DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SEGÚN EL ESTÁNDAR ISO 27001 PARA EL CASO ESTUDIO DE LA EMPRESA QWERTY S.A.

JOHN FREDY QUINTERO MÉNDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTA

2021

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SEGÚN EL ESTÁNDAR ISO 27001 PARA EL CASO ESTUDIO DE LA EMPRESA QWERTY S.A.

JOHN FREDY QUINTERO MÉNDEZ

PROYECTO APLICADO

HERNANDO JOSE PEÑA HIDALGO

DIRECTOR DE PROYECTO DE GRADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ

2021

DEDICATORIA

Este proyecto de Seguridad informática se lo dedico a mi familia, Amigos, docentes y compañeros que me apoyaron incondicionalmente en el desarrollo de este nuevo logro en mi vida profesional.

AGRADECIMIENTOS

Ofrezco mis agradecimientos a la Universidad Nacional y a Distancia ya que me brindo la oportunidad de cursar la especialización en seguridad informática, siempre brindando el apoyo necesario para culminar con a cabalidad y con éxito cada ciclo de esta meta propuesta.

A los directores del proyecto por su tiempo y dedicación en transferir sus valiosos conocimientos, por la paciencia y el esmero constante para lograr el desarrollo del trabajo.

RESUMEN

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

El manejo que se da hoy en día a la información relaciona varios aspectos de gran importancia, los cuales se relacionan desde la recepción de la información en su adecuado manejo tanto de documentos físicos como de información almacenada de forma virtual, hasta los distintos sistemas de información que tenga la organización o distintos medios de sistemas externos a los que esté obligada a reportar información.[1]

En la actualidad se mantiene una falsa idea en la cual se sustenta que la seguridad de la información es una de las tareas imposibles de desarrollar y aplicar en un país subdesarrollado como el nuestro, pero la gran realidad al respecto consiste en que con el conocimiento necesario y claramente con grande esfuerzo se puede alcanzar un nivel de ciberseguridad alto, siempre con el apoyo constante de las directivas.

Según lo expresado anteriormente se propone como objetivo principal el mejoramiento del sistema de gestión de seguridad de la compañía, basado en la metodología establecida en la cual, por medio de la identificación del problema principal y la respectiva investigación sobre un trabajo de campo, se realizarán las actividades necesarias para contribuir con el mejoramiento continuo de la compañía.

[1] Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. [en línea]. [Citado Noviembre, 2020] Disponible en: http://docplayer.es/2402949-Analisis-de-riesgos-de-la-seguridad-de-la-informacion- para-la-institucion-universitaria-colegio-mayor-del-cauca.html?cv=1

Los esperado de dicho proyecto consiste en el mejoramiento interno de la seguridad de la información para la compañía QWERTY SA. estableciendo un control adecuado por medio de manuales, políticas y objetivos, según el análisis detallado de la evaluación de riesgos en la compañía.

PALABRAS CLAVES

Seguridad informática, sistema de seguridad, tecnología, tic's, seguridad de la información, ISO 27001.

ABSTRACT

The Company QWERTY S.A. It is a company in the technology sector that seeks technological development in Colombian communities through the use of Information Technology. It currently has 120 employees, including managers, administrative and operational, who regularly use the information media for data consultation.

The management that is given today to the information relates several aspects of great importance, which are related from the reception of the information in its adequate handling of both physical documents and information stored in a virtual way, to the different systems of information that has the organization or different means of external systems to which we are obliged to inform information.

At present, the false idea that information security is one of the impossible tasks to develop and apply in an underdeveloped country like ours is maintained, but the great reality in this regard is that with the necessary knowledge and clearly with great effort can reach a high level of security, always with the constant support of directives.

As stated above, the main objective is to improve the company's security management system, based on the methodology established in the quality, through the identification of the main problem and the respective research on a field work, is carried out the activities necessary to contribute to the continuous improvement of the company.

The expected of this project is the internal improvement of information security for the company QWERTY SA. establishing adequate control through manuals, policies and objectives, according to the detailed analysis of the risk assessment in the company.

KEYWORDS

Computer security, security system, technology, tic’s, information security, ISO 27001.

TABLA DE CONTENIDO

Pág.

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

En la actualidad existen distintos mecanismos que generan un grado mayor de inseguridad en la información de todas las compañías, la misma se encuentra vulnerable a constantes riesgos por ende se debería emplear un modo de trabajo que permita implementar efectivamente un mayor control sobre la seguridad de la información y activos informáticos que involucre a todo el personal interno y externo de la compañía.

El método más efectivo que permite mayor nivel de seguridad de la información es conocido como un Sistema de Gestión de la Seguridad de la Información[2] y se basa en distintos estándares, modelos y normas las cuales a través de una serie de mejores prácticas aseguran una adecuada gestión de la seguridad de la información. La norma internacional más reconocidas y sobre la cual se basará este trabajo es la ISO/IEC 27001 que establece las guías, procedimientos y procesos para gestionarla apropiadamente mediante un proceso de mejoramiento continuo.

Para el desarrollo efectivo de este proyecto se hace necesario evaluar los riesgos a los que están expuestos los activos informáticos y emplear un enfoque metodológico que permita mitigarlos o mantenerlos a un nivel aceptable, además de establecer un plan de mejoramiento continuo.

El presente proyecto tiene como finalidad diseñar un Sistema de Gestión de la Seguridad de la Información para la empresa caso de estudio QWERTY S.A. mediante un análisis de la situación actual de la compañía identificando los objetivos establecidos que sugiere la norma ISO 27001, la selección de una metodología de evaluación de riesgos informáticos, el establecimiento de una política de seguridad informática institucional que sea liderada por la alta gerencia, además de generar la documentación respectiva para los Planes de Continuidad de Negocio con el fin de mantener y/o restaurar los servicios críticos y el análisis y selección de un modelo

[2] DISEÑAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN MEDIANTE LA NORMA ISO 27001 EN EL INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR CENTRO ZONAL VIRGEN Y TURÍSTICO DE LA REGIONAL BOLÍVAR. [En línea].[Citado Octubre, 2020]. Disponible en: http://stadium.unad.edu.co/preview/UNAD.php?cv=1&url=%2Fbitstream%2F10596%2F6169%2F1%2F4559 3318.pdf

de Gobierno de Tecnología Informática que se ajuste a las necesidades institucionales.[3]

[3] ANALISIS PARA LA IMPLEMENTACION DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION SEGÚN LA NORMA ISO 27001 EN LA EMPRESA SERVIDOC S.A. [En línea].[Citado Julio, 2020 Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/6341/16453917.pdf?sequence=1

1. PLANTEAMIENTO DEL PROBLEMA

1.1. Presentación del problema

La Empresa QWERTY S.A. es una empresa tecnológica que busca el desarrollo en comunidades colombianas a través del uso de Tecnologías de Información. Actualmente cuenta con 120 colaboradores entre directivos, administrativos y operativos, quienes hacen uso de forma regular de los medios de información para consulta de datos Para dar respuesta a este requerimiento tecnológico, el centro de estudios cuenta con una dependencia de sistemas que brinda soporte a la infraestructura tecnológica 24/7.

Actualmente la empresa QWERTY S.A, no cuenta con un Sistema de Gestión de Seguridad de la Información establecido, incurriendo constantemente en actividades importantes que se consideran amenazas permanentes en el manejo de la información de la empresa.

Hoy en día el ministerio de las tecnologías de la información nos brinda grandes herramientas tecnológicas que ayudan a contrarrestar dichas amenazas a la información, herramientas que con un excelente manejo pueden ayudar en gran medida a fortalecer la seguridad de la información en la empresa QWERTY S.A, pero sin un diseño adecuado de un sistema de gestión de la información no se lograra a cabalidad con lo planteado a nivel de seguridad.

La tercerización de los sistemas de información y la falta de control sobre las bases de datos representan para la entidad factores de riesgo que exponen a principales amenazas en el manejo de la información como lo son spam, malware, etc.

Algunos incidentes presentados en la compañía con respecto a la seguridad de la información son los siguientes:

- Perdida a gran cantidad de información almacenada.
- Reconstrucción de Bases de datos por manipulación inadecuada
- Duplicación de datos y archivos

Según lo anterior se evidencia la falta de un sistema de gestión de la información de manera urgente, por lo mismo cabe demostrar el cual responda a las necesidades puntuales de seguridad minimizando los riesgos existentes detectados.

1.2. Formulación del problema

¿Cómo el diseño de un sistema de gestión de seguridad de la información le proveerá a la empresa QWERTY S.A. los lineamientos necesarios para optimizar la seguridad de la información al interior de la empresa?

2. ALCANCE

El presente proyecto comprende la fase de diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI) y no de su implementación.

3. JUSTIFICACIÓN

Un adecuado manejo de la seguridad de la información crea un blindaje a los datos almacenados en la empresa QWERTY S.A, todo lo anterior delimitado bajo un correcto diseño de un sistema de gestión de la información.

Los riesgos que se presentan a diario en el manejo de la información en una empresa están comprendidos desde la perdida de la información más básica, como una carta de reunión hasta la base de datos del cliente más importante para la compañía, involucran perdida de información en un pc hasta amenazas cibernéticas que se pueden manifestar en desconfiguración de los servidores, generando grandes pérdidas para la empresa impactando la operación, generando reportes financieros negativos o dañando la reputación de la empresa en todos sus clientes.

Un sistema de gestión de la seguridad de la información en una organización consiste en un conjunto de procesos que ayuda a organizar y gestionar de forma eficiente la accesibilidad a la información siempre asegurando la confidencialidad e integridad de esta, partiendo de la base en que la información es considerada el activo más importante para toda compañía y por ende la misma debe ser custodiada con integridad y confiablidad, manteniendo siempre su disponibilidad en buen estado cuando sea requerida, Un sistema de gestión de la seguridad de la información – SGSI basado en la norma ISO/IEC 27001 mejorara a gran nivel la seguridad de la información disminuyendo la probabilidad que existan vulnerabilidades y riesgos para la empresa.[4]

La norma ISO/IEC 27001 Se ha convertido en la norma principal a nivel mundial en temas relacionados con seguridad de la información, la misma puede ser implementada en todo tipo de organización4 y está redactada por los mejores especialistas del mundo proporcionando una metodología óptima para implementar la gestión de la seguridad de la información en una organización, su filosofía se basa en la gestión de riesgos, lo cual la hace ideal para el caso estudio planteado

[4] DISEÑAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN MEDIANTE LA NORMA ISO 27001 EN EL INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR CENTRO ZONAL VIRGEN Y TURÍSTICO DE LA REGIONAL BOLÍVAR. [En línea].[Citado Octubre, 2020]. Disponible en: http://stadium.unad.edu.co/preview/UNAD.php?cv=1&url=%2Fbitstream%2F10596%2F6169%2F1%2F4559 3318.pdf

donde el enfoque es investigar donde están los riesgos y luego tratarlos sistemáticamente, por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.

Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, personas, bienes, etc., ISO 27001 ha detallado cómo amalgamar todos estos elementos dentro del sistema de gestión de seguridad de la información (SGSI).

Como propósito final de este trabajo se tiene proyectado diseñar un documento donde se establezca el sistema de gestión de seguridad de la información, previo diseño y autorización de la dirección debe ser implementado según estándares dirigidos por la gerencia de la compañía en cada uno de los sectores y distintas sedes existentes, cada funcionario de la compañía deberá tener pleno conocimiento del sistema de gestión para fortalecer la compañía en ámbitos de seguridad informática.

