DISEÑO DEL SISTEMA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA QWERTY S.A.

EDWIN ANDERSON VARGAS HERNÁNDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2020

DISEÑO DEL SISTEMA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA QWERTY S.A.

EDWIN ANDERSON VARGAS HERNÁNDEZ

Proyecto de Grado Aplicado con Enfoque Directivo – Administrativo
presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Ingeniera YENNY STELLA NUÑEZ ÁLVAREZ
Tutora de Curso
Ingeniero ALEXANDER LARRAHONDO
Asesor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2020

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá, 29 de diciembre de 2020

DEDICATORIA

Dedico este trabajo, a Dios por permitirme realizar este gran paso para mi vida y a mi familia por su apoyo incondicional durante mi formación académica.

AGRADECIMIENTOS

Ofrezco mi más respetuoso y sincero agradecimiento a la Universidad Nacional Abierta y a Distancia (UNAD), quien abrió sus puertas para ofrecerme una oportunidad de ingresar y especializarme en una de las mejores profesiones que hay a nivel mundial, acreditándonos como orgullosos Especialistas en Seguridad Informática egresados de este valioso Plantel Educativo; Aunado a ello, agradezco al personal docente de la Universidad, por habernos apoyado y otorgado su valioso conocimiento y experiencias para consolidar nuestra labor profesional que vamos a aplicar en para servir a nuestra sociedad y al progreso de nuestro país.

Por último, agradezco a todas las personas quienes nos apoyaron en este proyecto y confiaron en nuestras aptitudes para que éste se desarrollara a feliz término.

CONTENIDO

pág.

INTRODUCCIÓN **17**
1. DEFINICIÓN DEL PROBLEMA **18**
1.1 ANTECEDENTES DEL PROBLEMA **18**
1.2 FORMULACIÓN DEL PROBLEMA **18**
2 JUSTIFICACIÓN **19**
3 OBJETIVOS **20**
3.1 OBJETIVOS GENERAL **20**
3.2 OBJETIVOS ESPECÍFICOS **20**
4 MARCO REFERNCIAL **21**
4.1 MARCO conceptual **21**
4.1.1 Seguridad Informática. 21
4.1.2 Seguridad de la información. 21
4.1.3 Sistema de Gestión de Seguridad de la Información 21
4.2 MARCO teórico **22**
4.2.1 Análisis de riesgos. 22
4.2.2 Probabilidad de amenaza. 24
4.2.3 Magnitud del daño. 24
4.2.4 ISO/IEC 27000. 25
4.2.5 Ciclo de mejora continua. 27
4.3 ANTECEDENTES **28**
4.3.1 Estado actual. 28
4.4 MARCO CIENTÍFICO O TECNOLÓGICO **32**
4.4.1 Metodología de análisis de riesgos por *Magerit*. 32
4.5 MARCO LEGAL **37**
5 DISEÑO METODOLÓGICO **39**
5.1 Tipo de investigación **39**
5.1.1 Investigación Descriptiva. 39
5.2.2 Recolección de Información. 39
6 DESARROLLO DE LOS OBJETIVOS **40**
6.1 DESARROLLO DE OBJETIVO 1 ..... **40**
6.1.1 Diagnóstico de situación del problema. 40
6.1.2 Indicadores del problema. 40

6.2 DESARROLLO DE OBJETVO 2 41
6.2.1 Formulación de requerimientos. 41
6.3 DESARROLLO DE OBJETIVO 3 42
6.3.1 Elección de metodología para realizar la gestión de riesgos. 42
6.3.2 Análisis de implementación de los controles de la ISO 27001 en QWERTY S.A. 42
6.3.3 Identificación de activos de información. 44
6.3.3.1 Activos primarios. 48
6.3.3.2 Activos de soporte. 48
6.3.3.3 Caracterización de activos. 50
6.3.4 Valoración de activos. 53
6.3.4.1 Valoración cualitativa. 56
6.3.4.2 Valoración cuantitativa. 64
6.3.5 Enfoque de evaluación del riego. 65
6.3.6 Análisis y evaluación del riesgo. 76
6.3.7 Salvaguardas y propuesta para la gestión del riesgo. 82
6.3.8 Plan de tratamiento de riesgos. 83
6.3.9 Informe de evaluación de riesgos. 83
6.3.9.1 Metodología aplicada. 83
6.3.9.2 Proceso de evaluación y tratamiento de riesgo. 83
6.3.9.3 Iniciativas para el tratamiento del riesgo. 84
6.3.9.4 control de efectividad. 84
6.3.9.5 Supervisión de la evaluación y tratamiento de riesgos. 84
6.4 DESARROLLO OBJETIVO 4 84
6.4.1 Controles. 84
6.4.1.1 Implementación de los controles de la ISO 27001 en QWERTY S.A. 85
6.4.2 Recomendaciones. 87
6.4.3 Calculo de costos. 88
6.4.3.1 Costos de adquisición de equipos y servicios. 88
6.4.3.2 Costos recursos humanos. 89
6.4.3.3 Costos de recursos administrativos. 89
6.4.3.4 Total de recursos. 90
6.4.4 Cronograma de actividades para la implementación del SGSI en QWERTY S.A. 90
6.4.5 Manual del sistema de gestión de seguridad de la información de QWERTY S.A. 91
6.4.6 Procedimientos documentados. 91
7 CONCLUSIONES 92
8 RECOMENDACIONES 93
BIBLIOGRAFÍA 94
anexos 105

LISTA DE TABLAS

pág.

