba	Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	X			Solo los desarrolladores tienen acceso a los datos de prueba, están custodiados en un servidor virtual del área de sistemas.
C	A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	X			En los contratos con los proveedores se cuenta con los requisitos de seguridad que deben cumplir.

C	A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	X			En los contratos con los proveedores se cuenta con los requisitos de seguridad que deben cumplir.
C	A15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	X			En los contratos con los proveedores se cuenta con los requisitos de seguridad que deben cumplir.
C	A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la	X			Se realiza el seguimiento y evaluación a los servicios prestados por los proveedores de

			prestación de servicios de los proveedores.				acuerdo al cronograma establecido para tal fin
C	A15.2.2	Gestión del cambio en los servicios de los proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la reevaluación de los riesgos.	X			Se tiene el procedimiento de control del cambio con los proveedores.
C	A16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	X			Se tiene establecidos los roles y responsabilidades dentro del SGSI.

C	A16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	X			Procedimiento de reporte de incidentes y vulnerabilidades de seguridad.
C	A16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	X			Procedimiento de reporte de incidentes y vulnerabilidades de seguridad.
C	A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	X			Se analizan los incidentes reportados y se toman las decisiones pertinentes, queda soportado en actas de reuniones.
C	A16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de	X			A los incidentes presentados se les da tratamiento de acuerdo a lo establecido.

			acuerdo con procedimientos documentados.				
C	A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	X			Se cuenta con una carpeta compartida donde se colocan todos los casos documentados con la solución dada.
C	A16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.		X		Se debe establecer el procedimiento de recolección y mantenimiento de evidencias.
C	A17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas,	X			Se cuenta con el procedimiento Gestión de la Continuidad de la Seguridad.

			por ejemplo, durante una crisis o desastre.				
C	A17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	X			Se cuenta con el procedimiento Gestión de la Continuidad de la Seguridad.
C	A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	X			Se realizan revisiones de acuerdo al cronograma establecido.

C	A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	X			Se cuenta con servicios de respaldo que pueden garantizar la disponibilidad de las aplicaciones y servicios.
C	A18.1.1	Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	X			Se tiene identificada la legislación que aplica a la organización.
C	A18.1.2	Derechos propiedad intelectual (DPI)	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y		x		es obligación de la Organización asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los

			contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.				derechos de propiedad intelectual
C	A18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.		x		Se deben definir políticas claras y en donde los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada.
C	A18.1.4	Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.	X			Se tienen políticas de control de acceso a activos que contienen información crítica
C	A18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos,		x		Se está incumpliendo con legislación y reglamentación pertinentes, se debe

			legislación y reglamentación pertinentes.				implementar controles criptográficos.
C	A18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.		X		No se ha realizado aun la primera revisión.
C	A18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad		x		El área encargada debe revisar regularmente el cumplimiento del de los procesos de información, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.

			apropiadas, y cualquier otro requisito de seguridad.				
C	A18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.		x		Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Anexo L

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

EMPRESA DE TELECOMUNICACIONES QWERTY S.A

MAYO 2020

Contenido

1. INTRODUCCIÓN

La Empresa QWERTY S.A. es una empresa del sector tecnológico que busca el desarrollo en tecnología en comunidades colombianas a través del uso de las mismas. Debido al volumen de inventario y de clientes externos y colaboradores internos que hacen uso de estas tecnologías se hace necesario la implementación de normas y controles de seguridad para la protección de la información; teniendo en cuenta que la seguridad de la información es prioridad para la Empresa QWERTY S.A , En este documento se describen las Políticas y Procedimientos de Seguridad de la Información definidas para la Empresa; para la elaboración de este manual se tomara como guía la norma la norma ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013.

Las políticas relacionadas en este manual hacen parte importante del sistema de seguridad de la información de la Empresa Qwerty S.A, convirtiéndose en la guía para la implantación de los controles, procedimientos y estándares definidos.

1. OBJETIVO

El objetivo de este manual es definir las políticas aplicables a la infraestructura e información de la empresa Qwerty S.A, su finalidad es poder garantizar la aplicación y utilización del buen uso y manejo de la información.

2. ALCANCE

El manual de seguridad de la información será aplicable a todos los departamentos de la empresa el cual tiene como objetivo abarcar todos los aspectos administrativos entre estos estará el control y vigilancia por partes de los directivos, administrativos, proveedores y personal encargado de garantizar el cumplimiento y la aplicación de las políticas de seguridad consignadas en este manual que deben ser cumplidos.

3. POLÍTICA GLOBAL DE SEGURIDAD DE LA INFORMACIÓN

La Empresa Qwerty S.A prestadora de servicios tecnológicos reconoce que para poder dar continuidad al negocio uno de sus objetivos primordiales es la protección de la información ya que este es un activo fundamental para poder mantenerse en el mercado por lo que debe tomar decisiones eficientes enfocadas en la garantizar la integridad, confiabilidad y disponibilidad de la información.

Así como a la protección de toda aquella infraestructura que la soporta con el fin de poder generar confiabilidad en los clientes y pode competir con otras empresas en el campo tecnológico.

Dicho manual será acatado por Directivos, funcionarios, personal externo, proveedores y todos aquellos que tengan algún tipo de relación con la empresa estos se comprometen a adoptar los lineamientos contenidos en el presente documento con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

Este Documento fue realizado bajo políticas y métodos específicos los cuales sirvieron de guía para la formulación de las normas y políticas adecuadas para el manejo de la información estableciendo normas de seguridad de la información las cuales están fundamentadas en la norma Internacional ISO 27001:2013

La aplicación del manual está bajo la responsabilidad de las Directivas de la organización junto con el Departamento encargado de difundir y encargasen de la aplicación y manual de manejo y seguridad de la información este contara con autonomía para modificar la Política Global o las Políticas de Seguridad de la Información de acuerdo con las necesidades de revisión establecidas periódicamente o cuando se considere necesario.

4. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

Para la organización Qwerty S.A es un principio fundamental trabajar continuamente en la protección de los activos de la información contra todo tipo de amenazas internas, externas, llevadas a cabo deliberadamente o algún caso fortuito para llevar a cabo esto es importante tener en cuenta los siguientes principios:

- La responsabilidad general de la seguridad de la información está a cargo de del Departamento TI quien será el responsable de la Seguridad, y este estará bajo la supervisión de los Directivos que son la máxima autoridad del SGSI.
- Cualquier modificación a esta política se concretará y desarrollará en normativas y procedimientos del SGSI, las cuales se integrarán en la medida de lo posible con otros sistemas de gestión de la organización esto con el fin de optimizar recursos y buscar la mejora continua de la eficiencia y eficacia de la gestión de los procesos.
- Proteger la información confidencial tanto de los Directivos, proveedores cliente y colaboradores de la organización.
- Mantener la integridad de la información ingresada, referente a lo concerniente a la actividad económica de la empresa.
- Garantizar la confidencialidad de la información.

- Permitir la disponibilidad la información garantizando que esta pueda ser utilizada en el momento que los servicios ofrecidos por la organización lo requieran acuerdo a las necesidades de cada dependencia.
- Se debe garantizar la ejecución y cumplimiento de las disposiciones legales, regulatorias y contractuales relacionadas con la seguridad de la información.

5. LINEAMIENTOS Y NORMAS DE SEGURIDAD DE LA INFORMACIÓN

5.1. CUMPLIMIENTO Y SANCIONES

5.1.2 Principio: Todos los colaboradores de la empresa Qwerty S.A Directivos, proveedores y los usuarios que se benefician de sus servicios se comprometen a cumplir y respetar el manual de políticas de la seguridad de la información.