4. OBJETIVOS

4.1. Objetivo general

Diseñar el sistema de gestión en la seguridad de la información según el estándar ISO 27001 para el caso estudio de la empresa QWERTY S.A., que establezca un control interno de seguridad.

4.2. Objetivos específicos

- Analizar la situación de la compañía QWERTY S.A. con relación a la gestión de la seguridad de la información, identificando los activos de la información de la compañía.

- Realizar el respectivo análisis y evaluación del riesgo según la metodología establecida con anterioridad.

- Establecer un control interno de seguridad de la información por medio de políticas y procedimientos definidos en un manual de sistema de gestión en la seguridad.

5. MARCO REFERENCIAL

5.1. Marco teórico

A continuación, se relacionan los fundamentos principales a tener en cuenta en los cuales se sustenta dicha investigación para el desarrollo del presente proyecto:

5.1.1. Seguridad de la Información

Un SGSI en una organización contempla varios aspectos de gran importancia como lo es el diseño, implantación, mantenimiento de una detallada agrupación de procesos que cumplen como función general gestionar eficientemente la accesibilidad de la información, permitiendo siempre asegurar la confidencialidad, integridad y disponibilidad de los activos de información disminuyendo a la mínima expresión los riesgos de seguridad de la información.

La seguridad de la información relaciona todas aquellas medidas y procedimientos necesarios para proteger la información sin importar el tipo de almacenamiento, se basa en tres factores importantes, los cuales son integridad, confiabilidad y disponibilidad.[5]

La seguridad de la información en una compañía es un proceso de mejora continua que demanda la participación de toda la organización y pretende conservar los principios de la información: [5]

• La **confidencialidad**, asegurando que solo las personas debidamente autorizadas tengan acceso a la información.

• La **disponibilidad**, asegurando que la información esté totalmente disponible para las personas debidamente autorizadas cuando ellos la requieran.

La **integridad**, asegurando que la información no sea modificada sin la debida autorización.

• La **autenticidad**, con el propósito de garantizar la identidad de la persona que genera la información. La autenticidad de la información es la capacidad de

[5] SEGURIDAD DE LA INFORMACIÓN [En línea].[Citado, noviembre, 2020]. Disponible en: https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

asegurar que el emisor de la información es quien dice ser y no un tercero que esté intentando suplantarlo.

• El **no repudio**, con el propósito de conocer exactamente quienes son los actores que participan en una transacción o una comunicación y no puedan negarlo en ningún momento. El no repudio evita que el emisor o el receptor nieguen la transmisión de un mensaje. [6]

• La **trazabilidad**, con el objetivo de poder monitorear o rastrear cualquier operación que se realiza sobre la información desde su mismo origen.

Sistema de información:

Es considerado un conjunto de distintos elementos que se relacionan entre si con la finalidad de procesar, almacenar y transmitir los datos de la compaña, de este modo generar reportes e información confiable y de forma oportuna, en una compañía es de vital importancia que la información sea rápida, veras, de calidad, objetiva y completa.

Todo sistema de información se compone de procedimientos, recursos físicos y humanos.

5.1.2. Magerit 3.0

Metodología empleada para el análisis de riesgos diseñada por el ministerio de administraciones públicas español, donde se reglamentan los pasos para el análisis y gestión del riesgo.[7]

5.1.3. Normas ISO /IEC 27000

La familia de las normas ISO/IEC 27000, son un marco de referencia de seguridad a nivel mundial desarrollado por la International Organization for Standardization - ISO e International Electrotechnical Commission – IEC, que proporcionan un marco, lineamientos y mejores prácticas para la debida gestión de seguridad de la información en cualquier tipo de organización. Estas normas especifican los

---

[6] Wikipedia, Seguridad de la información

[7] METODOLOGIA PARA EVALUAR RIESGOS. [En línea]. [Citado, Julio, 2020] Disponible en: https://colaboracion.dnp.gov.co/CDT/Prensa/Metodologia-para-evaluar-los-riesgos.pdf

requerimientos que deben cumplir las organizaciones para establecer, implementar, poner en funcionamiento, controlar y mejorar continuamente un Sistema de Gestión de Seguridad de la Información.

Las siguientes son algunas de las normas que componen la familia ISO/IEC 27000, las cuales serán el marco teórico que se tendrá en cuenta para efectos del presente trabajo:

Normas ISO 27000

Entre las normas internacionales que relacionan la seguridad informática se conoce como una de vital importancia la ISO/IEC 27000:2016.[6]

En esta norma se establecen varios parámetros que tienen como principal objetivo brindar ayuda a las organizaciones en términos de seguridad de la información. [7]

Normas ISO 27001

La ISO 27001 es una metodología que se basa en la evaluación de riesgos y la implementación de controles que permitan mitigar los riesgos hallados lo cual cumple con la finalidad de mantener asegurada la información con el apoyo de revisiones periódicas.[8]

Amenazas:

los activos de la compañía se encuentran en constantes amenazas con respecto a la seguridad informática presente en la compañía, las amenazas más conocidas en QWERTY S.A son:

- Troyanos
- Spam
- Phising
- Trashing

Algunos objetos informáticos que se requiere tener en cuenta para la investigación son:

- Software de la compañía
- Correo electrónico

[8] **TECNICAS., INSTITUTO COLOMBIANO DE NORMAS.** Tecnología de la información. Técnicas de seguridad de la información (SGSI). Visión general y vocabulario. Bogotá D.C.: ICONTEC, NTC- ISO/IEC 27001:2017.

- Documentación existente ya sea en base de datos, documento físico o digital.
- Toda política diseñada para la seguridad de la información debe contener los siguientes aspectos:
- Objetivos precisos con respecto a la seguridad de la información
- Una vez diseñada es obligatoria su divulgación para su efectivo cumplimiento
- Alta gerencia comprometida con el diseño e implementación de la política en seguridad de la información.
- Es de obligación mantener actualizada dicha política de manera continua.

Tratamiento del Riesgo:

Según la ISO 27001 el plan de tratamiento de riesgos correspondiente a la seguridad de la información se considera la parte más compleja de la implantación de la norma.

El plan de tratamiento de riesgos tiene como finalidad realizar un respectivo control para mitigar el nivel de impacto que puede generar dicho riesgo sobre la información, No todos los riesgos tienen el mismo origen, se debe enfocar en los más importantes, los llamados riesgos no aceptables.[9]

En el tratamiento del riesgo se pueden tomar 4 medidas diferentes:

- Aceptación del riesgo.
- Rechazo del riesgo.
- Transferencia del riesgo.
- Mitigación del riesgo.

Si la empresa no toma una decisión, equivale a la aceptación del riesgo. El tratamiento dentro del Proceso de Gestión de Riesgos trata de conducirlo a un nivel aceptable aplicando alguna de estas medidas. [10]

[9] SGSI. [En línea]. Disponible en: https://www.pmg-ssi.com/2017/05/iso-27001-plan-de-tratamiento-de- riesgos-de-seguridad-de-la-información/

[10]Tratamiento de riesgos [En línea]. Disponible en: https://www.ealde.es/tratamiento-del-riesgo-iso-31000/

5.2. Marco legal

5.2.1. Ley estatutaria 1581. de 2012

Entró en vigor la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.[11] Esta ley es de vital importancia para el proyecto ya que para mantener el debido proceder de la documentación es necesario mantener la protección de datos personales que se manejan en la compañía.

5.2.2. Ley 33 de 1987 y la ley 565 del 2000

Ratifican las obligaciones internacionales para la protección del software como objeto del Derecho de Autor. A partir de lo anterior, el Estado Colombiano, cumple con lo establecido en el TODA y en el Convenio de Berna, en su normativa.[12], Esta ley es la base fundamental de reglamentación en el proyecto ya cumple con la misión de la compañía en el diseño de software, por ende, se debe respetar en totalidad el derecho de autor en toda la seguridad de la información.

5.2.3. Decreto 1360 de 1989

"Por el cual se reglamenta la inscripción del soporte lógico (software en el Registro Nacional del Derecho de Autor)", incorporó el concepto del software en la normativa colombiana.[13]

5.3. Marco contextual

QWERTY S.A es una empresa colombiana con más de 36 años de experiencia ofreciendo Soluciones de Tercerización de Procesos de Negocio BPO (Business ProcessOutsourcing) y Soluciones Tecnológicas de Información (IT Information Technology) en los distintos sectores de servicio.

---

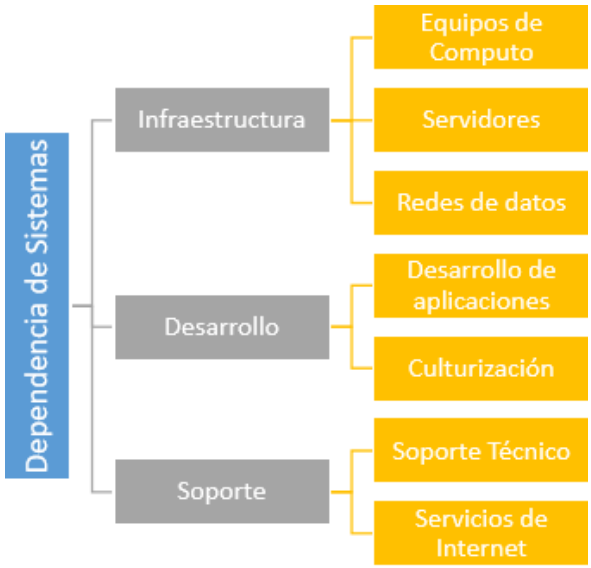
[11] ALCALDIA MAYOR DE BOGOTA, ley 1581 de 2012, Régimen Legal de Bogotá, (octubre 17 de 2020) Colombia

[12] UNIVERSIDAD EXTERNADO DE COLOMBIA, Departamento de propiedad intelectual [En línea]. Disponible en: https://propintel.uexternado.edu.co/la-proteccion-del-software-desde-la-propiedad-intelectual-en- colombia-conveniencia-de-la-creacion-de-una-normativa-especial-que-garantice-los-derechos-de-los- desarrolladores/

[13] UNIVERSIDAD EXTERNADO DE COLOMBIA, Departamento de propiedad intelectual [En línea]. Disponible en: https://propintel.uexternado.edu.co/la-proteccion-del-software-desde-la-propiedad-intelectual-en- colombia-conveniencia-de-la-creacion-de-una-normativa-especial-que-garantice-los-derechos-de-los- desarrolladores/

A continuación, se presenta la figura 1. Organigrama dependencia sistemas QWERTY SAS, en la cual se ostenta los departamentos involucrados en la dependencia se sistemas, los cuales son los directamente involucrados de generar los estándares básicos sobre seguridad informática.

Figura. 1. Organigrama dependencia sistemas QWERTY S.A.S.