Tabla 1. Categorización de activos de QWERTY S.A. 53
Tabla 2. Análisis del impacto ante modificaciones de los activos de QWERTY S.A 63
Tabla 3. Valoración cuantitativa del riesgo de los activos de la empresa QWERTY S.A. 64
Tabla 4. Frecuencia de las amenazas que inciden sobre los activos de QWERTY S.A 72
Tabla 5. Costos de adquisición de Equipos Tecnológicos y Servicios 88
Tabla 6. Costos de Recursos Humanos 89
Tabla 7. Costos de Recursos Administrativos 89
Tabla 8. Costo total de recursos para la Implementación del SGSI 90
Tabla 9. Cronograma de actividades 90
Tabla 10. Activos y valoración cuantitativa 105

LISTA DE CUADROS

pág

Cuadro 1. Series de la norma ISO/IEC 27000 25
Cuadro 2. Funciones de las áreas de la empresa QWERTY S.A. 29
Cuadro 3. Indicadores y solución del problema 41
Cuadro 4. Activos de información del departamento de sistemas de QWERTY S.A. 44
Cuadro 5. Activos primarios 48
Cuadro 6. Activos de soporte 49
Cuadro 7. Categorización de los activos de QWERTY S.A. 51
Cuadro 8.Probabilidad del riesgo - Magerit 54
Cuadro 9. Impacto del riesgo - Magerit 54
Cuadro 10. Valoración del riesgo (Impacto vs Probabilidad) 55
Cuadro 11. Valoración del riesgo 56
Cuadro 12. Valoración de la dimensión y ubicación de los activos de QWERTY S.A 57
Cuadro 14. Valoración de los atributos de los activos de QWERTY S.A 62
Cuadro 15. Identificación de amenazas y vulnerabilidades – Magerit 66
Cuadro 16. Amenazas y vulnerabilidades que requieren atención Urgente para la empresa QWERTY S.A 74
Cuadro 17.Análisis y evaluación de riesgos 76
Cuadro 18. Salvaguardas para la empresa QWERTY S.A. 83
Cuadro 19. Plan de tratamiento de riesgos de los activos de la empresa QWERTY S.A. 106
Cuadro 20. Controles para la empresa QWERTY S.A. de acuerdo con la evaluación de amenazas y riesgos 115
Cuadro 21. Controles definidos para la implementación del SGSI en la empresa QWERTY S.A. 117

LISTA DE FIGURAS

Pág.

Figura 1. Características de la Seguridad de la Información 22
Figura 2. Ciclo PHVA 27
Figura 3. Dependencia de sistemas de la empresa QWERTY S.A.....29
Figura 4. Diagnóstico del problema actual de la empresa QWERTY S.A 40
Figura 5. Gráfico del porcentaje de implementación de los controles de la norma ISO/IEC 27001 43
Figura 6. Gráfico de los tipos de controles implementados por QWERTY S.A 43
Figura 7. Categorización de activos 53
Figura 8. Gráfica de la dimensión de autenticidad de los activos de QWERTY S.A. 58
Figura 9. Gráfica de la dimensión de trazabilidad de los activos de QWERTY S.A 59
Figura 10. Gráfica de la dimensión de confidencialidad de los activos de QWERTY S.A. 59
Figura 11. Gráfica de la dimensión de Integridad de los activos de QWERTY S.A. 60
Figura 12. Gráfica de la dimensión de disponibilidad de los activos de QWERTY S.A 60
Figura 13. Gráfico del análisis del impacto ante modificaciones de los activos de la empresa QWERTY S.A 64
Figura 14. Gráfico del análisis de la valoración cuantitativa del riesgo de los activos de la empresa QWERTY S.A.....65
Figura 15. Gráfico del porcentaje de frecuencia de las amenazas sobre los activos de QWERTY S.A 73
Figura 16. Gráfico de probabilidad de vulneración de los activos 73
Figura 17. Diagrama de Pareto de los activos más afectados 75
Figura 18. Gráfico del nivel de aceptación del riesgo 82
Figura 19. Gráfico de la Clasificación de la Gestión ISO 27001 de la empresa QWERTY S.A. 85
Figura 20. Gráfico de porcentaje de cumplimiento final de la empresa durante la aplicación del sistema.....86

Figura 21. Gráfico de tipo de controles implementados de acuerdo con la norma ISO 27001 86

Figura 22. Gráfico de porcentaje de cumplimiento por dominio de los controles definidos 87

LISTA DE ANEXOS

pág.

Anexo A. Valoración cuantitativa de activos 105
Anexo B. Plan de tratamiento de Riesgos 106
Anexo C. Controles necesarios de acuerdo con los resultados de la evaluación de riesgos y amenazas 115
Anexo D. Controles definidos para la implementación del SGSI 117
Anexo E. Manual del sistema.....155
Anexo F. Procedimientos documentados 185
Anexo G. Formatos Y Formularios.....197
Anexo H. Difusión en la empresa QWERTY S.A. 205

GLOSARIO

ACTIVO DE INFORMACIÓN: Es cualquier cosa que tenga un valor para una organización y que por ende deba ser protegida.

