# IMPLEMENTAR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA QWERTY S.A.

MARLEN ROCIO ONTIBÓN ROMERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2.020

# IMPLEMENTAR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA QWERTY S.A.

MARLEN ROCÍO ONTIBÓN ROMERO

Proyecto de Grado – Proyecto Aplicado presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMATICA

Ing. Yenny Stella Núñez Álvarez
Directora de Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2.020

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

## DEDICATORIA

A Dios, quien le da sentido a mi vida, a mi hija, mi inspiración y a mi madre que siempre ha sido un ejemplo a seguir y con su apoyo incondicional ha hecho posible cumplir esta nueva meta en mi vida.

## AGRADECIMIENTOS

Agradezco a las directivas, directores, tutores y asesores de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su dedicación y acompañamiento a lo largo del proceso de formación, hacen posible a través de la modalidad virtual, acceder a la formación en el nivel de especialización, a quienes como yo, tenemos una familia y laboramos para proveer el sustento y un mejor futuro a nuestros hijos.

**CONTENIDO**

pág.

INTRODUCCIÓN ..... 15
1. DEFINICIÓN DEL PROBLEMA ..... 16
1.1 ANTECEDENTES DEL PROBLEMA ..... 16
1.2 FORMULACIÓN DEL PROBLEMA ..... 17
2. JUSTIFICACIÓN ..... 18
3. OBJETIVOS ..... 19
3.1. OBJETIVOS GENERAL ..... 19
3.2. OBJETIVOS ESPECÍFICOS ..... 19
4. MARCO REFERENCIAL ..... 20
4.1. MARCO TEÓRICO ..... 20
4.1.1. Seguridad informática ..... 20
4.1.2. Análisis de Riesgos ..... 21
4.1.3. Norma ISO 27000 ..... 22
4.1.4. Metodologías para el análisis de riesgos ..... 24
4.1.5. Sistema de gestión de Seguridad de la Información ..... 25
4.2. MARCO CONTEXTUAL ..... 26
4.3. ANTECEDENTES ..... 32
4.3.1. MARCO LEGAL ..... 32
5. ENFOQUE METODOLÓGICO ..... 35
5.1. Metodología Magerit ..... 35
5.2. Metodología para la implementación del SGSI ..... 36
6. DESARROLLO DE LOS OBJETIVOS ..... 39
6.1. estimaciones ..... 39
6.1.1. Lo que se espera lograr con la implementación ..... 39
6.1.2. Determinación del tiempo estimado para el diseño del sistema ..... 39
6.1.3. Proyección del valor del diseño e implementación del sistema ..... 40
6.2. IDENTIFICACION DE ACTIVOS ..... 46
6.2.3. Enfoque de evaluación de los riesgos ..... 77
6.2.4. Informe de evaluación de los riesgos ..... 86
6.2.5. Plan de tratamiento de riesgos ..... 90
6.3. Manual de seguridad de la Información. Para Qwerty S.A. ..... 101
6.2.2. Procedimientos ..... 105
6.3.3. Política de seguridad de la información ..... 113
6.3.4. Declaración de aplicabilidad ..... 129
6.3.5. Sensibilización y capacitación en seguridad de la información en Qwerty S.A. 145
6.3.6. Resultados ..... 148

7. CONCLUSIONES.....151
8. RECOMENDACIONES .....152
9. BIBLIOGRAFÍA .....153

## LISTA DE TABLAS

pág.

Tabla 1. Probabilidad de ocurrencia del riesgo .....69

## LISTA DE FIGURAS

Pág.

Figura 1. Estructura de Qwerty S.A.....27
Figura 2. Ciclo Deming y la ISO 27001.....36
Figura 3. Cumplimiento de requerimientos ISO27001 .....57
Figura 4. Estructura Organizacional.....103

## LISTA DE CUADROS

pág.

Cuadro 1. Activos de información de Qwerty S.A. .....29
Cuadro 2. Tiempo estimado para el diseño del sistema .....39
Cuadro 3. Costo del diseño.....41
Cuadro 4. Costo de Implementación.....41
Cuadro 5. Escala medición impacto.....46
Cuadro 6. Activos de información Qwerty S.A. .....47
Cuadro 7. Escala de valoración de cumplimiento de requerimientos ISO 27001 ...49
Cuadro 8. Cumplimiento de requerimientos ISO27001 Qwerty S.A.....49
Cuadro 9. Valoración cualitativa de activos de Qwerty S.A. .....57
Cuadro 10. Valoración cuantitativa de activos de Qwerty S.A. .....60
Cuadro 11. Valoración cuantitativa de activos de Qwerty S.A. Continuación.....61
Cuadro 12. Valoración de Amenazas y vulnerabilidades.....63
Cuadro 13. Valoración del Riesgo .....69
Cuadro 14. Riesgos priorizados.....77
Cuadro 15. Evaluación de riesgos .....86
Cuadro 16. Plan de tratamiento de riesgos.....90
Cuadro 17. Normatividad de seguridad de la información aplicable a Qwerty S.A. ..... 102
Cuadro 18. Roles y responsabilidades SGSI.....103
Cuadro 19. Procedimiento de Gestión de Cambios.....108
Cuadro 20. Procedimiento Control de Versiones.....110
Cuadro 21. Procedimiento Gestión de incidentes de seguridad de la información ..... 111
Cuadro 22. Declaración de aplicabilidad.....129
Cuadro 23. Evaluación de necesidades. Continuación.....146
Cuadro 24. Actividades de sensibilización y capacitación y sus costos.....147

## GLOSARIO

ADMINISTRACIÓN DEL RIESGO. Toda actividad, procedimiento o mecanismo que es utilizado por una organización para mitigar los riesgos de seguridad que se haya determinado deban ser tratados en una organización para evitar que afecten los objetivos de una empresa.

AMENAZA. “Todas aquellas situaciones o acciones que pueden alterar, o impactar o afectar negativamente los activos de información de una empresa”[1].

AUTENTICIDAD. Se refiere al proceso de identificación y validación de un usuario dentro de una red empresarial o sistema.

CONFIABILIDAD. Corresponde con la protección contra alteraciones no autorizadas de la información.

CONFIDENCIALIDAD. Indica que la información sólo puede ser accedida por personas autorizadas desde los diferentes procesos de negocio.

DISPONIBILIDAD. Hace referencia a que la información pueda ser recuperada, o consultada cuando se requiera por las personas autorizadas desde los diferentes procesos de negocio.

ESTIMACIÓN DEL RIESGO. “Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo”[2].

EVITACIÓN DEL RIESGO. “Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación”[3].

IMPACTO. “Cambio adverso en el nivel de los objetivos del negocio logrados”[4].

INFORMACIÓN. “Es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada”.

INTEGRIDAD. Tiene relación con la precisión, validez y completes que debe mantener la información a través de los diferentes procesos de negocio.

---

[1] MARKUS Erb, Gestión de Riesgo en la Seguridad Informática. [Consultado 1 de mayo de 2020] Disponible en: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades
[2] ICONTEC, NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27005, p 2.
[3] Ibid, p 2.
[4] Ibid, p 2.

PILARES DE LA INFORMACIÓN. Corresponde con las características que debe poseer la información: la confidencialidad, integridad y disponibilidad.

PRIORIZACIÓN DEL RIESGO. Es la valoración cuantitativa o cualitativa que una organización puede efectuar de un riesgo, a partir de la cual se determina si requiere o no tratamiento.

REDUCCIÓN DEL RIESGO. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo[5].

RETENCIÓN DEL RIESGO. Aceptación de la pérdida o ganancia proveniente de un riesgo particular[6].

RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN. Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización[7].

RIESGO. "Probabilidad de que una amenaza se materialice aprovechando una vulnerabilidad y causando daño (impacto) en un proceso o sistema"[8].

SEGURIDAD DE LA INFORMACIÓN. Se ocupa de la protección de: la integridad, disponibilidad y confidencialidad de los activos de información de una empresa.

SEGURIDAD INFORMÁTICA. Se ocupa de la protección de la infraestructura tecnológica de una empresa.

TOLERANCIA. Nivel mínimo o máximo aceptable de un factor de riesgo antes de que requiera una intervención orientada a su tratamiento y mitigación.

TRANSFERENCIA DEL RIESGO. Compartir con otra de las partes la pérdida o la ganancia de un riesgo[9].

TRAZABILIDAD. En todo momento es posible identificar nuevas transacciones y cuando se registran.

VULNERABILIDAD. Es toda debilidad asociada a un activo de información que puede ser explotada por un atacante.

---

[5] ICONTEC, NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27005, p 2.
[6] Ibid, p 2.
[7] Ibid, p 2.
[8] ESCRIVÁ, G. G., Romero, S. R. M., & Ramada, D. J. (2013). Seguridad informática. España: Macmillan Iberia, S.A. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43260?page=1
[9] ICONTEC, NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27005, p 2.

## RESUMEN

La implementación de un Sistema de Gestión de Seguridad de la información en cualquier empresa representa un reto para el cual es necesario contar con el apoyo de personal externo que cuente conocimiento y la experticia necesaria para lograr atender las expectativas como las planteadas para Qwerty S.A., empresa dedicada a la formación que está muy interesada e adelantar esta implementación para proteger sus activos de información.

La labor de implementación, conlleva en sí misma un proceso de apropiación, interiorización y adopción de la cultura de la seguridad, teniendo en cuenta que uno de los activos más importantes reside precisamente en las personas que hacen parte de la organización, sobre las cuales recae acciones y actitudes que pueden ser determinantes a tal punto, que se pueden constituir en el sostén y la mayor fortaleza de cualquier Sistema de Gestión de Seguridad de la Información.

Es por todo esto, que a partir de su experiencia y la preocupación por proteger a sus usuarios y operar en condiciones adecuadas de seguridad ha optado por abordar este proyecto por fases, de tal manera que pueda adelantar la implementación en una fase inicial e ir fortaleciendo este sistema con el tiempo. En consecuencia, espera que como parte de este proceso pueda conformar un equipo de proyecto integrado por personal externo e interno, que durante este proceso permita el buen término del mismo y posteriormente asuma los diferentes roles necesarios para apoyar a la organización con la dinámica que debe mantenerse para la adecuada gestión de riesgos y mantenimiento del sistema de gestión de seguridad de la información con la premisa del mejoramiento continuo.

## ABSTRACT

The implementation of an Information Security Management System in any company represents a challenge for which it is necessary to have the support of external personnel who have the knowledge and expertise necessary to meet the expectations such as those set for Qwerty SA, a company dedicated to training who are very interested and forward this implementation to protect their information assets.

The implementation work, involves in itself a process of appropriation, internalization and adoption of the safety culture, taking into account that one of the most important assets resides precisely in the people who are part of the organization, on whom falls actions and attitudes that can be decisive to such an extent that they can become the support and the greatest strength of any Information Security Management System.

It is for all this that based on its experience and concern to protect its users and operate in adequate security conditions, it has chosen to approach this project in phases, so that it can advance implementation in an initial phase and gradually strengthen this system over time. Consequently, it hopes that as part of this process it will be able to form a project team made up of external and internal personnel, who during this process will allow its success and subsequently assume the different roles necessary to support the organization with the dynamics it should Maintain itself for proper risk management and maintenance of the information security management system with the premise of continuous improvement.

# INTRODUCCIÓN

La implementación de un sistema de seguridad de la información en cualquier empresa sin importar el tamaño de la misma, es más importante de lo que a primera vista puede parecer para la alta dirección de la empresa. El reto de hoy día es formar más profesionales para que con el conocimiento necesario puedan emprender y asumir proyectos como el que quiere estructurar Qwerty S.A., quien ha visto con preocupación que la seguridad de la información es una necesidad sin la cual, asumir nuevos retos de crecimiento puede exponer su empresa y todo lo que ha construido a lo largo del tiempo que viene prestando servicios de formación. Por tanto, ha decidido emprender este proyecto de Diseño del Sistema de Gestión de Seguridad de la Información para la empresa y aunque cuenta con algunas restricciones y limitantes quiere iniciarlo en el corto plazo, de tal manera que pueda minimizar los riesgos asociados a la seguridad de la información y los posibles impactos sobre su proyecto de crecimiento.

Para abordar esta implementación, recurrirá a personal externo quien dirigirá, estructurará e implementará el proyecto con la participación de los empleados de Qwerty S.A. y el apoyo de la alta dirección.

Para la ejecución del proyecto, se tomará como referencia las normas ISO27000 aplicables, los lineamientos de gestión de proyectos PMI, entre otros estándares aplicables y metodologías, observando la normatividad y legislación vigente aplicable en Colombia tanto para el sector al que pertenece Qwerty S.A., como a nivel de seguridad de la información, transacciones electrónicas, protección de datos personales, entre otros.

Este proyecto corresponde con la opción de proyecto aplicado para optar por el grado de especialista en seguridad informática.

# 1. DEFINICIÓN DEL PROBLEMA

## 1.1 ANTECEDENTES DEL PROBLEMA

De acuerdo con el escenario descrito para la opción de proyecto aplicado: Diseño del Sistema de Gestión de Seguridad para la empresa Qwerty S.A:

Qwerty S.A., es una empresa del sector de tecnología cuya labor está orientada a impulsar el desarrollo de comunidades colombianas, a través del uso de tecnologías de la información. Para hacerlo, cuenta con un equipo de 120 personas entre directivos, administrativos y operativos que consultan datos para realizar sus labores.

Para operar, cuenta con un área de sistemas que realiza labores relacionadas con el aprovisionamiento de infraestructura, desarrollo de aplicaciones y servicios de soporte a la empresa 24 horas 7 días de la semana.

Dentro de los servicios que soporta están: correo electrónico, gestión y mantenimiento de infraestructura de computación, equipos de apoyo a la gestión educativa, internet, gestión de usuarios y contraseñas, apoyo al sistema de gestión de calidad, apoyo a las dependencias.

Para su operación cuenta con la siguiente infraestructura:

- ✓ Siete (7) servidores
- ✓ Dieciocho (18) equipos de cómputo
- ✓ Dos impresoras corporativas
- ✓ Un (1) cortafuegos
- ✓ Cuatro (4) Hub
- ✓ Seis (6) switches
- ✓ Seis (6) teléfonos IP
- ✓ Dos (2) puntos de acceso

## 1.2 FORMULACIÓN DEL PROBLEMA

Qwerty S.A., con el soporte de su área de tecnología administra y gestiona servicios a nivel de infraestructura, desarrollo y soporte 24/7 con algunas limitantes en el control de acceso, servidores que se encuentran en un área física que no cumple condiciones climáticas adecuadas, no tiene segmentación de red, no hay monitoreo a la actualización del software antivirus, en el sistema de nómina y facturación en días de alto flujo, el registro de datos puede ser realizado por personal de prácticas o contratos de aprendizaje y el firewall de la empresa no está configurado para autorizar o denegar conexiones. Situaciones por las cuales, Qwerty S.A., ha decidido implementar un sistema de gestión de seguridad de la información para la empresa basado en la norma ISO 27001 y requiere que se adelante el diseño que incluya: lo que se espera lograr, el tiempo estimado para el diseño del sistema y una proyección de costos e implementación del sistema.

# 2. JUSTIFICACIÓN

Qwerty S.A. no ha tenido ninguna incidencia de seguridad de la información hasta el momento, no obstante, habiendo identificado algunas debilidades al interior de su organización, es consciente de que existen riesgos de seguridad a los que está expuesto, que pueden comprometer su operatividad y la empresa misma.

La opción de proyecto aplicado con el caso de Qwerty S.A., permite ejemplificar por una parte, la situación en la que se encuentran muchas empresas que aún no cuentan con un sistema de gestión de seguridad de la información y pese a que pueden tener un conocimiento o conciencia mínima de su realidad y de los casos cada vez más cercanos que se conocen a través de medios de comunicación sobre los incidentes que se han venido presentando a diferentes niveles, porque nadie está exento de ser objeto de alguna intrusión o ataque. Si nos remitimos a valoraciones efectuadas con las empresas más grandes del mundo, de acuerdo con la información publicada por la firma consultora EY[10] quien consultó a 1400 líderes de seguridad confirmaron que la ciberseguridad no es un tema estratégico para el 55% de las empresas, el 87% opera con un presupuesto limitado, no obstante el 77% busca trabajar con técnicas de protección más allá de lo básico.

Cifras que confirman que es necesario, por una parte, que exista interés en la formación en seguridad informática y por otra parte identificar estrategias que haga que las empresas dejen de ver la seguridad de la información sólo como un gasto y la incluyan como un tema estratégico que requiere inversión y atención, lo que al parecer es tendencia y se podrá lograr en la medida que se facilite el acceso a profesionales con conocimiento en este tipo de implementaciones y que puedan guiar adecuadamente, para que la seguridad de la información igualmente sea viable para las empresas.

[10] POSADA, J.; 20 de noviembre 2018. Más del 80% de las juntas directivas no hacen de la ciberseguridad un tema estratégico para sus compañías. Disponible en EY Colombia página web de EY Colombia. Disponible desde Internet en: https://eycolombia.ey.com/2018/11/20/mas-del-80-de-las-juntas-directivas-no-hacen-de-la-ciberseguridad-un-tema-estrategico-para-sus-companias/ .

# 3. OBJETIVOS

## 3.1. OBJETIVOS GENERAL

Diseñar una adecuada gestión de los riesgos de seguridad a los que está expuesto Qwerty S.A., manteniendo la confidencialidad, integridad y disponibilidad de su información.

## 3.2. OBJETIVOS ESPECÍFICOS

- Definir, adoptar y mantener las políticas de seguridad a través de las cuales se establecen los lineamientos a seguir en Qwerty S.A., respecto de la seguridad de la información.

- Identificar los riesgos de seguridad de Qwerty S.A.

- Salvaguardar la confidencialidad, integridad y disponibilidad de la información de Qwerty S.A., proveedores y clientes.

- Promover la cultura de seguridad de la información al interior de Qwerty S.A.

# 4. MARCO REFERENCIAL

Para efectuar el diseño e implementación de un sistema de gestión de seguridad de la información aplicando la norma ISO 27001, es necesario tener claridad sobre las definiciones básicas, así como el marco teórico de la seguridad de la información, sobre los cuales se estructura un sistema de gestión de la seguridad, como el que se busca diseñar y estructurar para cumplir los objetivos planteados en el desarrollo del presente proyecto aplicado.

## 4.1. MARCO TEÓRICO

**4.1.1. Seguridad informática.** Siendo "la disciplina que con base en políticas y normas internas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos a los que está expuesta."[11] Dentro de la cual es preciso tener en cuenta las siguientes definiciones:

- Información. "Es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada"[12].

- Informática: Estudia la recepción, envío, almacenamiento y el tratamiento de los datos que procesados se transforman en información.

- Seguridad Informática: Se ocupa de la protección de la infraestructura tecnológica de una empresa.

- Seguridad de la Información: Se ocupa de la protección de: la integridad, disponibilidad y confidencialidad de los activos de información de una empresa.

- Pilares de la información: Corresponde con las características que debe poseer la información: la confidencialidad, integridad y disponibilidad.

[11] BACA, Urbina (2016), Gabriel. Introducción a la seguridad informática, Grupo Editorial Patria, 2016. ProQuest Ebook Central, Disponible en: http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=4849850 , p12.
[12] NORMAS ISO, ISO 27001 Seguridad de la información. Disponible en internet de: https://www.normas-iso.com/iso-27001/

- Confidencialidad: Indica que la información debe estar protegida contra accesos no autorizados, evitando alteración o robo de información[13].

- Integridad: Propiedad de la información relativa a su exactitud y completitud[14].

- Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada[15].

- Confiabilidad: Corresponde con la protección contra alteraciones no autorizadas de la información.

- Autenticidad: Se refiere al proceso de identificación y validación de un usuario dentro de una red empresarial o sistema.

- Trazabilidad: En todo momento es posible identificar nuevas transacciones y cuando se registran.

- No repudio: Es la capacidad de asociar a una transacción y operación la identidad del usuario que las ha efectuado sin posibilidad de que niegue su autoría.

- Riesgo tecnológico: situaciones que pueden presentarse como consecuencia del mal uso voluntario e involuntario del personal de la empresa, así como del mal funcionamiento, obsolescencia, inadecuadas configuraciones de recursos tecnológicos de la empresa.

- Cambio organizacional: Corresponde con el cambio que debe efectuarse en los procesos para adoptar un esquema de seguridad que permita implementar un nivel adecuado de seguridad en la organización.

- Gestión de cambio: Actividades que se desarrollan al interior de una organización con el objetivo de facilitar los procesos de ajuste en los procesos y su adopción al interior de una organización.

**4.1.2. Análisis de Riesgos**. El análisis de riesgos es una actividad que se debe realizar de manera permanente en Qwerty S.A. como parte de la gestión de la seguridad.

---

[13] BACA, Urbina (2016), Gabriel. Introducción a la seguridad informática, Grupo Editorial Patria, 2016. ProQuest Ebook Central, [Consulta 12 de mayo de 2020] Disponible en: http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=4849850 , p13.

[14] ISO27000.ES [Sitio Web] Glosario [Consulta 12 de mayo de 2020] Disponible en: http://www.iso27000.es/glosario.html

[15] Ibid.

- Riesgo: Estimación del grado de exposición a una amenaza que puede materializarse.

- Amenaza: Todas aquellas situaciones o acciones que pueden alterar, o impactar o afectar negativamente los activos de información de una empresa.

- Vulnerabilidad: Es toda debilidad asociada a un activo de información que puede ser explotada por un atacante.

- Administración del riesgo: Toda actividad, procedimiento o mecanismo que es utilizado por una organización para mitigar los riesgos de seguridad que se haya determinado deban ser tratados en una organización para evitar que afecten los objetivos de una empresa.

- Priorización del riesgo: Es la valoración cuantitativa o cualitativa que una organización puede efectuar de un riesgo, a partir de la cual se determina si requiere o no tratamiento.

- Tolerancia: Nivel mínimo o máximo aceptable de un factor de riesgo antes de que requiera una intervención orientada a su tratamiento y mitigación.

**4.1.3. Norma ISO 27000**. La familia de normas ISO27000 es un conjunto de estándares[16] conformado por una serie de buenas prácticas aplicables en diferentes ámbitos de la seguridad de la información que incluye: la implementación, mantenimiento y mejora continua. Dentro de las normas que incluye esta familia encontramos las siguientes[17]:

- ISO/IEC 27011: Publicada en diciembre de 2008, es la guía de interpretación de implementación de la norma en empresas del sector comunicaciones basada en ISO/IEC 27002.

- ISO/IEC 27000: Publicada en diciembre de 2008, contiene la visión general de normas que componen la serie 27000 y vocabulario.

- ISO/IEC 27004: Publicada en diciembre de 2008, es la guía para desarrollo y uso de métricas y técnicas aplicables para determinar eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.

---

[16] ISO 27000.es [En Línea]. (Recuperado en 05 mayo de 2020) Disponible en: https://www.iso27000.es/iso27000.html

[17] INTEDYA. ISO27000 y el conjunto de estándares de Seguridad de la Información. (Recuperado en 05 mayo de 2020) Disponible en: http://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjunto-de-estandares-de-seguridad-de-la-informacion.html

- ISO/IEC 27003: Publicada en febrero de 2010, es la guía de implementación de un SGSI, desde la concepción hasta la ejecución de planes de implementación y el proceso de obtención de aprobación por la dirección.

- ISO/IEC 27005: Publicada en junio de 2005, contiene las directrices para la gestión de riesgos en seguridad de la información. Diseñada para ayudar a la aplicación de seguridad de la información con un enfoque de riesgos.

- ISO/IEC 27006: Publicada en octubre de 2011, es la guía de auditoría para certificación de un SGSI como complemento de la ISO 19011.

- ISO/IEC TR 27008: Publicada en octubre de 2011, es la guía de auditoría para revisar la implementación y operación de controles seleccionados de un SGSI.

- ISO/IEC 27007: Publicada en diciembre de 2011, contiene los requisitos para acreditación de entidades de auditoría y certificación de SGSI.

- ISO/IEC 27006: Publicada en diciembre de 2011, contiene los requisitos para acreditación de entidades de auditoría y certificación de SGSI.

- ISO/IEC 27013: Publicada en octubre de 2012, es la guía de implementación integrada de ISO/IEC 27001:2005 y de ISO/IEC 20000-1[18] (Gestión de servicios de TI).

- ISO/IEC 27010: Publicada en octubre de 2012, es la guía para gestión de seguridad de la información cuando se comparte información entre organizaciones o sectores ISO/IEC 27010:2012 sin importar la forma o medio.

- ISO/IEC TR 27015: Publicada en noviembre de 2012, es la guía de SGSI orientada a entidades financieras y de seguros como complemento de ISO/IEC 27002:2005 para implementar un SGSI.

- ISO/IEC 27014: Publicada en abril de 2013, es la guía de gobierno corporativo de la seguridad de la información.

- ISO/IEC 27001:2013 - ISO/IEC 27002:2013[19]: Publicada en octubre de 2013, es la revisión de las normas ISO 27001 (de requisitos) e ISO 27002 (guía de implementación) (14 dominios, 35 objetivos de control y 114 controles).

[18] ISO/IEC 20000 Disponible en: https://es.wikipedia.org/wiki/ISO/IEC_20000
[19] ISO/IEC 27002, Information Technology. Security Techniques. Code of practice for information security controls. Disponible en: https://www.iso27001security.com/html/27002.html

- ISO/IEC TR 27016: Publicada en febrero de 2014, es la guía de valoración aspectos financieros de la seguridad de la información.

- ISO/IEC TR 27018: Publicada en julio de 2014, es el código de buenas prácticas en cloud computing sobre controles para protección de datos.

- ISO/IEC TR 27017: Publicada en diciembre de 2015, es la guía de seguridad para Cloud computing alineada a ISO/IEC 27002 y controles adicionales en entornos de nube.

- ISO/IEC TR 27009: Publicada en junio de 2016, contiene los requisitos para el uso de la norma ISO/IEC/27001 en cualquier sector indicando como incluir requisitos adicionales.

- ISO IEC/27005: Hace parte de la estandarización ISO. Se considera con un alcance completo en el análisis como en la gestión de riesgos. Permite un análisis completo cuantitativo. Es un estándar internacional que le permite y le faculta mayor aceptación.

**4.1.4. Metodologías para el análisis de riesgos**. Dentro de las metodologías que podemos encontrar para efectuar el análisis de riesgos encontramos las siguientes:

- Magerit: Esta metodología permite análisis completo cualitativo y cuantitativo, no requiere autorización y es de carácter público. Posee un archivo extenso de inventarios en referencia a recursos de información, tipos de activos y amenazas. Esta metodología permite: analizar y mitigar riesgos, concientizar a los responsables sobre la existencia de riesgos y la necesidad de mitigarlos, Preparar a la organización para procesos de auditoría, propone escalas de: valores cualitativos, cuantitativos y de indisponibilidad de servicio, análisis de amenazas, escala estimación del riesgo, catálogos de amenazas y medidas de control. Está estructurada en tres libros. Incluye como fases para su desarrollo: a. Análisis de riesgos. b. Identificación, valoración de activos. c. Identificación y valoración de amenazas.

- Mehari[20]: Usa un modelo extenso de análisis de riesgos cualitativos y cuantitativos. Incluye bases de conocimiento, manuales y guías Diagnostica la seguridad, analiza interesados y análisis de riesgos. Para su desarrollo incluye las fases: a. Establecer contexto. b. Tipos y relación de activos. c. Análisis de

[20] MOGOLLON Abraham. Comparativo metodologías de análisis de riesgos. Disponible en: https://www.academia.edu/14195886/An%C3%A1lisis_Comparativo_Metodolog%C3%ADas_de_an%C3%A1lisis_de_Riesgos

vulnerabilidades de activos. d. Escenarios de riesgos. e. Análisis de amenazas. f. Acciones de mitigación de riesgos.

- Octave: Esta metodología permite: Tener una visión tecnológica de la organización. Efectuar una planificación de acciones para mitigar riesgos, generando una estrategia de protección de la organización, facilitar el cumplimiento de regulaciones de seguridad de la información. Identificar vulnerabilidades a nivel de infraestructura. Identificar perfiles de amenazas sobre activos. Clasificar activos en: sistemas (software, hardware, datos) y personas. Describe criterios para desarrollar guías de evaluación y administración de riesgos. Evalúa riesgos de seguridad de la información y propone plan de mitigación de riesgos. Incluye como fases: a. Visión de la organización. b. Visión tecnológica. c. Planificación de medidas y reducción de riesgos[21].

**4.1.5. Sistema de gestión de Seguridad de la Información**. Es el conjunto de políticas, procedimientos, lineamientos y controles a través de los cuales una organización protege sus activos de información, efectuando la gestión de los riesgos de seguridad de la información a los que están expuestos sus activos de información[22].

La implementación del SGSI – Sistema de Gestión de Seguridad de la Información para Qwerty S.A, se efectúa atendiendo lo establecido en la norma técnica NTC-27001:2013 que contiene las prácticas, NTC-27002:2013 que contiene los requisitos y la NTC-19011 de Auditorías internas.

La implementación del sistema de gestión de seguridad de la información, atiende y debe dar cumplimiento a:

- ✓ Documento Conpes 3854 Política Nacional de Seguridad Digital
- ✓ Documento Conpes 3920 Política Nacional de explotación de datos.
- ✓ Ley 527 de 1999, Ley de comercio electrónico
- ✓ Ley 1581 de 2012 Ley de Protección de datos
- ✓ Decreto 1074 de 2015 Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.
- ✓ Decreto 2364 de 2012
- ✓ Ley 1266 de 2008

[21] ALEMAN Novoa. Metodologías para el análisis de riesgos en los SGSI. [Consulta: 25 de Abril de 2020] Disponible en: http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

[22] GÓMEZ F LUIS, ANDRÉS A ANA, Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. (2012). Disponible en: https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?ppg=36&docID=3205110&tm=1545148818931

- ✓ Ley 1712 de 2014

## 4.2. MARCO CONTEXTUAL

**4.2.1. Consideraciones.** Para la implementación del sistema de gestión de seguridad de la información en Qwerty S.A., se debe tener en cuenta las siguientes situaciones:

- 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 servidores DHCP, HTTP y PBX se encuentran en un espacio donde no se cumplen condiciones de climatización óptimas.

- La configuración de la red de comunicaciones se encuentra en el mismo segmento.

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

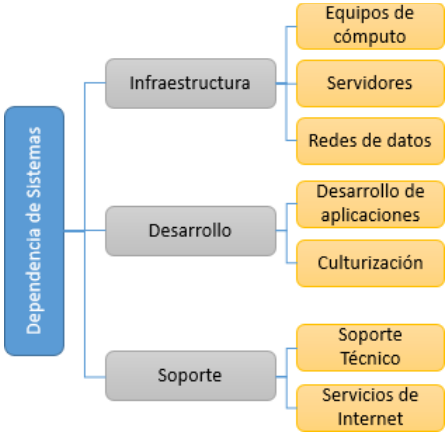
- Debido al alto flujo en la oficina de nómina y facturación, la alimentación de la información en el sistema en ocasiones la diligencia personal de prácticas de otras dependencias o contratos de aprendizaje.