Fuente: guía actividad seminario UNAD

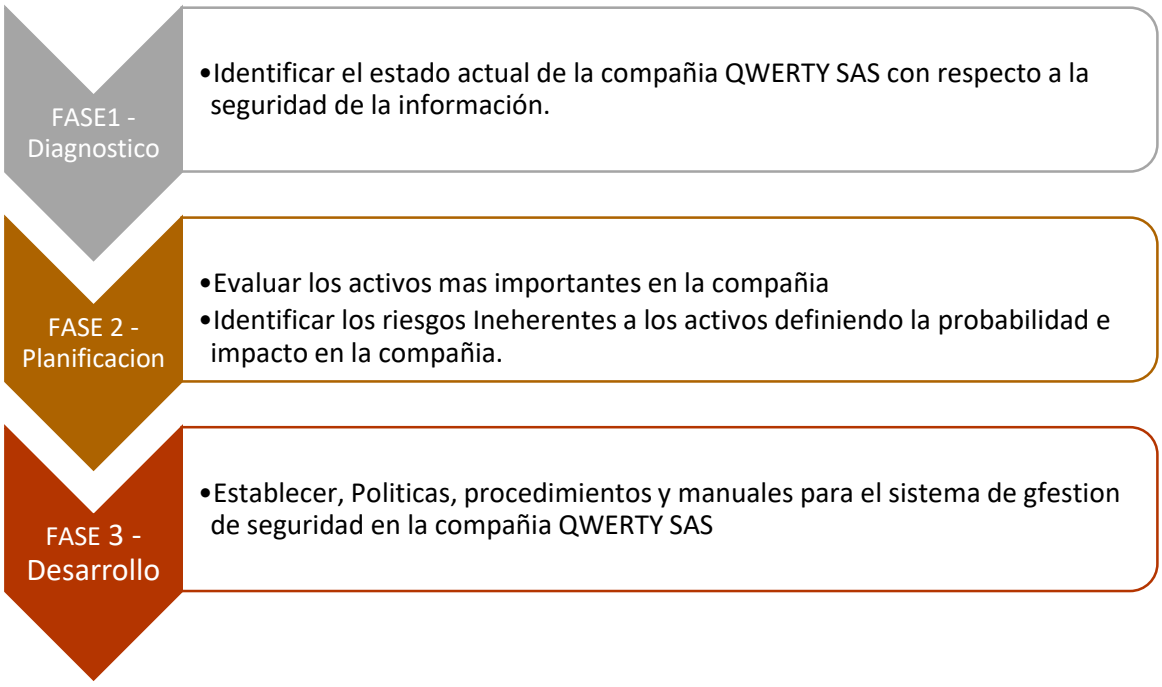
6. DISEÑO METODOLÓGICO

En el presente capitulo se definen las fases para llevar a cabo el desarrollo del presente proyecto DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SEGÚN EL ESTÁNDAR ISO 27001 PARA EL CASO ESTUDIO DE LA EMPRESA QWERTY S.A. teniendo en cuenta los objetivos planteados y el alcance al cual se quiere llegar.

En este tipo de investigación, la información de interés es recogida de forma directa de la fuente, mediante encuestas, cuestionario, entrevista o reuniones.

Según los requerimientos que se definen en la norma ISO/IEC 27001:2013 para el diseño del Sistema de Gestión de Seguridad de la Información, se definen 3 fases para el desarrollo del proyecto estipuladas en la Figura 2.

Figura. 2. Fases Desarrollo del proyecto



Fuente: Propia

7. RESULTADOS

Para el presente proyecto se tendrá como base de implementación el ciclo PHVA, donde se realizará el diagnostico respectivo de la compañía para determinar actividades susceptibles de mejora, posterior a ello se realizará el análisis de riesgos para poder efectuar las mejoras requeridas bajo un plan de tratamiento de riesgos, dando como resultado final se presenta el manual de seguridad bajo un periodo de prueba donde se estudiarán los resultados obtenidos con el fin de mantener la mejora continua en los procesos.

7.1. Diagnóstico y análisis de la compañía

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

La situación actual en QWERTY S.A. en materia de seguridad informática está asociada básicamente a que:

- QWERTY 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.

Para dar solución a la problemática presentada por el caso de estudio para la empresa QWERTY S.A., se llevará a cabo un análisis de la compañía con relación a la seguridad de la información, identificando inicialmente los activos de la información para posterior a ello realizar el análisis de riesgos.

A partir del análisis de riesgos se establecerá un control interno de la seguridad de la información como producto a entregar, la metodología a emplear para el análisis de riesgos a tomar como guía es la Metodología de análisis y gestión de riesgos de los sistemas de información MAGERIT.

7.1.1. Inventario de Activos

El Departamento de Sistemas cuenta con distintos activos de la información los cuales se asignan a distintos cargos y en ocasiones a otras dependencias, la distribución de estos se presenta a continuación en la Tabla 1. Inventario de activos compañía QWERTY S.A.

Tabla 1. Inventario de activos compañía QWERTY S.A

Activo	Descripción	ubicación	Cantidad
Servidor de impresión	Equipo de cómputo que conecta dos impresoras: Destinadas a:	Oficina de sistemas	1
Servidor marca dell en torre	Una (1) Impresora HP LaserJet Enterprise serie 600, activo que brinda el servicio para la dependencia de nómina y facturación. Permite la concurrencia de hasta 25 usuarios y el volumen mensual de impresión es de 200 a 25000 páginas	Oficina de nómina y facturación	1
PowerEdge T440	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	Dependencia directiva y administrativa	1
Servidor de archivos FTP: Servidor marca dell en torre PowerEdge T130	Equipo de cómputo que tiene como función el almacenamiento y la administración de los archivos que se están generando en el interior de la organización como son: Digitalización de documento de entrada y de salida, audios generados en reuniones, asambleas y otro tipo de encuentros, video, generados por 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 del plan máximo	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

Tabla 1. (Continuación)

Activo	Descripción	ubicación	Cantidad
Servidor de nómina y facturación Servidor marca dell en torre PowerEdge T440 Características de servidor Apache 2.4.25 PHP 5.6.30 - 7.1.1 MySQL 5.7.17 phpMyAdmin 4.6.6	Plataforma de desarrollo propio. Tiene como función el almacenamiento y la administración de la nómina y facturación de la empresa QWERTY S.A.		2
Servidor DHCP Servidor marca dell en torre PowerEdge T440	Servidor que asigna y administra de forma dinámica el direccionamiento dentro de la organización		2
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

Tabla 1. (Continuación)

Activo	Descripción	ubicación	Cantidad
Técnicos de mantenimiento	Personal técnico encargado de realizar el mantenimiento preventivo a los equipos de computo	Departamento de sistemas	2
Teléfonos IP	Sistema de comunicación a través de teléfonos Voz IP, que comunica las oficinas y departamentos del centro.	Dependencias del centro	6
Puntos de acceso	Puntos de acceso al servicio de internet en el campus universitario	Departamento de sistemas	2

Fuente propia

Las actividades para desarrollar tomando como guía la metodología serán:

- Realizar la respectiva valoración de amenazas y vulnerabilidades para cada activo identificado.
- Definir los riesgos principales de seguridad en la información.
- Construir la matriz de riesgos.
- Diseñar el plan de tratamiento y gestión de riesgos de seguridad de la información.

Valoración de las amenazas

Para determinar el nivel de impacto de las amenazas e indicar el nivel de daño posible en los activos de la información existentes en la compañía, se diseña la tabla 2. Medición de la degradación de amenazas con la finalidad de dar un valor a la ocurrencia de un fenómeno.

Tabla 2. Medición de la degradación de amenazas

MA	100%	Muy alta	Daño muy grave
A	75%	Alta	Daño grave
MA	50%	Media	Daño importante
B	25%	Baja	Daño menor
MB	1%	Muy Baja	Daño despreciable

Fuente: propia

7.2. Evaluación y tratamiento de riesgos de seguridad

La evaluación y tratamiento de riesgos es considerado según la ISO 27001 una parte fundamental en todo sistema de gestión de la seguridad de la información, con base en ello se presenta a continuación, la tabla 3. Donde se establecen los riesgos de seguridad a los cuales están expuestos día a día los activos de la compañía.

Tabla 3. Riesgos de seguridad

ACTIVO DE INFORMACIÓN SELECCIONADO	RIESGOS DE SEGURIDAD
Código fuente	R1 - Pérdida parcial de información provocado por la falta de actualización de software.
	R2 - No disponibilidad de la información en el momento necesario provocado por deficiencias en los controles de acceso.
Gestión documental	R3 - Pérdida de información en gestión documental, como consecuencia del mal manejo de protocolos de seguridad en la web.
	R4 - Perdida de confidencialidad de la información como consecuencia en la falta de Biométrico en la compañía.
	R5 - mala reputación con el cliente debí al incumplimiento de acuerdos debido a la indisponibilidad de la información
Servidores	R6 - Divulgación de información confidencial a terceros, debido a La configuración de la red de comunicaciones.
	R7 - Perdida de información en la compañía como consecuencia de malas prácticas al no realizar BackUp de la inf.
Equipos	R8 - Deterioro del equipo de cómputo, como consecuencia de espacio donde no se cumplen condiciones de climatización optimas
Antivirus	R9 - Pérdida de información como consecuencia de un pobre seguimiento a las actualizaciones o estado del antivirus
	R10 - Daño de hardware provocado desactualización de los antivirus.

Tabla 3. (Continuación)

Activo De Información Seleccionado	Riesgos De Seguridad
Talento humano	R11 - información insuficiente 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.

Fuente: Encuesta compañía QWERTY S.A.

7.2.1. Valoración de los riesgos

La principal medida para realizar la valoración de riesgos corresponde a un análisis de los hallazgos determinados anteriormente donde se identifica cada una de las situaciones que pueden afectar la seguridad de la información, la probabilidad de ocurrencia se determinara según la tabla 4. Donde se indica el valor de ocurrencia a emplear según la probabilidad asignada por hallazgo.

Tabla 4. Valoración de la probabilidad

Probabilidad	Frecuencia De Ocurrencia	Valor
Muy Bajo	Por lo menos una vez cada año	1
Bajo	Por lo menos una vez cada semestre	2
Medio	Por lo menos una vez cada trimestre	3
Alto	Por lo menos una vez cada mes	4
Muy Alto	Por lo menos una vez cada quince días	5

Fuente: propia

La valoración de los riesgos en términos de probabilidad e impacto de ocurrencia se obtiene según la siguiente ecuación.

$$Riesgo\ Inherente = \text{Probabilidad} * \text{Impacto}$$

Se considera un riesgo inherente a todo riesgo existente de manera intrínseca en el desarrollo común de una actividad, dicho riesgo no se puede eliminar por lo tanto se debe identificar en el plan de gestión de la compañía.

Una vez identificado el riesgo se analiza la probabilidad de ocurrencia y su nivel de impacto, así se determina el debido actuar dando prioridad siempre a todo riesgo identificado como alto o crítico, en la tabla 5. Se observa la relación probabilidad-impacto para identificar el nivel del riesgo inherente identificado.

Tabla 5. Riesgo Inherente

Probabilidad	**Impacto**				
	Muy Bajo	**Bajo**	**Medio**	**Alto**	**Muy Alto**
Muy Bajo	Muy bajo	Muy bajo	Bajo	Bajo	Medio
Bajo	Muy bajo	Bajo	Medio	Medio	Alto
Medio	Bajo	Medio	Medio	Alto	Alto
Alto	Bajo	Medio	Alto	Critico	Critico
Muy Alto	Medio	Alto	Alto	Critico	Critico

Fuente: propia

Una vez identificado el nivel de impacto del riesgo inherente se asigna una valoración para cada nivel de impacto y probabilidad, siendo 1 el nivel muy bajo y 5 el nivel muy alto, seguido a ello se aplica la fórmula de riesgo inherente para signar la respectiva valoración como se indica en la tabla 6.