ACUERDOS DE CONFIDENCIALIDAD: Son documentos en los cuales los empleados de una empresa o terceros (contratistas) realizan acuerdos voluntarios de responsabilidad y reserva con la información que se les pueda confiar, prohibiendo así su divulgación, uso indebido o explotación en virtud de trabajo que desempeñan.

AMENAZA: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

ANÁLISIS DE RIESGOS: Proceso sistémico de identificación del origen, probabilidades y comparación de dichas variables contra criterios de evaluación para evidenciar las consecuencias potenciales de pérdida de Confidencialidad, Integridad y Disponibilidad de la información.

AUTENTICACIÓN: Protocolo de verificación de la identidad de un cliente o recurso a un servicio o sistema tecnológico al cual se intenta acceder.

CIFRADO: Es el cambio de la lógica y orden de datos subordinados que hacen parte de una información, con el fin de asegurar la confidencialidad y prevenir la fuga o interceptación de esta.

CONFIDENCIALIDAD: Es la característica que tiene la información para no ser divulgada, accedida o disponible a quienes no estén autorizados.

CRIPTOGRAFÍA: Disciplina que recopila principios y procesos para cambiar el orden lógico de los datos con el fin de proteger su contenido de alteraciones, repudio o prevenir el acceso no autorizado a esta.

DISPONIBILIDAD: Es la propiedad que tiene la información para garantizar que quienes deban y tengan el permiso de acceder a ella, puedan hacerlo en el tiempo y momento que sea necesario.

DISPOSITIVOS DE ALMACENAMIENTO: Son los componentes tecnológicos que contienen y almacenan datos e información.

HARDWARE: Componente o elemento tecnológico, diseñado e integrado electrónicamente para trabajar junto a algún componente de software para prestar algún servicio o con un fin determinado.

INCIDENTE DE SEGURIDAD: Es un evento adverso y debidamente comprobado, que amenaza y afecta las Política de Seguridad de la Información en una empresa determinada.

INTEGRIDAD: Es una propiedad de la información que comprende que todos los datos que la componen se encuentren de manera inalterada y completa.

RECURSOS TECNOLÓGICOS: Es aquel compendio de elementos de hardware y software que son el soporte tecnológico de una empresa u organización para el desarrollo de sus actividades.

RESPALDO: Es el proceso de realizar una copia de seguridad o back up de toda una información que deba ser protegida contra una inminente falla o eliminación involuntaria o errónea, que puedan significar perdida de datos.

SISTEMA DE INFORMACIÓN: Es un conjunto organizado de procesos y medios en donde se integran e interactúan procesamiento y almacenamiento de datos para ofrecer un servicio o efectuar diversas tareas dentro de una organización.

SOFTWARE: Es un compendio o conjunto de programas (medios digitales) los cuales se manipulan mediante hardware para realizar tareas de manera lógica y específica, para ofrecer un servicio.

SOFTWARE MALICIOSO: Es una variación o modificación de un programa mediante códigos hostiles y dañinos, que tienen como fin infiltrarse y causar daño en cualquier recurso tecnológico o sistema de información.

VULNERABILIDADES: Son aquellas brechas de seguridad inherentes a los activos de información, que pueden ser aprovechadas por terceros de forma dolosa o pueden ser factores de riesgo involuntario, que en sí pueden perjudicar a la entidad u organización.

RESUMEN

Este trabajo consistió en la ejecución de un proyecto aplicado, donde se realizó el diseño de un sistema de gestión de seguridad de la información, el cual permitió mejorar y dinamizar la administración de los activos de información de la empresa QWERTY S.A., asegurando el control del cumplimiento de su misión basados en la normatividad vigente.

La empresa QWERTY S.A. actualmente se especializa en el desarrollo tecnológico en comunidades colombianas a través del uso de tecnologías de información, donde cuenta con 120 colaboradores entre directivos, administrativos y operativos, quienes usan de forma regular los medios de información para la consulta de datos, pero la empresa presenta algunas fallas de seguridad en sus sistemas y manejo de recursos tecnológicos, lo cual hace que sea vulnerable ante cualquier incidente que se presente y ponga en riesgo la integridad de la empresa.

Por lo anterior, la empresa QWERTY S.A., preocupada por la seguridad de sus activos de información, acudió a la universidad UNAD, en donde solicitó la asignación de un director de proyecto para que diseñara un sistema de gestión de seguridad de la información.

Para dar respuesta a dicha solicitud se creó un sistema gestión de seguridad de la información, de acuerdo con la norma ISO 27001, a partir de los procesos, activos de información y falencias que presentaba la entidad.

Palabras Clave: Activos de Información, Seguridad de información, Seguridad Informática.

ABSTRACT

This work consisted in the execution of an applied project, where the design of an information security management system was carried out, which improves and streamlines the administration of the information assets of the company QWERTY SA, ensuring control of compliance with its mission based on current regulations.

The company QWERTY SA specializes in the technological development, in the development of information technologies, has 120 collaborators among the responsible, administrative and operational, who use the regular way the information media for the query of data, but the The company has some security flaws in its systems and management of technological resources, which makes it vulnerable to any incident that arises and puts the integrity of the company at risk.

Due to the above, QWERTY S.A., concerned about the security of its information assets, went to the UNAD university, where it requested the assignment of a project director for the design of an information security management system.

The response to this request has become an information security management system, in accordance with ISO 27001, based on the processes, information assets and shortcomings that the entity presents.