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

**4.2.2. Descripción De La Empresa.** Qwerty S.A. es una empresa del sector de tecnológico dedicada a impulsar el desarrollo de comunidades en Colombia a través del uso de la tecnología. Cuenta con 120 empleados entre directivos, administrativos y operativos, quienes hacen uso regular de medios para la consulta de datos.

El centro de estudios cuenta con una dependencia de sistemas que tiene la siguiente estructura tal como aparece en la figura 1:

Figura 1. Estructura de Qwerty S.A.




Fuente: Tomado de la propuesta para el desarrollo de la alternativa de proyecto aplicado UNAD.

**4.2.3. Áreas.** Qwerty S.A. cuenta con las siguientes áreas, cada una de las cuales tiene las siguientes funciones:

**Área de Infraestructura**. Soporte al acceso a la red interna y a internet. Revisión de diseños de cableado estructurado.

**Área de desarrollo**. Apoyo técnico a las dependencias de la organización del centro en desarrollo de medios eficientes para lograr actividades basadas en usos de tecnologías de la informática y las telecomunicaciones.

**Área de Soporte**. Mantenimiento de computadores (sólo equipo propiedad del centro).

Realiza copias de seguridad de los sistemas de información y los servidores virtuales que se encuentran en las dependencias de la empresa Qwerty S.A.

La asistencia que se ofrece es la siguiente:

**Apoyo 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 óptimo 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.

**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 óptimo 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.

La empresa cuenta con un canal de internet de 25 megas en ancho de banda dedicado para poder dar desarrollo a sus actividades rutinarias.

**4.2.3.1. Activos del Área de Sistemas.** El Departamento de Sistemas cuenta con los siguientes activos de información relacionados a su cargo:

En el cuadro 1 se relacionan los siguientes recursos tecnológicos con los que cuenta Qwerty S.A. para la gestión de sus procesos:

Cuadro 1. Activos de información de Qwerty S.A.

| Activo | Descripción | Ubicación | Cantidad |
|---|---|---|---|
| Servidor de Impresión: | Equipo de cómputo que conecta dos impresoras: Destinadas a: | Oficina de nómina y facturación | 1 |
| Servidor marca Dell en torre PowerEdge T440 Ver ficha técnica | 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 | | |
| | 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 y docentes | Dependencia directiva y administrativa | 1 |

Cuadro 1. Activos de información de Qwerty S.A. Continuación

| Activo | Descripción | Ubicación | Cantidad |
|---|---|---|---|
| Servidor de archivos FTP: Servidor marca Dell en torre PowerEdge T130 Ver ficha técnica | 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 docentes 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 Plan Máximo Ver ficha del proveedor | 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 |

Cuadro 1. Activos de información de Qwerty S.A. Continuación

| Activo | Descripción | Ubicación | Cantidad |
|---|---|---|---|
| Servidor DHCP Servidor marca Dell en torre PowerEdge T440 | Equipos de cómputo donde se gestiona información online relacionada con el desarrollo del objeto social Presupuesto:<br>• Proveedores<br>• Órdenes de compra<br>• Inventarios | Dependencia de desarrollo tecnológico | 3 |
| Cortafuegos Cisco ASA 5505 Ver ficha técnica | 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 Cómputo Sistemas operativos win 10 Pro | Equipos destinados para el desarrollo del objeto social | Dependencia de infraestructura | 3 |
| Equipos de Cómputo 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 |

Cuadro 1. Activos de información de Qwerty S.A. Continuación

| Activo | Descripción | Ubicación | Cantidad |
|---|---|---|---|
| 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: Construcción propia del autor

## 4.3. ANTECEDENTES

### 4.3.1. MARCO LEGAL

Qwerty S.A. debe dar cumplimiento a la normatividad relacionada con su objeto que se relaciona a continuación[23]:

En relación con la naturaleza de Qwerty S.A. como entidad dedicada a la formación:

- CPC. Artículos 26, 27, 67, 6, 69, 70 y 71.
- Ley 30 de 1992. “Por el cual se organiza el servicio público de la Educación Superior”.
- Ley 115 de 1994. “Por la cual se expide la ley general de educación”.
- Ley 749 de 2002. “Por la cual se organiza el servicio público de la educación superior en las modalidades de formación técnica profesional y tecnológica, y se dictan otras disposiciones”.
- Ley 1188 de 2008. “por la cual se regula el registro calificado de programas de educación superior y se dictan otras disposiciones”.
- Ley 1740 de 2014. “Por la cual se desarrolla parcialmente el artículo 67 y los numerales 21, 22 y 26 del artículo 189 de la Constitución Política, se regula la inspección y vigilancia de la educación superior, se modifica parcialmente la Ley 30 de 1992 y se dictan otras disposiciones”.

[23] MINTIC. Normativa, Disponible en: https://www.mintic.gov.co/portal/inicio/Normatividad/

- Ley 1212 de 1993. “Por el cual se establecen los requisitos para el reconocimiento como universidad de una institución universitaria o escuela tecnológica”.

- Resolución 1036 de 2004.” Por la cual se definen las características específicas de calidad para los programas de pregrado y especialización en Educación”.

- Decreto 3697 de 2007. “Por el cual se fijan plazos para presentar Solicitudes de registro calificado”.

- Resolución 2773 de 2013. “Por la cual se definen las características específicas de calidad para los programas de formación profesional de pregrado en Ingeniería”.

- Decreto 1075 de 2015. “Por medio del cual se expide el Decreto Único Reglamentario del Sector Educación”.

- Decreto 2566 de 2015. “Por el cual se establecen las condiciones mínimas de calidad y demás requisitos para el ofrecimiento y desarrollo de programas académicos de educación superior y se dictan otras disposiciones”.

Por otra parte, en términos de la regulación en temas de tecnologías de la Información y las Comunicaciones en Colombia:

- Ley 527 de 1999, Ley de comercio electrónico.

- Ley 1266 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.

- Ley 1581 de 2012 Ley de Protección de datos.

- Decreto 2364 de 2012, Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.

- Ley 1712 de 2014, Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- Decreto 1074 de 2015, Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.

- Decreto 1078 de 2015 - Por medio del cual se expide el decreto único reglamentario del sector de tecnologías de la información y las comunicaciones.

- Decreto 1008 de 2018 - Por el cual se establecen los lineamientos generales de la política de gobierno digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del decreto número 1078 de 2015, decreto único reglamentario del sector de tecnologías de la información y las comunicaciones.

- Documento Conpes 3854, Política Nacional de Seguridad Digital.

- Documento Conpes 3920, Política Nacional de explotación de datos.

# 5. ENFOQUE METODOLÓGICO

Para el desarrollo del proyecto aplicado con Qwerty S.A. se aplicarán las siguientes metodologías:

## 5.1. METODOLOGÍA MAGERIT

Cuando hablamos de seguridad en una organización, necesariamente debemos referirnos a los riesgos existentes en la misma, e inevitablemente uno de los objetivos principales es precisamente poder efectuar una identificación de las amenazas y vulnerabilidades, a partir de las cuales se puedan determinar cuáles son los riesgos a los que está expuesta Qwerty S.A. Con el uso de la metodología Magerit[24] como metodología para el análisis de riesgos, será posible cumplir los siguientes objetivos:

**5.1.1. Directos**. Al seguir la metodología Magerit[25] para la gestión de riesgos:

- Generar conciencia a los responsables de Qwerty sobre los riesgos existentes y la necesidad de mitigarlos.
- Analizar los riesgos que se derivan del uso de la tecnología en Qwerty S.A.
- Planificar el tratamiento oportuno de los riesgos de Qwerty S.A.

**5.1.2. Indirectos**. Que se derivan de la gestión de riesgos:

- Preparar a Qwerty S.A. para los procesos de evaluación, auditoría y certificación.

Lo anterior con el fin de proteger la: confidencialidad, integridad y disponibilidad de los activos de información de Qwerty S.A. junto con la autenticidad y trazabilidad.

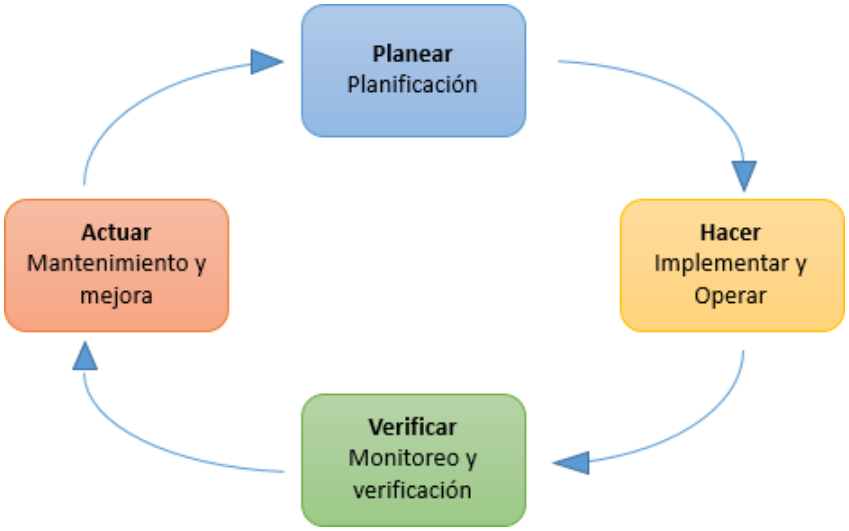
[24] MAGERIT versión 3.0 Metodología de Análisis y Gestión de Riesgos de los sistemas de Información, Libro I – Método, 5-may-2019, Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

[25] MAGERIT versión 3.0 Metodología de Análisis y Gestión de Riesgos de los sistemas de Información, Libro II – Catálogo de Elementos, 5-may-2019, Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XNEBj-hKjcc

## 5.2. METODOLOGÍA PARA LA IMPLEMENTACIÓN DEL SGSI

Como metodología para la implementación del SGSI en Qwerty S.A., basado en el estándar ISO27001 que aplica la propuesta del ciclo Deming para su establecimiento y gestión[26], en la cual podemos identificar en la figura 2 las siguientes fases:

Figura 2. Ciclo Deming y la ISO 27001




Fuente: Construcción propia del autor a partir de etapas descritas por Deming

A partir de las cuales se tendrán las siguientes fases para la implementación[27], que permitirán que Qwerty pueda contar con un Sistema que debe estar integrado a la organización, alineado a sus objetivos[28]:

[26] GÓMEZ F LUIS, ANDRÉS A ANA, Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. (2012). Disponible en: https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?ppg=36&docID=3205110&tm=1545148818931

[27] ISO/IEC 27002, Information Technology. Security Techniques. Code of practice for information security controls. Disponible en: https://www.iso27001security.com/html/27002.html

[28] ISO 27001: la mejora continua en los Sistemas de Gestión de Seguridad de la Información. Disponible en: https://www.pmg-ssi.com/2017/07/iso-27001-mejora-continua/

**5.2.1. Fase 1**: **Planificación**. Dentro de la cual es necesario:

- Identificar el contexto de Qwerty S.A.
- Estructurar la definición del proyecto y obtener aprobación de la dirección.
- Definir el alcance del SGSI, en términos de la organización y su localización[29].
- Definir y obtener aprobación de la dirección de la política de seguridad que debe cubrir objetivo de seguridad, requisitos legales, contexto de la gestión de riesgos, criterios para valorar riesgos y debe ser aceptada por la alta dirección[30].
- Definir roles y responsabilidades del SGSI.
- Definir requisitos y normatividad aplicable al SGSI

**5.2.2. Fase 2: Diagnóstico e implementación**. Dentro de la cual es necesario:

- Levantamiento de activos de información
- Efectuar el análisis de riesgos (valoración de riesgos) lo que incluye determinar: impacto, nivel de riesgo, determinar tratamiento[31].
- Obtener la declaración de aplicabilidad aprobada por la Dirección con objetivos de control implementados y lo que no se van a implementar justificando decisión.
- Efectuar el tratamiento de riesgos, evaluando e identificando en detalle cómo se implementará cada control incluido en la declaración de aplicabilidad aprobada.

**5.2.3. Fase 3**: **Monitoreo y revisión**. Dentro de la cual es necesario:

- Efectuar el monitoreo, medición, análisis y evaluación.
- Realizar auditorías internas

[29] ISO 27001: La implementación de un Sistema de Gestión de Seguridad de la Información mediante el ciclo PHVA. Disponible en: https://www.isotools.pe/iso-27001-implementacion-sistema-gestion-seguridad-informacion-ciclo-phva/
[30] Ibid .
[31] Ibid .

- Efectuar la revisión por la Dirección

**5.2.4. Fase 4: Acciones correctivas**. Dentro de la cual es necesario:

- Estructurar plan de implementación de acciones correctivas ante hallazgos de auditoría y resultados de revisión por la dirección.
- Construir plan de remediación.

Las técnicas específicas que se utilizarán para efectuar el análisis de riesgos son:

- Análisis a través de tablas.
- Técnicas gráficas
- Sesiones a través de las cuales se realizarán entrevistas y reuniones.
- Documentación disponible que aplique y puedan ser tomados como referencia.

# 6. DESARROLLO DE LOS OBJETIVOS

## 6.1. ESTIMACIONES

**6.1.1. Lo que se espera lograr con la implementación.** Con la implementación del sistema de gestión de seguridad de la información se espera que Qwerty S.A.:

- Pueda operar con un nivel mínimo aceptable de seguridad.
- Trate adecuadamente sus activos de información, teniendo en cuenta la prioridad y criticidad de cada uno.
- Mitigue los riesgos asociados a los activos de información de Qwerty S.A.
- Adopte una mejor forma de hacer las cosas considerando la seguridad de la información.

**6.1.2. Determinación del tiempo estimado para el diseño del sistema.** De acuerdo con las características y dimensiones de Qwerty S.A., en el cuadro 2, el tiempo estimado para la implementación total es de aproximadamente seis meses:

Cuadro 2. Tiempo estimado para el diseño del sistema

| | | | Mes 1 | | | | Mes 2 | | | | Mes 3 | | | | Mes 4 | | | | Mes 5 | | | | Mes 6 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Actividades | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| Planificación | 1 | Definir alcance | | | | | | | | | | | | | | | | | | | | | | | | |
| | 2 | Definir política de seguridad | | | | | | | | | | | | | | | | | | | | | | | | |
| | 3 | Identificar activos y riesgos | | | | | | | | | | | | | | | | | | | | | | | | |
| | 4 | Analizar y evaluar riesgos | | | | | | | | | | | | | | | | | | | | | | | | |
| | 5 | Identificar y evaluar opciones de tratamiento riesgos | | | | | | | | | | | | | | | | | | | | | | | | |
| | 6 | Identificar objetivos de control para tratar riesgos | | | | | | | | | | | | | | | | | | | | | | | | |
| | 7 | Obtener aprobación de riesgos residuales por la alta Dirección | | | | | | | | | | | | | | | | | | | | | | | | |
| | 8 | Definir y suscribir por la alta dirección declaración de aplicabilidad | | | | | | | | | | | | | | | | | | | | | | | | |

Cuadro 2. Tiempo estimado para el diseño del sistema Continuación

| | | Actividades | Mes 1 | | | | Mes 2 | | | | Mes 3 | | | | Mes 4 | | | | Mes 5 | | | | Mes 6 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| Hacer | 9 | Definir plan de tratamiento de riesgos | | | | | | | | ■ | | | | | | | | | | | | | | | | |
| | 10 | Implementar plan de tratamiento de riesgos | | | | | | | | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | | | | | | | | |
| | 11 | Implementar controles | | | | | | | | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | | | | | | | | |
| | 12 | Definir sistema de medición | | | | | | | | | | | | | | | | | ■ | | | | | | | |
| | 13 | Formar y socializar temas de seguridad a toda la organización | | | | | | | | | | | | | | | | | | ■ | ■ | | | | | |
| | 14 | Implementar procedimientos gestión de incidentes | | | | | | | | | | | | | | | | | | | ■ | | | | | |
| Verificar | 15 | Ejecutar procedimientos de monitoreo | | | | | | | | | | | | | | | | | | | | ■ | | | | |
| | 16 | Medir efectividad de controles | | | | | | | | | | | | | | | | | | | | ■ | | | | |
| | 17 | Revisar regularmente riesgos | | | | | | | | | | | | | | | | | | | | | ■ | | | |
| | 18 | Programar y ejecutar auditorías internas | | | | | | | | | | | | | | | | | | | | | ■ | | | |
| | 19 | Revisión del SGSI por parte de la dirección | | | | | | | | | | | | | | | | | | | | | | ■ | | |
| | 20 | Actualizar plan de seguridad | | | | | | | | | | | | | | | | | | | | | | | ■ | |
| Actuar | 21 | Implementar mejoras identificadas | | | | | | | | | | | | | | | | | | | | | | | | ■ |
| | 22 | Implementar acciones preventivas y correctivas | | | | | | | | | | | | | | | | | | | | | | | | ■ |

Fuente: Construcción propia del autor

Donde la etapa de diseño como tal, del Sistema de Gestión de Seguridad de la Información requiere aproximadamente dos meses.

**6.1.3. Proyección del valor del diseño e implementación del sistema.** El costo estimado de diseño e implementación del sistema es el siguiente:

**6.1.3.1.** Costos de Diseño. En el cuadro 3. Costo del diseño, podemos ver la estimación.

Cuadro 3. Costo del diseño

| | Componentes | Tiempo de dedicación | Costo Estimado incluido IVA | Costo Total incluido IVA |
|---|---|---|---|---|
| **Costo personal** | | | | |
| 1 | Director de proyecto (Profesional Senior Seguridad Informática) | Completo | 8.000.000 | 8.000.000 |
| 2 | Profesional de seguridad informática | Completo | 5.000.000 | 5.000.000 |
| 3 | Profesional área de infraestructura | Parcial | 2.500.000 | 2.500.000 |
| 4 | Profesional área de soporte | Parcial | 2.500.000 | 2.500.000 |
| 5 | Profesional área de desarrollo | Parcial | 2.500.000 | 2.500.000 |
| 6 | Documentador | Completo | 2.500.000 | 2.500.000 |
| **Costos logística** | | | | |
| 1 | Portátiles | 3 | 600.000 | 1.800.000 |
| 2 | Software Ofimático | 3 | 226.100 | 678.300 |
| 3 | Software análisis de riesgos (Pilar Basic) | 1 | 2.537.675 | 2.537.675 |
| 4 | Insumos | 1 | 500.000 | 500.000 |
| **Total** | | | | 28.515.975 |

Fuente: Construcción propia del autor

**6.1.3.2.** Costos de Implementación. En el cuadro 4 Costos de implementación se puede ver la estimación en costos para la implementación

Cuadro 4. Costo de Implementación

| | Componentes | Tiempo de dedicación | Costo Estimado | Costo Total incluido IVA |
|---|---|---|---|---|
| **Costos Implementación controles** | | | | |
| 1 | Implementar plan tratamiento de riesgos | Parcial | 7.500.000 | 7.500.000 |
| 2 | Implementar control de acceso de clientes | Externo | 4.083.000 | 4.858.770 |
| 3 | Implementar control de climatización servidores DHCP, HTTP y PBX | Externo | 2.500.000 | 2.500.000 |
| 4 | Implementar segmentación de red | Externo | 7.200.000 | 8.568.000 |
| 5 | Implementar mecanismo validación actualización de antivirus | Externo - Interno | 3.500.000 | 3.500.000 |

Cuadro 4. Costo de Implementación Continuación

| | Componentes | Tiempo de dedicación | Costo Estimado | Costo Total incluido IVA |
|---|---|---|---|---|
| **Costos Implementación controles** | | | | |
| 6 | Implementar contingencia para nómina y facturación en fechas de alto flujo. | Interno | 1.000.000 | 1.000.000 |
| 7 | Configuración e implementación de reglas para autorización o denegación de conexiones o transmisión de datos | Externo - Interno | 4.800.000 | 5.712.000 |
| **Socialización SGSI** | | | | |
| 1 | Socialización | Parcial | 4.000.000 | 4.760.000 |
| 2 | Campañas de apropiación | Parcial | 2.000.000 | 2.380.000 |
| **Costos Auditoría interna** | | | | |
| 1 | Formación auditores internos | 3 | 600.000 | 1.800.000 |
| 2 | Auditor senior externo | 1 | 7.000.000 | 7.000.000 |
| 3 | Auditores internos | 3 | 2.537.675 | 7.613.025 |
| 4 | Insumos | 1 | 500.000 | 500.000 |
| **Total** | | | | 57.691.795 |

Fuente: Construcción propia del autor

**6.1.3.3.** Objetivos de Seguridad de la Información. Los objetivos de seguridad de la información considerando el equipo de trabajo en el que participarán empleados de Qwerty S.A., son los siguientes:

- Estructurar y adoptar las políticas de información para Qwerty S.A propuestas por el equipo de proyecto y aprobadas por la alta dirección de Qwerty S.A.

- Efectuar una adecuada gestión de la seguridad de la información en Qwerty, haciendo participe en el proceso de estructuración el equipo de trabajo quien podrá a partir del conocimiento facilitar y hacer más asertiva a la realidad a partir del conocimiento propio o de otros empleados de la organización.

- Identificar y gestionar los riesgos de seguridad de Qwerty S.A., labor que será efectuada por el equipo de trabajo a partir del conocimiento de la organización como de aquellos empleados que serán incluidos en el proceso.

- Promover la cultura de seguridad de la información en Qwerty S.A., iniciando con la formación del equipo de trabajo, quienes tendrán un rol, así como de todos y cada uno de los miembros de la organización, frente a los cuales asumirán el rol de multiplicadores y se mantendrá como equipo que soportará la mejora continua de acuerdo con el ciclo Deming que adopta este sistema de gestión.

**6.1.3.4.** Riesgos inherentes al proyecto. Se identifican los siguientes riesgos propios del proyecto de implementación del SGSI:

- Retrasos en tiempo por cambio de integrantes del equipo de proyecto durante la implementación.

- Retraso en tiempo por aplazamiento de sesiones de trabajo con otras áreas de Qwerty S.A.

- Mayores tiempos para la implementación por situaciones internas o externas a Qwerty que puedan tener un impacto en el proyecto.

- Caer en imprecisiones o no considerar información relevante durante la implementación, comprometiendo la efectividad de la gestión de riesgos en Qwerty S.A.

- Baja apropiación y aceptación del SGSI dentro de Qwerty S.A.

- Definir inadecuadamente el alcance del SGSI exponiendo el cumplimiento de los objetivos del sistema mismo y por ende las expectativas de la alta dirección.

- Bajo nivel de competencia del personal de Qwerty S.A. clave dentro del SGSI.

**6.1.3.5.** Activos De Información por Dependencia. Los siguientes son los activos de información identificados en Qwerty S.A.:

**Activos esenciales**. Teniendo en cuenta los componentes esenciales de un sistema de información: datos y servicios, los siguientes son los activos esenciales de Qwerty S.A.:

- Datos/Información: Los datos y la información son un activo más de la empresa y se mantienen en medios electrónicos o físicos, adicionalmente pueden ser transmitidos a través de diferentes medios. En Qwerty S.A. encontramos los siguientes datos e información:

    - Estudiantes
    - Empleados
    - Proveedores
    - Nómina
    - Órdenes de compra
    - Inventarios

- Facturación
- Hojas de vida
- Documentos digitales

- Servicios: Los servicios de los que depende la operación de Qwerty S.A. actualmente son los siguientes:

  - FTP
  - Correo electrónico google
  - Internet
  - Certificados laborales
  - Nómina
  - Recibos de pago
  - Red inalámbrica
  - Red alámbrica
  - Impresión
  - DHCP
  - Voz IP

- Software: Qwerty S.A. cuenta con el siguiente software:

  - Sistema de nómina
  - Sistema de facturación
  - Windows 10 Pro
  - Joomla 2.5
  - Apache
  - PHP
  - MySQL
  - Apache 2.4.25
  - PHP 5.6.30 - 7.1.1
  - MySQL 5.7.17
  - phpMyAdmin 4.6.6
  - Sistema de proveedores
  - Sistema de compras
  - Sistema de inventarios
  - Software Antivirus

- Equipamiento informático (Hardware): Qwerty S.A. cuenta con la siguiente infraestructura:

  - 1 Servidor de impresión Dell PowerEdge T440
  - 1 Impresora HP LaserJet Enterprise serie 600

- 1 Impresora/Escáner SMART MultiXpress M4370LX
- 1 Servidor Dell Torre PowerEdge T130
- 2 Servidor Dell Torre PowerEdge T440
- 1 Servidor Dell Torre PowerEdge T440
- 3 Equipos de cómputo en la dependencia de desarrollo tecnológico
- 1 Cortafuegos Cisco ASA 5505
- 3 Equipos de cómputo en la dependencia de infraestructura
- 10 Equipos de cómputo en la dependencia de prueba de software
- 5 Equipos de cómputo en la dependencia de prueba de software
- 4 Puntos de acceso alámbrico (HUB)
- 6 Switches Cisco Catalyst 2960
- 6 Teléfonos IP
- 2 Puntos de acceso

- Redes de comunicaciones: Qwerty S.A., cuenta con una red con un único segmento, áreas sin control de acceso, cuenta con servicios inalámbricos y puntos locales.

- Soporte de información. Qwerty S.A. cuenta con los siguientes dispositivos a través de los cuales almacena información de la empresa:

    - Discos locales
    - Almacenamiento google sobre correos electrónicos.

- Equipamiento. Considerando que en este punto se refiere a otros equipos que soportan los sistemas y servicios de Qwerty S.A. encontramos:

    - Rack
    - Mobiliario
    - Sistema control de acceso con cubrimiento parcial
    - Sistema de control de temperatura con cubrimiento parcial

- Personal. En Qwerty S.A. los empleados que tienen relación con la operación de los sistemas y servicios disponibles son:

    - Directivos
    - Administrativos
    - Operativos
    - Técnicos
    - Docentes
    - Personal de practicas

- Contratos de aprendizaje
- Estudiantes

- Valoración De Activos. Aplicando la metodología Magerit es indispensable valorar los activos según las siguientes dimensiones:

  - Disponibilidad: Propiedad o características de los activos en el que las entidades o propiedades pueden acceder a los mismos cuando lo requieren.

  - Integridad de los datos Propiedad o característica en la que el activo no es modificado de manera no autorizada.

  - Confidencialidad Propiedad en la que un activo no se pone a disposición, ni se revela a personas, procesos o entidades no autorizadas.

  - Autenticidad Propiedad en la que una entidad es quien dice ser quien es o garantiza la fuente de la que proceden los datos.

  - Trazabilidad Propiedad en que las actuaciones de una entidad pueden ser imputadas o vinculadas solamente a la entidad misma.