Tabla 6. Valoración de riesgos probabilidad vs impacto

Probabilidad	**Impacto**				
	Muy Bajo (1)	**Bajo (2)**	**Medio (3)**	**Alto (4)**	**Muy Alto (5)**
Muy Bajo (1)	1	2	3	4	5
Bajo (2)	2	4	6	8	10
Medio (3)	3	6	9	12	15
Alto (4)	4	8	12	16	20
Muy Alto (5)	5	10	15	20	25

Fuente: propia

Al identificar la valoración de riesgos probabilidad vs impacto en la tabla 6, se procede a crear la calificación de riesgos asignando una valoración cada rango, lo anterior se identifica en la tabla 7.

Tabla 7. Calificación valoración de riesgos

Valoración Del Riesgo	Calificación
Muy bajo	1 – 2
Bajo	3 - 4
Medio	5 - 9
Alto	10 - 15
Critico	16 - 25

Fuente: propia

Según lo establecido en la tabla 6 y tabla 7 se asigna una valoración de probabilidad, impacto, calificación y nivel de riesgo a todos los riesgos de seguridad identificados, en la tabla 8, se observa la valoración de riesgos para la empresa QWERTY.

Tabla 8. Valoración de los riesgos en QWERTY S.A

Activo De Información Seleccionado	Riesgos De Seguridad	Valoración Del Riesgo			
		PROBABILIDAD	IMPACTO	CALIFICACIÓN	NIVEL DE RIESGO
Código fuente	R1 - Pérdida parcial de información provocado por la falta de actualización de software.	4	3	12	Alto
	R2 - No disponibilidad de la información en el momento necesario provocado por deficiencias en los controles de acceso.	2	5	10	Alto
Gestión documental	R3 - Pérdida de información en gestión documental, como consecuencia del mal manejo de protocolos de seguridad en la web.	2	4	8	Medio
	R4 - Perdida de confidencialidad de la información como consecuencia en la falta de Biométrico en la compañía.	2	4	8	Medio

Tabla 8. (Continuación)

Activo De Información Seleccionado	Riesgos De Seguridad	Valoración Del Riesgo			
		PROBABILIDAD	IMPACTO	CALIFICACIÓN	NIVEL DE RIESGO
	R5 - mala reputación con el cliente debí al incumplimiento de acuerdos debido a la indisponibilidad de la información	2	4	8	Medio
Servidores	R6 - Divulgación de información confidencial a terceros, debido a La configuración de la red de comunicaciones.	4	3	12	Alto
	R7 - Perdida de información en la compañía como consecuencia de malas prácticas al no realizar BackUp de la inf.	2	3	6	Medio
Equipos	R8 - Deterioro del equipo de cómputo, como consecuencia de espacio donde no se cumplen condiciones de climatización óptimas.	2	5	10	Alto
Antivirus	R9 - Pérdida de información como consecuencia de un pobre seguimiento a las actualizaciones o estado del antivirus	3	4	12	Alto
	R10 -Daño de hardware provocado desactualización de los antivirus.	2	3	6	Medio
Talento humano	R11 - información insuficiente 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.	3	5	15	Alto

Fuente: propia

Una vez asignada la valoración a los riesgos existente en QWERTY, se determina el mapa de calor, el cual cumple con la finalidad de identificar la cantidad de riesgos identificados en la tabla 8 por cada nivel de impacto, en la tabla 9 se observa la cantidad de riesgos encontrados.

Tabla 9. Mapa de calor

PROBABILIDAD	IMPACTO				
	Muy Bajo (1)	**Bajo (2)**	**Medio (3)**	**Alto (4)**	**Muy Alto (5)**
Muy Bajo (1)					
Bajo (2)			2	3	2
Medio (3)				2	1
Alto (4)			2		
Muy Alto (5)					

Fuente: propia

En la tabla 9, se define la cantidad de riesgos encontrados por probabilidad de impacto para determinar el mapa de calor de riesgos en la compañía, en la tabla 10 se relacionan en cada nivel de impacto el riesgo asignado según estudio.

Tabla 10. Mapa de calor riesgos

PROBABILIDAD	IMPACTO				
	Muy Bajo (1)	**Bajo (2)**	**Medio (3)**	**Alto (4)**	**Muy Alto (5)**
Muy Bajo (1)					
Bajo (2)			R10, R7	R3, R4, R5	R2, R8
Medio (3)				R7, R9	R11
Alto (4)			R1, R6		
Muy Alto (5)					

Fuente: propia

7.2.2. Estrategia de tratamiento de riesgos

Según la metodología MAGERIT, el paso a seguir consiste en el plan de tratamiento de riesgos relacionados con los activos de la información establecidos, como primera medida se debe establecer ciertas estrategias que mitiguen los riesgos hallados.

Acorde a lo anterior se establece en la tabla 11, la estrategia de tratamiento de riesgos para la compañía QWERTY S.A, indicando una pequeña descripción a cada estrategia.

Tabla 11. Estrategia de tratamiento

ESTRATEGIA DE TRATAMIENTO DEL RIESGO	DESCRIPCIÓN
Evitar	Relaciona la cancelación de toda aquella actividad que pueda causar el riesgo.
Reducir	indica la creación e implementación de planes de acción, que ayuden con la mitigación del riesgo.
Transferir	Hace relación a solucionar por medio de terceros el riesgo encontrado
Aceptar	No se implementará ninguna acción ya que el riesgo no genera mayor impacto.

Fuente: propia

Control interno de seguridad de la información

Una vez establecidas las estrategias del plan de tratamiento de riesgos se determinan los planes de acción para cada riesgo identificando, generando un control de riesgo para cada una.

7.2.3. Plan de tratamiento de riesgos

El plan de tratamiento de riesgos presentado en la tabla 12, hace referencia a las acciones que se definen con el fin de reducir los riesgos de Seguridad en la información para aquellos riesgos que superan el nivel aceptable de la compañía.

El resultado del plan corresponde al producto de la probabilidad de ocurrencia por el impacto que podrían ocasionar las amenazas por el aprovechamiento de las vulnerabilidades en los sistemas de seguridad de la información en la compañía.

Tabla 12. Plan de tratamiento de riesgos

	Caracterización del riesgo		**Afectación**			**Plan de tratamiento**			
ACTIVO DE INFORMACIÓN SELECCIONADO	**RIESGOS DE SEGURIDAD**	**NIVEL DE RIESGO**	**Confidencialidad**	**Disponibilidad**	**Integridad**	**estrategia de tratamiento de riesgos**	**Identificación del control**	**Descripción plan de acción**	**Responsable**
Código fuente	R1 - Pérdida parcial de información provocada por la falta de actualización de software.	Alto		D		Reducir el riesgo	CR1	Definir dentro de la política de seguridad de la información un procedimiento que garantice este proceso.	Jefe TI

Tabla 12. (Continuación)

	Caracterización del riesgo		Afectación			Plan de tratamiento			
ACTIVO DE INFORMACIÓN SELECCIONADO	**RIESGOS DE SEGURIDAD**	**NIVEL DE RIESGO**	**Confidencialidad**	**Disponibilidad**	**Integridad**	**estrategia de tratamiento de riesgos**	**Identificación del control**	**Descripción plan de acción**	**Responsable**
Código fuente	R2 - No disponibilidad de la información en el momento necesario provocado por deficiencias en los controles de acceso.	Alto		D		Reducir el riesgo	CR2	Clasificar la información de la compañía en confidencial y publica, con el fin de establecer criterios en el control de acceso.	Jefe TI
							CR3	Establecer una persona responsable de la custodia de la información determinando el Adecuado control de acceso	
Gestión documental	R3 - Pérdida de información en gestión documental, como consecuencia del mal manejo de protocolos de seguridad en la web.	Medio		D	I	Reducir el riesgo	CR4	Adquirir un software seguro que garantice la confidencialidad de la información.	Jefe TI
							CR5	Obtener el certificado SSL	Director compañía

Tabla 12. (Continuación)

	Caracterización del riesgo		Afectación			Plan de tratamiento			
ACTIVO DE INFORMACIÓN SELECCIONADO	**RIESGOS DE SEGURIDAD**	**NIVEL DE RIESGO**	**Confidencialidad**	**Disponibilidad**	**Integridad**	**estrategia de tratamiento de riesgos**	**Identificación del control**	**Descripción plan de acción**	**Responsable**
Gestión documental	R4 - Perdida de confidencialidad de la información como consecuencia en la falta de Biométrico en la compañía.	Medio		D		Reducir el riesgo	CR6	Establecer el proceso biométrico para el ingreso a la compañía	Jefe TI
	R5 - mala reputación con el cliente debido al incumplimiento de acuerdos debido a la indisponibilidad de la información.	Medio			I	Reducir el riesgo	CR5	Generar espacios de capacitación al personal de la compañía con respecto a la importancia en la seguridad de la información.	Jefe RRHH Y

Tabla 12. (Continuación)

	Caracterización del riesgo		Afectación			Plan de tratamiento			
ACTIVO DE INFORMACIÓN SELECCIONADO	**RIESGOS DE SEGURIDAD**	**NIVEL DE RIESGO**	**Confidencialidad**	**Disponibilidad**	**Integridad**	**estrategia de tratamiento de riesgos**	**Identificación del control**	**Descripción plan de acción**	**Responsable**
Servidores	R6 - Divulgación de información confidencial a terceros, debido a La configuración de la red de comunicaciones.	Alto	C			Reducir el riesgo	CR5	Generar espacios de capacitación al personal de la compañía con respecto a la importancia en la seguridad de la información.	Jefe TI
	R7 - Perdida de información en la compañía como consecuencia de malas prácticas al no realizar BackUp de la inf.	Alto		D		Reducir el riesgo	CR7	Definir dentro de la política de seguridad de la información un procedimiento que garantice este proceso.	Jefe TI

Tabla 12. (Continuación)

ACTIVO DE INFORMACIÓN SELECCIONADO	RIESGOS DE SEGURIDAD	NIVEL DE RIESGO	Confidencialidad	Disponibilidad	Integridad	estrategia de tratamiento de riesgos	Identificación del control	Descripción plan de acción	Responsable
Equipos	R8 - Deterioro del equipo de cómputo, como consecuencia de espacio donde no se cumplen condiciones de climatización óptimas.	Alto		D	I	Reducir el riesgo	CR8	Diseñar e implementar un método que se componga de un aire acondicionado que permita un espacio con condiciones climáticas optimas	Jefe TI
Antivirus	R9 - Pérdida de información como consecuencia de un pobre seguimiento a las actualizaciones o estado del antivirus.	Alto		D	I	Reducir el riesgo	CR9	Adquirir un software seguro que garantice la confidencialidad de la información.	Jefe TI
							CR10	Establecer un control por medio de cronograma que establezca un día fijo de actualización de software en la compañía	Jefe TI

Tabla 12. (Continuación)

	Caracterización del riesgo		Afectación			Plan de tratamiento			
ACTIVO DE INFORMACIÓN SELECCIONADO	**RIESGOS DE SEGURIDAD**	**NIVEL DE RIESGO**	**Confidencialidad**	**Disponibilidad**	**Integridad**	**estrategia de tratamiento de riesgos**	**Identificación del control**	**Descripción plan de acción**	**Responsable**
Antivirus	R10 - Daño de hardware provocado desactualización de los antivirus.	Medio			I	Reducir el riesgo	CR11	Usar únicamente software licenciados que garanticen el adecuado uso de los sistemas en el proceso de actualización de servidores.	Jefe TI
Talento humano	R11 - información insuficiente 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.	Alto	C	D	I	Reducir el riesgo	CR12	Diseñar un parámetro que contenga este ítem en la política de seguridad de la compañía.	Jefe TI
							CR13	Generar espacios de capacitación al personal de la compañía con respecto a la importancia en la seguridad de la información.	Jefe RRHH Y Jefe TI

Fuente: propia

7.2.4. Informe de evaluación de los riesgos

En la evaluación de riesgos se identificaron 11 riesgos en total, 7 de ellos con clasificación alta y 4 con clasificación media, detallados en la Tabla 12. Plan de tratamiento de riesgos, de estos 7 riesgos identificados con afectación alta observamos que 2 de ellos tienen afectación muy alta, los cuales puede llegar a reflejar un impacto importante de afectación en la compañía, de este modo se debe enfocar un tratamiento de riesgos adecuado principalmente en ellos y minimizar su afectación.