Keywords: Informatic Security, Information Assets, Information Security.

INTRODUCCIÓN

La empresa QWERTY S.A. es una de las entidades que le apuesta al desarrollo tecnológico de las comunidades colombianas, pero pese a ello no cuenta con un Sistema de seguridad que le ayude a salvaguardar sus activos de información de manera adecuada, dado a ello, presenta fallas en la implementación adecuada de las tecnologías como Firewall, protección de los servicios, gestión y control del ingreso de personas a las instalaciones de la empresa y la mala configuración de la red, lo cual hace que esta, se vea vulnerable ante cualquier ataque que pueden emplear los ciberdelincuentes para afectar los intereses de la organización.

Por tanto, en el presente trabajo se pretende establecer un modelo de gestión de la ciberseguridad para la empresa QWERTY S.A. haciendo uso de estándares y metodologías para la buena gestión de la información a través de la norma ISO 27001, enfocado en la línea de investigación "*Gestión de Sistemas*" establecida por la universidad, el cual tiene por objeto "*Apoyar el desarrollo productivo, tecnológico y social empresarial a través del análisis, diseño, implementación o administración de sistemas de información y las TIC que estén basados en la plantificación, dirección, control, evaluación y realimentación de actividades procedimentales*". Entre los aspectos metodológicos que se abordaran en el presente documento, estará el establecimiento de una fases que abordaran el problema de una manera analítica y procedimental de forma directa, puesto que pese a contar con alguna información esencial para iniciar el proyecto, existen limitantes tales como: No se cuenta con una recopilación de datos mediante encuestas aplicadas al personal de la empresa para realizar un estudio estadístico que pueda dar un enfoque más detallado sobre la problemática que presenta la empresa, No existe una matriz de diagnóstico en la cual se compare el nivel de cumplimiento de seguridad que viene aplicado la organización con la transversalidad de los procesos que así establece la norma ISO 27000, con el fin de crear nuevos procesos de seguridad. mejorar o corregir lo que ya se está aplicando y mitigar gastos.

El diseño del sistema de gestión de seguridad de la información otorgará a la empresa QWERTY S.A. las herramientas necesarias para asegurar los activos de información y la consolidación adecuada de sus procesos, generando una cultura efectiva en la administración y cuidado de los recursos al personal de planta, generando una percepción de credibilidad y confianza en sus clientes, y por ende, un alto impacto en la imagen institucional.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En el progreso de tecnologías de la información y las comunicaciones a nivel mundial viene trascendiendo con el paso del tiempo y la evolución de la humanidad, también esto ha causado que los delitos muten a la par, como el hurto o la estafa, entre otros, los cuales se han visto obligados a trasladarse del plano físico (robo a instalaciones y entidades a mano armada) a lo digital (robo de bases de datos y archivos digitales, entre otros). Esta situación viene preocupando enormemente a la sociedad en general, tal como nos lo muestra la revista *Semana*[1] en su publicación de la sección "*Tecnología del 13 de febrero del año 2019"*, donde nos ilustra brevemente sobre la situación actual de Colombia frente a la Ciberseguridad con base a un balance entregado por la plataforma *Comparitech* sobre el análisis de servicios tecnológicos; nuestro país ocupa el puesto 39 entre 60 países estudiados, evidenciando que nos encontramos en un rango medio de seguridad en la red, aunado a ello, Colombia produce el 0.5% de los ataques al software financiero con el que se pretende robar a los usuarios de estos sistemas.

La empresa QWERTY S.A., actualmente se especializa en el desarrollo tecnológico en comunidades colombianas a través del uso de tecnologías de información, haciendo parte de esta gran red en donde se transporta y gestiona sus recursos, contando con 120 colaboradores entre directivos, administrativos y operativos, quienes usan de forma regular los medios de información para cumplir con la misionalidad de la empresa; Por ende, mediante un comunicado allegado a la Universidad UNAD, la nombrada empresa solicita ayuda para resolver la problemática que puede causar una posible materialización de los riesgos y amenazas informáticas sobre sus activos de información, ya que no cuentan con una metodología o sistema de seguridad que prevenga y supervise la gestión de sus procesos de manera adecuada.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo prevenir y contrarrestar los riesgos y las vulnerabilidades que pueden afectar los activos de información de la empresa QWERTY S.A.?

[1] Revista Semana. Así está Colombia en el ranking de ciberseguridad mundial. {En línea}. Fecha. {03 de diciembre de 2019}. Disponible en: https://www.semana.com/nacion/articulo/asi-esta-colombia-en-el-ranking-de-ciberseguridad-mundial/601118

2 JUSTIFICACIÓN

Hoy en día las empresas y entidades ya no se interesan solo por proteger dinero, estructuras, entre otros bienes materiales; para ellas la seguridad de *la información* es el activo más importante, siendo éste el primordial recurso a proteger, a través de la implementación de las medidas necesarias que aseguren su integridad, confidencialidad y disponibilidad, obteniéndose como resultado final, un beneficio prioritario para la organización y sus clientes.