Para la medición de las dimensiones aplicamos la escala del cuadro 5:

Cuadro 5. Escala medición impacto

| Valor | | Criterio |
|---|---|---|
| 10 | extremo (E) | daño extremadamente grave |
| 9 | muy alto (MA) | daño muy grave |
| 6-8 | alto (A) | daño grave |
| 3-5 | medio (M) | daño importante |
| 1-2 | bajo (B) | daño menor |
| 0 | despreciable (D) | irrelevante a efectos prácticos |

Fuente: Construcción basada en Magerit

## 6.2. IDENTIFICACION DE ACTIVOS

**6.2.1. Activos de Información.** En el cuadro 6 se relacionan los activos de información de Qwerty S.A.:

Cuadro 6. Activos de información Qwerty S.A.

| Activos Qwerty S.A. | | | |
|---|---|---|---|
| | **Nombre del activo** | **Clasificación** | **Cantidad** |
| 1 | Estudiantes | [D] Datos | |
| 2 | Empleados | [D] Datos | |
| 3 | Proveedores | [D] Datos | |
| 4 | Nómina | [D] Datos | |
| 5 | Órdenes de compra | [D] Datos | |
| 6 | Inventarios | [D] Datos | |
| 7 | Facturación | [D] Datos | |
| 8 | Hojas de vida | [D] Datos | |
| 9 | Documentos digitales | [D] Datos | |
| 10 | Audios de reuniones, asambleas | [D] Datos | |
| 11 | Contenido Página Web GoDaddy | [D] Datos | |
| 12 | FTP | [S] Servicio | |
| 13 | Correo electrónico google | [S] Servicio | |
| 14 | Internet | [S] Servicio | |
| 15 | Certificados laborales | [S] Servicio | |
| 16 | Nómina | [S] Servicio | |
| 17 | Recibos de pago | [S] Servicio | |
| 18 | Red inalámbrica | [S] Servicio | |
| 19 | Red alámbrica | [S] Servicio | |
| 20 | Impresión | [S] Servicio | |
| 21 | DHCP | [S] Servicio | |
| 22 | Voz IP | [S] Servicio | |
| 23 | Servidor de impresión Dell PowerEdge T440 | [HW] Hardware | 1 |
| 24 | Impresora HP LaserJet Enterprise serie 600 | [HW] Hardware | 1 |
| 25 | Impresora/Escáner SMART MultiXpress M4370LX | [HW] Hardware | 1 |
| 26 | Servidor Dell Torre PowerEdge T130 | [HW] Hardware | 1 |
| 27 | Servidor Dell Torre PowerEdge T440 | [HW] Hardware | 2 |
| 28 | Servidor Dell Torre PowerEdge T440 | [HW] Hardware | 1 |
| 29 | Equipo de cómputo | [HW] Hardware | 3 |
| 30 | Cortafuegos Cisco ASA 5505 | [HW] Hardware | 1 |
| 31 | Equipo de cómputo | [HW] Hardware | 3 |
| 32 | Equipo de cómputo | [HW] Hardware | 10 |
| 33 | Equipo de cómputo | [HW] Hardware | 5 |
| 34 | Puntos de acceso alámbrico (HUB) | [HW] Hardware | 4 |

Cuadro 6. Activos de información Qwerty S.A. Continuación

| Activos Qwerty S.A. | | | |
|---|---|---|---|
| | **Nombre del activo** | **Clasificación** | **Cantidad** |
| 35 | Switches Cisco Catalyst 2960 | [HW] Hardware | 6 |
| 36 | Teléfonos IP | [HW] Hardware | 6 |
| 37 | Puntos de acceso | [HW] Hardware | 2 |
| 38 | Directivos | [P] Personal | |
| 39 | Administradores | [P] Personal | |
| 40 | Docentes | [P] Personal | |
| 41 | Estudiantes | [P] Personal | |
| 42 | Especialista correo electrónico | [P] Personal | |
| 43 | Sistema de nómina | [SW] Software | |
| 44 | Sistema de facturación | [SW] Software | |
| 45 | Windows 10 Pro | [SW] Software | |
| 46 | Joomla 2.5 | [SW] Software | |
| 47 | Apache | [SW] Software | |
| 48 | PHP - Sitio Web | [SW] Software | |
| 49 | MySQL - Sitio Web | [SW] Software | |
| 50 | Apache 2.4.25 - Sitio Web | [SW] Software | |
| 51 | PHP 5.6.30 - 7.1.1 - Nómina y facturación | [SW] Software | |
| 52 | MySQL 5.7.17 - Nómina y facturación | [SW] Software | |
| 53 | phpMyAdmin 4.6.6 - Nómina y facturación | [SW] Software | |
| 54 | Sistema de proveedores | [SW] Software | |
| 55 | Sistema de compras | [SW] Software | |
| 56 | Sistema de inventarios | [SW] Software | |
| 57 | Software Antivirus | [SW] Software | |
| 58 | Red de datos | [COM] Redes de comunicaciones | |
| 59 | Red de datos inalámbrica | [COM] Redes de comunicaciones | |

Fuente: Construcción propia del autor

**6.2.2. Análisis de cumplimiento de requerimientos ISO 27001**. Teniendo en cuenta el estado actual de Qwerty S.A. frente al cumplimiento de los requerimientos de la norma ISO27001, el siguiente es el resultado del análisis:

En primer lugar considerando la escala definida en el cuadro 7 para la valoración:

Cuadro 7. Escala de valoración de cumplimiento de requerimientos ISO 27001

| Valor | Denominación | Escala | Descripción |
|---|---|---|---|
| N0 | No aplicable | - | No es aplicable a la empresa |
| N1 | Inexistente | - | Carencia de controles |
| N2 | Inicial | 25 | No existe un control formal, no hay procedimientos se aplican prácticas derivadas de la experiencia. |
| N3 | Definido | 50 | Existen controles que se aplican según procedimientos formalmente adoptados y socializados |
| N4 | Administrado | 75 | Hay seguimiento y medición de procedimientos a través de indicadores |
| N5 | Optimizado | 100 | Se aplica la mejora continua |

Fuente: Construcción propia del autor

De acuerdo con la información dispuesta de la firma Qwerty S.A. en el cuadro 8 podemos identificar el estado de cumplimiento de los requerimientos de la ISO27001 en términos cualitativos y cuantitativos:

Cuadro 8. Cumplimiento de requerimientos ISO27001 Qwerty S.A.

| Sección | Requerimientos ISO 27001 | Estado | Nivel de cumplimiento |
|---|---|---|---|
| **A.5** | **Políticas de Seguridad de la información** | | **12,50** |
| **A.5.1** | **Orientación de la dirección para la gestión de la seguridad de la información** | | **12,50** |
| A.5.1.1 | Políticas para la Seguridad de la información | Inicial | **25** |
| A.5.1.2 | Revisión de las políticas para la seguridad de la información | Inexistente | **-** |
| **A.6** | **Organización de la seguridad de la información** | | **-** |
| A.6.1 | Organización interna | Inexistente | **-** |

Cuadro 8. Cumplimiento de requerimientos ISO27001 Qwerty S.A. Continuación

| Sección | Requerimientos ISO 27001 | Estado | Nivel de cumplimiento |
|---|---|---|---|
| A.6.1.1 | Roles y responsabilidades para la seguridad de la información | Inexistente | - |
| A.6.1.2 | Separación de deberes | Inicial | 25 |
| A.6.1.3 | Contacto con las autoridades | Inexistente | - |
| A.6.1.4 | Contacto con grupos de interés especial | Inexistente | - |
| A.6.1.5 | Seguridad de la información en la gestión de proyectos | Inexistente | - |
| **A.6.2** | **Dispositivos moviles y teletrabajo** | | **-** |
| A.6.2.1 | Política para dispositivos móviles | Inexistente | - |
| A.6.2.2 | Teletrabajo | Inexistente | - |
| **A.7** | **Seguridad de los recursos humanos** | | **22,22** |
| **A.7.1** | **Antes de asumir el empleo** | | **25,00** |
| A.7.1.1 | Selección | Inicial | 25 |
| A.7.1.2 | Términos y condiciones de empleo | Inicial | 25 |
| **A.7.2** | **Durante la ejecución del empleo** | | **16,67** |
| A.7.2.1 | Responsabilidad de la dirección | Inicial | 25 |
| A.7.2.2 | Toma de conciencia, educación y formación en la seguridad de la información | Inicial | 25 |
| A.7.2.3 | Proceso disciplinario | Inexistente | - |
| **A.7.3** | **Terminación y cambio de empleo** | | **25,00** |
| A.7.3.1 | Terminación o cambio de responsabilidades de empleo | Inicial | 25 |
| **A.8** | **Gestión de activos** | | **11,11** |
| **A.8.1** | **Responsabilidad por los activos** | | **25,00** |
| A.8.1.1 | Inventario de activos | Definido | 50 |
| A.8.1.2 | Propiedad de los activos | Inicial | 25 |
| A.8.1.3 | Uso aceptable de los activos | Inicial | 25 |
| A.8.1.4 | Devolución de los activos | Inexistente | - |
| **A.8.2** | **Clasificación de la información** | | **8,33** |
| A.8.2.1 | Clasificación de la información | Inexistente | - |
| A.8.2.2 | Etiquetado de la información | Inexistente | - |
| A.8.2.3 | Manejo de activos | Inicial | 25 |
| **A.8.3** | **Manejo de medios** | | **-** |
| A.8.3.1 | Gestión de medios removibles | Inexistente | - |
| A.8.3.2 | Disposición de los medios | Inexistente | - |

Cuadro 8. Cumplimiento de requerimientos ISO27001 Qwerty S.A. Continuación

| Sección | Requerimientos ISO 27001 | Estado | Nivel de cumplimiento |
|---|---|---|---|
| A.8.3.3 | Transferencia de medios físicos | Inexistente | - |
| **A.9** | **Control de acceso** | | **33,96** |
| **A.9.1** | **Requisitos de negocio** | | **25,00** |
| A.9.1.1 | Política de control de acceso | Inicial | **25** |
| A.9.1.2 | Acceso a redes y a servicios de red | Inicial | **25** |
| **A.9.2** | **Gestión de acceso a usuarios** | | **45,83** |
| A.9.2.1 | Registro y cancelación del registro a usuarios | Definido | **50** |
| A.9.2.2 | Suministro de acceso de usuarios | Definido | **50** |
| A.9.2.3 | Gestión de derechos de acceso de privilegiado | Definido | **50** |
| A.9.2.4 | Gestión de información de autenticación secreta de usuarios | Definido | **50** |
| A.9.2.5 | Revisión de los derechos de acceso de usuarios | Definido | **50** |
| A.9.2.6 | Retiro o ajuste de los derechos de acceso | Inicial | **25** |
| **A.9.3** | **Responsabilidades de los usuarios** | | **50,00** |
| A.9.3.1 | Uso de información de autenticación secreta | Definido | **50** |
| **A.9.4** | **Control de acceso a sistemas y aplicaciones** | | **15,00** |
| A.9.4.1 | Restricción de acceso a la información | Inicial | **25** |
| A.9.4.2 | Procedimiento de ingreso seguro | Inicial | **25** |
| A.9.4.3 | Sistema de gestión de contraseñas | Inicial | **25** |
| A.9.4.4 | Uso de programas utilitarios privilegiados | Inexistente | - |
| A.9.4.5 | Control de acceso a códigos fuente de programas | Inexistente | - |
| **A.10** | **Criptografía** | | **12,50** |
| **A.10.1** | **Controles criptográficos** | | **12,50** |
| A.10.1.1 | Política sobre el uso de controles criptográficos | Inexistente | - |
| A.10.1.2 | Gestión de llaves | Inicial | **25** |
| **A.11** | **Seguridad física y del entorno** | | **16,67** |
| **A.11.1** | **Áreas seguras** | | **17** |
| A.11.1.1 | Perímetro de seguridad física | Inicial | **25** |

Cuadro 8. Cumplimiento de requerimientos ISO27001 Qwerty S.A. Continuación

| Sección | Requerimientos ISO 27001 | Estado | Nivel de cumplimiento |
|---|---|---|---|
| A.11.1.2 | Controles de acceso físico | Inexistente | - |
| A.11.1.3 | Seguridad de oficinas, recintos e instalaciones | Inicial | **25** |
| A.11.1.4 | Protección contra amenazas externas y ambientales | Inicial | **25** |
| A.11.1.5 | Trabajo en áreas seguras | Inicial | **25** |
| A.11.1.6 | Áreas de despacho y carga | No aplicable | - |
| **A.12** | **Seguridad de las operaciones** | | **12,50** |
| **A.12.1** | **Procedimientos operacionales y responsabilidades** | | **6** |
| A.12.1.1 | Procedimientos de operación documentados | Inexistente | **-** |
| A.12.1.2 | Gestión de cambios | Inexistente | **-** |
| A.12.1.3 | Gestión de capacidad | Inicial | **25** |
| A.12.1.4 | Separación de los ambientes de desarrollo, pruebas, y operación | Inexistente | **-** |
| **A.12.2** | **Protección contra códigos maliciosos** | | **25** |
| A.12.2.1 | Controles contra códigos maliciosos | Inicial | **25** |
| **A.12.3** | **Copias de respaldo** | | **-** |
| A.12.3.1 | Respaldo de información | Inexistente | - |
| **A.12.4** | **Registro de seguimiento** | | **19** |
| A.12.4.1 | Registro de eventos | Inexistente | **-** |
| A.12.4.2 | Protección de la información de registro | Inicial | **25** |
| A.12.4.3 | Registros del administrador y del operador | Inicial | **25** |
| A.12.4.4 | Sincronización de relojes | Inicial | **25** |
| **A.12.5** | **Control de software operacional** | | **13** |
| A.12.5.1 | Instalación de software en sistemas operativos | Inexistente | **-** |
| A.12.5.2 | Protección de la información de registro | Inicial | **25** |
| **A.12.6** | **Gestión de la vulnerabilidad técnica** | | **25** |
| A.12.6.1 | Gestión de las vulnerabilidades técnicas | Inicial | **25** |
| A.12.6.2 | Restricciones sobre la instalación del software | Inicial | **25** |

Cuadro 8. Cumplimiento de requerimientos ISO27001 Qwerty S.A. Continuación

| Sección | Requerimientos ISO 27001 | Estado | Nivel de cumplimiento |
|---|---|---|---|
| **A.12.7** | **Consideraciones sobre auditorías de sistemas de información** | | **-** |
| A.12.7 | Controles de auditorías de sistemas de información | Inexistente | **-** |
| **A.13** | **Seguridad de las comunicaciones** | | **10,42** |
| **A.13.1** | **Gestión de la seguridad de las redes** | | **8** |
| A.13.1.1 | Controles de redes | Inicial | **25** |
| A.13.1.2 | Seguridad de los servicios de red | Inexistente | **-** |
| A.13.1.3 | Separación en las redes | Inexistente | **-** |
| **A.13.2** | **Transferencia de información** | | **13** |
| A.13.2.1 | Políticas y procedimientos de transferencias de información | Inexistente | **-** |
| A.13.2.2 | Acuerdos sobre transferencia de información | Inicial | **25** |
| A.13.2.3 | Mensajería electrónica | Inicial | **25** |
| A.13.2.4 | Acuerdos de confidencialidad o de divulgación | Inexistente | **-** |
| **A.14** | **Adquisición, desarrollo y mantenimiento de sistemas** | | **18,52** |
| **A.14.1** | **Requisitos de seguridad de los sistemas de información** | | **17** |
| A.14.1.1 | Análisis y especificación de requisitos de seguridad de la información | Inexistente | **-** |
| A.14.1.2 | Seguridad de servicios de las aplicaciones en redes públicas | Inicial | **25** |
| A.14.1.3 | Protección de transacciones de los servicios de las aplicaciones | Inicial | **25** |
| **A.14.2** | **Seguridad de los procesos de desarrollo y de soporte** | | **14** |
| A.14.2.1 | Políticas de desarrollo seguro | Inexistente | **-** |
| A.14.2.2 | Procedimientos de control de cambios en sistemas | Inicial | **25** |
| A.14.2.3 | Revisión técnica de las aplicaciones después de cambios en la plataforma de operación. | Inicial | **25** |

Cuadro 8. Cumplimiento de requerimientos ISO27001 Qwerty S.A. Continuación

| Sección | Requerimientos ISO 27001 | Estado | Nivel de cumplimiento |
|---|---|---|---|
| A.14.2.4 | Restricciones en los cambios a los paquetes de software. | Inicial | **25** |
| A.14.2.5 | Principios de construcción de los sistemas seguros | Inexistente | **-** |
| A.14.2.6 | Ambiente de desarrollo seguro | Inicial | **25** |
| A.14.2.7 | Desarrollo contratado externamente | Inicial | **25** |
| A.14.2.8 | Pruebas de seguridad de sistemas | Inexistente | **-** |
| A.14.2.9 | Prueba de aceptación de sistemas | Inexistente | **-** |
| **A.14.3** | **Datos de prueba** | | **25** |
| A.14.3.1 | Protección de datos de prueba | Inicial | **25** |
| **A.15** | **Relaciones con los proveedores** | | **25,00** |
| **A.15.1** | **Seguridad de la información en la relación con los proveedores** | | **25** |
| A.15.1.1 | Política de seguridad de la información para las relaciones con proveedores | Inicial | **25** |
| A.15.1.2 | Tratamiento de la seguridad de los acuerdos con los proveedores | Inicial | **25** |
| A.15.1.3 | Cadena de suministro de tecnología de información y comunicación | Inicial | **25** |
| **A.15.2** | **Gestión de la prestación de servicios de proveedores** | | **25** |
| A.15.2.1 | Seguimiento y revisión de los servicios de los proveedores | Inicial | **25** |
| A.15.2.2 | Gestión de cambios en los servicios de los proveedores | Inicial | **25** |
| **A.16** | **Gestión de incidentes de seguridad de la información** | | **3,57** |
| **A.16.1** | **Gestión de incidentes y mejores en la seguridad de la información** | | **4** |
| A.16.1.1 | Responsabilidades y procedimientos | Inicial | **25** |
| A.16.1.2 | Reporte de eventos de seguridad de la información | Inexistente | **-** |
| A.16.1.3 | Reporte de debilidades de seguridad de la información | Inexistente | **-** |

Cuadro 8. Cumplimiento de requerimientos ISO27001 Qwerty S.A. Continuación

| Sección | Requerimientos ISO 27001 | Estado | Nivel de cumplimiento |
|---|---|---|---|
| A.16.1.4 | Evaluación de eventos de seguridad de la información y decisiones sobre ellos | Inexistente | - |
| A.16.1.5 | Respuesta a incidentes de seguridad de la información | Inexistente | - |
| A.16.1.6 | Aprendizaje obtenido de los incidentes de seguridad de la información | Inexistente | - |
| A.16.1.7 | Recolección de evidencia | Inexistente | - |
| **A.17** | **Aspectos de seguridad de la información** | | - |
| **A.17.1** | **Continuidad de seguridad de la información** | | - |
| A.17.1.1 | Planificación de la continuidad de la seguridad de la información | Inexistente | - |
| A.17.1.2 | Implementación de la continuidad de la seguridad de la información | Inexistente | - |
| A.17.1.3 | Verificación, visión y evaluación de la continuidad de la seguridad de la información | Inexistente | - |
| **A.17.2** | **Redundancias** | | - |
| A.17.2.1 | Disponibilidad de instalaciones de procesamiento de información | Inexistente | - |
| **A.18** | **Cumplimiento** | | **15,00** |
| **A.18.1** | **Cumplimiento de requisitos legales y contractuales** | | **15** |
| A.18.1.1 | Identificación de la legislación aplicable y de los requisitos contractuales | Inicial | **25** |
| A.18.1.2 | Derechos de propiedad intelectual | Inicial | **25** |
| A.18.1.3 | Protección de registros | Inicial | **25** |
| A.18.1.4 | Privacidad y protección de información de datos personales | Inexistente | - |
| A.18.1.5 | Reglamentación de controles criptográficos | Inexistente | - |
| **A.18** | **Cumplimiento** | | **23,33** |
| **A.18.1** | **Cumplimiento de requisitos legales y contractuales** | | **30** |

Cuadro 8. Cumplimiento de requerimientos ISO27001 Qwerty S.A. Continuación

| Sección | Requerimientos ISO 27001 | Estado | Nivel de cumplimiento |
|---|---|---|---|
| A.18.1.1 | Identificación de la legislación aplicable y de los requisitos contractuales | Definido | **50** |
| A.18.1.2 | Derechos de propiedad intelectual | Definido | **50** |
| A.18.1.3 | Protección de registros | Definido | **50** |
| A.18.1.4 | Privacidad y protección de información de datos personales | Inexistente | **-** |
| A.18.1.5 | Reglamentación de controles criptográficos | Inexistente | **-** |
| **A.18.2** | **Revisiones de seguridad de la información** | | **17** |
| A.18.2.1 | Revisión independiente de la seguridad de la información | Inexistente | **-** |
| A.18.2.2 | Cumplimiento con las políticas y nomas de seguridad | Inicial | **25** |
| A.18.2.3 | Revisión del cumplimiento técnico | Inicial | **25** |
| | **Cumplimiento Qwerty** | | **14,49** |

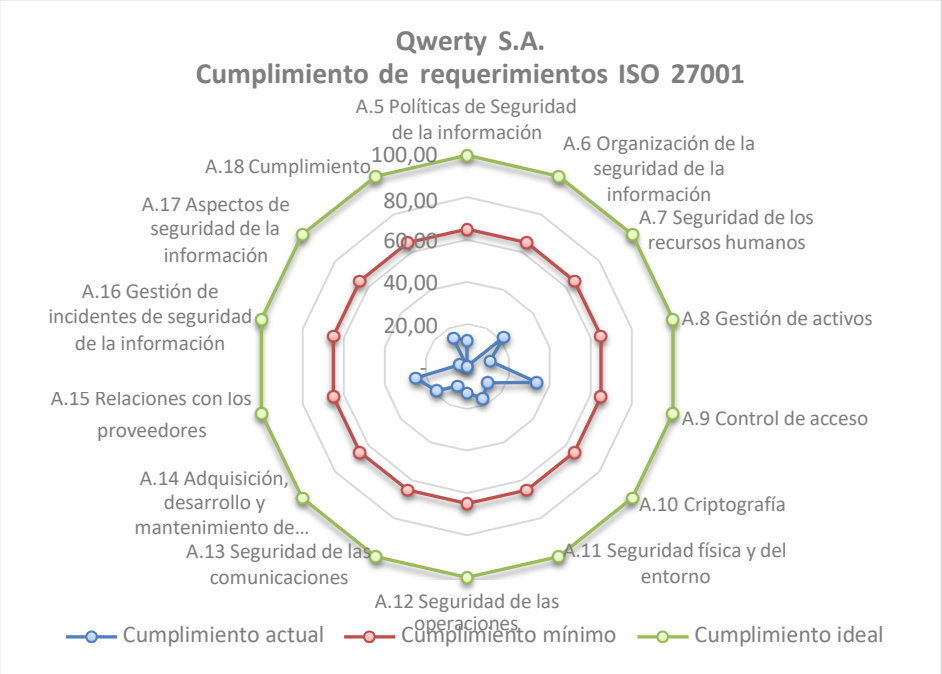
Fuente: Construcción propia del autor

Donde el resultado final indica que Qwerty S.A. tiene un cumplimiento de los requisitos de la norma ISO27001 del 25,45%, por lo que existe una brecha del 74,55%.

Gráficamente[32] por cada uno de los numerales o secciones en la figura 3 podemos visualizar el estado de cumplimiento, el nivel mínimo y el máximo para Qwerty S.A.:

[32] INCIBE, Colección: Protege tu empresa. Plan director de seguridad. [Consulta 8 de mayo de 2020] Disponible en: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf, p15.

Figura 3. Cumplimiento de requerimientos ISO27001




Fuente: Construcción propia del autor

En donde identificamos que Qwerty tiene un nivel de riesgo mayor en los siguientes dominios: A6. Organización de la seguridad de la información, A8. Gestión de activos, A10. Criptografía, A11. Seguridad física y del entorno, A12. Seguridad de las operaciones, A13. Seguridad de las comunicaciones, A14. Adquisición, desarrollo y mantenimiento de sistemas y A16. Gestión de incidentes de seguridad de la información. Esta información es vital para la toma de decisiones, la priorización y la definición de la declaración de aplicabilidad.

**6.2.3. Valoración Cualitativa De Activos De Qwerty S.A**. En el cuadro 9 se puede visualizar el resultado de la valoración cualitativa de activos de Qwerty S.A.

Cuadro 9. Valoración cualitativa de activos de Qwerty S.A.

| | | DIMENSIONES | | | | |
|---|---|---|---|---|---|---|
| | | Autenticidad | Trazabilidad | Confidencialidad | Integridad | Disponibilidad |
| | ACTIVO DE INFORMACIÓN | A | T | C | I | D |
| | 1. Datos / Información: | | | | | |
| 1.1 | Estudiantes | A | M | M | A | A |
| 1.2 | Empleados | A | A | A | A | M |
| 1.3 | Proveedores | A | M | M | A | M |

Cuadro 9. Valoración cualitativa de activos de Qwerty S.A. Continuación

| | | DIMENSIONES | | | | |
|---|---|---|---|---|---|---|
| | | Autenticidad | Trazabilidad | Confidencialidad | Integridad | Disponibilidad |
| | ACTIVO DE INFORMACIÓN | A | T | C | I | D |
| 1.4 | Nómina | A | M | A | A | M |
| 1.5 | Órdenes de compra | A | M | A | M | B |
| 1.6 | Inventarios | M | B | B | A | B |
| 1.7 | Facturación | A | M | M | MA | M |
| 1.8 | Hojas de vida | M | M | A | A | M |
| 1.9 | Documentos digitales | B | B | B | B | B |
| 1.10 | Audios de reuniones, asambleas | B | B | M | B | M |
| 1.11 | Contenido Página Web GoDaddy | M | M | M | A | A |
| | **2. Servicios:** | | | | | |
| 2.1 | FTP | B | B | B | M | B |
| 2.2 | Correo electrónico google | A | M | M | B | M |
| 2.3 | Internet | A | M | A | A | A |
| 2.4 | Certificados laborales | M | M | M | B | B |
| 2.5 | Nómina | A | M | A | M | M |
| 2.6 | Recibos de pago | A | A | A | A | A |
| 2.7 | Red inalámbrica | M | M | M | M | M |
| 2.8 | Red alámbrica | M | M | M | M | A |
| 2.9 | Impresión | B | B | B | B | M |
| 2.10 | DHCP | A | M | A | M | A |
| 2.11 | Voz IP | M | B | M | B | M |
| | **3. Equipamiento informático (Hardware)** | | | | | |
| 3.1 | Servidor de impresión Dell PowerEdge T440 | A | B | A | A | A |
| 3.2 | Impresora HP LaserJet Enterprise serie 600 (Nómina y Facturación) | B | B | B | B | B |
| 3.3 | Impresora/Escáner SMART MultiXpress M4370LX (Directivos, administrativos y docentes) | B | B | B | B | M |
| 3.4 | Servidor Dell Torre PowerEdge T130 (FTP) | B | B | B | M | B |
| 3.5 | Servidor Dell Torre PowerEdge T440 (Nómina y Facturación) | MA | A | MA | MA | A |
| 3.6 | Servidor Dell Torre PowerEdge T440 (DHCP) | MA | A | MA | MA | MA |
| 3.7 | Equipo de cómputo (Dep. Desarrollo Tecnológico) | B | B | B | B | B |

Cuadro 9. Valoración cualitativa de activos de Qwerty S.A. Continuación

| | | DIMENSIONES | | | | |
|---|---|---|---|---|---|---|
| | | Autenticidad | Trazabilidad | Confidencialidad | Integridad | Disponibilidad |
| | ACTIVO DE INFORMACIÓN | A | T | C | I | D |
| 3.8 | Cortafuegos Cisco ASA 5505 | MA | MA | A | MA | MA |
| 3.9 | Equipo de cómputo (Dep Infraestructura) | M | B | B | B | B |
| 3.10 | Equipo de cómputo (Dep control y seguimiento) | M | B | B | B | B |
| 3.11 | Equipo de cómputo (Dep. de prueba de software) | M | B | B | B | B |
| 3.12 | Puntos de acceso alámbrico (HUB) | A | B | A | A | A |
| 3.13 | Switches Cisco Catalyst 2960 | A | B | A | A | A |
| 3.14 | Teléfonos IP (Dep. del centro) | B | B | B | B | B |
| 3.15 | Puntos de acceso alámbrico (HUB) (Dep. de Sistemas) | A | B | A | A | M |
| | **4. Personal** | | | | | |
| 4.1 | Directivos | A | A | A | A | B |
| 4.2 | Administradores | A | A | A | A | M |
| 4.3 | Docentes | A | A | A | A | A |
| 4.4 | Estudiantes | A | A | A | A | A |
| 4.5 | Especialista correo electrónico | M | A | A | M | M |
| | **5. Software** | | | | | |
| 5.1 | Sistema de nómina | A | A | A | A | A |
| 5.2 | Sistema de facturación | A | A | A | A | A |
| 5.3 | Windows 10 Pro | B | B | B | B | B |
| 5.4 | Joomla 2.5 (GoDaddy) | A | A | A | A | A |
| 5.5 | Apache (GoDaddy) | A | A | A | A | A |
| 5.6 | PHP (GoDaddy) | A | A | A | A | A |
| 5.7 | MySQL (GoDaddy) | MA | MA | MA | MA | MA |
| 5.8 | Apache 2.4.25 (Nómina y facturación) | A | A | A | A | A |
| 5.9 | PHP 5.6.30 - 7.1.1 (Nómina y facturación) | A | A | A | A | A |
| 5.10 | MySQL 5.7.17 (Nómina y facturación) | MA | MA | MA | MA | MA |
| 5.11 | phpMyAdmin 4.6.6 (Nómina y facturación) | A | A | A | A | A |
| 5.12 | Sistema de proveedores | M | MA | MA | MA | A |
| 5.13 | Sistema de compras | MA | MA | MA | MA | A |

Cuadro 9. Valoración cualitativa de activos de Qwerty S.A. Continuación

| | | DIMENSIONES | | | | |
|---|---|---|---|---|---|---|
| | | Autenticidad | Trazabilidad | Confidencialidad | Integridad | Disponibilidad |
| | ACTIVO DE INFORMACIÓN | A | T | C | I | D |
| 5.14 | Sistema de inventarios | M | M | M | M | A |
| 5.15 | Software Antivirus | MA | MA | MA | MA | MA |
| | **6. Redes de comunicaciones** | | | | | |
| 6.1 | Red de datos | MA | MA | MA | MA | MA |
| 6.2 | Red de datos inalámbrica | MA | MA | MA | MA | M |

Fuente: Construcción propia del autor aplicando metodología Magerith

**6.2.4. Valoración Cuantitativa De Activos De Qwerty S.A**. En el cuadro 10 se puede visualizar el resultado de la valoración cuantitativa de activos de Qwerty S.A.