Los riesgos identificados de alto impacto afectan en primera instancia la confidencialidad de la compañía, por lo cual se dio especial atención a este ítem, pues es considerado un pilar fundamental para la seguridad de la información en la compañía QWERTY SAS.

Se establecen planes de acción recurrentes en el plan de tratamiento de riesgos con el fin de minimizar su nivel de impacto, de este modo se mantener un adecuado control sobre su efecto, teniendo en cuenta que dichos riesgos son inminentes y no desaparecerán.

7.3. Control interno de seguridad de la información

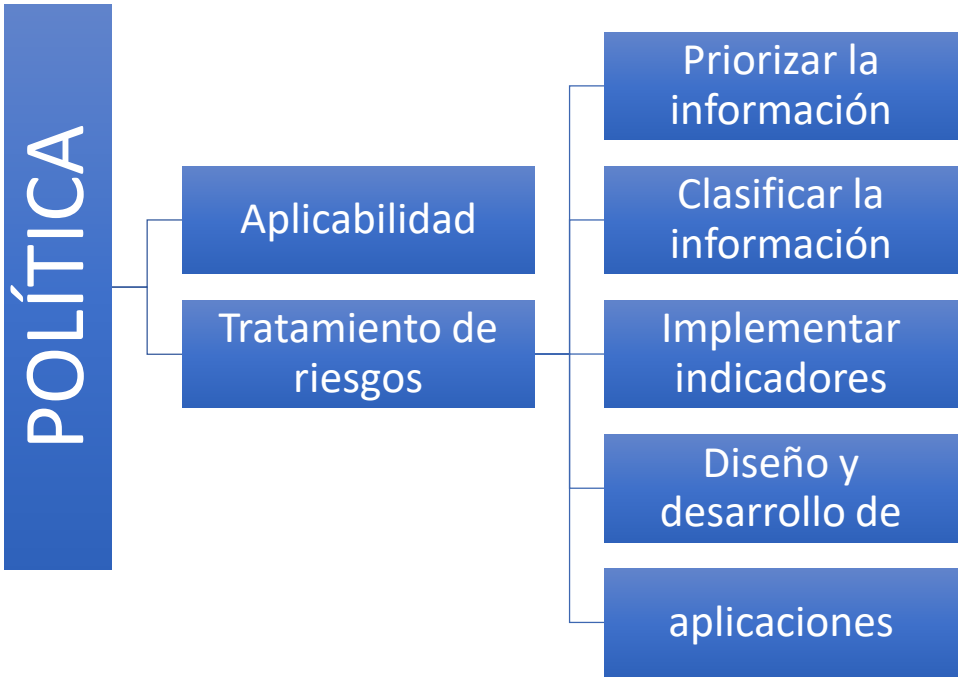
7.3.1. Alcance del SGSI

El Sistema de gestión de la seguridad informática aplica a la compañía en general, es decir todo aquel que tena un vínculo laboral con QWERTY SAS firmado por un contrato establecido, aplica para todas las dependencias desde las áreas directivas, administrativas, hasta las operativas de QWERTY SAS, adicional a lo anterior se hace especial énfasis en el alcance que tiene en terceros vinculados a la compañía con el fin de tercerizar procesos fijos en la compañía.

7.3.2. Estructura del SGSI

A continuación, en la figura 3 se establecen las dependencias y componentes necesarios para cumplir a cabalidad el SGSI, dando prioridad a la política finalizando en los procedimientos necesarios para el correcto cumplimiento de la política.

Figura. 3. Estructura SGSI - QWERTY S.A



Fuente: propia

Objetivos

- Establecer buenas prácticas para el manejo de la información, que brinde una seguridad de la información óptima.
- Garantizar la confidencialidad, disponibilidad e integridad de la información dentro y fuera de la compañía.
- Instaurar el alcance definitivo para el Sistema de Gestión en la seguridad de la información.

Definición de roles y responsabilidades de seguridad

Todos los funcionarios de la compañía QWERTY SAS son responsables de la seguridad de la información de la compañía, adicional al compromiso anterior

algunos roles cuentan con responsabilidades especificas adicionales en el SGSI como lo son:

1. **Responsable del funcionamiento del SGSI**

La persona designada de velar por el correcto funcionamiento del SGSI en QWERTY SAS es el Ingeniero de sistemas a cargo del área, sus principales funciones son:

- Garantizar la disponibilidad total de los recursos requeridos por los funcionarios para la definición, la implementación y el mantenimiento del SGSI.
- Definir los parámetros mínimos necesarios que den guía al oficial de seguridad de la información.
- Asegurar el adecuado seguimiento a la implementación y el cumplimiento de los controles de seguridad
- Apoyar a los funcionarios y contratistas para que cumplan con las responsabilidades de su rol frente al SGSI.

2. **Propietario de los activos de información**

Todo funcionario perteneciente a la compañía QWERTY SAS el cual tenga bajo su responsabilidad algún activo de información tendrá las siguientes funciones:

- Identificar, definir y evaluar los riesgos a los que pudieran estar expuestos los activos de información de los cuales es propietario.
- Definir los requerimientos de seguridad de los activos de información en relación con su confidencialidad, integridad y disponibilidad.
- Efectuar una verificación periódica de la correcta ejecución de los controles requeridos sobre los activos de información bajo su responsabilidad.

3. **Usuario de la información**

Hace referencia a todo funcionario activo de QWERTY SAS que utiliza la información de la compañía para desempeñar sus funciones cargo, sus responsabilidades son:

- Conocer la clasificación de los activos de información que maneja.
- No divulgar la información clasificada sin autorización del propietario del activo de información.

- Utilizar los activos de información exclusivamente para el desempeño de sus funciones y obligaciones dentro y fuera de la compañía.

4. Guardia de los activos de información

Es todo funcionario de QWERTY SAS responsable de administrar y hacer efectivos los controles que el propietario del activo de información haya definido, sus responsabilidades son:

- Administrar los recursos donde residen los activos de información dando los permisos definidos por el propietario del activo a los usuarios interesados.

- Implementar y mantener los controles requeridos en los contenedores donde estén almacenados los activos de información que se encuentren a su cargo.

Medidas de seguridad de Información

- Analizar y controlar los riesgos hallados con respecto a la seguridad de la información con la finalidad de mantener un nivel óptimo en la compañía.

- Mantener la integridad de toda la documentación existente en la compañía.

- Todos los servidores de la compañía deben cumplir la reglamentación especificada en el manual de seguridad.

- La confidencialidad de la información es vital ante los clientes con respecto a los planes de desarrollo.

- Suplir todas las necesidades de todas las partes interesadas.

Principios de seguridad de información

En la compañía QWERTY S.A., se toma la decisión de afrontar algunos riesgos que según estudios previos son comprensibles y manejable con un respectivo control y un adecuado tratamiento, lo anterior se puede identificar en la política de SGSI donde se estableció el tratamiento de riesgos para cada uno de los existentes.

Todo el personal de la compañía tendrá a disponibilidad dicha política previa socialización de esta donde se explicará todo lo relevante para el desarrollo de sus funciones.

Se harán disponibles informes regulares con información de la situación de la seguridad.

Se realizará un respectivo control regular a todos los riesgos hallados o por hallar con la finalidad de tomar medidas optimas a tiempo y se mantenga el riesgo bajo control o en un nivel de riesgo bajo.

Bajo ningún motivo se permite la infracción de las normas y leyes establecidas, no será tolerable dicha infracción.

Responsabilidades

El equipo directivo será el directamente responsable de garantizar que la seguridad de la información se gestione de una forma adecuada en toda la compañía.

Cada responsable de área será responsable de garantizar bajo su mando mantengan un adecuado control sobre la información de acuerdo con todas las normas establecidas.

Todo el personal tanto administrativo como operativo de la compañía tiene la responsabilidad de mantener control sobre la seguridad de la información de toda la compañía y brindar un adecuado manejo.

7.3.3. Manual de políticas de seguridad de la información

El presente manual describe la política de seguridad de la información diseñada para a compañía QWERTY SAS, para su elaboración se tiene como fundamento los requisitos identificados en el estándar ISO/IEC 27001.

Código: **Versión: 1** **Fecha:** **Página: 1 de 19**	**MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	**QWERTY S.A**

Contenido

1. INTRODUCCIÓN

QWERTY S.A identifica la seguridad de la información como un pilar fundamental en el desarrollo óptimo de los objetivos principales de la compañía, razón por la cual se crea dicho manual para establecer la forma en la cual la información será manejada, procesada y almacenada.

En este documento se describe las políticas y procedimientos necesarios para la correcta seguridad de la información en la compañía QWERTY S.A.

Las políticas incluidas en este manual se constituyen como parte fundamental del sistema de gestión de seguridad de la información y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

La seguridad de la información es una prioridad para QWERTY S.A, por tanto, es responsabilidad de todos velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas.

2. OBJETIVO

El presente documento tiene como finalidad establecer las políticas en seguridad de la información para la compañía QWERTY S.A, de este modo se prevé regular la gestión de la seguridad de la información al interior de la entidad.

3. ALCANCE

Las políticas de seguridad de la información cubren todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios y terceros que laboren o tengan relación laboral en QWERT S.A, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

4. DEFINICONES

Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Control: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye policías, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Incidente de Seguridad: es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, la consecuencia, el número de veces ocurrido o el origen (interno o externo).

Propietario de la información: es la unidad organizacional o proceso donde se crean los activos de información.

SGSI: Sistema de Gestión de Seguridad de la Información.

Vulnerabilidades: son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por el instituto (amenazas), las cuales se constituyen en fuentes de riesgo.

Guías de clasificación de la información: directrices para catalogar la información de la entidad y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer diferencias entre las

medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información.

5. POLITICA DE SEGURIDAD DE LA INFORMACIÓN

Alcance

Aplica a todas las dependencias de la empresa QWERTY SAS y sus procesos internos sus recursos a la totalidad de procesos internos y tercerizados vinculados a través de acuerdos o contratos y todo el personal con contratación directa que utilicen o afectan las condiciones de calidad de la información.

Objetivos

- Proteger tanto la información de la empresa QWERTY SAS, como los activos utilizados para su procesamiento, almacenamiento y acceso con el fin de asegurar que la información se mantiene integra, disponible y es confiable para la toma de decisiones.

- Definir las directrices de la empresa QWERTY SAS para la valoración, análisis y evaluación de riesgos de seguridad de la información con el fin de garantizar continuidad e integridad de los sistemas de información.