En contexto, un Sistema de Gestión de Seguridad de la Información juega un papel importante en la actualidad, puesto que establece el uso adecuado de la información contenida tanto a nivel físico (documentos, equipos tecnológicos, etc.) como digital (datos, archivos), los cuales se procesan para la toma de decisiones o la prestación un servicio en particular. La clave para el desempeño y competitividad de un negocio depende principalmente en la calidad de la gestión de su información para satisfacer necesidades tanto del cliente interno como externo, partiendo del principio esencial, que la seguridad es lo primordial.

Por lo anterior, el diseño de un Sistema de Gestión de Seguridad de la Información sustentado en un modelo de prácticas de seguridad como lo es la norma ISO/IEC 27001:2013, otorgará a la empresa QWERTY S.A., factores de prevención y oportunidad de mejora necesarios para asegurar sus activos de información apoyando el cumplimiento de su Misión. Un Sistema de Gestión de Seguridad de la Información, demuestra ante la sociedad el compromiso de la organización hacia la seguridad de sus intereses y el aporte a su evolución vanguardista, generando una estrategia eficaz y proactiva en la seguridad de la información, estructurando roles de responsabilidad coherentes a las políticas, procesos y procedimientos de la entidad ante la sociedad y así poder establecer mecanismos para reducir el impacto de las amenazas que pudieren poner en riesgo la organización.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Proponer un modelo de gestión de seguridad de la información para la empresa QWERTY S.A haciendo uso de los estándares establecidos en la norma ISO 27001:2013.

3.2 OBJETIVOS ESPECÍFICOS

- Realizar el diagnóstico de situación del problema que presenta la empresa QWERTY S.A., con relación a la Gestión de Seguridad de la Información.

- Formular los requerimientos de QWERTY S.A. con relación al Sistema de Gestión de Seguridad de la Información.

- Definir el plan de tratamiento de riesgos, mediante la metodología de identificación, clasificación y valoración de los activos de información.

- Definir las políticas de la Seguridad de la Información para la empresa con base a la norma ISO 27001:2013.

4 MARCO REFERNCIAL

Para diseñar este sistema, debemos estar al tanto de algunos temas que abordaremos a continuación:

4.1 MARCO CONCEPTUAL

4.1.1 Seguridad Informática. Este concepto consiste proteger de diversas formas los recursos y sistemas informáticos de determinada empresa, de forma que estos se utilicen de forma adecuada, controlando el acceso y la legibilidad de la información que allí se contiene, teniendo en cuenta, que estos accesos siempre se realicen dentro de los límites de autorizados[2].

Objetivos de la seguridad informática:

Los activos de información son los elementos que la seguridad de la información debe proteger. Por ende, estos se precisan de la siguiente forma:

Información: Es el objeto de mayor importancia de una empresa u organización, se hace presente en medios tanto físicos como digitales, algunos son: Datos, Documentos digitales, Archivos, Logs, entre otros.

Equipos: Se compone del conjunto de hardware y software que son de propiedad o uso de la empresa.

Usuarios: Son aquellas personas que integran la organización o empresa y que hacen uso de la tecnología con el fin de ofrecer o prestar un servicio.

4.1.2 Seguridad de la información. Es el conjunto de medidas preventivas y reactivas que ejecutan las organizaciones para permitir la protección de la información con el fin de mantener sus características de la confidencialidad, la disponibilidad e integridad.

4.1.3 Sistema de Gestión de Seguridad de la Información. Es un conjunto adecuado de medidas para la protección de la información y los sistemas que la gestionan, los cuales implementa una organización en cuanto a su acceso, uso, publicación o eliminación no autorizada[3].

---

[2] ISOTools Excellence. ISO 27001 ¿Cómo proteger la información de terceras personas?. {En línea}. Fecha. {04/12/19}. Disponible en https://www.pmg-ssi.com/2015/04/iso-27001-proteger-informacion-terceras-personas/

[3] ISOTools Excellence. op. cit.

En la gestión de la seguridad de la información, se abarcan tres aspectos dentro de este contexto que se relacionan en un todo e influyen para asegurar el proceso:

Confidencialidad: es la característica en la cual se condiciona la divulgación de la información, solo a aquellas personas o sistemas debidamente autorizados.

Integridad: esta característica busca proteger la información de modificaciones no autorizadas y mantener intacto cada dato o componente que lo integra.

Disponibilidad: es una propiedad donde la información se dispone de manera accesible en el tiempo y modo en el que aquellos que tengan autorización lo requieran.

Figura 1. Características de la Seguridad de la Información

Fuente: INFOSEGUR. 1- Conceptos básicos de la seguridad informática, 1.2- Objetivos de la seguridad informática. [En línea]. {10 de noviembre de 2013}. Disponible en: https://infosegur.wordpress.com/tag/no-repudio/

4.2 MARCO TEÓRICO

4.2.1 Análisis de riesgos. Como habíamos mencionado anteriormente, la Información es el activo más importante de una organización, por lo que es indispensable emplear una técnica que la mantenga segura. Por este motivo, la información se puede blindar con seguridad lógica, a través de la aplicación de barreras y procedimientos que resguardan el acceso a ella, restringiendo el acceso a personas que no están autorizadas[4].

[4] ISOTools Excellence. ISO 27001 ¿Cómo proteger la información de terceras personas?. {En línea}. Fecha. {04/12/19}. Disponible en https://www.pmg-ssi.com/2015/04/iso-27001-proteger-informacion-terceras-personas/

Primordialmente para aplicar la gestión del riesgo se debe realizar un análisis que tiene como fin referenciar que componentes en un sistema necesitan protección, cuáles son sus debilidades y amenazas que los ponen en riesgo, esto en pro de dar un valor al grado de riesgo al que están sometidos y otorgar una solución o alternativa de protección.