5.1.3. Políticas de seguridad de la información:

- Los colaboradores, proveedores clientes o contratistas dan por entendido que todo incumplimiento de algunas de las normas contenidas en este manual será considerado como causal para la aplicación de las diferentes medidas correctivas dentro de las que se encuentran sanciones disciplinarias o contractuales, dentro de las que se tendrá encuentra la gravedad de la falta y de esta forma se determinará si será motivo para la terminación del contrato.
- Se establecen políticas que garanticen que tanto los colaboradores y ejecutivos estén comprometidos con la seguridad de la información de la empresa por lo que se les asignaran funciones y responsabilidades frente a la manejo de la información y de los activos; así como el departamento encargado de TI y seguridad de la empresa será quien habilite los accesos y permiso de la información para quienes la necesiten pero estos deberán asumir la responsabilidad de la misma y acatar las normas a las que está sujeta el manejo de la información así como las consecuencias al mal manejo de la misma.

- Tanto los colaboradores como ejecutivos de la empresa serán responsables de garantizar el uso y el manejo de la información y velar porque se le dé un uso adecuado, así como de informar cualquier tipo de irregularidad al área encargada. Cada funcionario será responsable de garantizar que las personas que trabajan bajo su control protegen la información de acuerdo con las normas establecidas por la organización.

5.1.4 Políticas de la infraestructura Organizacional

- Se fijará un esquema de seguridad de la información en donde se determinarán los cargos a los cuales se les asignarán funciones y responsabilidades.
- La Junta Directiva se comprometerá a difundir las políticas de la información de la seguridad a todo el personal de la organización y estar presta a cualquier tipo de modificación y aclaración en caso de que hiciera falta.
- Se crearán canales seguros para trasmitir la información y garantizar que todo el personal este informado.
- Se fijará un comité de seguridad el cual tendrá la función de analizar los incidentes de seguridad y realizar el debido proceso con las áreas encargadas.
- El comité de seguridad deberá definirá el procedimiento para realizar el análisis de Riesgo de la seguridad y así mismo para clasificar la información.
- El comité de Seguridad verificara y controlara que las políticas de seguridad se están implementando de manera adecuada.

5.1.5. Políticas del manejo de la información

La Empresa Qwerty S.A definirá los requisitos de clasificación de la información y los controles de protección a los cuales estarán definidos, esta se clasificará y se documentará de acuerdo a las normas establecidas por el comité de seguridad.

El Comité de seguridad difundirá la guía de clasificación de la información y se encargará de que se suministren las guías y herramientas de cifrado de la información.

El comité de Seguridad y el área de Tecnología definirán el método de cifrado a utilizar; se clasificará la información de acuerdo a su importancia.

Las funcionarias que hagan uso de la información deben regirse por la guía las cuales tienen las directrices para el manejo y clasificación de la misma para darle una correcta manipulación.

Toda la información tanto en medios físicos como tecnológicos debe ser protegida por medio de controles

6. PROPIEDAD INTELECTUAL

La propiedad intelectual del desarrollo de software, productos y servicios de la entidad será protegida mediante la asignación de derechos a la sede principal de la empresa.

Se incluirán avisos de propiedad intelectual en los proyectos de desarrollo y servicios ofrecidos por la empresa.

7. POLÍTICA DE CONTINUIDAD DEL NEGOCIO

Con el fin de que la organización pueda dar continuidad y lograr los objetivos propuestos en la aplicación de este manual de seguridad toda información considerada crítica y de vital importancia para el desarrollo de la actividad económica de la empresa deberán contar con una copia de respaldo y con un plan de contingencia en caso de presentarse ataques a la seguridad de la información.

- Todos los sistemas de información que tengan como función ser el soporte para el desarrollo de la actividad de la entidad contaran con un plan de recuperación que permita a la organización garantizar una respuesta efectiva y eficiente ante cualquier tipo de evento.

Se deberá tener toda eventualidad documentada y al día en caso de ser necesaria.

- Los proveedores deberán contar con un plan de contingencia en caso de presentar una amenaza a la seguridad de la información.
- Se harán respaldos de bases de datos y de toda aquella información considerada crítica, estas deben garantizar la integridad, confiabilidad y disponibilidad de la misma.
- Las copias de respaldo del software desarrollado por la organización deberán estar contar con un soporte actualizado de tal forma que se pueda garantizar la correcta restauración de los sistemas en caso de presentarse algún tipo de eventualidad.
- Los medios que utilizados para realizar el respaldo de respaldo de la información confidencial del negocio deberán ser correctamente almacenados cumpliendo los requerimientos de seguridad y preservación de los medios.
- El departamento encargado deberá realizar pruebas de restauración esto con el fin de verificar la integridad de la información.

7. POLÍTICAS DE LAS COMUNICACIONES /TRANSFERENCIA DE INFORMACIÓN Y SEGURIDAD DE LAS REDES

- Se debe asegurar el canal de transmisión donde se envían los archivos confidenciales entre los diferentes componentes haciendo uso del Internet, con la finalidad de que estos no puedan ser interceptados, ni violentados en su contenido por terceras personas; para ello se debe establecer protocolos de transferencia segura como TLS - Transport Layer Security en versiones reciente que no hayan sido vulneradas, como TLS V1.2.

- Los jefes de áreas y demás ejecutivos de la organización deben tener firmas digitales para el uso de su correo electrónico a fin de enviar y recibir sus correos con este control garantizando el no repudio, la confidencialidad e integridad de la transacción; así como la identificación y comprobabilidad legal tanto de la emisión como de la recepción de contenido del mismo.

- Los procesos de transferencia de información de forma segura, envió de correo electrónico con firma digital y manejo de las herramientas de cifrado de la información deben estar debidamente documentados procedimentalmente; para su adecuado gestión por las partes interesadas, considerando los estándares de seguridad y uso de puertos seguros que le puedan ser aplicables y su activación con los certificados digitales correspondientes, independientemente del algoritmo de cifrado implementado, tanto para la información cifrada como del canal de autenticación a nivel comunicaciones.

- La configuración del servidor SFTP debe ser realizada por el personal idóneo para esta tarea respetando los estándares de calidad como sus diferentes técnicas al momento de realizar la misma, como la documentación de la configuración ya que debe estar muy consciente de la gran responsabilidad de la cual está por implementar, para la empresa como de los acuerdos o de las cláusulas de confidencialidad para esta.

- La organización debe asegurar la protección de la información que sea transmitida o recepcionada a través de sus redes de datos tanto a nivel interno como externo; estableciendo de medios confiables de transferencia de información que consideren procedimientos, controles de acceso, manejo y de configuración a los componentes asociados; así como acuerdos de transferencia con quienes interactúe con el fin de garantizar la confidencialidad e integridad de los datos y a su vez se minimicen los riesgos de seguridad que puedan presentarse en intercambio de la información.

- El área encargada debe garantizar el borrador de la información de una manera segura.

9. POLÍTICA DE CONTROL DE ACCESO FÍSICO.

- El comité de Seguridad establecerá procedimientos para la autorización y controles al acceso de los sistemas y redes de la organización Qwerty S.A; este debe asegurar que las redes inalámbricas de la Organización cuenten con métodos de autenticación que evite accesos no autorizados.