- Establecer responsabilidades en la administración de los activos de información.

Responsabilidades

- **La junta directiva de la empresa QWERTY SAS**: dan aprobación a esta política y son los únicos responsables de autorizar cualquier modificación a la misma.

- **Los propietarios de los activos:** Son responsables de establecer y documentar la clasificación de la información y de establecer los permisos de acceso de acuerdo a funciones y competencia de los usuarios de la organización.

- **El área de soporte:** Es responsable de cumplir las funciones asignadas en los procedimientos que dan soporte a la política de seguridad como son la administración de usuarios, actividades operativas asignadas al SGSI.

- **El área de infraestructura:** Debe garantizar el cumplimiento de los procedimientos que dan soporte a la implementación de controles de la infraestructura que incluye equipos, redes, cableado, equipos activos y su configuración.

- **El área de desarrollo:** debe garantizar la ejecución de prácticas seguras de desarrollo de software y segur las pautas establecidas para el de control de cambios.

- **Los usuarios de la información:** son responsables de conocer y cumplir la política de seguridad de información vigente en cuanto a Manejo de usuario y contraseñas, Uso adecuado de los activos y acatar las normas establecidas para asegurar la confidencialidad de la información a la que tiene acceso.

- **Jefe dependencia de Nomina:** tiene como responsabilidad Notificar a todo empleado que se vincula a la empresa QWERTY SAS la política de seguridad de la información, suscribir los acuerdos de confidencialidad, desarrollar plan de capacitación continua a cerca de la seguridad y asegurar que se cumplan de los procedimientos de selección y desvinculación definidos en el SGSI.

- **Jefe de compras:** Hacer la divulgación de la política de seguridad para proveedores, Suscribir los acuerdos de confidencialidad con proveedores que requieren información de QWERTY SAS para realizar la actividad para la que son contratados.

- **El gestor de Proyectos con comunidades:** debe seguir las buenas prácticas de seguridad de la información en la definición e implementación de proyectos para las comunidades.

- **Área de soporte:** Mantener actualizados los sistemas operativos de los equipos, asegurando que en la medida que estos pierdan soporte del fabricante se debe planificar y asegurar la renovación con la debida anticipación.

- Garantizar que los usuarios no tienen permisos de administrador del equipo que les permita instalar software o cambiar parámetros del sistema.

Es responsabilidad de los usuarios atender las siguientes obligaciones:

- No Instale Software desconocido sin la aprobación de dependencia de sistemas.

- No cambie los parámetros del sistema operativo sin el visto bueno de la dependencia de tecnología.

- Todo software, paquete, programa, aplicación que se instale en la compañía por cuenta propia y cause errores en el sistema, será responsabilidad del usuario.

- Si se presentan comportamientos inusuales en sus archivos o en las memorias USB o en el equipo de cómputo asignado debe informar al área de soporte para su análisis y diagnóstico.

Generalidades

Control de acceso

- El acceso a la infraestructura de QWERTY SAS para personal externo debe ser autorizado al menos por un director de QWERTY SAS, quien deberá notificarlo a la Dirección de la dependencia de sistema quien cuenta con la discreción para autorizar su habilitación.

- Todo el personal es responsable del el IDusuario y contraseña que recibe para el uso y acceso de los recursos, el cual es único e intransferible, por lo que está prohibido compartirlo con otras personas.

- Está prohibido proporcionar información a personal externo, de los mecanismos de control de acceso de QWERTY SAS

- La utilización de dispositivos extraíbles para almacenamiento de información (memorias USB, CD R/RW, DVD R/RW, discos duros extraíbles.) debe ser autorizado por el director y supervisado por la Dirección de Tecnología.

Dispositivos removibles

- Los puertos USB de los equipos de la compañía están restringidos para los usuarios y solo serán habilitados con la debida justificación de la necesidad de su uso, en cuyo caso se deben atender las siguientes indicaciones:

- No Abrir Memorias USB en el equipo sin examinarla con el antivirus.

- Evite conectar memorias USB de personas ajenas a la compañía sin antes consultar con el área de soporte para evitar propagación de virus por este medio.

- No conecte dispositivos diferentes a los autorizados por la dependencia de sistemas y para los que fueron habilitados los puertos USB a los equipos bajo su responsabilidad.

6. POLÍTICA DE SEGURIDAD PARA PROVEEDORES

Objetivo

Establecer las directrices frente a la seguridad de la información aplicable a Proveedores de la Empresa QWERTY SAS, para evitar la pérdida o usos indebidos de información que como consecuencia pueda dañar la reputación de la organización o afectar su funcionamiento.

Alcance

Esta política aplica a todas las actividades realizadas por quien preste servicios como proveedor a QWERTY SAS, independientemente del tipo de servicio que preste.

Responsabilidades

- **Prestación del servicio**

Todo proveedor, ya sea persona natural o jurídica, que realice labores para QWERTY SAS debe cumplir con las normas establecidas en este documento.

Los proveedores deben asegurar que todo su personal tiene la formación y capacitación apropiada para el desarrollo del servicio prestado, tanto para lo que fue contratado como en el manejo confidencial de la información que se le entrega para realizar su labor y es su responsabilidad garantizar que siguen las directrices definidas para gestión de usuarios y contraseñas de la política de seguridad informática de QWEERTY SAS.

Es responsabilidad del proveedor informar cualquier cambio en el personal de su organización que afecte el servicio que presta a QWEERTY SAS

- **Confidencialidad de la información**

La información de QWERTY SAS se debe considerar por defecto, tiene el carácter de confidencial, con excepción de aquella que se encuentra en medios masivos de difusión, o que expresamente así lo defina QWERTY SAS.

Salvo autorización expresa de QWWERTY SAS los proveedores deben mantener confidencialidad de la información a la que tiene acceso de forma indefinida.

Los proveedores sólo tendrán acceso datos de carácter personal cuando sea necesario para el desempeño de su labor, de los cuales se debe asegurar que se guarda la debida confidencialidad y una vez terminada la labor deben devolver los archivos y destruir cualquier medio lógico de la misma que tengan en su poder.

En el tratamiento de datos de carácter personal fuera de las instalaciones de QWERTY SAS, debe garantizarse por parte del proveedor el nivel de seguridad apropiado al tipo de archivo.

- **Propiedad Intelectual**

Para garantizar el cumplimiento de las normas de propiedad intelectual está estrictamente prohibido el uso de software en los sistemas de información de QWERTY SAS sin la correspondiente licencia.

También está prohibido el uso, reproducción, transformación o comunicación de cualquier tipo de obra protegida por la propiedad intelectual sin la debida autorización de quien tenga los derechos de propiedad intelectual.

- **Intercambio de Información**

En el intercambio (Transmisión o recepción) de información entre las partes, se considerarán no autorizadas los siguientes tipos de archivos y por lo tanto generan sanciones a los proveedores que las permitan en su personal:

- Material protegido por las leyes de Protección Intelectual sin la debida autorización.
- Material pornográfico, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
- Envío de archivos a terceras partes de información de la organización sin la debida autorización de QWERTY SAS.
- Archivos que infrinjan la normativa de protección de datos de carácter personal.
- Software o aplicativos no relacionadas con el negocio.

- **Utilización de los recursos**

Los recursos que QWERTY SAS pone a disposición del proveedor deben ser utilizados exclusivamente para el cumplimiento de las obligaciones para la que le fueron proporcionados, estos recursos son objeto de auditoria y se aplicaran los mecanismos de control que se requieran para validar su utilización dentro de lo acordado.

Para que un equipo de cómputo del proveedor sea conectado a la red de QWERTY SAS deberán estar homologados (sistemas operativos, Antivirus), debidamente licenciados y le aplican las políticas de restricción de navegación a través del servicio de internet de la Organización.

Está prohibido Introducir voluntariamente en la red de QWERTY SAS o de sus clientes cualquier tipo de malware.

Está prohibido Intentar acceder sin la debida autorización a áreas restringidas de procesamiento de información, cuando esto se permita debe quedar registrado en bitácora de acceso fecha, hora identificación y motivo del acceso.

Está prohibido distorsionar o falsear tanto la información de QWERTY SAS a la que tienen acceso como los registros de auditoria de los Sistemas de Información de QWERTY SAS.

7. POLITICA MANTENIMIENTO Y DESARROLLO DE APLICACIONES

Objetivo

Definir y ejecutar tareas con el propósito de brindar a los usuarios a través del Software herramientas de trabajo funcionales que garanticen, automaticen y agilicen la operatividad de sus labores.

Alcance

Este procedimiento inicia desde la solicitud de mantenimiento y/o creación de aplicaciones de software hasta su implementación y seguimiento.

Responsabilidades

- **Director Dependencia de Sistemas**

  Responsable de evaluar la posibilidad del mantenimiento y desarrollo del software dado el requerimiento de las áreas de la organización, Generar planes de trabajo, revisar su ejecución y generar acciones para su cumplimiento. Validar cumplimiento de cronogramas y definir prioridades en actividades de desarrollo.

- **Ingeniero de desarrollo**
  Responsable del mantenimiento del Software, es decir, de escribir código fuente, realizar pruebas de escritorio y generar los archivos ejecutables. Reportar cronograma y seguimiento de actividades a la dirección de sistemas, realizar la actividad de codificación de software observando las condiciones de seguridad de la información.

- **Analista Tester**
  Encargado de definir y ejecutar pruebas funcionalidad y de seguridad de las aplicaciones desarrolladas a partir del requerimiento de desarrollo y la lista de chequeo definida para validar la seguridad de las aplicaciones.

Generalidades

Términos y condiciones

- **Software**

Es un conjunto de instrucciones compiladas que dependiendo de la secuencia de las mismas y los parámetros ingresados procesa datos para generar un resultado, son utilizados para Simplificar procesamiento de información. En esta clasificación encontramos los sistemas operativos, utilitarios, antivirus, aplicaciones específicas, ERP, malware, virus troyanos y toda suerte de elementos que pueden alterar afectar los datos.

- **Programas Fuente**

Para el caso de QWERTY SAS todo el Software Operativo a excepción de la Nómina, la Contabilidad y los inventarios, son desarrollos propios, es decir los aplicativos son escritos y mantenidos por personal de QWERTY SAS. Las fuentes, son archivos escritos en un lenguaje de programación que contienen toda la funcionalidad de los aplicativos.

- **Solicitudes**

En términos generales los usuarios generan una necesidad de mantenimiento o desarrollo de nuevas aplicaciones de Software que puede convertirse en una corrección puntual de un ejecutable, la modificación de un listado o reporte, un nuevo reporte, una nueva opción dentro del sistema, un módulo nuevo, una nueva funcionalidad y hasta un nuevo aplicativo. Estas necesidades se generan a través de un e-mail o una solicitud escrita.

Las solicitudes de desarrollo deben contener como mínimo la siguiente información: Alcance, Propósito, descripción detallada de la funcionalidad, Usuarios y permisos sobre la funcionalidad, Definición de términos que requieran explicación para facilitar el entendimiento de la descripción Funcional.

- **Arquitectura de la solución y Desarrollo**

A partir de la solicitud aprobada por el director de sistemas El ingeniero de desarrollo debe definir y documentar diseño de la solución teniendo en cuenta: Funcionalidad, capacidades de los recursos de procesamiento y condiciones de seguridad de la información, en caso de estimar que los recursos de procesamiento no son suficientes debe informar a la dirección de sistemas antes de continuar con el desarrollo.