Clasificación y flujo de información:

- Identificar el tipo de información y clasificarlo

  - Confidencial (Acceso restringido, el cual solo debe ser manejado por personal interno debidamente autorizado).

  - Privado (Acceso restringido, solo debe ser manejado por personal interno).

  - Sensitivo (Acceso controlado: De conocimiento del personal interno y externo con permiso).

  - Público.

- Análisis de flujo de información

  - Observación de quienes manejan información y de qué tipo.

  - Identificación de grupos externos que requieran o dependan de la información.

  - Determinación de posibles cambios que se requieran en el manejo de la información.

La clasificación de los datos tiene el propósito de evaluar y ubicar dentro de un parámetro debidamente concienciado la información y datos que deban ser protegidos, teniendo en cuenta algunos aspectos tales como qué tipo de personas tendrán acceso a ella, los niveles de autorización. Una vez clasificada la información, se deben verificar los flujos de la información, observando e identificando de forma minuciosa y analítica el manejo que se viene presentado de esta y así finalmente determinar los posibles cambios que se requieran.

Ahora bien, teniendo en cuenta lo anterior, es preciso aclarar que existen varios métodos para valorar un riesgo, sin embargo, todos ellos apuntan a llegar casi al mismo resultado y conclusión.

En este ámbito, uno de los métodos más usados para el enfoque de la seguridad informática es el análisis del riesgo.

La valoración del riesgo se expresa en la fórmula matemática:

Riesgo = Probabilidad de Amenaza x Magnitud de Daño

En este proceso de analizar el riego, a groso modo, es preciso reconocer la importancia de cada riesgo, teniendo en cuenta sus características:

- Dinámico y cambiante (Interacción entre amenaza y vulnerabilidad).

- Diferenciado (Tiene diferentes caracteres de vulnerabilidad).

- No siempre puede ser percibido de la misma manera por cada uno de los miembros de la organización, por ello es importante determinar que quienes participan en su análisis, sean personas especialistas y sean los responsables directos de cada proceso, para así detectar el riesgo de manera adecuada.

Sí la probabilidad de amenaza y magnitud de daño es alta, entonces este riesgo y peligro para el sistema será directamente proporcional, lo cual nos da a entender que es necesario implementar medidas de protección.

4.2.2 Probabilidad de amenaza. *Ataque*, es el termino en el cual una amenaza se convierte realidad, Aunque, esto no nos indica si tuvo éxito o no[5]. Por tal motivo, es indispensable estimar la probabilidad de una amenaza a través de algunas consideraciones principalmente; Grado de interés por parte de individuos externos, Nivel de vulnerabilidad y Frecuencia de ocurrencia de los incidentes. Al igual se debe hacer una valoración de la probabilidad de la amenaza, en donde se debe evaluar de acuerdo con una calificación: Baja (Es cuando existe una lejana posibilidad de ocurrencia de un ataque), Mediana (Existe una poco probable condición de ataque a corto plazo, pero no es suficiente para evitarlo), Alta (Un ataque es inminente, no existen impedimentos tanto internos como externos que lo eviten). Estos parámetros son una aproximación del reflejo de una realidad y por ende es fundamental que la organización defina sus propias condiciones para evaluarlo.

4.2.3 Magnitud del daño. Cuando hablamos de Impacto, es el resultado consecuente de un ataque exitoso que perjudico las características esenciales de la seguridad informática en una organización, en donde se ve afectada toda la información o parte de ella, por eso es preciso aclarar que cuando hablamos de un impacto, estamos hablando que hubo pérdida de información, terceros tienen

[5] Ibíd.

acceso a la información o la información ha sido manipulada o sustraída, por ende, ha cambiado su legitimidad o no está disponible.

Por lo anterior, deberemos tener en cuenta los siguientes aspectos para valorar la magnitud del daño, con el fin de prever alternativas que nos ayuden a mitigar su alcance:

Consideraciones de las consecuencias del impacto:

- ¿Quién sufrirá los daños?
- Hubo incumplimiento de confidencialidad
- Hubo incumplimiento de obligaciones jurídicas (contratos, convenios)
- Cuál será el costo de la recuperación (imagen de la organización, recursos, etc.)

Valoración del impacto:

- Bajo: Daño aislado, no perjudica directamente a la organización.
- Medio: Causa desarticulación de uno componente de la organización, a futuro puede provocar consecuencias serias.
- Alto: A corto plazo puede desarticular a la organización, afectándola directamente[6].