Cuadro 10. Valoración cuantitativa de activos de Qwerty S.A.

| | | | DIMENSIONES | | | | | VALOR PROMEDIO |
|---|---|---|---|---|---|---|---|---|
| | | | Autenticidad | Trazabilidad | Confidencialidad | Integridad | Disponibilidad | |
| | ACTIVO DE INFORMACIÓN | RIESGO | A | T | C | I | D | |
| | **1. Datos / Información:** | | | | | | | |
| 1.1 | Estudiantes | ALTO | 8 | 5 | 5 | 8 | 8 | **7** |
| 1.2 | Empleados | ALTO | 8 | 8 | 8 | 8 | 5 | **7** |
| 1.3 | Proveedores | ALTO | 8 | 5 | 5 | 8 | 5 | **6** |
| 1.4 | Nómina | ALTO | 8 | 5 | 8 | 8 | 5 | **7** |
| 1.5 | Órdenes de compra | ALTO | 8 | 5 | 8 | 5 | 2 | **6** |
| 1.6 | Inventarios | MEDIO | 5 | 2 | 2 | 8 | 2 | **4** |
| 1.7 | Facturación | ALTO | 8 | 5 | 5 | 9 | 5 | **6** |
| 1.8 | Hojas de vida | ALTO | 5 | 5 | 8 | 8 | 5 | **6** |
| 1.9 | Documentos digitales | BAJO | 2 | 2 | 2 | 2 | 2 | **2** |
| 1.10 | Audios de reuniones, asambleas | MEDIO | 2 | 2 | 5 | 2 | 5 | **3** |
| 1.11 | Contenido Página Web GoDaddy | ALTO | 5 | 5 | 5 | 8 | 8 | **6** |
| | **2. Servicios:** | | | | | | | |
| 2.1 | FTP | MEDIO | 2 | 2 | 2 | 5 | 2 | **3** |
| 2.2 | Correo electrónico google | MEDIO | 8 | 5 | 5 | 2 | 5 | **5** |
| 2.3 | Internet | ALTO | 8 | 5 | 8 | 8 | 8 | **7** |

Cuadro 10. Valoración cuantitativa de activos de Qwerty S.A. Continuación

| | | | DIMENSIONES | | | | | VALOR PROMEDIO |
|---|---|---|---|---|---|---|---|---|
| | | | Autenticidad | Trazabilidad | Confidencialidad | Integridad | Disponibilidad | |
| | ACTIVO DE INFORMACIÓN | RIESGO | A | T | C | I | D | |
| 2.4 | Certificados laborales | MEDIO | 5 | 5 | 5 | 2 | 2 | **4** |
| 2.5 | Nómina | ALTO | 8 | 5 | 8 | 5 | 5 | **6** |
| 2.6 | Recibos de pago | ALTO | 8 | 8 | 8 | 8 | 8 | **8** |
| 2.7 | Red inalámbrica | MEDIO | 5 | 5 | 5 | 5 | 5 | **5** |
| 2.8 | Red alámbrica | ALTO | 5 | 5 | 5 | 5 | 8 | **6** |
| 2.9 | Impresión | MEDIO | 2 | 2 | 2 | 2 | 5 | **3** |
| 2.10 | DHCP | ALTO | 8 | 5 | 8 | 5 | 8 | **7** |
| 2.11 | Voz IP | MEDIO | 5 | 2 | 5 | 2 | 5 | **4** |
| | **3. Equipamiento informático (Hardware)** | | | | | | | |
| 3.1 | Servidor de impresión Dell PowerEdge T440 | ALTO | 8 | 2 | 8 | 8 | 8 | **7** |
| 3.2 | Impresora HP LaserJet Enterprise serie 600 (Nómina y Facturación) | BAJO | 2 | 2 | 2 | 2 | 2 | **2** |
| 3.3 | Impresora/Escáner SMART MultiXpress M4370LX (Directivos, administrativos y docentes) | MEDIO | 2 | 2 | 2 | 2 | 5 | **3** |
| 3.4 | Servidor Dell Torre PowerEdge T130 (FTP) | MEDIO | 2 | 2 | 2 | 5 | 2 | **3** |
| 3.5 | Servidor Dell Torre PowerEdge T440 (Nómina y Facturación) | MUY ALTO | 9 | 8 | 9 | 9 | 8 | **9** |
| 3.6 | Servidor Dell Torre PowerEdge T440 (DHCP) | MUY ALTO | 9 | 8 | 9 | 9 | 9 | **9** |
| 3.7 | Equipo de cómputo (Dep. Desarrollo Tecnológico) | BAJO | 2 | 2 | 2 | 2 | 2 | **2** |
| 3.8 | Cortafuegos Cisco ASA 5505 | MUY ALTO | 9 | 9 | 8 | 9 | 9 | **9** |

Cuadro 10. Valoración cuantitativa de activos de Qwerty S.A. Continuación

| | | | DIMENSIONES | | | | | VALOR PROMEDIO |
|---|---|---|---|---|---|---|---|---|
| | | | Autenticidad | Trazabilidad | Confidencialidad | Integridad | Disponibilidad | |
| | ACTIVO DE INFORMACIÓN | RIESGO | A | T | C | I | D | |
| 3.9 | Equipo de cómputo (Dep Infraestructura) | MEDIO | 5 | 2 | 2 | 2 | 2 | **3** |
| 3.10 | Equipo de cómputo (Dep control y seguimiento) | MEDIO | 5 | 2 | 2 | 2 | 2 | **3** |
| 3.11 | Equipo de cómputo (Dep. de prueba de software) | MEDIO | 5 | 2 | 2 | 2 | 2 | **3** |
| 3.12 | Puntos de acceso alámbrico (HUB) | ALTO | 8 | 2 | 8 | 8 | 8 | **7** |
| 3.13 | Switches Cisco Catalyst 2960 | ALTO | 8 | 2 | 8 | 8 | 8 | **7** |
| 3.14 | Teléfonos IP (Dep. del centro) | BAJO | 2 | 2 | 2 | 2 | 2 | **2** |
| 3.15 | Puntos de acceso alámbrico (HUB) (Dep. de Sistemas) | ALTO | 8 | 2 | 8 | 8 | 5 | **6** |
| | **4. Personal** | | | | | | | |
| 4.1 | Directivos | ALTO | 8 | 8 | 8 | 8 | 2 | **7** |
| 4.2 | Administradores | ALTO | 8 | 8 | 8 | 8 | 5 | **7** |
| 4.3 | Docentes | ALTO | 8 | 8 | 8 | 8 | 8 | **8** |
| 4.4 | Estudiantes | ALTO | 8 | 8 | 8 | 8 | 8 | **8** |
| 4.5 | Especialista correo electrónico | ALTO | 5 | 8 | 8 | 5 | 5 | **6** |
| | **5. Software** | | | | | | | |
| 5.1 | Sistema de nómina | ALTO | 8 | 8 | 8 | 8 | 8 | **8** |
| 5.2 | Sistema de facturación | ALTO | 8 | 8 | 8 | 8 | 8 | **8** |
| 5.3 | Windows 10 Pro | BAJO | 2 | 2 | 2 | 2 | 2 | **2** |
| 5.4 | Joomla 2.5 (GoDaddy) | ALTO | 8 | 8 | 8 | 8 | 8 | **8** |
| 5.5 | Apache (GoDaddy) | ALTO | 8 | 8 | 8 | 8 | 8 | **8** |
| 5.6 | PHP (GoDaddy) | ALTO | 8 | 8 | 8 | 8 | 8 | **8** |
| 5.7 | MySQL (GoDaddy) | MUY ALTO | 9 | 9 | 9 | 9 | 9 | **9** |
| 5.8 | Apache 2.4.25 (Nómina y facturación) | ALTO | 8 | 8 | 8 | 8 | 8 | **8** |

Cuadro 10. Valoración cuantitativa de activos de Qwerty S.A. Continuación

| | | | DIMENSIONES | | | | | VALOR PROMEDIO |
|---|---|---|---|---|---|---|---|---|
| | | | Autenticidad | Trazabilidad | Confidencialidad | Integridad | Disponibilidad | |
| | ACTIVO DE INFORMACIÓN | RIESGO | A | T | C | I | D | |
| 5.9 | PHP 5.6.30 - 7.1.1 (Nómina y facturación) | ALTO | 8 | 8 | 8 | 8 | 8 | 8 |
| 5.10 | MySQL 5.7.17 (Nómina y facturación) | MUY ALTO | 9 | 9 | 9 | 9 | 9 | 9 |
| 5.11 | phpMyAdmin 4.6.6 (Nómina y facturación) | ALTO | 8 | 8 | 8 | 8 | 8 | 8 |
| 5.12 | Sistema de proveedores | ALTO | 5 | 9 | 9 | 9 | 8 | 8 |
| 5.13 | Sistema de compras | MUY ALTO | 9 | 9 | 9 | 9 | 8 | 9 |
| 5.14 | Sistema de inventarios | ALTO | 5 | 5 | 5 | 5 | 8 | 6 |
| 5.15 | Software Antivirus | MUY ALTO | 9 | 9 | 9 | 9 | 9 | 9 |
| | **6. Redes de comunicaciones** | | | | | | | |
| 6.1 | Red de datos | MUY ALTO | 9 | 9 | 9 | 9 | 9 | **9** |
| 6.2 | Red de datos inalámbrica | ALTO | 9 | 9 | 9 | 9 | 5 | **8** |

Fuente: Construcción propia del autor aplicando metodología Magerit

**6.2.5. Valoración de Amenazas y vulnerabilidades**. En el cuadro 11 se visualiza el resultado de la identificación de amenazas y vulnerabilidades en Qwerty S.A.

Cuadro 11. Valoración de Amenazas y vulnerabilidades

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades |
|---|---|---|---|---|---|
| 1 | [D] Datos | Estudiantes | 7 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red |
| 2 | [D] Datos | Empleados | 7 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red |

Cuadro 11. Valoración de Amenazas y vulnerabilidades Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades |
|---|---|---|---|---|---|
| 3 | [D] Datos | Proveedores | 6 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red |
| 4 | [D] Datos | Nómina | 7 | [E.15] Alteración accidental de la información | En días de alto flujo de solicitudes el ingreso de datos es efectuado por personal de prácticas o por contrato de aprendizaje |
| 5 | [D] Datos | Órdenes de compra | 6 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red |
| 6 | [D] Datos | Inventarios | 4 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red |
| 7 | [D] Datos | Facturación | 6 | [E.15] Alteración accidental de la información | En días de alto flujo de solicitudes el ingreso de datos es efectuado por personal de prácticas o por contrato de aprendizaje |
| 8 | [D] Datos | Hojas de vida | 6 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red |
| 9 | [D] Datos | Documentos digitales | 2 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red |
| 10 | [D] Datos | Audios de reuniones, asambleas | 3 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red |
| 11 | [D] Datos | Contenido Página Web GoDaddy | 6 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades asociadas a la versión usadas de software con el que está implementado el sitio |

Cuadro 11. Valoración de Amenazas y vulnerabilidades Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades |
|---|---|---|---|---|---|
| 12 | [S] Servicio | FTP | 3 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red |
| 13 | [S] Servicio | Correo electrónico google | 5 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones |
| 14 | [S] Servicio | Internet | 7 | [A.7] Uso no previsto | No hay reglas implementadas en cortafuegos de control de acceso |
| 15 | [S] Servicio | Certificados laborales | 4 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas |
| 16 | [S] Servicio | Nómina | 6 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas |
| 17 | [S] Servicio | Recibos de pago | 8 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas |
| 18 | [S] Servicio | Red inalámbrica | 5 | [A.11] Acceso no autorizado | Solo hay un segmento de red |
| 19 | [S] Servicio | Red alámbrica | 6 | [A.11] Acceso no autorizado | Solo hay un segmento de red |
| 20 | [S] Servicio | Impresión | 3 | [E.1] Errores de los usuarios | No hay vulnerabilidad |
| 21 | [S] Servicio | DHCP | 7 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas |
| 22 | [S] Servicio | Voz IP | 4 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas |
| 23 | [HW] Hardware | Servidor de impresión Dell PowerEdge T440 | 7 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas |

Cuadro 11. Valoración de Amenazas y vulnerabilidades Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades |
|---|---|---|---|---|---|
| 24 | [HW] Hardware | Impresora HP LaserJet Enterprise serie 600 (Nómina y Facturación) | 2 | [E.1] Errores de los usuarios | No hay vulnerabilidad |
| 25 | [HW] Hardware | Impresora/Escáner SMART MultiXpress M4370LX (Directivos, administrativos y docentes) | 3 | [E.1] Errores de los usuarios | No hay vulnerabilidad |
| 26 | [HW] Hardware | Servidor Dell Torre PowerEdge T130 (FTP) | 3 | [E.2] Errores del administrador | Considerando que no se evidencia riesgo, solamente se considera la posibilidad de errores humanos |
| 27 | [HW] Hardware | Servidor Dell Torre PowerEdge T440 (Nómina y Facturación) | 9 | [I.7] Condiciones inadecuadas de temperatura o humedad | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas |
| 28 | [HW] Hardware | Servidor Dell Torre PowerEdge T440 (DHCP) | 9 | [I.7] Condiciones inadecuadas de temperatura o humedad | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas |
| 29 | [HW] Hardware | Equipo de cómputo (Dep. Desarrollo Tecnológico) | 2 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones |
| 30 | [HW] Hardware | Cortafuegos Cisco ASA 5505 | 9 | [A.11] Acceso no autorizado | No se han implementado reglas en el cortafuegos para autorizar o denegar conexiones o transmisión de datos |
| 31 | [HW] Hardware | Equipo de cómputo (Dep Infraestructura) | 3 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones |
| 32 | [HW] Hardware | Equipo de cómputo (Dep control y seguimiento) | 3 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones |
| 33 | [HW] Hardware | Equipo de cómputo (Dep. de prueba de software) | 3 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones |
| 34 | [HW] Hardware | Puntos de acceso alámbrico (HUB) | 7 | [A.8] Difusión de software dañino | Solo hay un segmento de red y no se monitorea la actualización del antivirus |

Cuadro 11. Valoración de Amenazas y vulnerabilidades Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades |
|---|---|---|---|---|---|
| 35 | [HW] Hardware | Switches Cisco Catalyst 2960 | 7 | [A.8] Difusión de software dañino | Solo hay un segmento de red y no se monitorea la actualización del antivirus |
| 36 | [HW] Hardware | Teléfonos IP (Dep. del centro) | 2 | | Solo hay un segmento de red y no se monitorea la actualización del antivirus |
| 37 | [HW] Hardware | Puntos de acceso alámbrico (HUB) (Dep. de Sistemas) | 6 | [A.8] Difusión de software dañino | Solo hay un segmento de red y no se monitorea la actualización del antivirus |
| 38 | [P] Personal | Directivos | 7 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco de ataque. |
| 39 | [P] Personal | Administradores | 7 | [E.2] Errores del administrador | Desconocimiento buenas prácticas |
| 40 | [P] Personal | Docentes | 8 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones |
| 41 | [P] Personal | Estudiantes | 8 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones |
| 42 | [P] Personal | Especialista correo electrónico | 6 | [E.4] Errores de configuración | Desconocimiento buenas prácticas |
| 43 | [SW] Software | Sistema de nómina | 8 | [E.15] Alteración accidental de la información | Registro de información por personas de otras áreas o contratos de aprendizaje sin ser entrenados |
| 44 | [SW] Software | Sistema de facturación | 8 | [E.15] Alteración accidental de la información | Registro de información por personas de otras áreas o contratos de aprendizaje sin ser entrenados |
| 45 | [SW] Software | Windows 10 Pro | 2 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades conocidas de la versión en uso |
| 46 | [SW] Software | Joomla 2.5 (GoDaddy) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades asociadas a la versión usadas de software con el que está implementado el sitio |
| 47 | [SW] Software | Apache (GoDaddy) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades asociadas a la versión usadas de software con el que está implementado el sitio |

Cuadro 11. Valoración de Amenazas y vulnerabilidades Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades |
|---|---|---|---|---|---|
| 48 | [SW] Software | PHP (GoDaddy) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades asociadas a la versión usadas de software con el que está implementado el sitio |
| 49 | [SW] Software | MySQL (GoDaddy) | 9 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades asociadas a la versión usadas de software con el que está implementado el sitio |
| 50 | [SW] Software | Apache 2.4.25 (Nómina y facturación) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades conocidas de la versión en uso |
| 51 | [SW] Software | PHP 5.6.30 - 7.1.1 (Nómina y facturación) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades conocidas de la versión en uso |
| 52 | [SW] Software | MySQL 5.7.17 (Nómina y facturación) | 9 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades conocidas de la versión en uso |
| 53 | [SW] Software | phpMyAdmin 4.6.6 (Nómina y facturación) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades conocidas de la versión en uso |
| 54 | [SW] Software | Sistema de proveedores | 8 | [E.21] Errores de mantenimiento / actualización de programas (software) | Desconocimiento buenas prácticas |
| 55 | [SW] Software | Sistema de compras | 9 | [E.21] Errores de mantenimiento / actualización de programas (software) | Desconocimiento buenas prácticas |
| 56 | [SW] Software | Sistema de inventarios | 6 | [E.21] Errores de mantenimiento / actualización de programas (software) | Desconocimiento buenas prácticas |
| 57 | [SW] Software | Software Antivirus | 9 | [A.8] Difusión de software dañino | Solo hay un segmento de red y no se monitorea la actualización del antivirus |
| 58 | [COM] Redes de comunicaciones | Red de datos | 9 | [A.11] Acceso no autorizado | Solo hay un segmento de red y no se monitorea la actualización del antivirus |
| 59 | [COM] Redes de comunicaciones | Red de datos inalámbrica | 8 | [A.11] Acceso no autorizado | Solo hay un segmento de red y no se monitorea la actualización del antivirus |

Fuente: Construcción propia del autor aplicando metodología Magerit

## 6.3. ANÁLISIS DE RIESGOS

**6.3.1. Valoración de riesgos de Qwerty S.A**. Considerando la tabla 1, en el cuadro 12 se puede visualizar el resultado de la valoración de riesgos en Qwerty S.A.

Tabla 1. Probabilidad de ocurrencia del riesgo

| Código | Descripción |
|---|---|
| 1 | Muy raro |
| 2 | poco probable |
| 3 | posible |
| 4 | muy alto |
| 5 | casi seguro |

Cuadro 12. Valoración del Riesgo

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo (1) | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo (2) | Valor del Riesgo (1)*(2) |
|---|---|---|---|---|---|---|---|
| 1 | [D] Datos | Estudiantes | 7 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 14 |
| 2 | [D] Datos | Empleados | 7 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 14 |
| 3 | [D] Datos | Proveedores | 6 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 12 |

Cuadro 12. Valoración del Riesgo Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo (1) | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo (2) | Valor del Riesgo (1)*(2) |
|---|---|---|---|---|---|---|---|
| 4 | [D] Datos | Nómina | 7 | [E.15] Alteración accidental de la información | En días de alto flujo de solicitudes la captura de datos la hace personal de prácticas o por contrato de aprendizaje | 2 | 14 |
| 5 | [D] Datos | Órdenes de compra | 6 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 12 |
| 6 | [D] Datos | Inventarios | 4 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 8 |
| 7 | [D] Datos | Facturación | 6 | [E.15] Alteración accidental de la información | En días de alto flujo de solicitudes el ingreso de datos es efectuado por personal de prácticas o por contrato de aprendizaje | 2 | 12 |
| 8 | [D] Datos | Hojas de vida | 6 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 12 |
| 9 | [D] Datos | Documentos digitales | 2 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 4 |

Cuadro 12. Valoración del Riesgo Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo (1) | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo (2) | Valor del Riesgo (1)*(2) |
|---|---|---|---|---|---|---|---|
| 10 | [D] Datos | Audios de reuniones, asambleas | 3 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 6 |
| 11 | [D] Datos | Contenido Página Web GoDaddy | 6 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades asociadas a la versión usadas de software con el que está implementado el sitio | 2 | 12 |
| 12 | [S] Servicio | FTP | 3 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 6 |
| 13 | [S] Servicio | Correo electrónico google | 5 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 10 |
| 14 | [S] Servicio | Internet | 7 | [A.7] Uso no previsto | No hay reglas implementadas en cortafuegos de control de acceso | 2 | 14 |
| 15 | [S] Servicio | Certificados laborales | 4 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 12 |
| 16 | [S] Servicio | Nómina | 6 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 18 |

Cuadro 12. Valoración del Riesgo Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo (1) | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo (2) | Valor del Riesgo (1)*(2) |
|---|---|---|---|---|---|---|---|
| 17 | [S] Servicio | Recibos de pago | 8 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 24 |
| 18 | [S] Servicio | Red inalámbrica | 5 | [A.11] Acceso no autorizado | Solo hay un segmento de red | 3 | 15 |
| 19 | [S] Servicio | Red alámbrica | 6 | [A.11] Acceso no autorizado | Solo hay un segmento de red | 3 | 18 |
| 20 | [S] Servicio | Impresión | 3 | [E.1] Errores de los usuarios | No hay vulnerabilidad | 1 | 3 |
| 21 | [S] Servicio | DHCP | 7 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 21 |
| 22 | [S] Servicio | Voz IP | 4 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 12 |
| 23 | [HW] Hardware | Servidor de impresión Dell PowerEdge T440 | 7 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 21 |
| 24 | [HW] Hardware | Impresora HP LaserJet Enterprise serie 600 (Nómina y Facturación) | 2 | [E.1] Errores de los usuarios | No hay vulnerabilidad | 1 | 2 |
| 25 | [HW] Hardware | Impresora/Escáner SMART MultiXpress M4370LX (Directivos, administrativos y docentes) | 3 | [E.1] Errores de los usuarios | No hay vulnerabilidad | 1 | 3 |

Cuadro 12. Valoración del Riesgo Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo (1) | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo (2) | Valor del Riesgo (1)*(2) |
|---|---|---|---|---|---|---|---|
| 26 | [HW] Hardware | Servidor Dell Torre PowerEdge T130 (FTP) | 3 | [E.2] Errores del administrador | Considerando que no se evidencia riesgo, solamente se considera la posibilidad de errores humanos | 2 | 6 |
| 27 | [HW] Hardware | Servidor Dell Torre PowerEdge T440 (Nómina y Facturación) | 9 | [I.7] Condiciones inadecuadas de temperatura o humedad | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 27 |
| 28 | [HW] Hardware | Servidor Dell Torre PowerEdge T440 (DHCP) | 9 | [I.7] Condiciones inadecuadas de temperatura o humedad | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 27 |
| 29 | [HW] Hardware | Equipo de cómputo (Dep. Desarrollo Tecnológico) | 2 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 4 |
| 0 | [HW] Hardware | Cortafuegos Cisco ASA 5505 | 9 | [A.11] Acceso no autorizado | No se han implementado reglas en el cortafuegos para autorizar o denegar conexiones o transmisión de datos | 4 | 36 |
| 31 | [HW] Hardware | Equipo de cómputo (Dep Infraestructura) | 3 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 6 |
| 32 | [HW] Hardware | Equipo de cómputo (Dep control y seguimiento) | 3 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 6 |

Cuadro 12. Valoración del Riesgo Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo (1) | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo (2) | Valor del Riesgo (1)*(2) |
|---|---|---|---|---|---|---|---|
| 33 | [HW] Hardware | Equipo de cómputo (Dep. de prueba de software) | 3 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 6 |
| 34 | [HW] Hardware | Puntos de acceso alámbrico (HUB) | 7 | [A.8] Difusión de software dañino | Solo hay un segmento de red y no se monitorea la actualización del antivirus | 3 | 21 |
| 35 | [HW] Hardware | Switches Cisco Catalyst 2960 | 7 | [A.8] Difusión de software dañino | Solo hay un segmento de red y no se monitorea la actualización del antivirus | 3 | 21 |
| 36 | [HW] Hardware | Teléfonos IP (Dep. del centro) | 2 | | Solo hay un segmento de red y no se monitorea la actualización del antivirus | 2 | 4 |
| 37 | [HW] Hardware | Puntos de acceso alámbrico (HUB) (Dep. de Sistemas) | 6 | [A.8] Difusión de software dañino | Solo hay un segmento de red y no se monitorea la actualización del antivirus | 3 | 18 |
| 38 | [P] Personal | Directivos | 7 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 14 |
| 39 | [P] Personal | Administradores | 7 | [E.2] Errores del administrador | Desconocimiento buenas prácticas | 2 | 14 |
| 40 | [P] Personal | Docentes | 8 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 16 |
| 41 | [P] Personal | Estudiantes | 8 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 16 |

Cuadro 12. Valoración del Riesgo Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo (1) | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo (2) | Valor del Riesgo (1)*(2) |
|---|---|---|---|---|---|---|---|
| 42 | [P] Personal | Especialista correo electrónico | 6 | [E.4] Errores de configuración | Desconocimiento buenas prácticas | 2 | 12 |
| 43 | [SW] Software | Sistema de nómina | 8 | [E.15] Alteración accidental de la información | Registro de información por personas de otras áreas o contratos de aprendizaje sin ser entrenados | 3 | 24 |
| 44 | [SW] Software | Sistema de facturación | 8 | [E.15] Alteración accidental de la información | Registro de información por personas de otras áreas o contratos de aprendizaje sin ser entrenados | 3 | 24 |
| 45 | [SW] Software | Windows 10 Pro | 2 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades conocidas de la versión en uso | 2 | 4 |
| 46 | [SW] Software | Joomla 2.5 (GoDaddy) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades asociadas a la versión usadas de software con el que está implementado el sitio | 2 | 16 |
| 47 | [SW] Software | Apache (GoDaddy) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades asociadas a la versión usadas de software con el que está implementado el sitio | 2 | 16 |
| 48 | [SW] Software | PHP (GoDaddy) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades asociadas a la versión usadas de software con el que está implementado el sitio | 2 | 16 |

Cuadro 12. Valoración del Riesgo Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo (1) | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo (2) | Valor del Riesgo (1)*(2) |
|---|---|---|---|---|---|---|---|
| 49 | [SW] Software | MySQL (GoDaddy) | 9 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades asociadas a la versión usadas de software con el que está implementado el sitio | 2 | 18 |
| 50 | [SW] Software | Apache 2.4.25 (Nómina y facturación) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades conocidas de la versión en uso | 2 | 16 |
| 51 | [SW] Software | PHP 5.6.30 - 7.1.1 (Nómina y facturación) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades conocidas de la versión en uso | 2 | 16 |
| 52 | [SW] Software | MySQL 5.7.17 (Nómina y facturación) | 9 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades conocidas de la versión en uso | 2 | 18 |
| 53 | [SW] Software | phpMyAdmin 4.6.6 (Nómina y facturación) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades conocidas de la versión en uso | 2 | 16 |
| 54 | [SW] Software | Sistema de proveedores | 8 | [E.21] Errores de mantenimiento / actualización de programas (software) | Desconocimiento buenas prácticas | 2 | 16 |
| 55 | [SW] Software | Sistema de compras | 9 | [E.21] Errores de mantenimiento / actualización de programas (software) | Desconocimiento buenas prácticas | 2 | 18 |

Cuadro 12. Valoración del Riesgo Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo (1) | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo (2) | Valor del Riesgo (1)*(2) |
|---|---|---|---|---|---|---|---|
| 56 | [SW] Software | Sistema de inventarios | 6 | [E.21] Errores de mantenimiento / actualización de programas (software) | Desconocimiento buenas prácticas | 2 | 12 |
| 57 | [SW] Software | Software Antivirus | 9 | [A.8] Difusión de software dañino | Solo hay un segmento de red y no se monitorea la actualización del antivirus | 4 | 36 |
| 58 | [COM] Redes de comunicaciones | Red de datos | 9 | [A.11] Acceso no autorizado | Solo hay un segmento de red y no se monitorea la actualización del antivirus | 3 | 27 |
| 59 | [COM] Redes de comunicaciones | Red de datos inalámbrica | 8 | [A.11] Acceso no autorizado | Solo hay un segmento de red y no se monitorea la actualización del antivirus | 3 | 24 |

Fuente: Construcción propia del autor aplicando Magerit

**6.2.3. Enfoque de evaluación de los riesgos**. De acuerdo con el resultado obtenido en la valoración de los riesgos, en el cuadro 13, se encuentra la matriz de riesgos priorizados según la valoración efectuada:

Cuadro 13. Riesgos priorizados

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo | Valor del Riesgo |
|---|---|---|---|---|---|---|---|
| 1 | [HW] Hardware | Cortafuegos Cisco ASA 5505 | 9 | [A.11] Acceso no autorizado | No se han implementado reglas en el cortafuegos para autorizar o denegar conexiones o transmisión de datos | 4 | 36 |

Cuadro 13. Riesgos priorizados Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo | Valor del Riesgo |
|---|---|---|---|---|---|---|---|
| 2 | [SW] Software | Software Antivirus | 9 | [A.8] Difusión de software dañino | Solo hay un segmento de red y no se monitorea la actualización del antivirus | 4 | 36 |
| 3 | [HW] Hardware | Servidor Dell Torre PowerEdge T440 (Nómina y Facturación) | 9 | [I.7] Condiciones inadecuadas de temperatura o humedad | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 27 |
| 4 | [HW] Hardware | Servidor Dell Torre PowerEdge T440 (DHCP) | 9 | [I.7] Condiciones inadecuadas de temperatura o humedad | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 27 |
| 5 | [COM] Redes de comunicaciones | Red de datos | 9 | [A.11] Acceso no autorizado | Solo hay un segmento de red y no se monitorea la actualización del antivirus | 3 | 27 |
| 6 | [S] Servicio | Recibos de pago | 8 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 24 |
| 7 | [SW] Software | Sistema de nómina | 8 | [E.15] Alteración accidental de la información | Registro de información por personas de otras áreas o contratos de aprendizaje sin ser entrenados | 3 | 24 |
| 8 | [SW] Software | Sistema de facturación | 8 | [E.15] Alteración accidental de la información | Registro de información por personas de otras áreas o contratos de aprendizaje sin ser entrenados | 3 | 24 |

Cuadro 13. Riesgos priorizados Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo | Valor del Riesgo |
|---|---|---|---|---|---|---|---|
| 9 | [COM] Redes de comunicaciones | Red de datos inalámbrica | 8 | [A.11] Acceso no autorizado | Solo hay un segmento de red y no se monitorea la actualización del antivirus | 3 | 24 |
| 10 | [S] Servicio | DHCP | 7 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 21 |
| 11 | [HW] Hardware | Servidor de impresión Dell PowerEdge T440 | 7 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 21 |
| 12 | [HW] Hardware | Puntos de acceso alámbrico (HUB) | 7 | [A.8] Difusión de software dañino | Solo hay un segmento de red y no se monitorea la actualización del antivirus | 3 | 21 |
| 13 | [HW] Hardware | Switches Cisco Catalyst 2960 | 7 | [A.8] Difusión de software dañino | Solo hay un segmento de red y no se monitorea la actualización del antivirus | 3 | 21 |
| 14 | [S] Servicio | Nómina | 6 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 18 |
| 15 | [S] Servicio | Red alámbrica | 6 | [A.11] Acceso no autorizado | Solo hay un segmento de red | 3 | 18 |
| 16 | [HW] Hardware | Puntos de acceso alámbrico (HUB) (Dep. de Sistemas) | 6 | [A.8] Difusión de software dañino | Solo hay un segmento de red y no se monitorea la actualización del antivirus | 3 | 18 |
| 17 | [SW] Software | MySQL (GoDaddy) | 9 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades asociadas a la versión usadas de software con el que está implementado el sitio | 2 | 18 |

Cuadro 13. Riesgos priorizados Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo | Valor del Riesgo |
|---|---|---|---|---|---|---|---|
| 18 | [SW] Software | MySQL 5.7.17 (Nómina y facturación) | 9 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades conocidas de la versión en uso | 2 | 18 |
| 19 | [SW] Software | Sistema de compras | 9 | [E.21] Errores de mantenimiento / actualización de programas (software) | Desconocimiento buenas prácticas | 2 | 18 |
| 20 | [P] Personal | Docentes | 8 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 16 |
| 21 | [P] Personal | Estudiantes | 8 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 16 |
| 22 | [SW] Software | Joomla 2.5 (GoDaddy) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades asociadas a la versión usadas de software con el que está implementado el sitio | 2 | 16 |
| 23 | [SW] Software | Apache (GoDaddy) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades asociadas a la versión usadas de software con el que está implementado el sitio | 2 | 16 |
| 24 | [SW] Software | PHP (GoDaddy) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades asociadas a la versión usadas de software con el que está implementado el sitio | 2 | 16 |

Cuadro 13. Riesgos priorizados Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo | Valor del Riesgo |
|---|---|---|---|---|---|---|---|
| 25 | [SW] Software | Apache 2.4.25 (Nómina y facturación) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades conocidas de la versión en uso | 2 | 16 |
| 26 | [SW] Software | PHP 5.6.30 - 7.1.1 (Nómina y facturación) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades conocidas de la versión en uso | 2 | 16 |
| 27 | [SW] Software | phpMyAdmin 4.6.6 (Nómina y facturación) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades conocidas de la versión en uso | 2 | 16 |
| 28 | [SW] Software | Sistema de proveedores | 8 | [E.21] Errores de mantenimiento / actualización de programas (software) | Desconocimiento buenas prácticas | 2 | 16 |
| 29 | [S] Servicio | Red inalámbrica | 5 | [A.11] Acceso no autorizado | Solo hay un segmento de red | 3 | 15 |
| 30 | [D] Datos | Estudiantes | 7 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 14 |
| 31 | [D] Datos | Empleados | 7 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 14 |

Cuadro 13. Riesgos priorizados Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo | Valor del Riesgo |
|---|---|---|---|---|---|---|---|
| 32 | [D] Datos | Nómina | 7 | [E.15] Alteración accidental de la información | En días de alto flujo de solicitudes el ingreso de datos es efectuado por personal de prácticas o por contrato de aprendizaje | 2 | 14 |
| 33 | [S] Servicio | Internet | 7 | [A.7] Uso no previsto | No hay reglas implementadas en cortafuegos de control de acceso | 2 | 14 |
| 34 | [P] Personal | Directivos | 7 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 14 |
| 35 | [P] Personal | Administradores | 7 | [E.2] Errores del administrador | Desconocimiento buenas prácticas | 2 | 14 |
| 36 | [D] Datos | Proveedores | 6 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 12 |
| 37 | [D] Datos | Órdenes de compra | 6 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 12 |
| 38 | [D] Datos | Facturación | 6 | [E.15] Alteración accidental de la información | En días de alto flujo de solicitudes el ingreso de datos es efectuado por personal de prácticas o por contrato de aprendizaje | 2 | 12 |

Cuadro 13. Riesgos priorizados Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo | Valor del Riesgo |
|---|---|---|---|---|---|---|---|
| 39 | [D] Datos | Hojas de vida | 6 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 12 |
| 40 | [D] Datos | Contenido Página Web GoDaddy | 6 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades asociadas a la versión usadas de software con el que está implementado el sitio | 2 | 12 |
| 41 | [S] Servicio | Certificados laborales | 4 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 12 |
| 42 | [S] Servicio | Voz IP | 4 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 12 |
| 43 | [P] Personal | Especialista correo electrónico | 6 | [E.4] Errores de configuración | Desconocimiento buenas prácticas | 2 | 12 |
| 44 | [SW] Software | Sistema de inventarios | 6 | [E.21] Errores de mantenimiento / actualización de programas (software) | Desconocimiento buenas prácticas | 2 | 12 |
| 45 | [S] Servicio | Correo electrónico google | 5 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 10 |