Una vez presentado el diseño y aprobado por la dirección de sistemas se debe proceder con la codificación del aplicativo.

- **Pruebas de Desarrollo**

A partir del requerimiento del usuario y del diseño definido por el Ingeniero de desarrollo el Tester debe construir la lista de chequeo para las pruebas de funcionalidad, con respecto a las pruebas de seguridad de la aplicación debe aplicar la lista de chequeo de seguridad de las aplicaciones definidas para esta validación

- **Ambiente de Pruebas**

Para la realización de las pruebas se cuenta con una base de datos que debe contener la información necesaria para realizar las pruebas del software, los ingenieros de desarrollo deben entregar los scripts para la creación de objetos a que haya lugar y el Tester debe probar que estos funcionen correctamente y a partir de los objetos generados realizar la aplicación de las pruebas.

Todo software desarrollado de forma externa debe pasar por el mismo procedimiento de pruebas a cargo del Tester antes de su aceptación y despliegue en producción.

- **Custodia Archivos Fuente**

Solamente los ingenieros de desarrollo tienen acceso para modificación de los archivos fuente, de los cuales se debe realizar copia de seguridad a diario por parte del área de soporte.

8. POLÍTICA CONTROL DE ACCESO

Objetivos

Establecer directrices para el manejo de contraseñas y administración de privilegios para evitar el acceso no autorizado a los sistemas de información de QWERTY SAS.

Alcance

Aplica a todos los medios utilizados por los usuarios para acceder a la información de la organización QWERTY SAS.

Responsabilidades

- **Administración de Privilegios**
  Cada propietario de la información debe establecer los niveles de acceso a la información y basado en esta definición el área de soporte asignara los perfiles a los usuarios asignados.

  Cualquier cambio en las funciones del usuario o de área que implique modificar el perfil del usuario con respecto a las aplicaciones de QWERTY SAS, deberán ser notificados al área de soporte para realizar los cambios respectivos.

  Cuando un empleado se retire de la organización este evento debe ser notificado para la deshabilitar el su usuario de Red, Correo y usuario de aplicaciones.

- **Equipo Desatendido**
  Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como password y protectores de pantalla cuando se retiren de su puesto de trabajo.

- **Administración de usuario y password**
  La asignación de permisos será solicitada por el jefe directo del usuario y una vez validado con los niveles de acceso definidos por los propietarios de la información será asignado por el área de soporte.

  Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.

  Todos los usuarios deberán observar los siguientes lineamientos para la construcción de sus contraseñas:

  - Debe estar compuestos de al menos 6 caracteres alfanuméricos
  - No deben ser iguales al usuario
  - No deben relacionarse con el trabajo o la vida personal del usuario
  - No debe ser igual a las tres contraseñas anteriormente definidas.

No está permitido compartir usuario y contraseña con otros empleados, es único e intransferible, cualquier acción realizada por otros es responsabilidad de quien tiene asignado este usuario y clave.

9. POLITICA CLASIFICACIÓN DE LA INFORMACIÓN

Objetivo

Identificar y clasificar adecuadamente la información de la organización QWERTY SAS, para reducir la afectación negativa de la seguridad de la información por un tratamiento no apropiado

Alcance

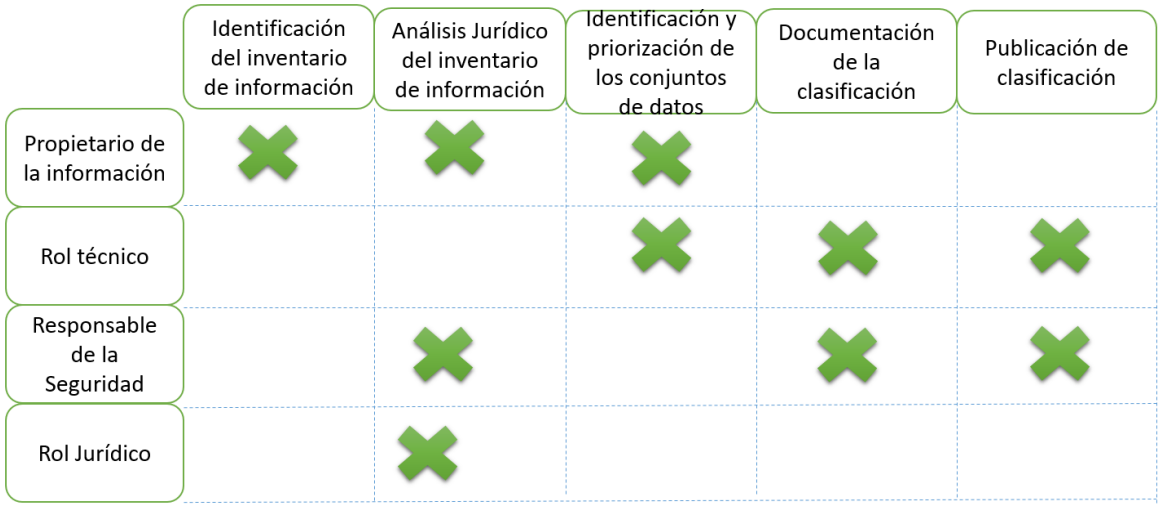
Aplica al 100% de los activos de información para las actividades de identificación, clasificación en función de su confidencialidad y mecanismo de etiquetado.

Los medios en que se encuentra la información objeto de esta clasificación son: Documentos electrónicos, bases de datos, documentos impresos, información verbal.

Responsabilidades

En la figura 4, se ilustra de manera global el cuadro de roles frente a las actividades de identificación de la información.

Figura. 4. Roles y Responsabilidades



Fuente: propia

- **Identificación de la información:**
  La revisión del inventario se debe realizar una vez al año para mantenerlo actualizado según reglamentación interna de la compañía.

  Para el registro de este inventario se debe utilizar el formato referenciado en la tabla 13.

Tabla 13. Formato registro inventario

ID	ÁREA	DESCRIPCIÓN	TIPO	UBICACIÓN	CLASIFICACIÓN	CRITICIDAD	PROPIETARIO
			• Impreso • Electrónico • B.datos		Nivel de confidencialidad	• Alta • Media • Baja	

Fuente propia

- **Clasificación de la información**

Para la clasificación de la información se debe tener en cuenta los niveles de codificación referenciados en la tabla 14, los cuales están alineados según lo establecido en la ley 1712 de 2014.

Tabla 14. Tipos de información

Tipo	Descripción
Publica Reservada	Disponible solo para un proceso o área de la organización, en caso de ser conocida por terceros puede generar impacto negativo a la reputación de la organización o de tipo legal por condiciones contractuales
Publica Clasificada	Información disponible únicamente los procesos internos de la organización, que en caso de ser conocida por personas externas a la organización puede afectar de forma negativa a los procesos o perder ventajas competitivas del negocio
Publica	Información que puede ser entregada o publicada si restricciones dentro o fuera de la organización sin que perjudique los procesos, la reputación o la competitividad de la organización
No Clasificada	Activos de información que se deben incluir en el inventario y que aún no han sido clasificados, deben ser tratados como PUBLICA RESERVADA hasta que asigne la clasificación definitiva

Fuente propia

10. PROCEDIMIENTO GESTIÓN DE INCIDENTES

Objetivo

Definir el procedimiento para asegurar el reporte, la recopilación y análisis de los incidentes para mantener la mejora continua del sistema de gestión de seguridad de la información de QWERTY SAS.

Alcance

Este procedimiento aplica a todos los empleados que por sus funciones tienen acceso a los sistemas de información de la compañía.

Responsabilidades

- **Usuarios**

Deben reportar toda anomalía o comportamiento fuera de lo norma que identifiquen en el sistema de información.

- **Área de soporte**

Registrar todo evento que sea reportado por los usuarios, tomar las medidas del caso, consolidar y reportar los casos al responsable de seguridad de la información.

- **Responsable de seguridad**

Debe analizar los casos, identificar las vulnerabilidades o causas del incidente y proponer las acciones a seguir.

- **Desarrollo Notificación y registro**
  - Se incluirán en el registro de incidentes todas aquellas anomalías reportadas por los usuarios que afecten o puedan afectar a la seguridad de los datos.
  - Cuando el área de soporte identifique una vulnerabilidad o debilidad en el sistema también debe incluirlo en el reporte de incidentes.
  - El reporte debe contener como mínimo la siguiente información:

Tabla 15. Información reporte

Fecha de la notificación.	
Usuario que hace el reporte.	
Descripción detallada del incidente o debilidad.	
Fecha y hora en que se presentó el incidente.	
Acciones iniciales realizadas.	

Fuente propia

- . **Gestión y tratamiento**

Con la información recopilada se debe iniciar la identificación de posibles causas y los efectos producidos por la situación presentada.

El responsable de seguridad debe evaluar si la acción inicialmente tomada por soporte es suficiente correctivo o si se deben tomar otras acciones, luego determinar las acciones preventivas para evitar la repetición del incidente o la reducción de la vulnerabilidad.

Una vez tomadas las acciones tanto correctivas como preventivas deben temer seguimiento para determinar su efectividad.

.

CONCLUSIONES

- Una vez analizada la situación de la compañía se concluye que el Sistema de Gestión de Seguridad de la Información diseñado se ajusta de acuerdo a las necesidades de la compañía QWERTY SAS; lo cual permite cumplir a cabalidad el propósito inicial, contar con un sistema de gestión de las seguridad de la información que permita tener un mejor control del sistema, un adecuado y oportuno manejo los riesgos de afectación de la información en términos de la disponibilidad, integridad y autenticidad de su información.

- Con el desarrollo de este proyecto, se logró Identificar los riesgos principales de afectación alta en materia de Gestión de Seguridad de la Información, lo anterior permitió diseñar una propuesta de tratamiento a realizar para cada riesgo, los controles adecuados para su mitigación y el plan de tratamiento asociados a cada control.

- la implementación de controles, procedimientos y políticas diseñados para la compañía QWERTY SAS permitirán que minimicen el riesgo a los que puedan estar expuestos sus activos de información. Por lo tanto al implementar un SGSI en la compañía permitirá alcanzar la certificación ISO 27001:2013 exigido contractualmente para la celebración de contratos con distintos clientes.

RECOMENDACIONES

Para la compañía QWERTY SAS, es recomendable en términos de seguridad de la información realizar auditorías internas de forma constante en una periodicidad no máxima de tres meses al año, lo anterior con la finalidad de llevar un control oportuno a las políticas de seguridad de la información contempladas en el Manual de seguridad establecido en el presente proyecto, siguiendo el protocolo de mejora continua es correspondiente realizar capacitaciones a todo el personal en periodos constantes para infundir el correcto actuar del personal de la compañía en el manejo de la información, al realizan capacitaciones mensuales al personal de la compañía donde se indique y se enseñe el correcto actuar de la seguridad de la información se creará una cultura segura que disminuirá de forma notable los riesgos de nivel alto.

El esquema de Seguridad de la Información plantado en este trabajo necesita actualización y retroalimentación constante, de lo contrario no se vera la mejora continua de forma correcta a riesgos futuros, ya que no evolucionará de la mano del crecimiento que tenga la compañía QWERTY SAS, el éxito en la implementación de este modelo planteado depende del apoyo de la Alta Gerencia y de todas las áreas en general de la compañia ya que serán las encargadas de su difusión y acatamiento en general.