- Todos los colaboradores y personas que tenga de una u otra manera algún vínculo comercial con la organización, deberá contar con un Id que le permita autenticarse y de esta forma poder tener control se su ingreso a la plataforma de la empresa; el Id con el contaran será un código único de usuario el cual no podrán compartir; para el acceder a los sistemas de información de la organización se debe requerir autenticación por parte de los usuarios.

9.1 Generación, eliminación y cancelación del Id de identificación de usuarios

Los Encargados de la creación, asignación, eliminación e inhabilitación del Id de los usuarios es el comité de seguridad de la empresa quienes deben asegurar la correcta administración de asignación de usuarios y privilegios.

El comité de seguridad deberá controlar que cuando el usuario tenga más de 5 intentos fallidos este será inhabilitado, así como cuando dure más de un periodo de tiempo sin acceder al sistema.

9.2 Definición de Perfiles

La autorización de acceso a los sistemas y bases de datos de los directivos y de todos aquellos que tenga vínculo con la empresa deberán ser creados en un grupo de usuarios donde el área encargada les asignara Roles y los permisos serán otorgados de acuerdo con estos grupos o roles.

Los roles o grupos de trabajo serán conformados de acuerdo a las responsabilidades y actividades equivalentes.

- Dentro de los perfiles asignados se contará uno para actividades de auditoría y sus permisos se limitarán únicamente a consulta.
- Otro tipo de perfiles como el de Administradores deberá contar con la aprobación del comité de seguridad quienes serán los únicos que pueden autorizar este tipo de perfiles para acceder modificar manipular las bases de datos.
- Los perfiles para el Departamento de desarrollo de aplicaciones contasen únicamente con la autorización para acceder a sus aplicativos y se limitaran a sus áreas de trabajo.
- El único Departamento que podrá acceder a todas las dependencias es el departamento de soporte y deberá llevar un control de modificaciones y cambios que este realice en los sistemas, así mismo no podrá realizar sin plena autorización del comité de seguridad de la empresa.
- Así mismo las estaciones de trabajo deberán contar con un bloqueo automático que se activara después de detectar un periodo de inactividad por parte del usuario por lo menos de 5 minutos.
- El equipo de trabajo (PC) deberá permanecer despejado, donde se evidencie que el escritorio cuenta únicamente con la información necesaria y concerniente a la actividad económica de la empresa.

9.3 Creación de las contraseñas

Todas las contraseñas deberán ser creadas de acuerdo a las normas y políticas fijadas por el comité de seguridad de la empresa, se utilizarán herramientas como generadores de contraseñas que permitan asegurar el cumplimiento mínimo de seguridad.

Las contraseñas deberán ser cambiadas mínimo cada 3 meses, están contaran con un nivel de confiabilidad lo que significa que al usuario a quien se le asigne un Id único de autenticación deberá garantizar el compromiso de responsabilidad.

9.3.1 Asignación de contraseñas

Las contraseñas y asignación de privilegios los colaboradores, proveedores y demás personas que tengan vínculos comerciales con la empresa serán controladas mediante un proceso con el fin de garantizar que se cumplan los siguientes requisitos:

- Un documento donde a la persona a quien se le asigne Id y contraseña se comprometa a manejarla con estricta confiabilidad al igual que asumir las consecuencias al no darle un correcto uso.
- Las contraseñan deberán ser almacenadas por medio de la utilización de un Algoritmo de cifrado al igual que los Id, están no podrán ser almacenadas en texto plano.

10. POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

El comité de Seguridad se encargará de almacenar, buscar mecanismos y herramientas para la trasmisión de la información considerada como reservada o de acceso restringido mediante técnicas de cifrado con el propósito de proteger su confidencialidad e integridad para esto implementará sistemas de cifrado como aplicativos que permitan llevar a cabo el procedimiento para el manejo de la información al igual que establecer estándares y normas de controles Criptográficos.

El Departamento de Los desarrolladores deberá cifrar la información reservada o restringida y garantizar que esta cuente la confiabilidad de los sistemas de almacenamiento de dicha información.

10.1 Políticas de controles criptográficos

- La organización Qwerty S.A junto con el área de infraestructura y seguridad informática deben establecer las herramientas que se utilizaran para le cifrado de la información, así mismo determinar los procedimientos necesarios para la gestión de las claves en cuanto a la generación, la longitud, y recuperación cuando se presente perdida, daño o divulgación de la misma. La cual debe aplicar un método de cifrado fuerte que no haya sido

rotos o ya vulnerados acorde a los reportes en la NIST https://csrc.nist.gov/ donde se promueve la validación de algoritmos criptográficos, con el ánimo de suplir las necesidades de la empresa o de los usuarios garantizando la protección junto con la confidencialidad e integridad de la información transmitida. Entre las que se puede destacar AES 256 bits para cifrado simétrico y Curva elíptica para cifrado asimétrico.

- Las llaves públicas de encriptación deben considerar la políticas de gestión de contraseñas para su generación; esta se hará aplicando procesos de expiración acorde a los criterios establecidos para cada herramienta de encriptación/y desencriptación , en los cuales se debe configurar tiempo para la expiración de la llave no superior a los 90 días y esta deberá ser reemplazada cada vez que las personas dueñas del proceso sean sustituidos del cargo o al momento de efectuar controles de cambios en las configuraciones de las herramientas.

- Los certificados digitales para entidad certificadora, herramientas sistemas de cifrado simétrico de documentos y demás recursos asociados para manejo de llaves o esquemas criptográficos; se deben custodiar de forma cifrada en cuanto a sus claves confidenciales dentro del Módulo de seguridad de hardware (HSM) como medio empleado por la empresa para resguardar de forma segura, protegida e identificables las claves criptográficas

11. POLITICAS DE SEGURIDAD FISICA

El centro de datos o Datacenter de Qwerty S.A donde se ubiquen los componentes y/o sistemas de información asociados a información confidencial de la entidad, deben estar resguardados en una zona restringida de acceso al público o al personal no autorizado, contemplando el uso de sistemas biométricos para el acceso, uso de sistema de video vigilancia, cerradura y enrejado apropiado para los racks y demás puertas de acceso a esta zona a fin de que la información salvaguarda dentro de estos activos no pueda ser accesible sin autorización, ni adulterada en su integridad.

11.1 Normas de Seguridad de La Información

La empresa debe garantizar que el sistema de seguridad permita llevar el control para el ingreso al Call Center, centros de datos, centros de cableado y otras áreas que contienen activos Considerados importantes de información; así como el archivo de control de ingreso y salida.

- Las instalaciones deberán contar son un sistema de respaldo de energía de mínimo 6 horas, así como sistemas de climatización que garanticen el buen funcionamiento de los equipos.
- No se permitirá el consumo de alimentos, bebidas y el consumo de cigarrillo dentro de las áreas de la empresa.
- El departamento encargado de soporte y mantenimiento deberá realizar el debido proceso donde se documentará y se dejará constancia del tipo de mantenimiento realizado a los equipos de tal forma que si se debe reparar dar de baja o realizar algún tipo de actualización se lleve control.
- Tanto los equipos de escritorio como los portátiles deberán contar con un firewall actualizado y configurado de tal forma que pueda garantizar la seguridad de la información allí contenida.
- En caso de que algún Directivo o colaborador de la empresa deba llevar un equipo portátil fuera de la instalación se dejara registro y una orden donde esta se compromete a responder tanto por la integridad física del equipo como por la información.
- En cuanto al uso del servicio de internet este es para uso exclusivo para el desarrollo de las actividades asignadas y no debe utilizarse para otro fin que no tenga relación con la organización.
- Al usar el internet se da por entendido que son responsables de buenas prácticas en Internet y que son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información.
- El uso para enviar, descargar o visualizar información que vaya contra la moral de las personas u de la organización está totalmente prohibido y acarrea sanciones.