Cuadro 13. Riesgos priorizados Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo | Valor del Riesgo |
|---|---|---|---|---|---|---|---|
| 46 | [D] Datos | Inventarios | 4 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 8 |
| 47 | [D] Datos | Audios de reuniones, asambleas | 3 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 6 |
| 48 | [S] Servicio | FTP | 3 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 6 |
| 49 | [HW] Hardware | Servidor Dell Torre PowerEdge T130 (FTP) | 3 | [E.2] Errores del administrador | Considerando que no se evidencia riesgo, solamente se considera la posibilidad de errores humanos | 2 | 6 |
| 50 | [HW] Hardware | Equipo de cómputo (Dep Infraestructura) | 3 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 6 |
| 51 | [HW] Hardware | Equipo de cómputo (Dep control y seguimiento) | 3 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 6 |

Cuadro 13. Riesgos priorizados Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo | Valor del Riesgo |
|---|---|---|---|---|---|---|---|
| 52 | [HW] Hardware | Equipo de cómputo (Dep. de prueba de software) | 3 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 6 |
| 53 | [D] Datos | Documentos digitales | 2 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 4 |
| 54 | [HW] Hardware | Equipo de cómputo (Dep. Desarrollo Tecnológico) | 2 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 4 |
| 55 | [HW] Hardware | Teléfonos IP (Dep. del centro) | 2 | | Solo hay un segmento de red y no se monitorea la actualización del antivirus | 2 | 4 |
| 56 | [SW] Software | Windows 10 Pro | 2 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades conocidas de la versión en uso | 2 | 4 |
| 57 | [S] Servicio | Impresión | 3 | [E.1] Errores de los usuarios | No hay vulnerabilidad | 1 | 3 |
| 58 | [HW] Hardware | Impresora/Escáner SMART MultiXpress M4370LX (Directivos, administrativos y docentes) | 3 | [E.1] Errores de los usuarios | No hay vulnerabilidad | 1 | 3 |
| 59 | [HW] Hardware | Impresora HP LaserJet Enterprise serie 600 (Nómina y Facturación) | 2 | [E.1] Errores de los usuarios | No hay vulnerabilidad | 1 | 2 |

Fuente: Construcción propia del autor

**6.2.4. Informe de evaluación de los riesgos.** De acuerdo con los resultados obtenidos durante el análisis de riesgos el siguiente en el cuadro 14, se puede ver el tratamiento propuesto de los riesgos:

Cuadro 14. Evaluación de riesgos

| Tipo de activo de información | Riesgo | Nombre del activo de información | Causas del riesgo |
|---|---|---|---|
| [HW] Hardware | R1 | Cortafuegos Cisco ASA 5505 | [A.11] Acceso no autorizado |
| | | | [A.7] Uso no previsto |
| | | | [A.23] Manipulación de equipos |
| | | | [A.25] Robo |
| | | | [A.26] Ataque destructivo |
| | | | [A.6] Abuso de privilegio de acceso |
| [HW] Hardware | R2 | Firewall CISCO ASA 5505 | [N.1] Fuego |
| | | | [N.2] Daños por agua |
| | | | [I.3] Contaminación mecánica |
| | | | [I.5] Avería de origen físico o lógico |
| | | | [I.6] Corte de suministro eléctrico |
| | | | [E.2] Errores del administrador |
| | | | [E.18] destrucción de la información |
| | | | [A.6] Abuso de privilegio de acceso |
| | | | [A.7] Uso no previsto |
| | | | [A.11] Acceso no autorizado |
| | | | [A.24] Denegación de servicio |
| | | | [A.25] Robo |
| | | | [A.26] Ataque destructivo |
| [SW] Software | R3 | Software Antivirus | [E.2] Errores del administrador |
| | | | [E.8] Difusión de software dañino |
| | | | [E.9] Errores de [re-] encaminamiento |
| | | | [E.10] Errores de secuencia |
| | | | [E.15] Alteración accidental de información. |
| | | | [E.18] destrucción de la información |
| | | | [E.19] fugas de la información. |
| | | | [E.20] Vulnerabilidad de los programas |
| | | | [E.21] Errores de mantenimiento / Actualización de programas |
| | | | [A.5] Suplantación de identidad de usuario |
| | | | [A.6] Abuso de privilegio de acceso |

Cuadro 14. Evaluación de riesgos Continuación

| Tipo de activo de información | Riesgo | Nombre del activo de información | Causas del riesgo |
|---|---|---|---|
| | | | [A.7] Uso no previsto |
| | | | [A.9] [RE-] Encaminamiento de mensajes. |
| | | | [A.10] Alteración de secuencia |
| | | | [A.11] Acceso no autorizado |
| | | | [A.15] Modificación deliberada de información. |
| | | | [A.18] destrucción de la información. |
| | | | [A.19] divulgación de información. |
| | | | [A.22] Manipulación de programas |
| [HW] Hardware | R4 | Servidor de archivos FTP Dell Torre Power Edge T440 (Nómina y Facturación) | [I.5] Avería de origen físico o lógico |
| | | | [I.6] Corte de suministro eléctrico |
| | | | [I.7] Condición inadecuada de temperatura o humedad |
| | | | [E.2] Errores del administrador |
| | | | [E.15] Alteración accidental de información. |
| | | | [E.18] destrucción de la información |
| | | | [E.23] Errores de mantenimiento / Actualización de equipos |
| | | | [E.24] Caída del sistema por agotamiento de recursos |
| | | | [E.25] Perdida de equipos. |
| | | | [A.6] Abuso de privilegio de acceso |
| | | | [A.7] Uso no previsto |
| | | | [A.11] Acceso no autorizado |
| | | | [A.23] Manipulación de equipos |
| | | | [A.26] Ataque destructivo |
| [HW] Hardware | R5 | Servidor Dell Torre PowerEdge T440 (DHCP) | [I.5] Avería de origen físico o lógico |
| | | | [I.6] Corte de suministro eléctrico |
| | | | [I.7] Condición inadecuada de temperatura o humedad |
| | | | [E.2] Errores del administrador |
| | | | [E.15] Alteración accidental de información. |
| | | | [E.18] destrucción de la información |
| | | | [E.23] Errores de mantenimiento / Actualización de equipos |
| | | | [E.24] Caída del sistema por agotamiento de recursos |

Cuadro 14. Evaluación de riesgos Continuación

| Tipo de activo de información | Riesgo | Nombre del activo de información | Causas del riesgo |
|---|---|---|---|
| | | | [E.25] Perdida de equipos. |
| | | | [A.6] Abuso de privilegio de acceso |
| | | | [A.7] Uso no previsto |
| | | | [A.11] Acceso no autorizado |
| | | | [A.23] Manipulación de equipos |
| | | | [A.26] Ataque destructivo |
| [COM] Redes de comunicaciones | R6 | Red de datos | [E.1] Errores del usuario |
| | | | [E.2] Errores del administrador |
| | | | [E.9] Errores de [re-] encaminamiento |
| | | | [E.10] Errores de secuencia |
| | | | [E.15] Alteración accidental de informac. |
| | | | [E.18] destrucción de la información |
| | | | [E.19] fugas de la información. |
| | | | [E.24] Caída del sistema por agotamiento de recursos |
| | | | [A.5] Suplantación de identidad de usuario |
| | | | [A.6] Abuso de privilegio de acceso |
| | | | [A.7] Uso no previsto |
| | | | [A.9] [RE-] Encaminamiento de mensajes. |
| | | | [A.10] Alteración de secuencia |
| | | | [A.11] Acceso no autorizado |
| | | | [A.13] Repudio |
| | | | [A.15] Modificación deliberada de información. |
| | | | [A.18] destrucción de la información. |
| | | | [A.19] divulgación de información. |
| | | | [A.24] Denegación de servicio |
| [D] Datos | R7 | Recibos de pago | [E.1] Errores del usuario |
| | | | [E.2] Errores del administrador |
| | | | [E.15] Alteración accidental de informac. |
| | | | [E.18] destrucción de la información |
| | | | [E.19] fugas de la información. |
| | | | [A.6] Abuso de privilegio de acceso |
| | | | [A.11] Acceso no autorizado |
| | | | [A.15] Modificación deliberada de información. |
| | | | [A.18] destrucción de la información. |
| | | | [A.19] divulgación de información. |

Cuadro 14. Evaluación de riesgos Continuación

| Tipo de activo de información | Riesgo | Nombre del activo de información | Causas del riesgo |
|---|---|---|---|
| [D] Datos | R8 | Sistema de nómina y facturación | [E.1] Errores del usuario |
| | | | [E.2] Errores del administrador |
| | | | [E.15] Alteración accidental de información. |
| | | | [E.18] destrucción de la información |
| | | | [E.19] fugas de la información. |
| | | | [A.6] Abuso de privilegio de acceso |
| | | | [A.11] Acceso no autorizado |
| | | | [A.15] Modificación deliberada de información. |
| | | | [A.18] destrucción de la información. |
| | | | [A.19] divulgación de información. |
| [COM] Redes de comunicaciones | R9 | Red inalámbrica | [E.2] Errores del administrador |
| | | | [A.7] Uso no previsto |
| | | | [A.11] Acceso no autorizado |
| | | | [A.12] Análisis de tráfico |
| | | | [A.14] Interceptación de información. |
| | | | [A.26] Ataque destructivo |
| [COM] Redes de comunicaciones | R10 | Switch CISCO Catayst 2960. | [N.1] Fuego |
| | | | [I.7] Condición inadecuada de temperatura o humedad |
| | | | [I.8] Fallo de servicio de comunicación |
| | | | [E.2] Errores del administrador |
| | | | [E.19] fugas de la información. |
| | | | [A.6] Abuso de privilegio de acceso |
| | | | [A.7] Uso no previsto |
| | | | [A.9] [RE-] Encaminamiento de mensajes. |
| | | | [A.10] Alteración de secuencia |
| | | | [A.11] Acceso no autorizado |
| | | | [A.12] Análisis de tráfico |
| | | | [A.14] Interceptación de información. |
| | | | [A.15] Modificación deliberada de información. |
| | | | [A.19] divulgación de información. |
| | | | [A.24] Denegación de servicio |

Cuadro 14. Evaluación de riesgos Continuación

| Tipo de activo de información | Riesgo | Nombre del activo de información | Causas del riesgo |
|---|---|---|---|
| [P] Personal | R11 | Estudiantes, directivos | [E.1] Errores del usuario |
| | | | [E.2] Errores del administrador |
| | | | [E.15] Alteración accidental de información. |
| | | | [E.19] fugas de la información. |
| | | | [A.5] Suplantación de identidad de usuario |
| | | | [A.6] Abuso de privilegio de acceso |

Fuente: Construcción propia del autor

**6.2.5. Plan de tratamiento de riesgos**. En el cuadro 15, se presenta el tratamiento de riesgos:

Cuadro 15. Plan de tratamiento de riesgos

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo | Valor del Riesgo | Transferir | Aceptar | Mitigar | Plan de tratamiento | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | Control aplicable | Descripción |
| 1 | [HW] Hardware | Cortafuegos Cisco ASA 5505 | 9 | [A.11] Acceso no autorizado | No se han implementado reglas en el cortafuegos para autorizar o denegar conexiones o transmisión de datos | 4 | 36 | | | X | A.13.1.1. | Controles de redes |
| 2 | [SW] Software | Software Antivirus | 9 | [A.8] Difusión de software dañino | Solo hay un segmento de red y no se monitorea la actualización del antivirus | 4 | 36 | | | X | A.13.1.3 | Separación de redes |
| 3 | [HW] Hardware | Servidor Dell Torre PowerEdge T440 (Nómina y Facturación) | 9 | [I.7] Condiciones inadecuadas de temperatura o humedad | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 27 | | | X | A.11.1.4 | Protección contra amenazas externas ambientales |

Cuadro 15. Plan de tratamiento de riesgos Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo | Valor del Riesgo | Transferir | Aceptar | Mitigar | Plan de tratamiento | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | Control aplicable | Descripción |
| 4 | [HW] Hardware | Servidor Dell Torre PowerEdge T440 (DHCP) | 9 | [I.7] Condiciones inadecuadas de temperatura o humedad | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 27 | | | X | A.11.1.4 | Protección contra amenazas externas ambientales |
| 5 | [COM] Redes de comunicaciones | Red de datos | 9 | [A.11] Acceso no autorizado | Solo hay un segmento de red y no se monitorea la actualización del antivirus | 3 | 27 | | | X | A.13.1.3 | Separación de redes |
| 6 | [S] Servicio | Recibos de pago | 8 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 24 | | | X | A.11.1.4 | Protección contra amenazas externas ambientales |
| 7 | [SW] Software | Sistema de nómina | 8 | [E.15] Alteración accidental de la información | Registro de información por personas de otras áreas o contratos de aprendizaje sin ser entrenados | 3 | 24 | | | X | A.7.2.2. | Toma de concienciа, educación y formación en la seguridad de la información |

Cuadro 15. Plan de tratamiento de riesgos Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo | Valor del Riesgo | Transferir | Aceptar | Mitigar | Plan de tratamiento | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | Control aplicable | Descripción |
| 8 | [SW] Software | Sistema de facturación | 8 | [E.15] Alteración accidental de la información | Registro de información por personas de otras áreas o contratos de aprendizaje sin ser entrenados | 3 | 24 | | | X | A.7.2.2. | Toma de concienciación, educación y formación en la seguridad de la información |
| 9 | [COM] Redes de comunicaciones | Red de datos inalámbrica | 8 | [A.11] Acceso no autorizado | Solo hay un segmento de red y no se monitorea la actualización del antivirus | 3 | 24 | | | X | A.13.1.3 | Separación de redes |
| 10 | [S] Servicio | DHCP | 7 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 21 | | | X | A.11.1.4 | Protección contra amenazas externas ambientales |
| 11 | [HW] Hardware | Servidor de impresión Dell PowerEdge T440 | 7 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 21 | | | X | A.11.1.4 | Protección contra amenazas externas ambientales |
| 12 | [HW] Hardware | Puntos de acceso alámbrico (HUB) | 7 | [A.8] Difusión de software dañino | Solo hay un segmento de red y no se monitorea la actualización del antivirus | 3 | 21 | | | X | A.13.1.3 | Separación de redes |
| 13 | [HW] Hardware | Switches Cisco Catalyst 2960 | 7 | [A.8] Difusión de software dañino | Solo hay un segmento de red y no se monitorea la actualización del antivirus | 3 | 21 | | | X | A.13.1.3 | Separación de redes |

Cuadro 15. Plan de tratamiento de riesgos Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo | Valor del Riesgo | Transferir | Aceptar | Mitigar | Plan de tratamiento | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | Control aplicable | Descripción |
| 14 | [S] Servicio | Nómina | 6 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 18 | | | X | A.11.1.4 | Protección contra amenazas externas ambientales |
| 15 | [S] Servicio | Red alámbrica | 6 | [A.11] Acceso no autorizado | Solo hay un segmento de red | 3 | 18 | | | X | A.13.1.3 | Separación de redes |
| 16 | [HW] Hardware | Puntos de acceso alámbrico (HUB) (Dep. de Sistemas) | 6 | [A.8] Difusión de software dañino | Solo hay un segmento de red y no se monitorea la actualización del antivirus | 3 | 18 | | | X | A.13.1.3 | Separación de redes |
| 17 | [SW] Software | MySQL (GoDaddy) | 9 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades asociadas a la versión usadas de software con el que está implementado el sitio | 2 | 18 | X | | | | |
| 18 | [SW] Software | MySQL 5.7.17 (Nómina y facturación) | 9 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades conocidas de la versión en uso | 2 | 18 | | X | | | |
| 19 | [SW] Software | Sistema de compras | 9 | [E.21] Errores de mantenimiento / actualización de programas (software) | Desconocimiento buenas prácticas | 2 | 18 | | | X | A.7.2.2. | Toma de concienciа, educación y formación en la seguridad de la información |

Cuadro 15. Plan de tratamiento de riesgos Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo | Valor del Riesgo | Transferir | Aceptar | Mitigar | Plan de tratamiento | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | Control aplicable | Descripción |
| 20 | [P] Personal | Docentes | 8 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 16 | | | X | A.7.2.2. | Toma de concienciación, educación y formación en la seguridad de la información |
| 21 | [P] Personal | Estudiantes | 8 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 16 | | | X | A.7.2.2. | Toma de concienciación, educación y formación en la seguridad de la información |
| 22 | [SW] Software | Joomla 2.5 (GoDaddy) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades asociadas a la versión usadas de software con el que está implementado el sitio | 2 | 16 | X | | | | |
| 23 | [SW] Software | Apache (GoDaddy) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades asociadas a la versión usadas de software con el que está implementado el sitio | 2 | 16 | X | | | | |
| 24 | [SW] Software | PHP (GoDaddy) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades asociadas a la versión usadas de software con el que está implementado el sitio | 2 | 16 | X | | | | |
| 25 | [SW] Software | Apache 2.4.25 (Nómina y facturación) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades conocidas de la versión en uso | 2 | 16 | | X | | | |

Cuadro 15. Plan de tratamiento de riesgos Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo | Valor del Riesgo | Transferir | Aceptar | Mitigar | Plan de tratamiento | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | Control aplicable | Descripción |
| 26 | [SW] Software | PHP 5.6.30 - 7.1.1 (Nómina y facturación) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades conocidas de la versión en uso | 2 | 16 | | X | | | |
| 27 | [SW] Software | phpMyAdmin 4.6.6 (Nómina y facturación) | 8 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades conocidas de la versión en uso | 2 | 16 | | X | | | |
| 28 | [SW] Software | Sistema de proveedores | 8 | [E.21] Errores de mantenimiento / actualización de programas (software) | Desconocimiento buenas prácticas | 2 | 16 | | | X | A.7.2.2. | Toma de concienciación, educación y formación en la seguridad de la información |
| 29 | [S] Servicio | Red inalámbrica | 5 | [A.11] Acceso no autorizado | Solo hay un segmento de red | 3 | 15 | | | X | A.13.1.3 | Separación de redes |
| 30 | [D] Datos | Estudiantes | 7 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos.<br>No hay segmentación de la red | 2 | 14 | | | X | A.11.1.2 | Controles de acceso físico |
| 31 | [D] Datos | Empleados | 7 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos.<br>No hay segmentación de la red | 2 | 14 | | | X | A.11.1.2 | Controles de acceso físico |

Cuadro 15. Plan de tratamiento de riesgos Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo | Valor del Riesgo | Transferir | Aceptar | Mitigar | Plan de tratamiento | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | Control aplicable | Descripción |
| 32 | [D] Datos | Nómina | 7 | [E.15] Alteración accidental de la información | En días de alto flujo de solicitudes el ingreso de datos es efectuado por personal de prácticas o por contrato de aprendizaje | 2 | 14 | | | X | A.8.1.3 | Uso aceptable de los activos |
| 33 | [S] Servicio | Internet | 7 | [A.7] Uso no previsto | No hay reglas implementadas en cortafuegos de control de acceso | 2 | 14 | | | X | A.13.1.1 | Controles de redes |
| 34 | [P] Personal | Directivos | 7 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 14 | | | X | A.7.2.2. | Toma de concienciа, educación y formación en la seguridad de la información |
| 35 | [P] Personal | Administradores | 7 | [E.2] Errores del administrador | Desconocimiento buenas prácticas | 2 | 14 | | | X | A.7.2.2. | Toma de concienciа, educación y formación en la seguridad de la información |
| 36 | [D] Datos | Proveedores | 6 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos.<br>No hay segmentación de la red | 2 | 12 | | | X | A.11.1.2 | Controles de acceso físico |

Cuadro 15. Plan de tratamiento de riesgos Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo | Valor del Riesgo | Transferir | Aceptar | Mitigar | Plan de tratamiento | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | Control aplicable | Descripción |
| 37 | [D] Datos | Órdenes de compra | 6 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 12 | | | X | A.11.1.2 | Controles de acceso físico |
| 38 | [D] Datos | Facturación | 6 | [E.15] Alteración accidental de la información | En días de alto flujo de solicitudes el ingreso de datos es efectuado por personal de prácticas o por contrato de aprendizaje | 2 | 12 | | | X | A.8.1.3 | Uso aceptable de los activos |
| 39 | [D] Datos | Hojas de vida | 6 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 12 | | | X | A.11.1.2 | Controles de acceso físico |
| 40 | [D] Datos | Contenido Página Web GoDaddy | 6 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades asociadas a la versión usadas de software con el que está implementado el sitio | 2 | 12 | X | | | | |
| 41 | [S] Servicio | Certificados laborales | 4 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 12 | | | X | A.11.1.4 | Protección contra amenazas externas ambientales |
| 42 | [S] Servicio | Voz IP | 4 | [I.9] Interrupción de otros servicios y suministros esenciales | El servidor está ubicado en una zona donde no hay condiciones climáticas adecuadas | 3 | 12 | | X | | | |
| 43 | [P] Personal | Especialista correo electrónico | 6 | [E.4] Errores de configuración | Desconocimiento buenas prácticas | 2 | 12 | | X | | | |

Cuadro 15. Plan de tratamiento de riesgos Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo | Valor del Riesgo | Transferir | Aceptar | Mitigar | Plan de tratamiento | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | Control aplicable | Descripción |
| 44 | [SW] Software | Sistema de inventarios | 6 | [E.21] Errores de mantenimiento / actualización de programas (software) | Desconocimiento buenas prácticas | 2 | 12 | | | X | A.7.2.2. | Toma de concienciación, educación y formación en la seguridad de la información |
| 45 | [S] Servicio | Correo electrónico google | 5 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 10 | | | X | A.7.2.2. | Toma de concienciación, educación y formación en la seguridad de la información |
| 46 | [D] Datos | Inventarios | 4 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 8 | | | X | A.11.1.2 | Controles de acceso físico |
| 47 | [D] Datos | Audios de reuniones, asambleas | 3 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 6 | | | X | A.11.1.2 | Controles de acceso físico |
| 48 | [S] Servicio | FTP | 3 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 6 | | | X | A.11.1.2 | Controles de acceso físico |

Cuadro 15. Plan de tratamiento de riesgos Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo | Valor del Riesgo | Transferir | Aceptar | Mitigar | Plan de tratamiento | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | Control aplicable | Descripción |
| 49 | [HW] Hardware | Servidor Dell Torre PowerEdge T130 (FTP) | 3 | [E.2] Errores del administrador | Considerando que no se evidencia riesgo, solamente se considera la posibilidad de errores humanos | 2 | 6 | | X | | | |
| 50 | [HW] Hardware | Equipo de cómputo (Dep Infraestructura) | 3 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 6 | | | X | A.7.2.2. | Toma de concienciа, educación y formación en la seguridad de la información |
| 51 | [HW] Hardware | Equipo de cómputo (Dep control y seguimiento) | 3 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 6 | | | X | A.7.2.2. | Toma de concienciа, educación y formación en la seguridad de la información |
| 52 | [HW] Hardware | Equipo de cómputo (Dep. de prueba de software) | 3 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 6 | | | X | A.7.2.2. | Toma de concienciа, educación y formación en la seguridad de la información |

Cuadro 15. Plan de tratamiento de riesgos Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo | Valor del Riesgo | Transferir | Aceptar | Mitigar | Plan de tratamiento | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | Control aplicable | Descripción |
| 53 | [D] Datos | Documentos digitales | 2 | [A.11] Acceso no autorizado | No hay control de acceso biométrico o de monitoreo de clientes internos y externos. No hay segmentación de la red | 2 | 4 | | | X | A.11.1.2 | Controles de acceso físico |
| 54 | [HW] Hardware | Equipo de cómputo (Dep. Desarrollo Tecnológico) | 2 | [A.30] Ingeniería social (picaresca) | Este es un vector de ataque en el que las personas son un blanco para atacar a las organizaciones | 2 | 4 | | | X | A.7.2.2. | Toma de concienciа, educación y formación en la seguridad de la información |
| 55 | [HW] Hardware | Teléfonos IP (Dep. del centro) | 2 | | Solo hay un segmento de red y no se monitorea la actualización del antivirus | 2 | 4 | | X | | | |
| 56 | [SW] Software | Windows 10 Pro | 2 | [E.20] Vulnerabilidades de los programas (software) | Vulnerabilidades conocidas de la versión en uso | 2 | 4 | | X | | | |
| 57 | [S] Servicio | Impresión | 3 | [E.1] Errores de los usuarios | No hay vulnerabilidad | 1 | 3 | | X | | | |
| 58 | [HW] Hardware | Impresora/Escáner SMART MultiXpress M4370LX (Directivos, administrativos y docentes) | 3 | [E.1] Errores de los usuarios | No hay vulnerabilidad | 1 | 3 | | X | | | |

Cuadro 15. Plan de tratamiento de riesgos Continuación

| N° | Tipo de activo | Nombre del activo de información | Valoración cuantitativa del riesgo | Amenazas Metodología Magerit | Vulnerabilidades | Probabilidad de ocurrencia del riesgo | Valor del Riesgo | Transferir | Aceptar | Mitigar | Plan de tratamiento | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | Control aplicable | Descripción |
| 59 | [HW] Hardware | Impresora HP LaserJet Enterprise serie 600 (Nómina y Facturación) | 2 | [E.1] Errores de los usuarios | No hay vulnerabilidad | 1 | 2 | | X | | | |

Fuente: Construcción propia del autor aplicando Magerit

### 6.3. **Manual de seguridad de la Información.** Para Qwerty S.A.:

**6.3.1. Propósito**. Este manual describe el SGSI de Qwerty S.A. cuyo fin es proveer un nivel adecuado de seguridad de la información de los clientes y de la organización.

**6.3.2. Contexto de la organización.** Se resalta de Qwerty S.A:

**Misión - visión**

De acuerdo con la información presentada en el caso para desarrollo del proyecto aplicado Qwerty S.A. busca el desarrollo tecnológico en comunidades colombianas a través del uso de Tecnologías de la información.

**Comprensión y entendimiento de las partes interesadas**

Las partes interesadas[33] en Qwerty S.A. son las siguientes:

- Directivos
- Funcionarios Administrativos
- Funcionarios Operativos
- Proveedores de servicios (internet, correo google, Sitio web Godaddy)
- Docentes

[33] La norma ISO 27001 Aspectos clave de su diseño e implantación. Disponible en: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

- Estudiantes
- Personal técnico
- Otros Proveedores
- Ministerio de Educación
- Secretaría de Educación
- ARL
- EPS

Las necesidades de las partes interesadas que son atendidas a través del sistema de gestión de seguridad de la información son las siguientes:

- Efectuar una mitigación de los riesgos de seguridad de la información identificados para Qwerty S.A.
- Apoyar el cumplimiento de los objetivos estratégicos de Qwerty S.A.
- Identificar las vulnerabilidades y amenazas existentes sobre los activos de información de Qwerty S.A.
- Dar cumplimiento a la normatividad vigente aplicable a Qwerty S.A. en relación con la seguridad de la información:

En el cuadro 16 se puede visualizar la normatividad aplicable a Qwerty S.A.:

Cuadro 16. Normatividad de seguridad de la información aplicable a Qwerty S.A.

| Norma | Descripción |
|---|---|
| **Ley 527/99** | Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos |
| **Ley 594/00** | Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones |
| **Ley 1266/08** | Por la cual se dictan 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. |
| **Ley 1273/09** | Por medio de la cual 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. |
| **CONPES 3701 de 2011** | Lineamientos de política para ciberseguridad y Ciberdefensa |
| **Ley 1581/12** | Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales |
| **Decreto 886 de 2014** | Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, en lo relativo al Registro Nacional de bases de datos. |
| **Decreto 1008 de 2018** | Política de Gobierno Digital |
| **LEY 1712 DE 2014** | Ley de Transparencia y del Derecho de Acceso a la Información Pública |

Cuadro 16. Normatividad de seguridad de la información aplicable a Qwerty S.A. Continuación

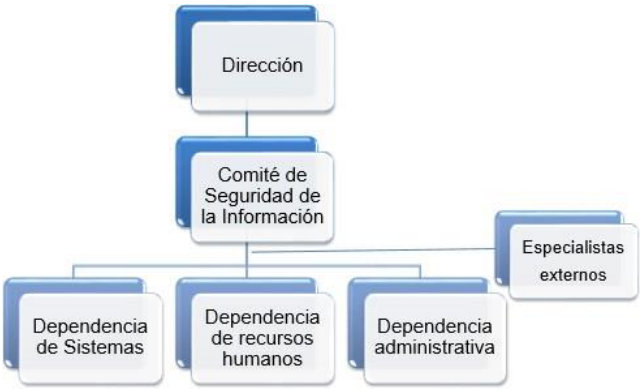
| Norma | Descripción |
|---|---|
| **Norma Técnica Colombiana NTC-ISO/IEC 27001.** | Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información |

Fuente: Recopilación efectuada por el autor.

Con la implementación del SGSI, se espera alcanzar un nivel aceptable de seguridad de la información en Qwerty S.A. que permita ejercer una gestión proactiva, mantener un adecuado nivel de confidencialidad, disponibilidad e integridad de los activos de información de Qwerty S.A.

**Roles y responsabilidades**. Para establecer el SGSI en Qwerty en la figura 4 se puede ver la estructura organizacional propuesta:

Figura 4. Estructura Organizacional




Fuente: Construcción propia del autor

En el cuadro 17 se puede identificar los roles[34] que tienen relación con el SGSI en Qwerty S.A.:

Cuadro 17. Roles y responsabilidades SGSI

| Roles | Responsabilidades |
|---|---|
| Alta Dirección | Incluye al Rector de Qwerty S.A y demás empleados que tienen a su cargo la toma de decisiones estratégicas. |

[34] MINTIC. Roles y responsabilidades. Seguridad y privacidad de la información. Guia 4 (2016). Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

Cuadro 17. Roles y responsabilidades SGSI Continuación

| Roles | Responsabilidades |
|---|---|
| Director del Sistema de Seguridad de la información | Responsable del funcionamiento del SGSI de Qwerty S.A. |
| Comité de seguridad de la información | Es el encargado de aprobar la política de seguridad, promover la gestión de la seguridad, estructurar y/o aprobar iniciativas de seguridad de Qwerty. |
| Parte interesada | Personas, organizaciones o instituciones que tienen interés directo sobre Qwerty S.A. |
| Administrador de servicios de tecnología | Responsables de la administración, disponibilidad y soporte de los servicios de tecnología |
| CIO | Responsable de la gestión del proceso de tecnología de Qwerty S.A. |
| Responsable de la seguridad física | Responsable de la seguridad física y acceso en instalaciones. |
| Responsables de riesgos | Responsables de la gestión, tratamiento de riesgos en Qwerty S.A. |
| Oficial de Seguridad | Responsable de interactuar con propietarios de activos de información para el cumplimiento del SGSI, líder de gestión de incidentes de seguridad, responsable de seguimiento en el cumplimiento de controles. |
| Propietario de activo de información | Empleado o contratista con responsabilidad sobre un activo de información de Qwerty S.A., establece su valoración, identifica riesgos, requerimientos de seguridad y controles requeridos. |
| Custodio de activo de información | Empleado o contratista responsable de hacer efectivos los controles definidos por el propietario del activo. |
| Dueño de proceso | Empleado o contratista responsable de un proceso de Qwerty S.A. |
| Usuario de información | Empleado o contratista usuario de información de Qwerty S.A. para desarrollar sus funciones. |

Cuadro 17. Roles y responsabilidades SGSI Continuación

| Roles | Responsabilidades |
|---|---|
| Equipo de implementación | Grupo de trabajo encargado de adelantar las labores de implementación del SGSI en coordinación con el director de seguridad de la información y el comité de seguridad de la información. |

Fuente: Construcción propia del autor

**Alcance del Sistema de Gestión de Seguridad de la Información**. El SGSI de Qwerty S.A. tiene una aplicabilidad sobre todos los activos, plataformas tecnológicas y procesos[35].