4.2.4 ISO/IEC 27000. Son una serie de normas que proporcionan estándares en materia de seguridad de la información y que son publicado por la Organización Internacional para la Estandarización – **ISO** y la Comisión Electrotécnica Internacional – **IEC**[7], esta serie tiene cerca de 37 publicaciones de las cuales veremos las siguientes:

Cuadro 1. Series de la norma ISO/IEC 27000

SERIES DE LA NORMA	DESCRIPCIÓN
ISO/IEC 27000	Aquí se otorga una visión general de las normas que hacen parte de la serie 27000, referenciando su alcance y propósito, recogiendo todas las definiciones y aportando adicionalmente las bases para la aplicación del SGSI.
ISO/IEC 27001	Es la serie principal que recopila los

[6] Ibíd.
[7] ISO 27000.es. (s.f.). ISO 27000.es, {En línea}. {04/12/2019} disponible en: http://www.iso27000.es/iso27000.html

Cuadro 1. (continuación)

	requisitos para la implementación de Sistema de Gestión de Seguridad de la Información - SGSI.
ISO/IEC 27002	Es un compendio de buenas prácticas en donde se relacionan 39 objetivos de control y 133 controles que se sugieren de manera detallada para la implementación de la seguridad de la información en una organización.
ISO/IEC 27003	Es una compilación de conceptos críticos importantes para la implementación de un sistema de gestión de la información con base en la serie 27001, donde se referencian los requisitos para su planeación y diseño, desde el inicio a través de los diferentes planes hasta la aprobación de la dirección de una organización.
ISO/IEC 27004	Se compone de un paso a paso para el desarrollo y uso de métricas y métodos de medición que pueden ser aplicables para evaluar la eficacia de un Sistema de gestión de la Información y sus controles implementados.
ISO/IEC 27005	Otorga las guías para la gestión del riesgo de seguridad de la información, referenciando conceptos generales que integra la serie 27001, ayudando así a aplicar de manera exitosa la seguridad de la información desde un enfoque de gestión del riesgo para una organización.
ISO/IEC 27009	Referencia los requisitos para el uso de serie 27001 en los diferentes sectores (industrial, agrícola, etc). Explica además como depurar y adicionar requisitos a los que trae consigo la norma 27001 de ser necesario y cómo incluir controles de acuerdo con lo que requiera la organización para la implementación del sistema.
ISO/IEC 27010	En particular, es una guía de seguridad puede ser adaptable y ejecutada a los intercambios o difusión de la

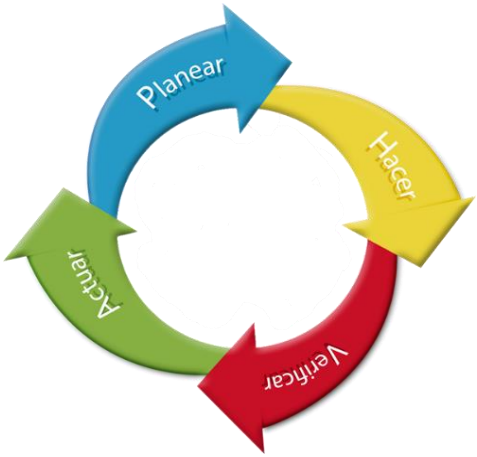
Cuadro 1. (continuación)

	información sensible cuando se requieran para la concesión de suministros y mantenimientos por terceros, en pro de la protección de la organización y su infraestructura, es aplicable tanto en lo público como en lo privado.
ISO/IEC 27011	Es un compendio de interpretación para la aplicación de un sistema de gestión de la seguridad de la información en los diversos sectores de las telecomunicaciones y empresas que se relacionan con este.

Fuente: ISO 27000.es. (s.f.). ISO 27000.es, {En línea}. {04/12/2019} disponible en: http://www.iso27000.es/iso27000.html

4.2.5 Ciclo de mejora continua. El ciclo de mejora continua PHVA (**planificar-hacer-verificar-actuar**) es un sistema de mejora continua, en el cual se establecen 4 fases o pasos de forma sistemática para gestionar de manera eficiente sus sistemas de gestión[8]:

Figura 2. Ciclo PHVA



Fuente: INFOSEGUR. 1- Conceptos básicos de la seguridad informática, 1.2- Objetivos de la seguridad informática. [En línea]. {14 de abril de 2020}. Disponible en: http://audycontrolintunivers2015.blogspot.com/2015/04/ciclo-phva.html

[8] JIMENO BERNAL, Jorge. Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua. {En línea}. Fecha. {04/12/19}. Disponible en https://www.pdcahome.com/5202/ciclo-pdca/

Fase Planificar: Aquí se constituyen objetivos y procesos que puedan mejorar, además de indicadores de medición para gestionar los objetivos a alcanzar.

Fase Hacer: Se pone en marcha el plan establecido donde se implementan las actividades planteadas para lograr la mejora

Fase Verificar: Después de realizada la mejora, se pacta un tiempo de prueba con el fin de constatar el adecuado engranaje y desarrollo de las acciones realizadas en las anteriores fases.

Fase Actuar: En esta fase se evalúan los resultados de las acciones efectuadas, con el fin de verificar el cumplimiento de los objetivos, en caso de que no se cumplan se verifican las posibles causas, generando las respectivas acciones.