12. POLITICAS DE SEGURIDAD EN EL PERSONAL

Los colaboradores de la organización Qwerty S.A deben asegurar el cumplimiento de las normas dispuestas en este manual los cuales se comprometen a cumplir con las responsabilidades asignadas como la confiabilidad de la información.

Estos deben conocer las responsabilidades asignadas a su cargo, así como los principios por lo que se rige la empresa.

En el momento de firmar contrato se capacitará al colaborador y se le hará firmar un acuerdo de confiabilidad de la información; así mismo se le dará a conocer las implicaciones que tendría en caso de incumplir cualquiera de las normas y políticas contenidas en este manual.

12.1 Reporte de incidentes de seguridad

Todo colaborador está en la obligación de reportarle al área encargada cualquier incidente de seguridad, amenaza, riesgo o vulnerabilidad.

- En caso de que la empresa verifique y compruebe que algún colaborador está infringiendo algún tipo de norma o está incumpliendo el acuerdo de confiabilidad la empresa está en la obligación de notificarle la terminación de contrato.
- Solamente se le dará paz y salvo a los colaboradores que ya no hagan parte de la empresa en el momento que el área encargada reciba equipos, documentación y cualquier elemento asignado cuando se realice la debida entrega y se haga verificación de la integridad de los mismos.

13. POLÍTICAS DE CAPACITACIÓN

La Empresa Qwerty S.A se compromete a difundir y capacitar a todo el colaborador que tengan algún tipo de vinculación directa o indirecta con la empresa en cuento a las normas y políticas de seguridad de la información contenidas en este manual.

- El comité de Seguridad se encargará de realizar el programa de capacitación y concientización del debido manejo y uso de los activos informáticos, así como de la información.
- Así mismo el comité de seguridad se encargará de difundir cada 6 meses actualizaciones o modificaciones a este manual.
- La empresa facilitara a sus colaboradores herramientas y mecanismos de capacitación con el fin de garantizar que los empleados están calificados en seguridad de la información.
- Los empleados especialistas en seguridad deberán contar con las debidas certificaciones referentes al tema. L
- Los colaboradores que se beneficien de los servicios de información de la entidad y hagan uso de los activos informáticos deberán cumplir y aplicar las políticas de seguridad de la información establecidas.
- Implementación de estrategias y planes que permitan que se concientice y entrene diferenciando entre el personal existente como del nuevo que permitan que el empleado tenga las herramientas que permita un mínimo de seguridad en el diario de sus actividades teniendo conocimiento en la identificación de amenazas y comportamientos no deseables entendiendo que la seguridad informática es una responsabilidad compartida y que cada uno es importante para ello.

14. POLÍTICA DE USO DE CORREO ELECTRÓNICO

El uso de correo electrónico perteneciente a la organización QWERTY S.A debe prestarse por un canal cifrado el cual debe ser garantizado por el área encargada.

Deberán cumplir las siguientes normas:

- Los usuarios son responsables de todas las actividades que se realicen con sus respectivas cuentas por lo que todo contenido e información que distribuya será responsabilidad exclusiva del usuario.
- Es responsabilidad de los usuarios informar al área encargada, cuando reciba correos de tipo SPAM, correo no deseado o de dudosa procedencia.
- Está prohibido utilizar el correo electrónico con propósitos no acordes a las funciones en la empresa, utilización del correo para la propagación y difusión de mensajes de índole político, religioso, ofensivo o contenido inapropiado y cualquier otro tema que no tenga que ver con la organización.
- Para los casos que se pierda de los datos para el ingreso a la cuenta de correo debe dirigirse por escrito al área encargada para su restablecimiento.
- Las cuentas que no se utilicen en un lapso de tiempo mayor a 90 días se notificara y pasado 120 días se desactivan temporalmente para su restablecimiento en el área encargada.
- La asignación y eliminación de cuentas del sistema se realizará solo por el personal encargado.

15. POLÍTICA DE DISPOSITIVOS MÓVILES

- Los equipos pertenecientes a la organización Qwerty S.A para salir deben ser autorizados por el responsable del área tecnológica y su salida se da una vez se verifique que:
- Tiene instalado antivirus actualizado y activado.
- Configuración de permisos de conexión USB.
- Restricción para la ejecución de aplicaciones
- Si posee información sensible este debe tener un sistema de autenticación ya sea contraseña, patrón, código de desbloqueo u otro método.

16. POLÍTICA DE SEGURIDAD DE RED

La empresa Qwerty S.A deberá modificar la arquitectura de la red realizando la segregación de esta y ubicando los equipos que se consideren contenga información crítica y de vital importancia para dar continuidad al negocio.

Esta también deberá contar con una red para visitantes y usuarios de otras dependencias.

- La conexión se debe realizar de manera segura por lo que ningún colaborador podrá realizar conexiones directas a redes externas.

- El firewall de la empresa será utilizado como único punto de acceso para conexiones a cualquier tipo de aplicación, así como a conexiones externas.
- Se deben aplicar controles de enrutamiento en la red con el fin de verificar el acceso a los recursos tecnológicos de la empresa.
- El acceso a las redes inalámbricas de la empresa será validado y autorizado únicamente por el comité de Seguridad.
- Se asignará una red para visitantes con las debidas protecciones de seguridad.
- El personal que desee hacer uso de la red inalámbrica solo podrá acceder a esta por medio de los equipos asignados por la entidad.
- Los funcionarios solo podrán acceder a conexiones de internet autorizados por la entidad.
- Los recursos de Tecnología de la Información son para uso exclusivo de la empresa.

17. POLÍTICAS DE USO DE LA INFORMACIÓN

Es responsabilidad de los Directivos, Colaboradores y cualquier persona que tenga vínculos comerciales con la organización garantizar el correcto uso y preservación de los activos informáticos dándoles un buen uso.

Se entiende que estos activos son propiedad de la organización en caso de que el activo sufra algún daño que no sea derivado del buen uso y manejo; será el colaborador quien deberá responder por el activo asignado.

- Para garantizar el debido uso de los recursos de tecnológicos de la información este se deberá hacerse bajo las normas y condiciones asignadas por el Departamento de soporte:
- Cualquier actualización, instalación de software en los equipos de cómputo será realizada y autorizada por el Departamento de soporte.
- Los colaboradores no podrán realizar ningún tipo de modificación a los activos Informáticos de la organización.
- Toda información considerada critica no será enviada por medios que no se consideren seguros y el área encargada garantizara el cifrado de la información, así como la asignación de claves de cifrado y él envió de estas por medios seguros.; al igual que la información no será ni discutida ni comunicada por medio telefónico.
- La utilización de recursos como impresoras, fotocopiadora, transmisión y recepción de fax deberán ser controlados, así como se les debe realizar una depuración periódica.
- Los equipos deben ser utilizados únicamente para el cumplimiento de la actividad económica de la operación los colaboradores no podrán acceder a páginas no autorizadas, redes sociales, descargar juegos, músicas y otro tipo de software que no sean autorizados por el área encargada.

- En caso de que se detente algún tipo de anomalía en el buen funcionamiento de los equipos este debe ser informado al área de soporte.
- En caso de encontrar algún tipo de vulnerabilidad el colaborador deberá informar inmediatamente al área encargada y bajo ninguna circunstancia este internet explotarla y hacer uso de esta para beneficio propio en caso de hacerlo esta será causal de una sanción.
- La configuración de los equipos informáticos estará a cargo del área de soporte.