- Activos de información: Incluye los activos de información identificados, contenedores de activos de información, instalaciones, empleados de Qwerty, contratistas y estudiantes.

- Plataformas tecnológicas: Incluye las plataformas que soportan la gestión de los procesos que se encuentran en el Datacenter de Qwerty S.A.

- Procesos: Incluye todos los procesos del mapa de procesos de Qwerty S.A.

**6.2.2. Procedimientos**. En el cuadro 18, se encuentran los procedimientos[36] que apoyarán al SGSI de Qwerty S.A.:

Cuadro 18. Procedimientos que soportan el SGSI de Qwerty S.A.

| Procedimiento | Descripción |
|---|---|
| Gestión de activos de información | Establece cómo se identifican, califica y clasifican los activos de información, incluido el tratamiento para asignación o devolución. |
| Administración técnica de servicios y sistemas de información. | Establece requisitos, actividades preventivas, de actualización, monitoreo que se deben efectuar y los registros que se deben mantener en la administración técnica de Sistemas y servicios en Qwerty S.A. |

[35] COLOMBIA COMPRA EFICIENTE [Sitio Web]. Alcance del Sistema de Seguridad de la información. Disponible en: https://www.colombiacompra.gov.co/sites/cce_public/files/cce_documentos/20160623alcancedelsgsi.pdf

[36] MINTIC. Procedimientos de seguridad de la información. Seguridad y privacidad de la información. Guía 3 (2016). De: https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

Cuadro 18. Procedimientos que soportan el SGSI de Qwerty S.A. Continuación

| Establece | Establece |
|---|---|
| Atención de requerimientos e incidentes mesa de ayuda. | Establece los requisitos y condiciones para la atención de requerimientos e incidentes sobre los sistemas de información y servicios de Qwerty, acuerdos de niveles de servicios y registros. |
| Criptografía | Establece las condiciones y especificaciones de uso de mecanismos criptográficos en Qwerty S.A., en sus sistemas de información, servicios y activos de información. Incluida la custodia de mecanismos criptográficos y la designación del responsable de los mismos. |
| Seguridad física | Establece las condiciones y requisitos para el acceso a las instalaciones de Qwerty S.A. y sus diferentes áreas y los registros que deben mantenerse incluyendo mecanismos de control de acceso[37]. |
| Seguridad Lógica | Establece las condiciones y requisitos para el acceso a la red LAN y los diferentes recursos de procesamiento disponibles de procesamiento en Qwerty S.A. |
| Protección de activos de información | Establece las condiciones ambientales, eléctricas, físicas que debe cumplir el sitio donde se ubique infraestructura que contenga información, servicios y sistemas de información. |
| Protección de traslado de activos de información | Establece condiciones y tratamiento para el traslado de activos de información dentro y fuera de Qwerty S.A. |
| Gestión de cambios | Establece las condiciones, requisitos y aspectos que deben planificarse para la ejecución de un cambio en la organización. |
| Protección contra códigos maliciosos | Establece las condiciones y acciones a aplicar para proteger a la organización y sus activos de información contra códigos maliciosos. |

[37] GIMENEZ A JOSÉ F., Seguridad en equipos informáticos. (2014). De: https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=4184155O.J

Cuadro 18. Procedimientos que soportan el SGSI de Qwerty S.A. Continuación

| Establece | Establece |
|---|---|
| Protección de redes | Establece los criterios, condiciones y acciones a aplicar para proteger las redes de comunicación internas Qwerty S.A., así como los registros que se deben mantener. |
| Relaciones con proveedores | Establece las condiciones y requerimientos que debe cumplirse para interactuar con proveedores y actividades de seguimiento y control. |
| Adquisición y mantenimiento de software | Establece requisitos y condiciones mínimas de seguridad que debe cumplir los sistemas de información y servicios de Qwerty, así como los servicios contratados a terceros. |
| Gestión de incidentes de seguridad de la información | Establece roles, acciones, responsabilidades y tratamiento ante un incidente de seguridad de la información en Qwerty S.A. |
| Capacitación de empleados y contratistas | Establecer la metodología a seguir para la capacitación de empleados y contratistas de Qwerty S.A, en seguridad de la información. |
| Gestión de proyectos | Establece metodología a seguir para la gestión de proyectos en Qwerty, desde su estructuración, ejecución, hasta el cierre. |
| Vinculación de empleados y contratistas | Establece los requisitos y validaciones de seguridad que debe observarse al vincular o desvincular personal a Qwerty S.A. |
| Etiquetado de información | Determina la forma en que se deberá marcar e identificar la información en la organización aplicando la clasificación establecida. |
| Tratamiento de copias de información | Establece las condiciones, marcación y tratamiento de copiar para traslado interno y externo, así como condiciones para su reutilización y destrucción. |

Cuadro 18. Procedimientos que soportan el SGSI de Qwerty S.A. Continuación

| Establece | Establece |
|---|---|
| Áreas vacías y trabajo supervisado | Establece acciones a seguir cuando un área de trabajo se encuentre vacía para evitar ingreso no autorizado, así como las condiciones para trabajo supervisado. |
| Identificación y gestión de vulnerabilidades | Determina acciones a seguir para la identificación de vulnerabilidades y las acciones de remediación a implementar. |
| Desarrollo de software | Establece las condiciones que deben atenderse para el desarrollo interno o externo de software y la política de desarrollo seguro establecida. |

Fuente: Construcción propia del autor

A continuación se encuentra el detalle de cada uno de los procedimientos operativos que se identifica deben ser implementados en Qwerty S.A para apoyar el SGSI.

**Procedimiento de gestión de Cambios**. En el cuadro 19 se puede ver detalle del procedimiento a través del cual se planifica la gestión de cambios para Qwerty S.A.

Cuadro 19. Procedimiento de Gestión de Cambios

| PROCEDIMIENTO | Control de cambios operativos |
|---|---|
| **OBJETIVO** | Mitigar los riesgos asociados a los cambios a efectuarse en ambientes productivos producto de actualizaciones, nuevas funcionalidades, actualizaciones tecnológicas, entre otros. |
| **DEFINICIONES** | **Líder del cambio**: Responsable del cambio su planificación y ejecución.<br><br>**Ejecutor**: Líderes técnicos o funcionales que participan o tienen bajo su responsabilidad la ejecución de alguna actividad dentro de la gestión de cambio.<br><br>**Riesgo**: Probabilidad de que algo suceda generando un impacto<br><br>**Comité de gestión de cambio:** Grupo con conocimiento y competencia para analizar, identificar riesgos y determinar si es viable o no la ejecución de un riesgo. |

Cuadro 19. Procedimiento de Gestión de Cambios. Continuación

| ACTIVIDADES | | DESCRIPCIÓN | RESPONSABLE | REGISTRO |
|---|---|---|---|---|
| 1 | Inicio | | | |
| 2 | Establecer alcance del cambio e identificar quienes intervienen | Descripción del alcance del cambio a realizar, identificación del líder del cambio, áreas involucradas, ejecutores del cambio | Líder del cambio | Formato de control de cambio |
| 3 | Formular plan con: actividades previas a ejecutar, actividades a ejecutar durante el cambio, actividades para regresar al estado inicial antes del cambio | Listar actividades a ejecutar antes, durante y posterior al cambio, relacionando responsable y fecha de ejecución de cada actividad. | Líder del cambio, ejecutores del cambio | Formato de control de cambio |
| 4 | Identificar y listar actividades de socialización de los cambios a realizar | Relación de actividades a ejecutar para socializar el cambio antes y después de ejecutado | Líder del cambio | Formato de control de cambio |
| 5 | Identificar riesgos | Identificar los riesgos asociados a la ejecución del cambio | Líder del cambio y ejecutores | Formato de control de cambio |
| 6 | Identificar y describir controles | Acciones preventivas a ejecutar antes, durante o posterior al cambio | Líder del cambio y ejecutores | Formato de control de cambio |
| 7 | Presentar a revisión por parte del comité de cambios | Aprobación y/u observaciones del comité de cambios al plan presentado | Comité de cambios, líder del cambio | Formato de control de cambio |
| 8 | Si el cambio se aprobó: pasar a la actividad 9<br>Si no: pasar a la actividad 11 | | | |
| 9 | Ejecutar el plan de actividades según fechas establecidas | Ejecución del plan | Líder del cambio | Formato de control de cambio |
| 10 | Generar reporte con resultados del cambio | Registrar resultados obtenidos con la ejecución del cambio | Líder del cambio | Formato de control de cambio |

Fuente: Construcción propia del autor

**Procedimiento de Control de versiones**. En el cuadro 20 se puede ver el detalle del procedimiento a través del cual se establece cómo efectuar el control de versiones en Qwerty S.A.

Cuadro 20. Procedimiento Control de Versiones

| PROCEDIMIENTO | | Control de versiones | | |
|---|---|---|---|---|
| **OBJETIVO** | | Controlar nivel de actualización de un formato o documento a través del uso de versiones. | | |
| **DEFINICIONES** | | **Versión**: Identificador numérico secuencial asignado a un documento para identificar versiones.<br>**Formato controlado**: Formatos a los que tras efectuarse una revisión y aprobación, se les asigna un número consecutivo posterior al que está reemplazando por una actualización o cambio.<br>**Autor:** Nombre de quien construye el documento o realiza la modificación. | | |
| **ACTIVIDADES** | | **DESCRIPCIÓN** | **RESPONSABLE** | **REGISTRO** |
| 1 | Inicio | | | |
| 2 | Presentar formato a controlar o nueva versión de formato controlado | Remitir documento o formato actualizado para revisión y aprobación | Líder de área que propone cambio o nuevo documento | Correo electrónico |
| 3 | Revisión del formato | Revisión y validación de cambios y datos de control de versión, autor | Responsable versionamiento de documentos | |
| 4 | El contenido del formato es correcto? | | Responsable versionamiento de documentos | |
| 5 | Si es correcto, pasar a actividad 6<br>Si no es correcto devolver para ajuste, pasar a actividad 9 | | Responsable versionamiento de documentos | |
| 6 | Asignar, versión, fecha de aprobación, nombre de quien aprobó. | Complementar formato con la versión, fecha de aprobación, autor, y nombre de quien aprobó el cambio | Responsable versionamiento de documentos | Repositorio |

Cuadro 20. Procedimiento Control de Versiones. Continuación

| ACTIVIDADES | | DESCRIPCIÓN | RESPONSABLE | REGISTRO |
|---|---|---|---|---|
| 7 | Remitir a solicitante | Envío de formato aprobado a solicitante | Responsable versionamiento de documentos | Correo electrónico |
| 8 | Socializar formato aprobado | Envío a través de correo electrónico a usuarios de Qwerty S.A. | Líder de área que propone cambio o nuevo documento | Correo electrónico |
| 9 | Fin | | | |

**Procedimiento de Gestión de incidentes de seguridad de la información**. En el cuadro 21, se puede ver el detalle del procedimiento a través del cual se establece cómo proceder en el evento que se presente un incidente de seguridad de la información en Qwerty S.A.

Cuadro 21. Procedimiento Gestión de incidentes de seguridad de la información

| PROCEDIMIENTO | Gestión de incidentes de seguridad de la Información | | |
|---|---|---|---|
| **OBJETIVO** | Establecer lineamientos para la identificación, atención, contención, respuesta y documentación de incidentes de seguridad. | | |
| **DEFINICIONES** | **Evento**: posible incumplimiento de las políticas de seguridad.<br>**Acción correctiva**: Medidas que se aplican para eliminar la causa de un incidente o no conformidad y prevenir su recurrencia.<br>**Gestión de incidentes:** Acciones ejecutadas para atender, contener, dar respuesta y documentar un incidente de seguridad de la información.<br>**Seguridad de la información:** Acciones orientadas a proteger la confidencialidad, integridad y disponibilidad de la información | | |
| **ACTIVIDADES** | | **DESCRIPCIÓN** | **RESPONSABLE** | **REGISTRO** |
| 1 | Inicio | | | |
| 2 | Reporte de posible incidencia | Empleados, contratistas o terceros generan reporte sobre un hecho que se considera es un incidente de seguridad y lo hacen a través de los canales establecidos (correo, teléfono, mesa de ayuda). Posibles casos a reportar: indisponibilidad de servicio, acceso no autorizado, pérdida de información, incumplimiento de política de seguridad de la información. | Empleados, contratistas | Correo electrónico - teléfono |

Cuadro 21. Procedimiento Gestión de incidentes de seguridad de la información. Continuación

| ACTIVIDADES | | DESCRIPCIÓN | RESPONSABLE | REGISTRO |
|---|---|---|---|---|
| 3 | Si es un incidente pasar a actividad 4.<br>Si no es un incidente fin | | | |
| 4 | Documentar incidente | Diligenciar formato incidente, asignar consecutivo. | Técnico área de infraestructura | Formato de registro de incidente<br>Correo electrónico |
| 5 | Escalar a responsable de seguridad de la información | Remitir reporte del evento al responsable de seguridad de la información | Técnico área de infraestructura | Correo electrónico |
| 6 | Determinar tratamiento incidente | A partir del reporte determinar si es un incidente de seguridad y efectuar un análisis que permita identificar posibles causas y acciones correctivas aplicar | Responsable seguridad de información | Formato de registro de incidente |
| 7 | Tratar incidente | Ejecutar acciones correctivas a ejecutar de manera inmediata y acciones posteriores, las cuales se deberán relacionar en plan de remediación. | Responsable de seguridad de la información - ingenieros área sistemas - otras áreas involucradas | Formato de registro de incidente |
| 8 | Generar reporte | De acuerdo con el análisis efectuado del incidente generar un reporte en el formato establecido en el que se identifique el nivel de impacto del incidente y si debe remitirse reporte a alguna autoridad. | Responsable de seguridad de la información | Formato de registro de incidente |
| 9 | Seguimiento a incidente | El responsable de seguridad dela información deberá hacer un seguimiento a la ejecución del plan de remediación cuando se exista hasta culminar su ejecución. | Responsable de seguridad de la información | Formato de registro de incidente |
| 10 | Fin | | | |

**6.3.3. Política de seguridad de la información**. Qwerty S.A. está comprometida con la protección de la confidencialidad, integridad y disponibilidad de la información de su población estudiantil y de la organización, para lo cual hace uso de los mejores estándares para la gestión de sus procesos y la protección de sus activos de información[38].

Con el objeto de dar cumplimiento a la política establecida se establecen las siguientes políticas que deben cumplirse en Qwerty S.A:

## POLÍTICAS DE SEGURIDAD FÍSICA

### Seguridad física y ambiental

*Objetivo.* Mantener condiciones adecuadas para la operación de elementos de cómputo en Qwerty S.A.

*Lineamientos:*

- La infraestructura de servidores deberá estar ubicada únicamente en áreas seguras en con control de acceso y condiciones adecuadas ambientales.
- Sólo personal autorizado que deba cumplir funciones que sólo pueden ejecutarse directamente sobre la infraestructura de servidores o demás componentes ubicados en estas áreas podrá tener acceso a estas áreas restringidas.
- El acceso a estas áreas de personal externo deberá estar expresamente autorizado por el responsable de seguridad y deberá permanecer acompañado por personal autorizado con acceso al área.
- No se permite el acceso al área de celulares o cualquier otro dispositivo móvil.
- No es permitido el ingreso a esta área de elementos inflamables o alimentos.
- El líder de seguridad junto con el líder de la dependencia de sistemas definirán los niveles de acceso de las personas autorizadas a acceder a estas áreas.
- Las condiciones eléctricas y de temperatura deben cumplir con las normas aplicables para centros de procesamiento de datos Tier 2.
- El cableado deberá tener la marcación adecuada que facilite su administración.
- Se debe mantener en el área extintores.

[38] INTECO. Implantación de un SGSI en la empresa. Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

**Seguridad y Mantenimiento de los Equipos**

*Objetivo.* Establecer las actividades mínimas de mantenimiento seguridad que se debe cumplir respecto de los equipos de cómputo de Qwerty S.A.

*Lineamientos:*

- Anualmente se debe establecer un plan de mantenimiento preventivo, el cual deberá ser ejecutado bajo la coordinación del área de infraestructura de Qwerty S.A.
- Para equipos de usuario final, las actividades de mantenimiento deberán incluir: limpieza externa e interna, limpieza del sistema (a través de utilitarios), verificación de estado de actualización de software antivirus, ejecución de escaneo de virus.
- Para servidores la labor deberá estar monitoreada en coordinación con los administradores correspondientes.
- Para UPS, plantas eléctricas, aire acondicionado y sistemas de detección de incendios se debe efectuar al menos un mantenimiento preventivo al año.
- Dentro de los equipos que serán objeto de mantenimiento están: servidores, equipos de usuario final, periféricos, entre otros que claramente deberán están identificados y pertenecen a Qwerty S.A.
- Cuando se requiera realizar actividades de mantenimiento correctivo y reemplazo de partes, se efectuará solamente cuando se autorice y esta labor se realizará en el área destinada para tal fin y por las personas autorizadas. Las partes que sean reemplazadas deberán quedar inventariadas y deberán ser tratadas según los instructivos correspondientes para asegurar que en el caso de medios de almacenamiento no quede información de Qwerty S.A. en ellos.

**Gestión de Medios Removibles**

*Objetivo.* Regular el tratamiento y uso de medios removibles en Qwerty S.A.

*Lineamientos*

- Los puertos USB, bluetooth de los equipos de cómputo de usuarios finales en Qwerty S.A. se mantendrán deshabilitados.
- Ningún usuario debe habilitar puertos USB, bluetooth a través de ningún mecanismo.
- La habilitación de puertos USB o bluetooth se efectuará solamente cuando se haya autorizado.

- Todo medio removible que contenga información de Qwerty S.A. debe ser custodiado por la persona que tenga bajo su custodia dicho elemento, evitando que pueda ser extraído, copiado o manipulado por personas no autorizadas.
- Los backups y demás medios removibles que contengan backups o información confidencial de Qwerty deberán mantenerse en un lugar bajo llave al que solo tenga acceso personal autorizado.
- Se debe mantener un inventario de medios removibles que contienen backups registrando datos como: consecutivo, fecha, contenido, ubicación.
- Cada medio removible debe estar rotulado externamente para identificar su contenido.
- Cuando se determine que haya concluido la vida útil de medios removibles que puedan contener información de Qwerty S.A., deberán ser sometidos a un proceso de eliminación segura de datos antes de proceder a su destrucción.

## POLÍTICAS DE ACCESO A LA RED

### Acuerdos de Confidencialidad.

*Objetivo.* Informar y suscribir un acuerdo sobre las responsabilidades y obligaciones frente a la seguridad de los activos de información de Qwerty por parte de: empleados, contratistas y terceros, durante su vinculación con Qwerty S.A. y posterior a la finalización de su vinculación.

*Lineamientos:*

- Desde el momento de su vinculación empleados y contratistas deben suscribir y dar cumplimiento al acuerdo de confidencialidad establecido por Qwerty S.A.
- Todo contratista debe suscribir acuerdos de confidencialidad.
- Los contratos suscritos por Qwerty con personas naturales o jurídicas, deberán incluir una cláusula de confidencialidad y suscribir acuerdo de confidencialidad.

### Computación Móvil.

*Objetivo:* Establecer las condiciones de uso de equipos portátiles y su acceso a la red de Qwerty S.A.

*Lineamientos:*

- Con los equipos que hayan sido asignados por Qwerty S.A. a empleados o contratistas, accederán a los servicios a los que están autorizados a través de la red inalámbrica haciendo uso de las credenciales que le hayan sido asignadas.
- Todo equipo que no pertenezca a Qwerty S.A., podrá tener acceso a la red inalámbrica de invitados, con acceso solo a los servicios permitidos.
- Está prohibido que los equipos portátiles sean conectados a la red física de Qwerty S.A.

**Control de Acceso Físico y lógico**

*Objetivo.* Establecer las condiciones de acceso a las instalaciones y a la red de Qwerty S.A.

*Lineamientos:*

- El área de infraestructura de Qwerty S.A., es la responsable de la creación de usuarios y asignación de roles y perfiles de acuerdo con las autorizaciones que le sean remitidas por los dueños de los activos de información, según lo establecido en el procedimiento de gestión de usuarios, manteniendo un registro actualizado de asignación y novedades, hasta su inactivación.
- Ningún usuario podrá revelar las credenciales que le hayan sido entregadas para acceder a los servicios y sistemas de Qwerty, ni debe hacer uso de credenciales de otro usuario.
- El área de infraestructura implementará mecanismos de control lógico que permita el acceso solamente a usuarios autorizados a la red, en la cual se mantendrá una segmentación.
- Las contraseñas por default de los sistemas y servicios deberán ser modificadas.
- Los propietarios de los activos de información deberán verificar regularmente las autorizaciones asignadas a los usuarios con acceso a la infraestructura, servicios y sistemas.
- Se deben mantener reglas de seguridad que permita exigir unas condiciones mínimas de complejidad que deben cumplir las contraseñas según lo establecido en la política de contraseñas.
- El acceso físico a las instalaciones deberá ser controlado por el área administrativa quien establecerá los procedimientos para el ingreso de empleados y visitantes, identificará las áreas, demarcando aquellas que se encuentran restringidas para visitantes. Los empleados deben hacer uso del

carnet de identificación en lugar visible, para los visitantes se entregará previo registro carnet que lo identifica como visitante.

- En el evento que algún área se quede sola se deberá evitar el acceso a personas diferentes de empleados del área, para lo cual utilizará mecanismos de control que impidan su acceso junto con el uso de cámaras que permitan a las personas de seguridad efectuar un monitoreo constante.
- Las áreas donde están ubicados: el centro de procesamiento, los servidores y centros de cableado, deberán tener acceso restringido solamente a las personas autorizadas, para lo cual se hará uso de mecanismos de control de acceso.
- La red inalámbrica estará configurada sobre una VLAN separada.
- La red inalámbrica de invitados estará configurada sobre una VLAN separada.
- La red física deberá segmentarse para que las áreas estén organizadas por segmentos, controlando el acceso de los usuarios entre segmentos.

**Política de dispositivos móviles**.

*Objetivo.* Establecer las condiciones de uso de dispositivos móviles en Qwerty S.A.

*Lineamientos:*

- El uso y acceso a través de dispositivos móviles por parte de empleados de Qwerty S.A. se efectuará únicamente para aquellas personas que estén autorizadas por el director de cada área, permitiéndoles el acceso y uso de servicios corporativos, única y exclusivamente para el desarrollo y cumplimiento de las funciones asignadas.
- Desde la red solo se permitirá el acceso a la red inalámbrica de invitados desde el cual las actividades que se efectúen desde este tipo de dispositivos estarán controlada y limitada a las actividades mínimas autorizadas.
- Se prohíbe al usuario hacer modificaciones de configuración, hardware o hacer uso de software para propósitos que contraríen lo establecido en el acuerdo de confidencialidad suscrito con Qwerty S.A.
- Se debe mantener un inventario de dispositivos móviles que pertenezcan a Qwerty S.A.
- En los dispositivos móviles se deberá instalar y mantener actualizado software antivirus, antispam, antispyware.
- Los dispositivos móviles de Qwerty S.A. deberán mantener contraseña de ingreso y bloqueo.
- No está permitido que en dispositivos móviles propiedad de Qwerty S.A. se mantengan imágenes, fotos, videos personales.

- Cualquier incidente de seguridad que se presente con estos dispositivos deberá ser informado al líder del área de manera inmediata.
- No está permitido que sobre dispositivos móviles de Qwerty S.A. se instale software no autorizado por la Dependencia de Sistemas.

## POLÍTICAS DE SEGURIDAD LÓGICA

### Gestión de Activos de Información

*Objetivo.* Establecer las condiciones de tratamiento de activos de información.

*Lineamientos:*

- Se debe levantar y mantener actualizado un inventario de activos de información de Qwerty S.A.
- Cada activo de información deberá tener asignada una persona responsable del mismo.
- La persona, proceso, o grupo de trabajo dueños del activo, son quienes tienen la responsabilidad de clasificar, valorar y aprobar las acciones orientadas a proteger la confidencialidad, disponibilidad e integridad del activo; establecerán restricciones, roles y autorizaciones que pueden otorgarse sobre el activo.
- La persona, proceso o grupo de trabajo dueños del activo, tienen la responsabilidad de reportar posibles incidencias de seguridad, para lo cual aplicarán los procedimientos establecidos.
- La persona, proceso o grupo de trabajo dueños del activo, son quienes autorizan o retiran permisos o privilegios sobre los activos de información.
- Es responsabilidad de la persona, proceso o grupo de trabajo dueños del activo, reportar las novedades que deban ser tenidas en cuenta en el inventario de activos de información.
- No está permitido que se tomen o generen copias de activos de información sin autorización.
- Cuando se requiera por alguna razón trasladar activos de información, se deberá dejar registro de dicho movimiento, autorización. El traslado de activos de información deberá quedar registrado.
- Los empleados, contratistas y terceros son responsables por las transacciones que sean registradas en los sistemas con los usuarios asignados.
- Todo elemento de hardware o software que requieran los usuarios, o contratistas deberán ser solicitados al área de sistemas quien atenderá según los recursos existentes.

- Toda información que se mantenga en medios removibles deberá tener la adecuada custodia por parte de la persona responsable de la misma.
- Ninguna persona debe efectuar maniobras que impliquen un mal uso de los activos de información de Qwerty S.A.

**Política de Roles**

*Objetivo.* Establecer las condiciones para la definición, asignación, modificación y eliminación de roles.

*Lineamientos:*

- La persona, proceso, o grupo de trabajo dueños de cada activo de información son los responsables de la definición de los roles y autorizaciones que pueden ser otorgados sobre el activo de información.
- Es responsabilidad de la persona, proceso o grupo de trabajo realizar revisiones periódicas, al menos una cada trimestre, para validar que las personas autorizadas son las que tienen autorización permitida.
- Al menos una vez al año la persona, proceso o grupo de trabajo debe realizar una revisión y actualización de roles de ser necesario.
- Los administradores de sistemas de información y aplicaciones, deberán tener solamente las autorizaciones necesarias para cumplir con sus funciones.
- El acceso a los servicios de red deberá estar restringido según los roles y perfiles de los usuarios.
- Los sistemas de información y aplicaciones deberán tener la capacidad de registrar eventos, autor y fecha.
- Ningún usuario debe acceder a sistemas, servicios o aplicaciones haciendo uso de las credenciales de otro usuario.

**Uso Adecuado de los Activos de Información**

*Objetivo.* Establecer las condiciones de tratamiento de los activos de información.

*Condiciones:*

- La persona, proceso, o grupo de trabajo dueños de cada activo de información son los responsables de la definición de las condiciones aceptables de uso de los activos de información.

- Los empleados, contratistas o terceros que tengan acceso a los activos de información deberán acatar y cumplir las condiciones de uso establecidas que le sean socializadas cuando se le asignan las autorizaciones.
- Las autorizaciones de acceso otorgadas a empleados o terceros son intransferibles.
- Cualquier situación o evento que pueda afectar la disponibilidad, integridad y confidencialidad del activo de información de la que tenga conocimiento los empleados, contratistas o terceros sobre un activo de información deberá ser reportada al dueño del activo de información y el líder de seguridad.

**Uso de Internet**

*Objetivo.* Establecer las condiciones de uso aceptable del servicio de internet.

*Lineamientos:*

- Los empleados, contratistas o terceros a quienes se les haya otorgado el acceso al servicio de internet, deberán hacer uso del mismo exclusivamente para el desarrollo de las labores asignadas dentro de Qwerty S.A.
- No está permitido descargar software, acceder a páginas que no tengan relación con las labores que cumple en Qwerty S.A.
- No está permitido el uso de software con el cual se pueda obviar o transgredir los controles implementados por Qwerty S.A. o hacer uso del servicio más allá de lo permitido por Qwerty S.A.
- Cuando se requiera ampliación de las autorizaciones sobre internet, se deberá solicitar autorización al área de sistemas con visto bueno del jefe del área al que pertenezca el solicitante.

**Uso del correo electrónico**

*Objetivo.* Establecer las condiciones de uso aceptable del servicio de internet.

*Lineamientos*

- Se asignará un buzón de correo electrónico a los empleados, contratistas o terceros a quienes se les haya otorgado el acceso a este servicio.
- El uso del servicio de correo está limitado al cumplimiento de funciones en Qwerty S.A.
- El área de infraestructura mantendrá una copia de respaldo de los últimos seis meses de cada buzón.

- No se permite el envío de archivos ejecutables, comprimidos o de una extensión mayor a 30 MB en un mensaje.
- El envío de información confidencial de Qwerty S.A. a través de este medio deberá ser remitido haciendo uso de mecanismos criptográficos que serán provistos por el área de infraestructura.
- No se debe abrir mensajes de correo electrónico que provengan de remitentes desconocidos.

**Uso de Redes Inalámbricas**

*Objetivo.* Establecer las condiciones de uso y acceso a las redes inalámbricas.

*Lineamientos:*

- Los empleados, contratistas y terceros que estén autorizados podrán tener acceso a la red inalámbrica privada de Qwerty con sus equipos portátiles para acceder a los servicios y sistemas a los que tengan autorización.
- No está permitido el uso de utilitarios a través de los cuales se transgreda controles implementados por Qwerty S.A. o efectuar acciones no autorizadas.
- Los visitantes podrán tener acceso a la red inalámbrica de invitados.

**Uso de Computación en la Nube**

*Objetivo.* Establecer las condiciones de uso y acceso a servicios de computación en la nube.

*Lineamientos:*

- El acceso al uso de servicios de computación en la nube debe ser gestionado únicamente por el área de sistemas de Qwerty S.A.
- La administración de los servicios y establecimiento de condiciones del servicio, acuerdo de niveles de servicio, requerimientos y especificaciones deben ser establecidos por el área de sistemas de acuerdo con los requerimientos del área usuaria.
- El área de sistemas monitoreará en coordinación el área usuaria la disponibilidad y cumplimiento de ANS por parte del proveedor de servicios.
- El área usuaria establecerá roles y autorizaciones a implementar y usuarios autorizados.