Se espera que a futuro se desarrollen otros proyectos basados en el que aquí se presenta planteando la posibilidad de mantener la conciencia de implementar y mantener el ciclo de vida del sistema de gestión de seguridad de la información planteado para la compañía, permitiendo detectar amenazas o debilidades a tiempo generadas día a día por el crecimiento de la compañía o por los avances tecnológicos.

BIBLIOGRAFÍA

1. ALVAREZ BASALDÚA, L. D., "Tesis Seguridad en Informática (Auditoría de Sistemas)". {en línea} {consultado marzo 2021} disponible en: http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

2. ISO 27001 / 27002. (s.f.). {en línea} {consultado en marzo de 2021} disponible en: http://www.pmg-ssi.com/2016/06/la-norma-iso-27002-complemento-para-la- iso27001/

3. NTC-ISO/IEC 27001. (2013). "ISO 27001: Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. Bogotá Colombia: Icontec". {en línea}. {consultado en marzo de 2021}. disponible en: https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISOIEC27001.pdf

4. 27001 ACADEMY ¿Qué es norma ISO 27001? [En línea]. {consultado en Abril de 2021}.Disponible en: https://advisera.com/27001academy/es/que-es-iso-27001/

5. ESCRIVÁ R., G.G., S.R.M., && Ramada, D.J. (2013). "Seguridad Informática". {En línea}. {Consultado en marzo de 2021}. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10820 9 63&pOO=

6. ROMERO, R. M., & Ramada, D. (2013). Seguridad Informática. Madrid: Macmillan Iberia S.A.

7. SISTEMA DE INFORMACIÓN. "Tipos de Información". {en línea} {Consultada en marzo de 2021}. Disponible en: https://www.gestiopolis.com/los-tipos-desistemas-de-informacion-en-las-empresas/

8. TARAZONA., CESAR .H.. "Amenazas informáticas y seguridad de la información". {en línea}. Consultada en marzo de 2021}. Disponible en: http://revistas.uexternado.edu.co/index.php/derpen/article/view/965

9. Flores-Ruiz, E., Miranda-Novales, M. G., & Villasís-Keever, M. Á. (2017). El protocolo de investigación VI: cómo elegir la prueba estadística adecuada. Estadística inferencial. Revista
Alergia De México, 64(3), 365-369. Recuperado de

10. http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=a9h&AN=1 25899428&lang=es&site=eds-live

11. ALVAREZ BASALDÚA, L. D., "Tesis Seguridad en Informática (Auditoría de Sistemas)". {en línea} {consultado marzo 2021} disponible en: http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

12. Roa, B. J. F. (2013). Seguridad informática. Madrid, ES: McGraw-Hill España. (pag.4-5). Recuperado de: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10692 4 60&p00=seguridad+informatica

13. Escrivá, G. G., Romero, S. R. M., & Ramada, D. J. (2013). Seguridad informática. Madrid, ES: Macmillan Iberia, S.A. 2-5 . Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10820 9 63&p00=seguridad+informatica

14. Borda Pérez, M. (2013). El proceso de investigación : visión general de su desarrollo. 1-79. Barranquilla, Colombia: Universidad del Norte. (pag.16–27). Recuperado de http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login . aspx?direct=true&db=nlebk&AN=710213&lang=es&site=eds-live&ebv=EB&ppid=pp_79

15. Ferreyro, A., & Longhi, A. L. D. (2014). Metodología de la investigación. Córdoba, Argentina: Encuentro Grupo Editor. (pag. 15-34) Recuoerado de http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login . aspx?direct=true&db=nlebk&AN=847674&lang=es&site=eds-live

16. Borda Pérez, M. (2013). El proceso de investigación : visión general de su desarrollo. (pag.80-186). Barranquilla, Colombia: Universidad del Norte. Recuperado de: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login . aspx?direct=true&db=nlebk&AN=710213&lang=es&site=eds-live&ebv=EB&ppid=pp_79

17. Baena, Paz, Guillermina María Eugenia. (2014). Metodología de la investigación, Grupo Editorial Patria. ProQuest Ebook Central. (pag.72-78) Recuperado de https://bibliotecavirtual.unad.edu.co:2538/lib/unadsp/detail.action?docID=3228 4 23

18. Borda Pérez, M. (2013). El proceso de investigación: visión general de su desarrollo. (pag.80-89). Barranquilla, Colombia: Universidad del Norte. Recuperado de http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=710213&lang=es&site=eds-live&scope=site.

19. Baena, Paz, Guillermina María Eugenia. (2014). Metodología de la investigación, Grupo Editorial Patria. ProQuest Ebook Central. (pag.74–82). Recuperado de https://bibliotecavirtual.unad.edu.co:2538/lib/unadsp/detail.action?docID=3228423.

20. Puerta Aponte, G. (26,11,2018). Trabajo de Grado NTC 1486. [Archivo de video]. Recuperado de http://hdl.handle.net/10596/23728

21. Generalidades de la informática, [En línea], disponible en: https://sites.google.com/site/navegadorteleinformatico/navegadorteleinformatico

22. MARTOS, Fernando. Centros Hospitalarios de Alta Resolución de Andalucía-Auxiliares Administrativos. Primer Edición. España.2006. 195 p. Recuperado de: https://books.google.com.co/books?id=SmwP1cZdI4cC&pg=PA195&dq=LA+METODOLOG%C3%8DA+MAGERIT+3.0&hl=es&sa=X&ved=0ahUKEwiK5d7u_KTJAhUJWCYKHadoB14Q6AEIJTAC#v=onepage&q=LA%20METODOLOG%C3%8DA%20MAGERIT%203.0&f=falsE

23. ISO 27001 / 27002. (s.f.). {en línea} {consultado en marzo de 2020} disponible en: http://www.pmg-ssi.com/2016/06/la-norma-iso-27002-complemento-para-la- iso27001/

24. NTC-ISO/IEC 27001. (2013). "ISO 27001: Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. Bogotá Colombia: Icontec". {en línea}. {consultado en marzo de 2019}. disponible en: https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISOIEC27001.pdf

25. ROMERO, R. M., & Ramada, D. (2013). Seguridad Informática. Madrid: Macmillan Iberia S.A.

26. POVEDA, José. Análisis y valoración de los riesgos-Metodologías. Artículo. Bogotá D.C.: Universidad Católica de Colombia. Programa de Ingeniería de

Sistema, 2013. 63 p. Recuperado de: https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-8.pdf

27. Norma y leyes que existen en Colombia para delitos informáticos, [en línea], disponible en: https://es.slideshare.net/santiagocisneros6/normas-y-leyes-que-existen-en-colombia-para-delitos-informaticos.

28. Seguridad para todos {consultado en marzo de 2021}. disponible en: Recuperado de: http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html

29. Díaz, Flor Nancy. Principales Estándares para la Seguridad de la Información IT. Investigación. Madrid-España, Universidad Pontificia de Salamanca. 2015. 83 p. Recuperado de: http://documents.mx/documents/rfc-2196-principalesestandares-para-la-seguridad-informacion-it.html

30. INSTITUTO COLOMBIANO DE NORMALIZACIÒN Y CERTIFICACIÒN. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. NTC-ISO-IEC 27001. Bogotá.: El Instituto, 2013. 37 p. 9

31. GONZALEZ, Frank. Diagnóstico y Actualización del Sistema de Gestión de Seguridad de la Información (SGSI) para Ventas y Servicios S.A. Trabajo de grado para Ingeniero de Sistemas. Bogotá D.C.: Universidad Católica de Colombia. Programa de Ingeniería de Sistema, 2013. 63 p.

32. AGUILERA, Purificación. Seguridad Informática: Ciclos Formativos. México: Editex, 2010, p.9. 33

33. SEGUNDA COHORTE DEL DOCTORADO EN SEGURIDAD ESTRATÉGICA. Seguridad de la Información. En: Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica, 2014, No. 1, p 15-16

34. ORGANIZACIÓN INTERNACIONAL PARA LA ESTANDARIZACIÓN. Sistema de Gestión de la Seguridad de la Información. ISO/IEC 27001. España.: El instituto, 2013. 14 p. 19Ibid., p. 3.

35. AGUIRRE CARDONA, Juan David y ARISTIZABAL BETANCOURT, Catalina: Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda. Pereira, 2013, 23 P. Trabajo de grado (Ingenieros de Sistemas). Universidad Tecnológica de Pereira. Facultad de Ingenierías. Programa de Ingeniería de Sistemas y Computación.

36. INSTITUTO COLOMBIANO DE NORMALIZACIÒN Y CERTIFICACIÒN. Gobierno Corporativo de la Tecnología de la Información. Norma Técnica NTC-ISO-IEC 38500. Bogotá.: El Instituto, 2009. 10 p. Recuperado de: http://tienda.icontec.org/brief/NTC-ISO-IEC38500.pdf

37. DE FREITAS, Vidalina. Análisis y Evaluación del Riesgo de la información: Caso de Estudio Universidad Simón Bolívar. Articulo como opción de grado de Magister en Ingeniería de Sistemas. Venezuela.: Revista Venezolana de Información, Tecnología y Conocimiento, 2009. 55 p.

38. AGUILERA, Purificación. Seguridad Informática: Ciclos Formativos. México: Editex, 2010. 9 p.

39. MARTOS, Fernando. Centros Hospitalarios de Alta Resolución de AndalucíaAuxiliares Administrativos. 1 ed. España: Mad-eduforma, 2006. 195 p.

40. Lanzan pólizas de seguros para amparar ataques informáticos. En: PORTAFOLIO. Bogotá, D.C.23, Agosto, 2015, 2. Sec. p.5

41. SEGUNDA COHORTE DEL DOCTORADO EN SEGURIDAD ESTRATÉGICA. Seguridad de la Información. En: Marzo, 2014, No. 1, p 15-16

42. INSTITUTO COLOMBIANO DE NORMALIZACIÒN Y CERTIFICACIÒN. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. NTC-ISO-IEC 27001. Bogotá, D.C.: El Instituto, 2013. 37 p.

43. INSTITUTO COLOMBIANO DE NORMALIZACIÒN Y CERTIFICACIÒN. Tecnología de la información. Técnicas de seguridad. Código de Práctica para la gestión de la Seguridad de la Información. Requisitos. NTC-ISO-IEC 27002. Bogotá, D.C..: El Instituto, 2013. 37 p.

44. MINISTERIO DEL INTERIOR Y DE JUSTICIA. Dirección nacional de derecho de autor. Unidad administrativa especial. Manual de Derecho de Autor. Bogotá, D.C.: El ministerio, 2010. 9 p.

45. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Formato e implementación de políticas de seguridad y privacidad de la información. Bogotá, D.C.: El ministerio, 2014. 19 p.

46. ORGANIZACIÓN INTERNACIONAL PARA LA ESTANDARIZACIÓN. Sistema de Gestión de la Seguridad de la Información. ISO/IEC 27001. España.: El instituto, 2013. 14 p.

47. AREVALO, Oscar William. Metodología de Análisis de Riesgo de la Empresa la

Casa de las Baterías S.A de C.V Trabajo de Grado. El Salvador: Universidad Tecnológica del Salvador. Facultad de Ingeniería. Desarrollo de Redes, 2009. 27 p.

48. DIAZ, Flor Nancy. Principales Estándares para la Seguridad de la Información IT. Investigación. España.: Universidad Pontificia de Salamanca, 2015. 83 p.