18. POLÍTICAS CONTRA EL CÓDIGO MALICIOSO

- El área de soporte del Departamento de tecnología deberá revisar todo documento electrónico con el fin de evitar que dichos documentos contengan código malicioso; así como archivos adjuntos, correo electrónico, medios de almacenamientos (cd, USB, DVD, etc.).
- El Departamento de soporte garantizará que el Software Antivirus cuente con la correcta configuración y este será actualizado periódicamente.

19. POLÍTICAS DE GESTIÓN DE ACTIVOS

- El área comité se seguridad se compromete a realizar la respectiva clasificación de los activos teniendo en cuenta la importancia de estos para dar la continuidad del negocio.
- La información contenida en cualquier formato deberá ser resguardada por cualquier colaborador o proveedor según su nivel de criticidad para la empresa, esta será rotulada para poder llevar un control de la misma.
- Se debe realizar una eliminación segura de la información esto con el fin de garantizar la confidencialidad; este tipo de proceso será realizado por personal autorizado que cuente con los perfiles y privilegios asignados para hacerlo.
- El Departamento de soporte validara periódicamente los logs y registros de cada uno de los sistemas.
- Se encargarán de validar que el software de identificación de vulnerabilidades, la actualización y configuración del firewall con el que cuenta la empresa, así como el uso e implementación de herramientas que puedan garantizar la integridad de la red y los activos informáticos.
- Se implementará una IDS su función será detención de virus, bloqueo de correo no deseado, se debe llevar un registro de incidentes y soluciones esto con el fin de tener un plan de contingencia en caso de volverse a presentar a futuro.
- El departamento de Desarrollo WEB se le implementará un WAF con el fin de prevenir vulnerabilidades en las aplicaciones.

- El área de soporte deberá realizar mantenimientos preventivos los equipos de cómputo, redes, sistema de climatización, servidores, equipos de monitoreo y todos aquellos activos que se consideren esenciales para poder dar continuidad de la operación de la organización.
- Se realizará monitoreo de todos aquellos activos que se consideren críticos para el buen funcionamiento de la organización.

20. POLÍTICAS DE VIRTUALIZACIÓN DE SERVICIOS

- La empresa se compromete a trabajar por la seguridad de la información en internet con el fin de garantizar los principios de confiabilidad, integridad y disponibilidad de la información.
- Los sitios web de la organización deberán estar protegidos por certificados de autenticación.
- El Departamento de desarrollo de Software y aplicaciones deberá revisar el código fuente antes de ejecutarlo esto con el fin de evitar vulnerabilidades en el mismo.
- Se realizarán Testing de seguridad donde todo proyecto realizar deberá pasar por diferentes pruebas para garantizar que si son seguros.
- El área de desarrollo someterá dichas aplicaciones a pruebas de Stress que permitan evitar ataques como denegación de servicio y caída del mismo por alto tráfico de peticiones.
- La red deberá ser segmentada y deberá contar con una zona DMZ donde tanto las aplicaciones, Servidores, bases de datos tengan su propia red, toda aplicación se someteré a pruebas con el fin de garantizar la seguridad n los servicios.

20.1 Políticas de continuidad del servicio

Todos Aquellos Activos informáticos que contengan los servicios virtuales que ofrece la empresa deberán estar soportados por medio de un plan de contingencia que garantice la continuidad de la prestación del servicio ante cualquier posible eventualidad.

21. POLÍTICAS TRATAMIENTO DE DATOS PERSONALES

La empresa Qwerty se compromete a proteger los datos personales de los Directivos, colaboradores, proveedores y todas aquellas personas que tengan vínculos comerciales con la empresa; dando cumplimiento a lo expresado en la ley estatutaria 1581 de 2012 Para el tratamiento de datos, así como de la transferencia de los mismos.

Se validarán URL, emisión de certificados SLL, serán restringidos link que no sea de la entidad.

- La empresa manejara políticas de recepción, manipulación, transferencia, recuperación, conservación y archivos de documentación donde contenga información considerada crítica y sensible para dar continuidad al negocio.
- La empresa deberá disponer de los espacios adecuados para la conservación de la información.
- Se deberá tener en cuenta las normas vigentes sobre la protección de la información.
- Cuando un colaborador sea traslado o se retire deberá entregar toda documentación y archivos al área encargada para poder dar el respetivo trámite ya sea de archivo o de eliminación de la información.

22. POLÍTICAS DE CUMPLIMIENTO

La empresa Qwerty S.A velara por el cumplimento de los requisitos legales y de contratación donde se realizará la identificación de la documentación dando cumplimiento a todas aquellas normas y leyes que estén relacionadas con la seguridad de la información.

- El Departamento de Jurídica se encargará de verificar toda la documentación referente a proyectos, desarrollo de aplicaciones WEB, así como la actualización de los requisitos legales y reglamentarios aplicados a la actividad comercial de la empresa.
- El comité de Seguridad deberá supervisar que todo el software utilizado por la empresa sea legalmente utilizado respetando los derechos de autor con su debida licencia; se llevará inventario de software y Sistemas operativos permitidos en las estaciones de trabajo, equipos móviles pertenecientes a la empresa para el desarrollo de las funciones laborales.
- Los colaboradores no están autorizados a realizar la instalación de software o sistema operativos diferentes a con los que ya cuentan en sus estaciones de trabajo.
- Los colaboradores serán notificados sobre la prohibición de la duplicación de software o su documentación sin la autorización del propietario.

23. FUNCIONES DEL COMITÉ DE SEGURIDAD

La misión principal del Comité de la Seguridad de la Información será la de revisar y actualizar anualmente las políticas de seguridad y presentar sus propuestas o cambios a las directivas de la entidad, con el fin de alcanzar su aprobación mediante acto administrativo, se deberá establecer un Estatuto que contemple procesos disciplinarios y sanciones administrativas destinados a los eventos en que se violen los términos y condiciones dispuestos.

- Este apoyara y aprobara las directrices de seguridad de la información y se encargara de definir planes de contingencia y estrategias para la mitigación de riesgos.
- Verificara que los proyectos de desarrollo cumplan con los estándares de calidad y autenticidad, derechos de autor y cuente con los estándares de seguridad.
- Definirá y controlará las estrategias que el comité encargado de la seguridad de la información decida implementar para el control de la misma.
- Propondrá normas y procedimientos aplicar.
- Le comité evaluará y promoverá las inversiones en seguridad de la Información.
- Garantizar que el siguiente manual sea difundido.
- Verificara que los colaboradores apliquen y den cumplimiento a las políticas consignadas en este manual.
- Promoverá cursos y certificaciones referentes a la seguridad de la información y a las buenas prácticas.
- Realizara actividades para concientizar al personal de la importancia de las buenas prácticas y manejo del uso de la información.
- Se deberá encargar de verificar y hacer seguimiento a incidentes relacionados de Virus, dejando por escrito la evidencia para que en futuros incidentes se tenga soporte y guía para solucionar.
- Se deberá dejar documentación e Iniciar con la aplicación de los procedimientos para el tratamiento de los incidentes arrojados por el seguimiento realizado.
- Establecer, implementar, operar, monitorear, mantener y mejorar un Sistema de Gestión de Seguridad de la Información - SGSI bajo la norma ISO 27001:2013

Anexo 8 manual de seguridad

Fecha de Realización:	28/12/2020
Programa:	Especialización en seguridad informática
Línea de Investigación:	Infraestructura tecnológica y seguridad en redes
Título:	Diseño de controles y normas de seguridad para la empresa QWERTY S.A. Que garanticen la preservación de la integridad confiabilidad y disponibilidad de los activos informativos de la organización.
Autor(es):	Johana Marcela Gaitán López
Palabras Claves:	Amenaza, Incidente, Riesgo, Salvaguardas, Vulnerabilidad.
Descripción:	La Empresa QWERTY S.A. es una empresa del sector tecnológico que busca el desarrollo Tecnológico en comunidades colombianas a través del uso de tecnologías de información. Debido al volumen de inventario y de clientes externos y colaboradores internos que hacen uso de estas tecnologías se hizo necesario la implementación de normas y controles de seguridad para la protección de la información. En el presente trabajo se dio contexto al planteamiento de normas y medidas de seguridad para la protección de los activos informáticos de QWERTY S.A se tomó como referencia los conceptos relacionados con normas y estándares de seguridad, metodologías y herramientas que permitieran mitigar y prevenir las consecuencias antes las amenazas.