- El respaldo de información y entrega de copias a Qwerty deberá estar regulado y acorde con las políticas de respaldo establecidas y pactadas con el proveedor del servicio.
- Las infracciones o incumplimientos al ANS deberá ser analizado para determinar si hay una afectación a la integridad, disponibilidad o confidencialidad de los activos de información en custodia.
- Se debe suscribir acuerdo de confidencialidad con el proveedor de servicios.

**Protección contra Software Malicioso**

*Objetivo.* Establecer acciones de protección contra software malicioso.

*Lineamientos:*

- El área de sistemas es la responsable de la instalación y actualización masiva de software antivirus, anti spam, antispyware, entre otros en los equipos de Qwerty S.A. y mantener un respaldo adecuado según la política establecida para tal fin sobre la información que se haya identificado debe ser respaldada y salvaguardada.
- El software antivirus, anti spam, antispyware debe ser configurado para evitar que los usuarios finales puedan inactivarlo o suspender la actualización o cambiar su configuración.
- Los empleados y contratistas deben ser capacitados para usar adecuadamente el software para detectar posibles amenazas o entender los mensajes de alerta que pueda recibir y las acciones que debe adelantar en el evento que se detecte alguna amenaza.
- Se debe instruir a los empleados y contratistas sobre las acciones que deben evitar para permitir que software malicioso sea descargado y propagado a través de la red de Qwerty, desde mensajes de correo de fuentes desconocidas, acceso a páginas falsas entre otras posibles amenazas a las que está expuesto.

**Gestión de Registros (logs)**

*Objetivo.* Establecer las condiciones aplicables a la creación, mantenimiento y acceso a logs.

*Lineamientos*

- Para las aplicaciones, sistemas y servicios activos en Qwerty se debe mantener un log que permita identificar cambios efectuados a la información y configuraciones, su autor junto con datos de fecha y hora de cambio.
- De aquellos sistemas en donde se mantenga información clasificada como confidencial se debe mantener una réplica del log en un servidor diferente al que no debe tener acceso el administrador del servidor.
- Se debe mantener un respaldo de los archivos de log, con al menos una copia que debe ser llevada a un medio de almacenamiento removible.
- La rotación y eliminación de logs debe ajustarse de acuerdo con la política de respaldo de manera tal que se pueda recuperar los logs de hasta tres años para consulta.

**Gestión de Vulnerabilidades Técnicas**

*Objetivo.* Establecer las condiciones para identificación y remediación de vulnerabilidades técnicas.

*Lineamientos:*

- El área de sistemas debe hacer el cambio de contraseñas default de los sistemas en uso e infraestructura instalada.
- El área de sistemas con el apoyo del líder de seguridad, deberá formular el plan de capacitación a empleados, que permita adquirir las competencias necesarias para el desarrollo de funciones manteniendo un nivel adecuado de seguridad en las operaciones.
- De acuerdo con los resultados obtenidos en el análisis de riesgos de seguridad, cuando se determine necesario, se efectuará con soporte de expertos externos, ethical hacking con el alcance previamente establecido, que permita identificar las posibles vulnerabilidades existentes.
- La ejecución del ethical hacking deberá estar coordinada por el líder de seguridad, con el apoyo del área de sistemas de Qwerty S.A.
- Las vulnerabilidades técnicas identificadas serán socializadas con el líder de seguridad y el área directiva.
- El líder de seguridad estructurará un plan de remediación el cual será ejecutado con apoyo del área de sistemas y cuando se determine necesario con soporte especializado externo.
- Se estructurarán campañas de prevención que a través de diferentes estrategias permita formar a empleados y contratistas en la prevención en seguridad informática.

**Política de respaldo de información**.

*Objetivo.* Establecer las condiciones para la obtención y custodia de copias de respaldo de información.

*Lineamientos:*

- De acuerdo con los requisitos establecidos por los dueños de los activos de información, el área de infraestructura de Qwerty S.A. efectuará un backup diario, un backup semanal y otro mensual. La copia que se efectúe en el mes de diciembre se mantendrá por tres años.
- Las copias de respaldo deberán estar ubicadas y almacenadas en un sitio con las condiciones medioambientales adecuadas y medidas de protección que eviten el acceso no autorizado a ellas.
- El área de infraestructura deberá establecer un procedimiento para el respaldo de información.
- Al menos una vez al año se debe efectuar dos pruebas de restauración que permita validar que los backups son consistentes.
- Para los sistemas y servicios críticos, se mantendrá en disco backup diario de la última semana para facilitar la atención de requerimientos de restauración.
- Las labores de respaldo deberán ser ejecutadas por una persona del área de infraestructura, con un esquema de backup en el que hay otra persona con el conocimiento y la competencia para asumir sus funciones cuando se requiera.
- El área de infraestructura debe mantener un inventario de sistemas, repositorios y servicios que deben ser respaldados identificando el tipo, ubicación, tiempo de retención.
- Los medios de almacenamiento externos deben ser rotulados para facilitar la identificación del contenido.

**Política de transferencia de información interna y externa**.

*Objetivo.* Establecer las condiciones para la transferencia de información interna y externa.

*Lineamientos:*

- Cuando se requiera transferir información que esté clasificada como reservada, el área de infraestructura proveerá los mecanismos que deberán ser utilizados para proteger la información de accesos no autorizados.
- Toda transferencia externa o interna de información deberá ser analizada para identificar riesgos que permitan identificar los mecanismos de seguridad que deben ser utilizados para proteger la disponibilidad, integridad y confidencialidad.
- El área de infraestructura identificará, obtendrá y administrará los mecanismos criptográficos a utilizar en Qwerty S.A.
- Ningún empleado o contratista está autorizado para gestionar, obtener o usar mecanismos criptográficos sin la autorización del área de infraestructura.
- Del área de infraestructura se asignará a una persona responsable por la administración y gestión de los mecanismos criptográficos, llaves y contraseñas.

## POLÍTICAS DE EQUIPOS CLIENTE

### Política de escritorio limpio y pantalla limpia.

*Objetivo.* Establecer las condiciones para el uso aceptable de escritorio y pantalla limpia.

*Lineamientos:*

- Es deber de los empleados de Qwerty mantener la documentación e información de Qwerty S.A., a la que tenga acceso en forma física o digital debidamente custodiada evitando el acceso a personas no autorizadas. Debe mantener su escritorio en debido orden y aquellos elementos o documentos que contengan o permitan acceso a servicios sensibles deberán permanecer bajo llave.
- No debe dejar documentos o elementos (medios de almacenamiento, tokens, llaves) abandonados.
- De igual manera, debe dejar sus equipos con bloqueo cuando se retire de su lugar de trabajo. Qwerty implementará mecanismos de autobloqueo de pantalla por inactividad de 15 minutos.

**Política para asignación de contraseñas**.

*Objetivo.* Establecer los requisitos para la creación de contraseñas.

*Lineamientos*

- Las contraseñas deben tener una longitud mínima de ocho caracteres, debe estar conformadas por al menos una letra Mayúscula, letras minúsculas, números y caracteres especiales como los siguientes :;.,¡”#$%&/()=?¡¿’\+*[]{} no deberán permitirse el nombre del usuario, números de identificación, fechas de nacimiento, nombres de familiares.
- El usuario que considere que su contraseña ha sido expuesta o vulnerada, debe cambiarla inmediatamente. El usuario deberá efectuar el cambio de contraseña al menos una vez cada tres meses.
- Los usuarios administradores deben usar contraseñas diferentes como administradores y en sus sesiones como usuarios de servicios, sistemas o aplicaciones.
- Se deben implementar controles para evitar ataques de fuerza bruta para intentar iniciar sesiones.

**Política SSO**

*Objetivo.* Establecer las condiciones para autenticación en Qwerty S.A.

*Lineamientos*

- Todo sistema que pueda integrarse al controlador de dominio deberá hacerlo. Aquellos sistemas que no dispongan de esta opción, tendrán que implementar los mecanismos necesarios que permitan atender la política de asignación de contraseñas. La implementación de nuevos sistemas o servicios deberá efectuarse considerando esta integración.

**Política de desarrollo seguro**.

*Objetivo.* Establecer las condiciones a considerar para el desarrollo de aplicaciones.

*Lineamientos*

- Las actividades de desarrollo interno en Qwerty deberán efectuarse siguiendo los estándares establecidos para el desarrollo de esta actividad, generando la documentación necesaria exigida la cual deberá quedar almacenada y versionada en el sistema establecido para este propósito, así como con el código fuente creado, el cual deberá quedar versionado y documentado según los lineamientos establecidos, haciendo uso del software y usuarios creados para este propósito.
- La construcción externa de software debe considerar: acuerdos de licencia, titularidad de derechos de autor, calidad del código, revisión del código para evitar código malicioso.
- Cuando el desarrollo sea efectuado externamente, se deberán fijar los entregables de acuerdo con lo establecido en los procedimientos internos de Qwerty S.A., incluyendo la ejecución de la fase de pruebas y despliegue.
- Se debe evaluar y determinar los ambientes que requiere cada sistema o servicio en Qwerty, donde como mínimo se debe contar con un ambiente de pruebas y el de producción.
- Se deben implementar y fijar controles para desplegar entre ambientes de desarrollo, prueba y producción.
- Las empresas externas con las que se contrate desarrollo externo deberán hacer uso de metodologías reconocidas para la construcción de software.
- Para el desarrollo interno de aplicaciones, se deberá considerar la segregación, el uso de mejores prácticas y lineamientos para la construcción de software.
- La información que se mantenga en los ambientes de prueba deberá ser controlada o creada para este propósito.
- El software adquirido o desarrollado deberá contar con el servicio de soporte.

**Política de teletrabajo**.

*Objetivo.* Establecer las condiciones para el desarrollo de labores en la modalidad de teletrabajo.

*Lineamientos*

- La modalidad de teletrabajo en Qwerty será autorizada individualmente y una vez exista esta autorización se proveerán los accesos y recursos para que tenga acceso a la red y servicios a los que está autorizado. Cuando esta actividad se ejecute en equipos del empleado se proveerá software antivirus que será instalado en la máquina desde la que tendrá acceso y en el acuerdo

de teletrabajo se le dará conocer y se comprometerá a dar cumplimiento a las condiciones de uso y acceso a los servicios e información.

- La actividad de teletrabajo deberá ser sometidas a un análisis y gestión de riesgos.
- Para cada usuario autorizado bajo esta modalidad, deberá determinarse por parte del área a la que pertenezca, sistemas y servicios a los que tendrá acceso, horarios en los que desarrollará su labor.
- Para el desarrollo de sus funciones a cada tele trabajador le será provista una VPN para acceder a la red de Qwerty S.A, los sistemas y servicios a los que está autorizado.
- El acceso y uso de equipos suministrados por Qwerty S.A. para cumplir labores de teletrabajo está autorizado únicamente al titular de esta autorización.
- Cuando finalice la opción de teletrabajo, se deberá restringir las autorizaciones dadas para el desarrollo bajo esta modalidad.

**Política de uso mecanismos criptográficos**.

*Objetivo.* Establecer las condiciones para el uso de mecanismos criptográficos en Qwerty S.A.

*Lineamientos:*

- El área de infraestructura es la única autorizada para gestionar y obtener mecanismos criptográficos ante entidades certificadoras autorizadas en Colombia. Para lo cual se designará un responsable de las solicitudes, custodia y administración de estos mecanismos, los cuales deberán ser almacenados en un servidor al cual sólo podrán tener acceso el administrador de los mismos y el empleado designado para para reemplazarlo en su ausencia.
- Qwerty podrá determinar y asignar diferentes tipos de control criptográficos según el tipo de dato y medio de transmisión a utilizar.
- La obtención de mecanismos se efectuará atendiendo las necesidades de protección de información según corresponda si es clasificada o reservada.
- Ni los funcionarios, ni contratistas de Qwerty pueden implementar mecanismos criptográficos (firmas digitales, certificados digitales, entre otros) sin autorización previa del área de infraestructura.
- La asignación de mecanismos, destrucción o reemplazo de llaves o contraseñas o el mismo mecanismo solo podrá ser efectuada por el área de infraestructura.

**Política de uso e instalación de software**.

*Objetivo.* Establecer las condiciones para el uso e instalación de software en Qwerty S.A.

*Lineamientos:*

- Ningún usuario final deberá, hacer uso de utilitarios para obviar los controles o mecanismos existentes, instalar software que no esté autorizado por Qwerty S.A. o acceder a servicios para los que no tiene autorización expresa de uso.
- No se permite la descarga e instalación de software de procedencia desconocida en equipos asignados por Qwerty S.A.
- Solo personal autorizado podrá efectuar la instalación de software en equipos de Qwerty S.A.
- La dirección de infraestructura controlará y evitará a través de software, los cambios de configuración y la instalación de software.
- Cuando un usuario final o área requiera instalar software deberá hacer su solicitud a la mesa de ayuda.

**6.3.4. Declaración de aplicabilidad**. Una vez identificados los controles que son aplicables para controlar las vulnerabilidades identificadas para Qwerty S.A., en el cuadro 22, se presenta las decisiones frente a la implementación de controles por parte de la alta dirección de Qwerty para: mitigar, evitar, aceptar o transferir el riesgo, de acuerdo con los requisitos legales, operativos, los objetivos de Qwerty y los costos asociados a la implementación, considerando la proporcionalidad entre el costo de la implementación del control y costo del impacto por la materialización del riesgo.

Cuadro 22. Declaración de aplicabilidad

| Dominio | | Objetivo | | | Control | Exclusión (Si/No) | Control existente | Control a implementar | Justificación |
|---|---|---|---|---|---|---|---|---|---|
| **5** | **Políticas de Seguridad de la información** | **5.1** | Orientación de la dirección para la gestión de la seguridad de la información | 5.1.1 | Políticas para la Seguridad de la información | No | | Se define y adopta la política de Seguridad para Qwerty S.A.<br>Se estructuran políticas de seguridad aplicables a Qwerty S.A. en la parte operativa | |

Cuadro 22. Declaración de aplicabilidad (Continuación)

| Dominio | | Objetivo | | | Control | Exclusión (Si/No) | Control existente | Control a implementar | Justificación |
|---|---|---|---|---|---|---|---|---|---|
| | | | | 5.1.2 | Revisión de las políticas para la seguridad de la información | No | | Se establecerá un responsable de cada política quien que anualmente deberá efectuar al menos una revisión de las políticas y las actualizará de ser necesario. | |
| 6 | **Organización de la seguridad de la información** | 6.1 | Organización interna | 6.1.1 | Roles y responsabilidades para la seguridad de la información | No | | Se definen roles y responsabilidades que deben ser asignados en Qwerty S.A. | |
| | | | | 6.1.2 | Separación de deberes | No | Existe separación de deberes | Se capacitará a personal de la empresa para asistir al área de nómina y facturación cuando se presente alto flujo de trabajo y requieran apoyo. Se mantendrá un log de auditoría de actividades del área de nómina que será revisado regularmente. | |
| | | | | 6.1.3 | Contacto con las autoridades | No | | De acuerdo con la normatividad Colombiana Qwerty S.A. mantendrá un registro actualizado de contactos con las autoridades a quien se debe reportar o contactar en el evento de incidentes de seguridad o quienes le puedan apoyar en la gestión de los diferentes tipos de incidentes que se puedan presentar. | |

Cuadro 22. Declaración de aplicabilidad (Continuación)

| Dominio | | Objetivo | | | Control | Exclusión (Si/No) | Control existente | Control a implementar | Justificación |
|---|---|---|---|---|---|---|---|---|---|
| | | | | 6.1.4 | Contacto con grupos de interés especial | No | | Qwerty S.A. mantendrá contacto con empresas y/o profesionales de seguridad que requiera para el apoyo en la realización de actividades internas de seguridad, auditorías de tercera parte, entre otros. Mantendrá actualizados servicios de soporte o suscripciones que le permitan acceder a comunidades o información de interés para implementar medidas preventivas de seguridad. | |
| | | | | 6.1.5 | Seguridad de la información en la gestión de proyectos | No | | Se implementará procedimiento para gestión de proyectos, incluyendo el análisis de riesgos y se observe la seguridad de la información en la gestión de proyectos. | |
| | | **6.2** | Dispositivos móviles y teletrabajo | 6.2.1 | Política para dispositivos móviles | No | | Se implementarán reglas a través del firewall que limite y controle las acciones que puede realizarse desde un dispositivo móvil en la red de Qwerty S.A. | |
| | | | | 6.2.2 | Teletrabajo | No | | Se definirá y establecerá política de teletrabajo y se implementarán reglas a través del firewall para permitir conexiones a través de vpn y control sobre el acceso y uso de servicios autorizados a teletrabajadores y horarios. | |
| **7** | **Seguridad de los recursos humanos** | **7.1** | Antes de asumir el empleo | 7.1.1 | Selección | No | | Se implementarán verificación de referencias, hoja de vida, certificaciones de estudio. | |

Cuadro 22. Declaración de aplicabilidad (Continuación)

| Dominio | | Objetivo | | | Control | Exclusión (Si/No) | Control existente | Control a implementar | Justificación |
|---|---|---|---|---|---|---|---|---|---|
| | | | | 7.1.2 | Términos y condiciones de empleo | No | | Se implementará acuerdo de confidencialidad que deberá quedar suscrito con los empleados o contratistas. Se efectuará inducción a nuevos empleados en donde se informe responsabilidades, derechos, rol. | |
| | | **7.2** | Durante la ejecución del empleo | 7.2.1 | Responsabilidad de la dirección | No | | Mediante la suscripción de compromiso la dirección exigirá el cumplimiento de las responsabilidades de seguridad de la información en Qwerty S.A. | |
| | | | | 7.2.2 | Toma de conciencia, educación y formación en la seguridad de la información | No | | Se realizarán campañas de socialización a través de mensajes enviados regularmente a todos los usuarios sobre tips de seguridad, recomendaciones y sesiones de capacitación en temas orientados a la prevención. | |
| | | | | 7.2.3 | Proceso disciplinario | Si | | Se establecerán sanciones que serán impuestas a los empleados a los que se identifique y evidencie que hayan cometido una infracción a la seguridad de la información. | |
| | | **7.3** | Terminación y cambio de empleo | 7.3.1 | Terminación o cambio de responsabilidades de empleo | No | | Cuando se desvincule a un empleado se entregará documento con el detalle de las responsabilidades y deberes que seguirán siendo válidos y debe cumplir a partir de la desvinculación. | |
| **8** | **Gestión de activos** | **8.1** | Responsabilidad por los activos | 8.1.1 | Inventario de activos | No | | Se establecerá procedimiento para mantener actualizado el inventario de activos ya identificados. | |

Cuadro 22. Declaración de aplicabilidad (Continuación)

| Dominio | | Objetivo | | | Control | Exclusión (Si/No) | Control existente | Control a implementar | Justificación |
|---|---|---|---|---|---|---|---|---|---|
| | | | | 8.1.2 | Propiedad de los activos | No | | Cada activo tendrá un responsable, y la designación se efectuará a través de acta de asignación. | |
| | | | | 8.1.3 | Uso aceptable de los activos | No | | En el acta de asignación se incluirán los requisitos de seguridad que debe atenderse y las reglas de uso aceptable. | |
| | | | | 8.1.4 | Devolución de los activos | No | | Cuando se desvincule un empleado deberá hacer entrega de los activos a su cargo mediante acta de devolución. | |
| | | **8.2** | Clasificación de la información | 8.2.1 | Clasificación de la información | No | | Se establecerá clasificación de la información según normatividad aplicable, criticidad y nivel de acceso que puede tener. | |
| | | | | 8.2.2 | Etiquetado de la información | No | | Se definirá procedimiento para etiquetado de información que sea generado a partir de la fecha de su adopción. Para la información histórica se efectuará a demanda. | |
| | | | | 8.2.3 | Manejo de activos | No | | Se definirán y adoptarán procedimientos para: protección de copias, registro de acceso a los activos, | |
| | | **8.3** | Manejo de medios | 8.3.1 | Gestión de medios removibles | No | | Se definirá y adoptará procedimiento para establecer tratamiento a medios que contengan información sensible de Qwerty S.A. su disposición. | |
| | | | | 8.3.2 | Disposición de los medios | No | | Dentro del procedimiento para establecer se incluirán acciones de disposición en cuanto a almacenamiento o acciones cuando se requiera reutilizarlos o desecharlos. | |

Cuadro 22. Declaración de aplicabilidad (Continuación)

| Dominio | | Objetivo | | | Control | Exclusión (Si/No) | Control existente | Control a implementar | Justificación |
|---|---|---|---|---|---|---|---|---|---|
| | | | | 8.3.3 | Transferencia de medios físicos | No | | Se establecerá lineamiento para transporte de medios cuando se requiera trasladar físicamente fuera de la organización o entre dependencias. | |
| **9** | **Control de acceso** | **9.1** | Requisitos de negocio | 9.1.1 | Política de control de acceso | No | | Se definirá y adoptará política de control de acceso físico y lógico. | |
| | | | | 9.1.2 | Acceso a redes y a servicios de red | No | Qwerty S.A. cuenta con un firewall Cisco ASA 5505 | Se efectuará una revisión de configuración y se implementarán nuevas reglas para autorizar o denegar conexiones y transferencia de datos, entre otros. | |
| | | **9.2** | Gestión de acceso a usuarios | 9.2.1 | Registro y cancelación del registro a usuarios | No | El área de sistemas de Qwerty S.A. efectúa la gestión de usuarios y contraseñas de los diferentes sistemas. | Se establecerá y adoptará política para las contraseñas, activación e inactivación de usuarios, uso adecuado de usuarios y contraseñas. | |
| | | | | 9.2.2 | Suministro de acceso de usuarios | No | | Se definirá y adoptará procedimiento para gestión de usuarios, roles y perfiles | |
| | | | | 9.2.3 | Gestión de derechos de acceso de privilegiado | No | | Dentro del procedimiento para gestión de usuarios se especificará el tratamiento y asignación y retiro de derechos de acceso privilegiados a usuarios. | |
| | | | | 9.2.4 | Gestión de información de autenticación secreta de usuarios | No | | En el acuerdo de confidencialidad se incluirán textos para establecer responsabilidades de los usuarios frente a información secreta. | |

Cuadro 22. Declaración de aplicabilidad (Continuación)

| Dominio | | Objetivo | | | Control | Exclusión (Si/No) | Control existente | Control a implementar | Justificación |
|---|---|---|---|---|---|---|---|---|---|
| | | | | 9.2.5 | Revisión de los derechos de acceso de usuarios | No | | Como lineamiento para Qwerty S.A., se establecerá la responsabilidad para los dueños de activos de revisar al menos una vez al mes las autorizaciones así como cada vez que ocurre un cambio. | |
| | | | | 9.2.6 | Retiro o ajuste de los derechos de acceso | No | | Dentro del procedimiento de gestión de usuarios se incluye la inactivación de los empleados una vez se desvinculen de Qwerty S.A. o se presenten traslados o cambio de funciones dentro de la organización. | |
| | | **9.3** | Responsabilidades de los usuarios | 9.3.1 | Uso de información de autenticación secreta | No | | Dentro del acuerdo de confidencialidad que será firmado antes de asumir el empleo, se estipulará la responsabilidad del usuario con el adecuado tratamiento de información secreta, buenas prácticas y errores que se debe evitar cometer. | |
| | | **9.4** | Control de acceso a sistemas y aplicaciones | 9.4.1 | Restricción de acceso a la información | No | Las aplicaciones requieren autenticación para acceder a las mismas | | |
| | | | | 9.4.2 | Procedimiento de ingreso seguro | Si | | | Con los controles incorporados en la autenticación de sistemas se atiende lo requerido en el control. |

Cuadro 22. Declaración de aplicabilidad (Continuación)

| Dominio | | Objetivo | | | Control | Exclusión (Si/No) | Control existente | Control a implementar | Justificación |
|---|---|---|---|---|---|---|---|---|---|
| | | | | 9.4.3 | Sistema de gestión de contraseñas | No | | Se implementará SSO para facilitar gestión de contraseñas | Se implementará SSO para facilitar gestión de contraseñas |
| | | | | 9.4.4 | Uso de programas utilitarios privilegiados | No | | Se implementarán reglas desde suite de antivirus para evitar la instalación y uso de programas utilitarios en equipos de la organización junto con reglas en el firewall para fortalecer este control. | |
| | | | | 9.4.5 | Control de acceso a códigos fuente de programas | No | | Se implementará y se hará uso de software libre para tener un repositorio de código fuente, programas y elementos asociados, controlando el acceso a los mismos. | |
| **10** | **Criptografía** | **10.1** | Controles criptográficos | 10.1.1 | Política sobre el uso de controles criptográficos | No | | Se definirá y establecerá política para la administración, gestión y uso de mecanismos criptográficos en Qwerty S.A. | |
| | | | | 10.1.2 | Gestión de llaves | No | | Se definirá y establecerá política para la administración, gestión y uso de mecanismos criptográficos en Qwerty S.A. | |
| **11** | **Seguridad física y del entorno** | **11.1** | Áreas seguras | 11.1.1 | Perímetro de seguridad física | No | | Se implementarán mecanismos de control de acceso a áreas donde se encuentren activos de información sensibles. | |
| | | | | 11.1.2 | Controles de acceso físico | No | | Se implementaran mecanismos para fortalecer el control de acceso en Qwerty S.A. | |
| | | | | 11.1.3 | Seguridad de oficinas, recintos e instalaciones | No | | Se implementara control, haciendo una evaluación y ajustes en ubicación de áreas e implementación de controles de acceso donde sea necesario. | |

Cuadro 22. Declaración de aplicabilidad (Continuación)

| Dominio | | Objetivo | | | Control | Exclusión (Si/No) | Control existente | Control a implementar | Justificación |
|---|---|---|---|---|---|---|---|---|---|
| | | | | 11.1.4 | Protección contra amenazas externas y ambientales | No | | Se implementará control revisando área, haciendo uso de mecanismos que protejan a Qwerty de amenazas ambientales. | |
| | | | | 11.1.5 | Trabajo en áreas seguras | No | | Se definirá y adoptará procedimiento a seguir para áreas que se encuentren vacías, trabajo supervisado, uso de dispositivos móviles, cámaras en áreas restringidas. | |
| | | | | 11.1.6 | Áreas de despacho y carga | No | | Se implementará control estableciendo áreas para carga y descarga de materiales, insumos, horarios. | |
| | | | | 11.2 | EQUIPOS | | | | |
| | | | | 11.2.1 | Ubicación y protección de los equipos | No | | Se implementará control de ingreso y acceso, y se reubicaran equipos | |
| | | | | 11.2.2 | Servicios de suministro | No | | Se implementará UPS con una autonomía de 20 minutos para servidores y se reubicarán servidores DHCP, HTTP y PBX hacia área que cuenta con condiciones adecuadas de climatización. | |
| | | | | 11.2.3 | Seguridad del cableado | No | | Se efectuará una revisión a la red lógica y eléctrica. | |
| | | | | 11.2.4 | Mantenimiento de equipos | No | El área de soporte provee servicios de mantenimiento a los equipos de Qwerty S.A. | Se revisará periodicidad y actividades ejecutadas determinando e implementando mejoras. | |
| | | | | 11.2.5 | Retiro de activos | No | | Se implementará exigencia de autorización para retiro de equipos de instalaciones de Qwerty S.A. | |

Cuadro 22. Declaración de aplicabilidad (Continuación)

| Dominio | | Objetivo | | | Control | Exclusión (Si/No) | Control existente | Control a implementar | Justificación |
|---|---|---|---|---|---|---|---|---|---|
| | | | | 11.2.6 | Seguridad de equipos y activos fuera de las instalaciones | No | | Se implementarán lineamientos a seguir para equipos que sean utilizados fuera de las instalaciones de Qwerty S.A. | |
| | | | | 11.2.7 | Disposición segura o reutilización de equipos | No | | Se definirá y adoptarán lineamientos para la reutilización o retiro de elementos de cómputo que puedan contener datos de la empresa | |
| | | | | 11.2.8 | Equipos de usuario desatendidos | No | | Se generara campaña para que los usuarios terminen sesiones activas, se configurarán tiempos de auto bloqueo por inactividad y protectores de pantalla con contraseña | |
| | | | | 11.2.9 | Política de escritorio limpio y pantalla limpia | No | | Se definirá y adoptará política de escritorio limpio y pantalla limpia | |
| **12** | **Seguridad de las operaciones** | **12.1** | Procedimientos operacionales y responsabilidades | 12.1.1 | Procedimientos de operación documentados | No | | Se implementará control generando lineamiento para que se genere la documentación necesaria. | |
| | | | | 12.1.2 | Gestión de cambios | No | | Se estructurará y adoptará documento para el registro de cambios en los procesos o sistemas de procesamiento de información. | |
| | | | | 12.1.3 | Gestión de capacidad | No | | Se implementará control estableciendo un plan de capacidad orientado a optimizar el uso de recursos disponibles. | |
| | | | | 12.1.4 | Separación de los ambientes de desarrollo, pruebas, y operación | No | | Se implementará ambiente de pruebas para los sistemas internos en uso. | |

Cuadro 22. Declaración de aplicabilidad (Continuación)

| Dominio | | Objetivo | | | Control | Exclusión (Si/No) | Control existente | Control a implementar | Justificación |
|---|---|---|---|---|---|---|---|---|---|
| | | **12.2** | Protección contra códigos maliciosos | 12.2.1 | Controles contra códigos maliciosos | No | | Se adoptará política prohibiendo uso de software no autorizado y recepción de archivos externos.<br>Se establecerán lineamientos para mantener actualizado el software antivirus | |
| | | **12.3** | Copias de respaldo | 12.3.1 | Respaldo de información | No | El área de soporte realiza copias de seguridad de sis.de inf. y servidores que de las dependencias de Qwerty S.A. | Se definirá y adoptará política de respaldo de información | |
| | | **12.4** | Registro de seguimiento | 12.4.1 | Registro de eventos | No | | Se implementará control para mantener registro de log en los sistemas críticos de QWERTY S.A. | |
| | | | | 12.4.2 | Protección de la información de registro | No | | Se implementará control para evitar modificaciones a registros de log | |
| | | | | 12.4.3 | Registros del administrador y del operador | No | | Se implementará procedimiento automático de actualización de relojes frente a servidor hora legal | |
| | | | | 12.4.4 | Sincronización de relojes | No | | | |
| | | **12.5** | Control de software operacional | 12.5.1 | Instalación de software en sistemas operativos | No | | Se establecerán lineamientos para efectuar actualizaciones al software, considerando procedimientos de rollback | |
| | | **12.6** | Gestión de la vulnerabilidad técnica | 12.6.1 | Gestión de las vulnerabilidades técnicas | No | | Se definirán roles y responsabilidades para la gestión de vulnerabilidades técnicas y acciones de remediación. | |

Cuadro 22. Declaración de aplicabilidad (Continuación)

| Dominio | | Objetivo | | | Control | Exclusión (Si/No) | Control existente | Control a implementar | Justificación |
|---|---|---|---|---|---|---|---|---|---|
| | | | | 12.6.2 | Restricciones sobre la instalación del software | No | | Se definirá y adoptará política para la instalación de software por parte de los usuarios. | |
| | | 12.7 | Consideraciones sobre auditorías de sistemas de información | 12.7.1 | Controles de auditorías de sistemas de información | No | | Se definirá lineamientos para la ejecución de auditorías y alcance de pruebas | |
| 13 | **Seguridad de las comunicaciones** | 13.1 | Gestión de la seguridad de las redes | 13.1.1 | Controles de redes | No | | Se implementará el control revisando configuración de firewall e implementando nuevas reglas, así como revisión y ajustes en red LAN (se segmentará la red), puntos de acceso alámbrico e inalámbricos. | |
| | | | | 13.1.2 | Seguridad de los servicios de red | No | | Se implementará el control revisando configuración de firewall e implementando nuevas reglas internas y externas, así como el uso de protocolos, mecanismos de encripción y vpn. | |
| | | | | 13.1.3 | Separación en las redes | No | | Se segmentará la red LAN. | |
| | | 13.2 | Transferencia de información | 13.2.1 | Políticas y procedimientos de transferencias de información | No | | Se establecerá, adoptará y socializarán políticas para la transferencia de información interna y externa en Qwerty S.A. | |
| | | | | 13.2.2 | Acuerdos sobre transferencia de información | No | | Se aplicará lineamientos de etiquetado de la información la cual será tenida en cuenta según política de transferencia establecida. | |
| | | | | 13.2.3 | Mensajería electrónica | No | | Se utilizaran mecanismos que permitan proteger la mensajería electrónica de información según su clasificación. | |

Cuadro 22. Declaración de aplicabilidad (Continuación)

| Dominio | | Objetivo | | | Control | Exclusión (Si/No) | Control existente | Control a implementar | Justificación |
|---|---|---|---|---|---|---|---|---|---|
| | | | | 13.2.4 | Acuerdos de confidencialidad o de divulgación | No | | Se establecerá, adoptará y socializarán acuerdos de confidencialidad que deberán ser suscritos interna y externamente en Qwerty S.A. | |
| **14** | **Adquisición, desarrollo y mantenimiento de sistemas** | **14.1** | Requisitos de seguridad de los sistemas de información | 14.1.1 | Análisis y especificación de requisitos de seguridad de la información | No | | Se establecerá lineamiento en relación con los requisitos mínimos que deben cumplir los sistemas de información en cuanto a seguridad de la información. | |
| | | | | 14.1.2 | Seguridad de servicios de las aplicaciones en redes públicas | No | | Se implementarán protocolos seguros para las aplicaciones que transfieran información a través de redes públicas. | |
| | | | | 14.1.3 | Protección de transacciones de los servicios de las aplicaciones | No | | Se utilizarán mecanismos emitidos por entidades certificadoras abiertas en Colombia para proteger transacciones que se realicen en Qwerty que se determine lo requieran. | |
| | | **14.2** | Seguridad de los procesos de desarrollo y de soporte | 14.2.1 | Políticas de desarrollo seguro | No | | Se establecerá y adoptará políticas de desarrollo de aplicaciones tomando como referente metodología estándar para esta actividad. | |
| | | | | 14.2.2 | Procedimientos de control de cambios en sistemas | No | | Se establecerá y adoptará lineamiento para la gestión de cambios en ambientes productivos en Qwerty S.A. | |

Cuadro 22. Declaración de aplicabilidad (Continuación)

| Dominio | | Objetivo | | | Control | Exclusión (Si/No) | Control existente | Control a implementar | Justificación |
|---|---|---|---|---|---|---|---|---|---|
| | | | | 14.2.3 | Revisión técnica de las aplicaciones después de cambios en la plataforma de operación. | No | | Se establecerá procedimiento para controlar el desarrollo de aplicaciones y nuevas funcionalidades en Qwerty S.A., dentro del cual se requerirá la ejecución de pruebas posterior a cambios efectuados en la plataforma, las cuales deberán ser exitosas para permitir su paso a productivo. | |
| | | | | 14.2.4 | Restricciones en los cambios a los paquetes de software. | No | | Todo cambio que se efectúe deberá seguir el procedimiento establecido, incluyendo control de versionamiento y pruebas. | |
| | | | | 14.2.5 | Principios de construcción de los sistemas seguros | No | | Dentro del procedimiento se establecerán lineamientos para establecer las condiciones de seguridad que deben cumplir los sistemas. | |
| | | | | 14.2.6 | Ambiente de desarrollo seguro | No | | Se crearán ambientes de desarrollo separados. | |
| | | | | 14.2.7 | Desarrollo contratado externamente | No | | Se establecerán lineamientos que deben ser atendidos cuando el desarrollo se construya externamente, incluyendo acuerdos de licenciamiento. | |
| | | | | 14.2.8 | Pruebas de seguridad de sistemas | No | | Toda intervención o desarrollo interno o externo para Qwerty S.A. debe ser sometido a pruebas unitarias e integrales como requisito para su paso a producción. | |
| | | | | 14.2.9 | Prueba de aceptación de sistemas | No | | Las nuevas aplicaciones y funciones que se implementen deberán ser sometidas a pruebas unitarias e integrales. | |

Cuadro 22. Declaración de aplicabilidad (Continuación)

| Dominio | | Objetivo | | | Control | Exclusión (Si/No) | Control existente | Control a implementar | Justificación |
|---|---|---|---|---|---|---|---|---|---|
| | | **14.3** | Datos de prueba | 14.3.1 | Protección de datos de prueba | No | | Los datos que sean utilizados en ambientes de pruebas deberán ser controlados y seleccionados para este propósito. | |
| **15** | **Relaciones con los proveedores** | **15.1** | Seguridad de la información en la relación con los proveedores | 15.1.1 | Política de seguridad de la información para las relaciones con proveedores | No | | La relación con proveedores se regirá por condiciones y acuerdos de niveles de servicio establecidos por Qwerty S.A. | |
| | | | | 15.1.2 | Tratamiento de la seguridad de los acuerdos con los proveedores | No | | Los acuerdos con proveedores se establecerán compromisos en cuanto al tratamiento de la información. | |
| | | | | 15.1.3 | Cadena de suministro de tecnología de información y comunicación | No | | Se incluirá en los acuerdos con proveedores los requisitos para tratar riesgos de seguridad. | |
| | | **15.2** | Gestión de la prestación de servicios de proveedores | 15.2.1 | Seguimiento y revisión de los servicios de los proveedores | No | | Se establece como lineamiento las actividades de seguimiento y revisión a proveedores | |
| | | | | 15.2.2 | Gestión de cambios en los servicios de los proveedores | No | | Se aplicarán los lineamientos de gestión de cambios a los servicios con proveedores. | |
| **16** | **Gestión de incidentes de seguridad de la información** | **16.1** | Gestión de incidentes y mejores en la seguridad de la información | 16.1.1 | Responsabilidades y procedimientos | No | | Se establecerán dentro de los roles, las responsabilidades frente a incidentes de seguridad de la información en Qwerty S.A. | |
| | | | | 16.1.2 | Reporte de eventos de seguridad de la información | No | | Los reportes de incidentes se efectuarán en formatos establecidos. | |
| | | | | 16.1.3 | Reporte de debilidades de seguridad de la información | No | | Regularmente se efectuarán verificaciones para identificar debilidades existentes. | |

Cuadro 22. Declaración de aplicabilidad (Continuación)

| Dominio | | Objetivo | | | Control | Exclusión (Si/No) | Control existente | Control a implementar | Justificación |
|---|---|---|---|---|---|---|---|---|---|
| | | | | 16.1.4 | Evaluación de eventos de seguridad de la información y decisiones sobre ellos | No | | Los eventos de seguridad serán tratados según lineamientos establecidos según la categorización establecida. | |
| | | | | 16.1.5 | Respuesta a incidentes de seguridad de la información | No | | La respuesta a incidentes se efectuará según procedimientos establecidos. | |
| | | | | 16.1.6 | Aprendizaje obtenido de los incidentes de seguridad de la información | No | | Se documentarán los incidentes y la documentación quedará disponible para posteriores consultas. | |
| | | | | 16.1.7 | Recolección de evidencia | No | | La recolección de evidencia se efectuará según procedimientos establecidos. | |
| 17 | **Aspectos de seguridad de la información** | **17.1** | Continuidad de seguridad de la información | 17.1.1 | Planificación de la continuidad de la seguridad de la información | Si | | Se implementará en una fase posterior iniciando con un BIA, entre tanto se implementarán las acciones preventivas y correctivas identificadas. | |
| | | | | 17.1.2 | Implementación de la continuidad de la seguridad de la información | Si | | Se implementará en una fase posterior iniciando con un BIA, entre tanto se implementarán las acciones preventivas y correctivas identificadas. | |
| | | | | 17.1.3 | Verificación, visión y evaluación de la continuidad de la seguridad de la información | Si | | Se implementará en una fase posterior iniciando con un BIA, entre tanto se implementarán las acciones preventivas y correctivas identificadas. | |
| | | **17.2** | Redundancias | 17.2.1 | Disponibilidad de instalaciones de procesamiento de información | No | | Se revisarán contingencias existentes para mantener su operatividad y se implementarán nuevas en relación con redundancias locales. | |
| 18 | **Cumplimiento** | **18.1** | Cumplimiento de requisitos legales y contractuales | 18.1.1 | Identificación de la legislación aplicable y de los requisitos contractuales | No | | Se efectuará un levantamiento sobre la normatividad aplicable vigente en Qwerty S.A. incluyendo la actividad contractual. | |

Cuadro 22. Declaración de aplicabilidad (Continuación)

| Dominio | | Objetivo | | | Control | Exclusión (Si/No) | Control existente | Control a implementar | Justificación |
|---|---|---|---|---|---|---|---|---|---|
| | | | | 18.1.2 | Derechos de propiedad intelectual | No | | Se efectuará una identificación de normatividad sobre propiedad intelectual aplicable a Qwerty S.A. | |
| | | | | 18.1.3 | Protección de registros | No | | Se definirán políticas de respaldo que protejan la información de Qwerty S.A. | |
| | | | | 18.1.4 | Privacidad y protección de información de datos personales | No | | Dentro de los acuerdos de confidencialidad, contratos se establecerán exigencias de cumplimiento respecto de la protección de datos personales según normatividad aplicable vigente. | |
| | | | | 18.1.5 | Reglamentación de controles criptográficos | No | | El uso de mecanismos criptográficos se regirá por los lineamientos internos establecidos. | |
| | | **18.2** | Revisiones de seguridad de la información | 18.2.1 | Revisión independiente de la seguridad de la información | No | | Las auditorías internas serán efectuadas con apoyo externo. | |
| | | | | 18.2.2 | Cumplimiento con las políticas y nomas de seguridad | No | | Las auditorías internas se efectuarán validando el cumplimiento de las políticas y normas de seguridad. | |
| | | | | 18.2.3 | Revisión del cumplimiento técnico | No | | Se establecerán revisiones regulares para validar cumplimiento técnico | |

Fuente: Construcción propia del autor

**6.3.5. Sensibilización y capacitación en seguridad de la información en Qwerty S.A.** Para la apropiación del Sistema de Gestión de Seguridad de la Información en la organización se estima necesario[39], de conformidad con lo establecido en la NIST SP 800-16[40], adelantar la sensibilización y capacitación de empleados y contratistas, este proceso estará centrado en las funciones, roles y responsabilidades, no en los cargos de los empleados. En el cuadro 23 se puede

[39] MINTIC. Elaboración de la política general de seguridad y privacidad de la información. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

[40] WILSON Mark, De Zafra Dorothea Information Technology Security Training Requirements: A Rol- and Performance-Based Model. Disponible en: https://dl.acm.org/doi/pdf/10.5555/2206227

visualizar el resultado de la evaluación de las necesidades de sensibilización y capacitación en Qwerty S.A.:

Cuadro 23. Evaluación de necesidades.

| Total empleados | 120 | | |
|---|---|---|---|
| Necesidades | Sensibilización a empleados sobre seguridad de la información. | | |
| | Fortalecer competencias de personal técnico que cumple funciones de administración de: firewall, suite de seguridad, redes, control de acceso. | | |
| | Formación en seguridad de la información. | | |
| **Tipo** | **Objetivo** | **Prioridad** | **Estrategia** |
| Concientización | Todos los empleados | 1 | Pantallas de bloqueo con tips preventivos en seguridad |
| | | 1 | Campañas con tips de seguridad a través de correo electrónico |
| | | 2 | Reconocimientos a acciones de seguridad |
| | | 1 | Sesiones preventivas sobre los cuidados con la realización de transacciones a través de internet, que se debe hacer con correos de procedencia desconocida, archivos adjuntos, links en mensajes, importancia mantener escritorio limpio, tener copias de respaldo. Acciones preventivas. |
| Entrenamiento basado en roles | Administrador avanzada de firewall | 1 | Desarrollo de competencias para:<br>Implementar reglas y mantenerlas.<br>Configurar firewall.<br>Creación de VPN |
| | Administración avanzada de red | 1 | Segmentar la red<br>Crear vlan<br>Implementar controles para restringir acceso a segmento de servidores, control de visibilidad y acceso entre segmentos |

Cuadro 23. Evaluación de necesidades. Continuación

| Tipo | Objetivo | Prioridad | Estrategia |
|---|---|---|---|
| | Administración suite de seguridad | 2 | Formación en administración de seguridad de la información |
| Educación | Auditoría interna de seguridad de la información. | 3 | Esta capacitación debe participar personal de las áreas: directiva, administrativa, sistemas. |
| | Sensibilización en seguridad de la información | 3 | Esta capacitación debe participar personal de las áreas: directiva, administrativa, sistemas. |

Necesidades para las cuales, de acuerdo con la prioridad calificada con 1, en el cuadro 24 se puede visualizar las siguientes actividades a través de las cuales se presenta la estimación de costos de la atención de las necesidades de capacitación:

Cuadro 24. Actividades de sensibilización y capacitación y sus costos

| Actividad | Costo unitario | Cantidad | Objetivo | Costo Total |
|---|---|---|---|---|
| Pantallas de bloqueo con tips preventivos en seguridad<br>Campañas con tips de seguridad a través de correo electrónico | Comunicador social (dos semanas) $2.000.000 Especialista en seguridad(una semana) $1.500.000 | 1 | Sensibilizar a empleados sobre seguridad de la información | $ 3.500.000 |
| Sesiones preventivas sobre los cuidados con la realización de transacciones a través de internet, que se debe hacer con correos de procedencia desconocida, archivos adjuntos, links en mensajes, importancia mantener escritorio limpio, tener copias de respaldo. Acciones preventivas. | Especialista en seguridad (tres sesiones a todos los empleados) $2.000.000 | 1 | Sensibilizar e informar a empleados sobre las acciones preventivas y cuidados que debe tener y el impacto de sus acciones sobre la seguridad de la información de Qwerty S.A. | $ 2.000.000 |

Cuadro 24. Actividades de sensibilización y capacitación y sus costos. Continuación

| Actividad | Costo unitario | Cantidad | Objetivo | Costo Total |
|---|---|---|---|---|
| Desarrollo de competencias para: Implementar reglas y mantenerlas. Configurar firewall. Creación de VPN | $ 7.631.320 | 1 | Crear capacidades en Qwerty S.A. para mantener y administrar adecuadamente el firewall | $7.631.320[41] |
| Segmentar la red Crear vlan Implementar controles para restringir acceso a segmento de servidores, control de visibilidad y acceso entre segmentos | $1.451.000 | 1 | Crear capacidades en Qwerty S.A. para mantener y administrar adecuadamente la red local. | $1.451.000[42] |
| Auditoría interna | $ 1.350.000 | 5 | Crear capacidades para orientar y mantener el sistema de gestión de seguridad de la información. | $6.750.000[43] |
| **Total sensibilización y capacitación** | | | | **$ 21.332.320** |

**6.3.6. Resultados**. A partir del análisis de riesgos efectuado:

- Se ha identificado que Qwerty S.A. afronta amenazas y vulnerabilidades, que expone sus activos de información a riesgos, que al materializarse podrían derivar en pérdidas de información, accesos no autorizados, ataques informáticos, interrupción de los servicios, entre otros, que podrían ocasionar

[41] Emagister. Cisco ASA Express Security. Disponible en: https://www.emagister.com.co/cisco-asa-express-security-cursos-2789357.htm

[42] Emagister. Uniminuto. Tecnología en redes y comunicaciones. Disponible en: https://www.emagister.com.co/cursos-administracion-redes-bogota-categprov-72-66_2.htm

[43] BUREAU VERITAS. Auditor Interno ISO/IEC 27001:2013 Sistemas de gestión en Seguridad de la Información. Disponible en: https://colombia.bureauveritastraining.com/course-details.aspx?id=COLU31

incidentes que podrían impactar negativamente sus operaciones, generarían daños reputacionales o afectaciones a terceros, incluso con un daño económico que llegar a ser altamente lesivo para la organización.

- Qwerty S.A., no cuenta con políticas de seguridad, por lo que se hace fue necesario construir diferentes políticas a través de las cuales se adopten lineamientos que permitan establecer condiciones mínimas que deben ser atendidas por empleados, contratistas y terceros para mantener un nivel adecuado de seguridad de la información.

- Dado que Qwerty S.A. no cuenta con una organización interna de seguridad de la información, se plantean roles y perfiles a implementar, de tal manera que la organización adquiera la capacidad necesaria para mantener el sistema de gestión de seguridad, así como de mantener la dinámica requerida dentro de la mejora continua que requieren los sistemas de gestión.

- Como parte de las interacciones que se requieren para tratar adecuadamente eventos tales como las incidencias de seguridad de la información que puedan ocurrir en Qwerty S.A., se planteó la necesidad de mantener contacto con las autoridades.

- Para los empleados, contratistas, proveedores y terceros se establece la necesidad de suscribir acuerdos de confidencialidad.

- Con el fin de lograr la concientización, educación y formación, necesaria para crear una cultura de seguridad de la información y adquirir la capacidad necesaria para operar en unas condiciones adecuadas de seguridad de la información, así como gestionar y mantener el sistema de gestión de seguridad, se ha planteado la necesidad de adelantar actividades orientadas a cumplir con este objetivo.

- Como parte de la implementación del SGSI, se adelantó el levantamiento del inventario de activos de información de Qwerty S.A. el cual se requiere que mantenga actualizado, así como el análisis de riesgos que debe efectuarse sobre el mismo en cada iteración dentro del proceso de mejora continua.

- Un aspecto clave, el cual debe apropiar Qwerty S.A. es la adopción de una clasificación de la información y la implementación de su rotulación de tal manera que se facilite efectuar el tratamiento adecuado sobre cada activo.

- Qwerty requiere fortalecer los controles en relación con la gestión de contraseñas, el acceso a usuarios autorizados, con el fin de corregir situaciones como las evidenciadas en el área de nómina y el apoyo que han obtenido con personal de otra área, lo que podrá temporalmente resolver una

necesidad de evacuar trabajo en tiempos de alto flujo, no obstante dicha práctica se considera una mala práctica que representa una vulnerabilidad de seguridad para Qwerty S.A.

- En cuanto a la información que se haya clasificado en Qwerty S.A. como confidencial o reservada, es necesario que se haga uso de mecanismos criptográficos que serán administrados por el área de infraestructura, quien evaluará y determinará el mecanismo a utilizar según el caso.

- Considerando la vulnerabilidad existente respecto de equipos ubicados en áreas con ausencia de control de acceso y/o de condiciones adecuadas ambientales, se ha determinado que es necesario resolverla implementando controles de acceso y temperatura adecuados.

- Considerando las amenazas identificadas por la desactualización de antivirus y la falta de reglas en el firewall que restrinjan el acceso a la red, se hace necesario además de efectuar con apoyo externo la configuración adecuada tanto en el firewall como en el antivirus, ajustar procedimientos, capacitar a los administradores para que se realicen las labores necesarias para administrar la tecnología existente, identificando y resolviendo posibles vulnerabilidades asociadas a esta labor y a los usuarios finales para que hagan un mejor uso de la tecnología y servicios.

Por tanto, una vez se han presentado los resultados del análisis, los directivos, han decidido tratar algunos de los riesgos identificados, implementando los controles sugeridos dentro del ejercicio, para lo cual destinarán recursos que permitan mitigar los riesgos identificados e incorporar un nivel aceptable de seguridad de sus activos de información.

Para hacerlo la organización es consciente de que este es un proceso cíclico y en consecuencia dará continuidad a las labores necesarias dentro del ciclo PHVA para mantener el Sistema de Gestión de Seguridad de la Información posterior a su implementación considerando que es necesario que la organización se ocupe de su sostenibilidad. Para lo cual, asignará funciones y roles[44] con el apoyo de personal externo que permitirá fortalecer las competencias, junto con la formación en auditoría interna de algunos de los miembros de su equipo.

Por otra parte, se resalta la importancia de los aspectos relacionados no solamente con la seguridad informática sino que requieren gestión, aspectos legales, éticos, externos e internos a Qwerty S.A. para lograr la efectividad del sistema de gestión de seguridad de la información que se espera.

[44] ISO/IEC 27000.ES CONTROLES. Organización. Disponible en https://www.iso27000.es/iso27002.html

# 7. CONCLUSIONES

Adelantar la implementación de un sistema de gestión de seguridad de la información en cualquier organización, requiere que el proyecto se trate como de la organización, no como un proyecto de tecnología, motivo por el cual el apoyo y participación en las decisiones por parte del área directiva es determinante para el éxito del proyecto.

Contando con este apoyo, un factor clave para toda implementación es conformar un equipo en el que participen, por una parte, profesionales de seguridad con el perfil y la experiencia adecuada para asumir los diferentes roles de los integrantes del equipo; y por otra, los empleados de la organización, de tal manera que con su participación, además de ser un medio eficaz para que adquieran conocimiento, se genere un vínculo con el sistema, permitiéndoles adquirir experiencia que será valiosa para apoyar a la organización con la mejora continua que requiere el SGSI, con la oportunidad de una vez formados se conviertan en multiplicadores constituyéndose en un apoyo fundamental para fomentar la cultura de la seguridad de la información en la organización.

En consecuencia, se resalta la importancia del talento humano y su rol estratégico para el sistema de seguridad de la información en Qwerty S.A., considerando que es un factor clave del éxito, la generación de una cultura de seguridad, así como la concientización sobre el impacto de las acciones que comprometan la seguridad de la información para la organización.

Igualmente en este proceso la fase de diagnóstico y análisis de riesgos es determinante dentro de la implementación del sistema de gestión de seguridad de la información, considerando que de la calidad de la información obtenida y el resultado del análisis, dependerá que el área directiva de Qwerty S.A. pueda tomar decisiones asertivas que permitan cumplir con el objetivo.

Qwerty S.A. es un referente que puede asimilarse en términos del estado de la seguridad de la información a muchas organizaciones que operan sin efectuar mayores acciones que le permitan asegurar y proteger la confidencialidad, integridad y disponibilidad de sus activos de información, exponiéndose a una diversidad de incidentes que pueden generar afectaciones tan graves que pueden llevar a la desaparición misma de la organización.

Con el desarrollo del proyecto aplicado para Qwerty S.A., tuve la oportunidad de afianzar los conocimientos adquiridos a lo largo de los diferentes cursos y prácticas adelantadas.

# 8. RECOMENDACIONES

- Hacer una revisión y configuración adecuada del firewall implementando reglas para tener un control de acceso adecuado a la red de la organización.
- Segmentar la red separando: servidores de equipos de usuario final.
- Implementar un mecanismo de control de acceso biométrico a las áreas en donde se encuentra infraestructura de servidores, componentes sensibles de red.
- Es necesario implementar una solución para asegurar las condiciones ambientales donde se encuentran equipos tales como servidores, considerando que un incremento en la temperatura puede causar un apagado automático o generar daños a la infraestructura misma o pérdidas de información.
- Implementar un mecanismo que permita al administrador conocer cuáles máquinas tienen o no instalado el antivirus y si se encuentra o no actualizada la base de datos de definiciones, de tal manera se pueda actuar preventivamente respecto de la actualización.
- Cuando se presente la necesidad de recurrir a personal adicional para atender la demanda de servicios en el área de nómina y facturación, se podrá apoyar y ampliar temporalmente la operación con personal de otra área, el cual deberá ser preparado adecuadamente para apoyar en estas fechas críticas.
- Para los servicios que se están soportando de manera externa:
    - En cuanto a correo electrónico, se sugiere revisar los acuerdos de niveles de servicio, políticas y condiciones de protección de datos personales, transfiriendo en este caso a través de las obligaciones pactadas las necesarias que obliguen al proveedor a operar en condiciones adecuadas de seguridad.
    - Para el sitio Web en Godaddy, de igual manera se sugiere revisar las condiciones de servicio e incluir las obligaciones necesarias que permitan proteger a los usuarios y a la organización de posibles ataques o suplantaciones de identidad.
- A partir de la implementación del sistema de gestión de seguridad de la información, es necesario que Qwerty S.A. de continuidad a las labores necesarias que permitan mantener el sistema, tanto como adelantar acciones que promuevan la adopción y mejora continua.
- Formar y organizar un grupo de apoyo con integrantes de las diferentes áreas que actúen como apoyo para efectuar el mantenimiento del sistema y acciones que contribuyan a la mejora continua.
- La implementación de controles, permitirá que Qwerty pueda contar con un SGSI que le permita establecer un nivel adecuado de seguridad.

## 9. BIBLIOGRAFÍA


ALEMAN NOVOA, Helena y RODRIGUEZ BARRERA, Claudia. Metodologías para el análisis de riesgos en los SGSI. Disponible en: http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

BACA URBINA, Gabriel. *Introducción a la seguridad informática*, Grupo Editorial Patria, 2016. ProQuest Ebook Central, Disponible en: http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=4849850

COLOMBIA COMPRA EFICIENTE [Sitio Web]. Bogotá; Alcance del Sistema de Seguridad de la información. [Consulta: 06 de mayo de 2020] Disponible en: https://www.colombiacompra.gov.co/sites/cce_public/files/cce_documentos/20160623alcancedelsgsi.pdf

ISO27000.ES [Sitio Web]. Glosario. [Consultado 12 de mayo de 2020]. Disponible en: http://www.iso27000.es/glosario.html

DÍAZ ARUETA, Gabriel., ALZÓRRIZ ARMENDÁRIZ, Ignacio, y SANCRISTOBAL RUIZ Elio. *Procesos y herramientas para la seguridad de redes.* Madrid, ES: UNED - Universidad Nacional de Educación a Distancia. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10862475&p00=seguridad+redes

ESCRIVÁ GASCÓ, Gema, ROMERO SERRANO, Rosa María, y RAMADA, David Jorge y ONRUBIA PEREZ, Ramón. *Seguridad informática*. España: Macmillan Iberia, S.A. Disponible en https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43260?page=1

GIMENEZ ALBACETE, José Francisco. *Seguridad en equipos informáticos*. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/44137

GÓMEZ F LUIS, ANDRÉS A ANA, Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. (2012). Disponible en: https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?ppg=36&docID=3205110&tm=1545148818931

ICONTEC NTC-ISO/IEC 27001. *Tecnología de la información Técnicas de seguridad, sistemas de gestión de la seguridad de la información*. Requisitos. (2019).

INCIBE, GOBIERNO DE ESPAÑA. MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL. Colección: Protege tu empresa. Plan director de seguridad. [Consultado 8 de mayo de 2020] Disponible en: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf, p15.

INTECO, GOBIERNO DE ESPAÑA, MINISTERIO DE INDUSTRIA Y TURISMO. Implantación de un SGSI en la empresa. Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

INTEDYA [Sitio Web]. ISO27000 y el conjunto de estándares de Seguridad de la Información. [Consultado 05 de mayo de 2020] Disponible en: http://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjunto-de-estandares-de-seguridad-de-la-informacion.html

ISO 27001 [Sitio Web] La implementación de un Sistema de Gestión de Seguridad de la Información mediante el ciclo PHVA. [Consultado 10 de mayo de 2020] Disponible en: https://www.isotools.pe/iso-27001-implementacion-sistema-gestion-seguridad-informacion-ciclo-phva/

ISO 27001 [Sitio Web] la mejora continua en los Sistemas de Gestión de Seguridad de la Información. [Consultado 05 de mayo de 2020] Disponible en: https://www.pmg-ssi.com/2017/07/iso-27001-mejora-continua/

ISO/IEC 27000.ES CONTROLES [Sitio Web]. Organización. [Consultado 09 de mayo de 2020] Disponible en: https://www.iso27000.es/iso27002.html

ISO/IEC 27002 [Sitio Web], Information Technology. Security Techniques. Code of practice for information security controls. [Consultado 13 de mayo de 2020] Disponible en: https://www.iso27001security.com/html/27002.html

La norma ISO 27001 Aspectos clave de su diseño e implantación. Disponible en: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

MAGERIT versión 3.0 Metodología de Análisis y Gestión de Riesgos de los sistemas de Información, Libro I – Método, Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

MAGERIT versión 3.0 Metodología de Análisis y Gestión de Riesgos de los sistemas de Información, Libro II – Catálogo de Elementos, Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XNEBj-hKjcc

MARKUS Erb, Gestión de Riesgo en la Seguridad Informática. Disponible en: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades.

MINTIC. Elaboración de la política general de seguridad y privacidad de la información. [Consultado 05 de septiembre de 2020] Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

MINTIC [Sitio Web]. Normativa, [Consultado 15 de septiembre de 2020] Disponible en: https://www.mintic.gov.co/portal/inicio/Normatividad/

MINTIC. Procedimientos de seguridad de la información. Seguridad y privacidad de la información. Guía 3 [Consultado 20 de octubre de 2020]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

MINTIC. Roles y responsabilidades. Seguridad y privacidad de la información. Guía 4 (2016). [Consultado 10 de septiembre de 2020] Disponible en:

https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

MOGOLLON, Abraham. *Comparativo metodologías de análisis de riesgos*. Disponible en: https://www.academia.edu/14195886/An%C3%A1lisis_Comparativo_Metodolog%C3%ADas_de_an%C3%A1lisis_de_Riesgos

DE ZAFRA, Dorothea. PITCHER, Sadie. NIST. SP 800-16. Information Technology Security Training Requirements: a Role- and Performance-Based Model," Disponible en: https://dl.acm.org/citation.cfm?id=2206227

EMAGISTER [Sitio Web]. Cisco ASA Express Security. [Consultado 4 de mayo de 2020] Disponible en: https://www.emagister.com.co/cisco-asa-express-security-cursos-2789357.htm

EMAGISTER [Sitio Web]. Uniminuto. Tecnología en redes y comunicaciones. . [Consultado 4 de mayo de 2020] Disponible en: https://www.emagister.com.co/cursos-administracion-redes-bogota-categprov-72-66_2.htm

BUREAU VERITAS [Sitio Web]. Auditor Interno ISO/IEC 27001:2013 Sistemas de gestión en Seguridad de la Información. [Consultado 4 de mayo de 2020] Disponible en: https://colombia.bureauveritastraining.com/course-details.aspx?id=COLU31