	Debido al volumen de inventario y de clientes externos y de los colaboradores de la organización que hacen uso de sus servicios se recomiendo la implementación de SGSI para el área de informática bajo la norma ISO/IEC 27001.

Fuentes bibliográficas destacadas:

AEC, A. E. Seguridad De La Información. {En línea} {06 de Abril del 2019} Disponible en: https://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

27000, I. Sistema de Gestión de la Seguridad de la Información, {en línea} {02 de Febrero del 2020}. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

27000. es, W. Sistema de Gestión de la Seguridad de la Información {en línea} {15 de Marzo del 2019}. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

AEC.ES. Seguridad De La Información. {En línea} {03 de febrero del 2020}. Disponible en: https://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

ALA/CFT, S. N. Ley Estatutaria 1266 de 2008. {En línea} {31 de Diciembre del 2008}. Disponible en: https://www.uiaf.gov.co/sistema_nacional_ala_cft/normatividad_sistema/leyes/ley_estatutaria_1266_2008

ALESSA, A. SGSI. {En línea} {09 de Junio del 2017} Disponible en: https://es.slideshare.net/AlessaParedes/sgsi-76786549

AMÉRICA ECONOMIA.COM. La fuga de información es una de las razones por las que las empresas pierden más dinero. {En línea}{27 de Julio del 2014}. Disponible en : https://mba.americaeconomia.com/articulos/notas/la-fuga-de-informacion-es-una-de-las-razones-por-las-que-las-empresas-pierden-mas-di

BERNARDO DAMELE Ag, M. S. SQLmap Herramienta automática de inyección de SQL y toma de base de datos. {En línea} {02 de Febrero del 2020}. Disponible en: http://sqlmap.org/

CAMELO, L. Marco legal de Seguridad de la Información en Colombia. {En línea} {23 de Febrero del 2010} Disponible en:

http://seguridadinformacioncolombia.blogspot.com/2010/02/marco-legal-de-seguridad-de-la.html

CASTILLO, I. M. Política General De Seguridad De La Información {En línea}. {03 de Marzo del 2019}. Disponible en: http://artesaniasdecolombia.com.co/PortalAC/images/politica-seguridad-informacion-proteccion-datos-personales.pdf

CCN, c. Margerit - Libro II - Catálogo de Elementos. {En línea} {10 de Octubre del 2012}. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

CCN-CERT. Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información {En línea} {10 de Octubre del 2012}. Disponible en https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html

CCN, Cert.Cni. ANEXO I Categorías de los sistemas ANEXO I Categorías de los sistemas\2. Dimensiones de la seguridad. {En línea} {19 de Abril del 2020}. Disponible en: https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1068

CERT, C, TÍTULO: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. {En línea} {05 de Marzo del 2020}, Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

COLOMBIA, C. ley de Delitos Informáticos en Colombia {En línea} {. 05 de Enero del 2009}. Disponible en: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

COLOMBIA, E. C. LEY 1273 DE 2009. {En línea} {05 de Enero del 2009}. Disponible en: http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf

COLOMBIA, E. C. LEY 603 DE 2000. {En línea} {27 de Julio del 2000}. Disponible en: http://derechodeautor.gov.co/documents/10181/182597/603.pdf/42c15f4a-afe5-4339-97ca-a61026450307

COMUNICACIÓN, I. N. Inteco. Obtenido de Implantación de un SGSI en la empresa: {En línea} {16 de Marzo del 2019} Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

COURSEWARE. Marco Contextual.{ en línea } { 27 de Agosto 2019 } Disponible en : Obtenido de

http://courseware.url.edu.gt/Facultades/Facultad%20de%20Ciencias%20Econ%C3%B3micas/T%C3%A9cnicas%20B%C3%A1sicas%20de%20Investigaci%C3%B3n/Segundo%20ciclo%202010/Marco%20de%20referencia/01%20Marco%20de%20referencia/marco_contextual.html

CUERVO, C. y. Política de seguridad del SGSI. {En línea} {04 Abril del 2019}. Disponible en: https://www.caroycuervo.gov.co/recursos/6.1.POLITICA_DE_SEGURIDAD_ICC_0.pdf

D. ESPINOSA, J. M... Gestión Del Riesgo En La Seguridad De La Información Con. {En Línea} {12 de Diciembre del 2014} Disponible en: http://web.usbmed.edu.co/usbmed/fing/v5n2/pdf/Articulo_Gestion_Riesgo_Seguridad_Informacion

DATA, Arquitectura Orientada a Servicios (SOA). {En línea} {02 de Febrero del 2020}. Obtenido de https://www.powerdata.es/soa

DUOC, B. {En línea} {2018}. Definición. Disponible en: uoc.cl/biblioteca/crai/definicion-y-proposito-de-la-investigacion-aplicada

DUOC, B. {En línea} {2018}. Definición. Disponible en: uoc.cl/biblioteca/crai/definicion-y-proposito-de-la-investigacion-aplicada

DUOC, B. {En línea} {2018}. Definición. Disponible en: uoc.cl/biblioteca/crai/definicion-y-proposito-de-la-investigacion-aplicada

DVWA. Damn Vulnerable Web Application {En Línea} {02 de Febrero del 2020}. Disponible en: http://www.dvwa.co.uk/

DVWA. {En línea} {06 de febrero del 2020} Disponible en: http://www.dvwa.co.uk/

EAR. {En línea} {06 de Febrero de 2019}. Disponible en: https://www.ar-tools.com/es/tools/pilar_basic/v74/download.html

ES-ET. Guía De Ransomware. {En línea} {Abril del 2019} Disponible en: https://www.welivesecurity.com/wp-content/uploads/2017/11/guia-ransomware.pdf

ESPAÑA, G. d. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid: © Ministerio de Hacienda y Administraciones Públicas. {En línea} {Abril del 2019}. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html

ESTEBAN, E. J. SGSI: Gestión y Seguridad.{ En línea} { abril del 2007} disponible en : http://secugest.blogspot.com/2007/04/sgsi-gestion-y-seguridad.html

EXCELLENCE, I. ISO 27001: Amenazas y vulnerabilidades {En Línea} {06 de Abril del 2015} Disponible en: https://www.pmg-ssi.com/2015/04/iso-27001-amenazas-y-vulnerabilidades/

EXCELLENCE, I. ISO 27001 Como implantar políticas de Gestión de un Sistema de Gestión de Seguridad de la Información. {En línea} {07 de Marzo del 2014}. Disponible en: https://www.pmg-ssi.com/2014/03/iso-27001-chttps://www.pmg-ssi.com/2014/03/iso-27001-como-implantar-politicas-de-gestion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/

FORTINET. Más del 80 por ciento de las compañías en Colombia son vulnerables a ataques informáticos. {En línea} {Noviembre del 2018} Disponible en: https://www.gartner.com/teamsiteanalytics/servePDF?g=/imagesrv/media-products/pdf/fortinet/fortinet-1-5VG5OU4.pdf

FORTINET. Más del 80 por ciento de las compañías en Colombia son vulnerables a ataques informáticos. {En línea} {Noviembre del 2018} https://www.gartner.com/teamsiteanalytics/servePDF?g=/imagesrv/media-products/pdf/fortinet/fortinet-1-5VG5OU4.pdf

GONZÁLEZ, S. F. Diagnostico Y Actualización Del Sistema De Gestión De. {En línea} {28 de 05 de 2013}. Disponible en: http://repository.ucatolica.edu.co:8080/bitstream/10983/866/2/Mantenimiento%20y%20Actualizacion%20de%20un%20sistema%20de%20gestion%20de%20seguridad%20de%20la%20informacion%20para%20ventas.pdf

GONZÁLEZ, W, Técnicas De Recolección De Datos. {En línea}. {13 de 05 de 2009}.Disponible en: http://recodatos.blogspot.com/2009/05/tecnicas-de-recoleccion-de-datos.html

HUERTA, A. Análisis de riesgos con MAGERIT en el ENS (II). {En línea}{26 de 04 de 2012}. Obtenido de https://www.securityartwork.es/2012/04/26/analisis-de-riesgos-con-magerit-en-el-ens-ii/

HUERTA, A. {En línea} {26 de Abril del 2012}. https://www.securityartwork.es/2012/04/26/analisis-de-riesgos-con-magerit-en-el-ens-ii/. Obtenido de https://www.securityartwork.es/2012/04/26/analisis-de-riesgos-con-magerit-en-el-ens-ii/

INFORMÁTICAS, O. p. (s.f.). Metodología Para La Gestión De La Seguridad Informática. {En línea} {Agosto del 2013} Disponible en:

https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf

INGENIEROS, A. E. (Encuesta-Global-Seguridad-Informacion-2018-19 {En línea} 19 de Febrero del 2020). Disponible en: https://es.scribd.com/document/423161641/Ey-Encuesta-Global-Seguridad-Informacion-2018-19

ISO, N. ISO 27001 Gestión De La Seguridad De La Información {En línea} {02 de Febrero de 2020}. Obtenido de https://www.normas-iso.com/iso-27001/

ISO, S. Sistemas de Gestión de Riesgos y Seguridad. {En línea} { Marzo del 2019). Disponible en: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

LEBET, G. Técnicas De Recolección De Datos. {En línea} {Abril del 2019} https://gabriellebet.files.wordpress.com/2013/01/tecnicas-de-recoleccic3b3n4.pdf

LIZARAZO, L. K. Planteamiento De Un SGSI Basado En La Norma ISO 27001:{} En línea} (27 de 08 de 2016). {27 de 08 de 2016}. Disponible en: http://polux.unipiloto.edu.co:8080/00003412.pdf

M. AMUTIO, J. C. Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libros I, II y III - . Madrid, España: Eds., MAGERIT {En línea} {2012} Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789

MARQUES, L. Mapa de los ataques cibernéticos en Latinoamérica. {En línea} {11 de Febrero del 2019). Disponible en : https://blog.f-secure.com/es/mapa-de-los-ataques-ciberneticos-en-latinoamerica-2018/

MIERES, J. Herramientas para evitar ataques. {En línea} {30 de Abril del 2009}. Obtenido de https://www.welivesecurity.com/wp-content/uploads/2014/01/herramientas_evitar_ataques_informaticos.pdf

MINISTERIO DE HACIENDA Y ADMINISTRACIÓN PÚBLICA. {En Línea} {2020} Obtenido de Margerit -V3 libro 1: https://es.scribd.com/document/337634447/2012-Magerit-v3-libro1-metodo-es-NIPO-630-12-171-8-pdf

MINTIC. Ley 1273 de 2009. {En línea} {04 de Enero del 2009} Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

MINTIC, Ley 1341 de 2009. {En línea}. {29 de Julio del 2009}. Disponible en https://www.mintic.gov.co/portal/604/w3-article-3707.html

MONTES, S. {En línea} {08 de 09 de 2018} Disponible en. https://www.larepublica.co/internet-economy/empresas-colombianas-solo-invierten-20-de-presupuesto-en-ciberseguridad-2768645

MONTES, S. Empresas colombianas solo invierten 20% de presupuesto en ciberseguridad {En Línea} {08 de Septiembre de 2018}. Disponible en: https://www.larepublica.co/internet-economy/empresas-colombianas-solo-invierten-20-de-presupuesto-en-ciberseguridad-2768645

NEGOCIOS, T. p. Qué es un ciberataque y qué tipos existen. { En línea} {03 de 02 de 2020}. Disponible en: https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-un-ciberataque-y-que-tipos-existen/

PAREDES, M. A. Sistema de Gestión de la Seguridad de la información SGSI {En línea}. {09 de 06 de 2017} Disponible en: https://es.slideshare.net/AlessaParedes/sgsi-76786549

PROFITLINE. Actualmente Como se encuentra Colombia en Seguridad Informática. {En línea} {26 de Febrero del 2019}. Disponible en: https://profitline.com.co/actualmente-como-se-encuentra-colombia-en-seguridad-informatica/

PUBLICA, M. d. Magerit 3.0 Proyectos de análisis de riesgos {En línea} {05 de Marzo del 2020}, Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

REPUBLICA, C. d. LEY ESTATUTARIA 1581 DE 2012. {En línea} {17 de 10 de 2012} Disponible en: https://www.sisben.gov.co/Documents/Informaci%C3%B3n/Leyes/LEY%20TRATAMIENTO%20DE%20DATOS%20-%20LEY%201581%20DE%202012.pdf

REYDES. Proyecto OWASP WebScarab. {En línea} {16 de 09 de 2014}. Disponible en: http://www.reydes.com/d/?q=Proyecto_OWASP_WebScarab

T.*, C. H. AMENAZAS INFORMÁTICAS Y. [En línea} {2019}. Disponible en: file:///C:/Users/JOHANAJANUS/Downloads/965-Texto%20del%20art%C3%ADculo-3375-2-10-20180126.pdf

TECNOLOGY, e. s. La Seguridad Como Rehén Tendencias 2017 {En línea} {Diciembre del 2017} Disponible en: https://www.welivesecurity.com/wp-content/uploads/2016/12/Tendencias-2017-eset.pdf

TECNOSFERA. En un segundo se presentan en promedio 9 infecciones con malware. {En línea} (15 de Agosto del 2018). Disponible en:

https://www.eltiempo.com/tecnosfera/novedades-tecnologia/aumento-de-ataques-ciberneticos-en-america-latina-en-2018-256078

TENABLE. Nessus. {En Línea} {02 de Febrero del 2020). Disponible en: https://www.tenable.com/downloads/nessus

TEZER, P. O. Cómo instalar y usar Logwatch Log Analyzer and Reporter en un VPS. {En línea} {23 de 11 de 2017}. Disponible en: https://www.digitalocean.com/community/tutorials/how-to-install-and-use-logwatch-log-analyzer-and-reporter-on-a-vps

TOOLS, Pear / Pilar. {En linea}. {02 de Febrero de 2020}. Disponible en: https://www.ar-tools.com/es/index.html

TURMERO, P. Administración del control de accesos, adecuado a los sistemas de información. {En línea} {01 de Abril del 2019}. Disponible en: https://www.monografias.com/trabajos102/administracion-del-control-accesos-adecuado-sistemas-informacion/administracion-del-control-accesos-adecuado-sistemas-informacion.shtml

UNAD. (Propuesta para el desarrollo de la alternativa de grado. Universidad Nacional Abierta y a distancia Obtenido de Escenario2_EnfoqueDirectivoAdministrativo.pdf

VALDEZ DELGADO, Andrés Israel Manual de procedimientos e higiene. {En línea} {2015}. Disponible en: https://dspace.ups.edu.ec/bitstream/123456789/10260/1/UPS-GT001284.pdf

Contenido del documento:	En el documento se desarrolla el diseño de un plan de seguridad de la información que contenga políticas claras sobre el uso y manipulación de los activos informáticos de la empresa Qwerty S.A lo que se busca es el mejoramiento de la seguridad de la información de los activos informáticos de la empresa mediante la utilización de diferentes herramientas y el uso de la metodología Margerit para el desarrollo de la investigación. Este tipo de investigación está vinculada a la realización de la investigación pura, lo cual nos sirvió de referencia para la elaboración del análisis de riesgos informáticos en la empresa QWERTY S.A este tipo de investigación nos permitió encontrar una posible solución a los problemas encontrados. Como parte del desarrollo de la investigación aplicada, se realizaron algunas actividades como lo son: • Generación del plan de trabajo y establecimiento de plazos de tiempo: se fijó un cronograma de actividades donde se especificaron las diferentes actividades a realizar con el fin de alcanzar los objetivos propuestos. Al igual que el tiempo para realizar las actividades. • Se definieron los objetivos del proyecto y el alcance del mismo teniendo en cuenta la formulación del problema. • Se verifico si la empresa en cuestión tenía archivos, para de esta forma poder recolectar información referente a la seguridad informática; tales como

	documentos de la organización para poder conocer el contexto y el entorno de la empresa su estructura, normas y reglamentación referente al tema. • Se realizó un reconocimiento del Entorno para poder evaluar los activos, su estado; la infraestructura de las instalaciones; poder medio del análisis de Riesgos se verifico si cumplen las normas mínimas de seguridad. • Se identificaron las vulnerabilidades de los activos; así mismo se realizó el respectivo análisis de estas para determinar su origen, por medio de la matriz de valoración de riesgos. • Después de realizar el respectivo análisis se formularon sugerencias y recomendaciones para finalmente discutir los resultados. • Se realizó entrega del informe técnico con los respectivos hallazgos para entregar como resultado el informe a las directivas de la organización. Dicho proceso se realizó con el siguiente orden: • Elaboración del cuestionario. • Entrevista e inspección de la empresa. • Consolidación de los resultados. • Análisis de los resultados. • Elaboración de informes y plan de acción. • Entrega de resultados.
Marco Metodológico:	"MAGERIT es la metodología aplicada para conocer las amenazas a los cuales se encuentran expuestos los activos que forman parte de la empresa QWERTY S.A. mediante la implementación de herramientas del análisis de

	riesgos esta dictamina el tipo de normas y políticas aplicar con el fin de proteger las tecnologías de la información.” Con la utilización de esta metodología que se busca es lograr los siguientes objetivos: • Concientizar a personas encargadas de los sistemas de información de los riesgos a los que pueden estar expuestos los activos informáticos al darles un uso inadecuado. • Proponer una metodología para llevar a cabo el análisis de riesgos. • Especificar y planificar que dimensión tienen las amenazas y de qué forma se pueden mantener bajo control. • Buscar mecanismos para que la organización este al día y atenta a los procesos de auditoría, certificaciones. Proceso que se deben llevar a cabo: **1**. catalogar de los activos según su importancia en la organización, **2.** Definir el tipo de amenazas a las que puedan estar expuestos los activos. **3.** verificar con qué tipo de salvaguardas se cuenta y que tan efectivas son frente una amenaza. **4.** Estimar el porcentaje de riesgo que puede tener una amenaza sobre un activo informático en la organización. **5**. Estimar el nivel de riesgo y el porcentaje ponderado de la ocurrencia de un evento. Técnica de Recolección y Procesamiento de Datos

	Para la elaboración de este trabajo se comenzara con el proceso de Observación, lo cual ayudará a extraer y validar la información recolectada durante este proceso, realizando la debida verificación de los elementos físicos de las diferentes áreas de la empresa, este proceso se llevara a cado teniendo en cuenta los tiempos de ejecución de cada actividad, de igual forma se llevara un registro de las observaciones realizadas verificando que se cumplan las normas de seguridad en cada área. Adicionalmente se le realiza una entrevista a los empleados de las oficinas con preguntas básicas sobre el conocimiento sobre la seguridad de la información que medidas aplican de estas; con qué frecuencia el área encargada hace el cambio de claves y si saben si estos cuenta con algún programa especializado para llevar el registro y control de las mismas. También se verificara el estado de los activos informáticos y la dependencia de los mismos, si estos cuentas con las últimas versiones de software y programas al igual del estado en que se encuentra todo esto para poder llegar a la conclusiones de a cuales amenazas y riesgos están expuestos los activos informáticos y de esta manera generar un informe para la gerencia

	con las recomendaciones y medidas pertinentes para cada caso.
Conceptos adquiridos :	Las Bases para realizar un análisis de riesgos identificando las amenazas a las que pueden estar expuesto los activos. Se ampliaron conocimientos sobre la aplicación de la norma ISO27001 sobre la formulación de políticas y normas y implementación de las salvaguardar para la mitigación de riesgos. Se adquirieron conocimiento técnico de las herramientas utilizadas para el análisis de vulnerabilidades.
Conclusiones:	1. Con la elaboración de este proyecto aplicado se lograron identificar los principales inconvenientes de seguridad que presenta la empresa Qwerty S: A se utilizaron herramientas como la observación directa, la aplicación de un cuestionario donde aplicado a algunos colaboradores de la organización ayudo a determinar qué áreas de la empresa se encuentran más en riesgo de presentar algún tipo de vulnerabilidad; este proceso sirvió para poder tener mayor claridad para poder definir el punto de partida para el desarrollo del SGSI. 2. Con la utilización de la metodología MAGERIT se lograron establecer los indicadores de gestión lo cual sirvió para identificar las amenazas a las que pueden estar expuestos los activos de la información de la organización Qwerty S. A se llegó a esta conclusión mediante el

	desarrollo y aplicación del análisis de riesgo cualitativo esto se hizo mediante un análisis de riesgos cualitativo, permitiendo identificar el nivel de madurez en la seguridad con el que contaba la empresa. 3. Con los datos recogidos mediante el tipo de análisis se permitió identificar las amenazas y así mismo poder recomendar los controles y políticas aplicar los cuales serán consignados en el planteamiento del SGSI para la empresa. 4. El análisis de riesgos, la definición de políticas de seguridad, la declaración de aplicabilidad y aplicabilidad de los controles conforma el diseño del SGSI bajo la norma ISO/IEC 27001 tiene su único fin en garantizar la integridad, disponibilidad y confiabilidad de la información.; La aplicación de (SoA) permitirá crear un sistema escalable para impulsar el rendimiento, reducción de costos de TI y mejorar los procesos de la organización