4.3 ANTECEDENTES

4.3.1 Estado actual. La empresa QWERTY S.A tiene actualmente las siguientes condiciones de funcionamiento:

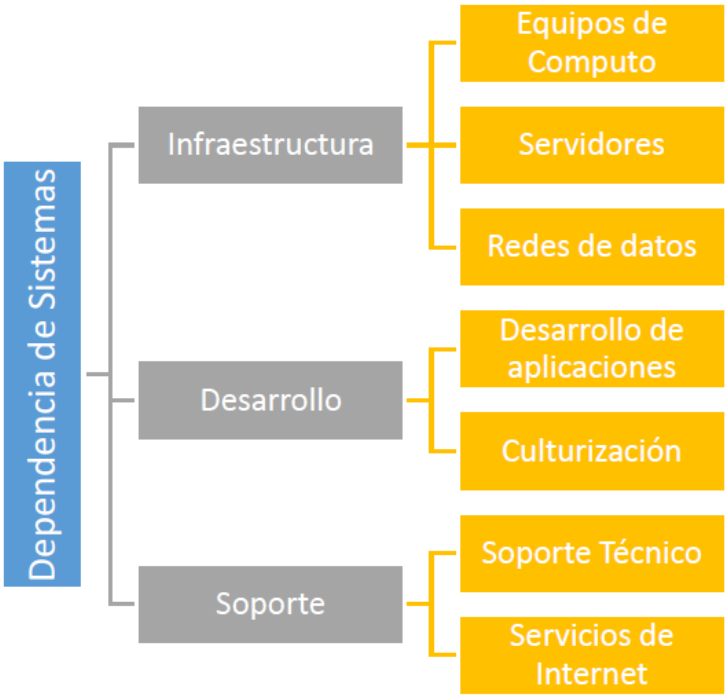
- La Empresa QWERTY S.A. es una empresa del sector tecnológico que busca el desarrollo tecnológico en comunidades colombianas a través del uso de Tecnologías de Información.

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

Para resolver las necesidades tecnológicas, el centro de estudios cuenta con una dependencia de sistemas que brinda soporte a la infraestructura tecnológica 24/7.

Figura 3. Dependencia de sistemas de la empresa QWERTY S.A.



Fuente: Documento Escenario2_EnfoqueDirectivoAdministrativo – UNAD

Las Funciones de las áreas son[9]:

Cuadro 2. Funciones de las áreas de la empresa QWERTY S.A.

Área de Infraestructura	Soporte al acceso a la red interna y a internet. Revisión de diseños de cableado estructurado
Área de desarrollo	Apoyo técnico a las dependencias de la organización del centro en desarrollo de medios eficientes para lograr actividades basadas en usos de tecnologías de la informática y las telecomunicaciones.
Área de Soporte	Mantenimiento de computadores (sólo equipos propiedad del Centro).

[9] *Documento Escenario2_EnfoqueDirectivoAdministrativo - Universidad UNAD*

Cuadro 2. (Continuación)

	Generación de conceptos técnicos para tramitar baja de equipos. Generación de conceptos técnicos para tramitar baja de equipos. Realiza copias de seguridad de los sistemas de información y servidores virtuales que se encuentran en las dependencias de la empresa QWERTY S.A.

Fuente: Documento Escenario2_EnfoqueDirectivoAdministrativo - UNAD

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

Asistencia para directivos, administrativos y operativos:

Apoya el servicio de correo electrónico institucional[10]: servicio que está contratado con Google, este servicio busca:

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

Apoyo en la gestión y mantenimiento de activos informáticos[11]:

Servicio que cumple la función de mantener en óptimo desempeño servicios tecnológicos como:

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

[10] Ibíd
[11] Ibíd

Apoyo en la gestión de usuarios y contraseñas[12]: Servicio que se enfoca en la gestión de usuarios y contraseñas usadas en las diferentes aplicaciones enfocadas en apoyar el desarrollo académico de la comunidad educativa:

• Correo electrónico
• Sistema de gestión de calidad

Apoyo a la dependencia de nómina y facturación[13]: En la dependencia de nómina y facturación se desarrollan las siguientes tareas:

• Generación de nómina de trabajadores

• Generación de recibos de pago

• Creación, alimentación y custodia de Hojas de vida

• Control del seguimiento al talento humano

• Generación certificados laborales y relacionados con el modelo de negocio

Aunado a lo anterior, se presenta las siguientes anotaciones[14]:

- QWERY S.A. no cuenta con un sistema de seguridad biométrico o de monitoreo que permita tener control de ingreso y egreso de los clientes internos y externos.

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

- 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.

[12] Ibíd
[13] Ibíd
[14] Ibid

4.4 MARCO CIENTÍFICO O TECNOLÓGICO

4.4.1 Metodología de análisis de riesgos por *Magerit*. En esta metodología se toma como referencia los siguientes documentos (MAGERIT – versión 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) [15]:

Libro I – Método
Libro II - Catálogo de Elementos
Libro III - Guía de Técnicas

Entre los cuales tenemos los siguientes aspectos generales:

Paso a paso

El análisis de riesgos nos permite tener un acercamiento metódico para determinar un riego en los procesos de la organización de acuerdo con los siguientes pasos:

1. Establecer cuáles son los activos importantes para la empresa
2. Establecer a qué amenazas se encuentran expuestos.
3. Establecer salvaguardas, analizado que tan eficientes son contra el riesgo
4. Valorar el impacto, aquí se determina como el análisis de la magnitud del daño ante una inminente amenaza sobre cada activo.
5. Evaluar el riesgo, se establece a raíz del cálculo de la valoración de la posible ocurrencia de la amenaza.

De acuerdo con lo anterior, verificaremos y analizaremos algunos aspectos primordiales:

Paso 1: Activos[16]

Se cataloga como el componente integral y funcional en un sistema de información de una organización, el cual puede sufrir un ataque accidental o doloso que afecte su integridad, disponibilidad y confidencialidad. En este concepto podemos incluir: Datos, información tanto impresa como digital, aplicaciones, recursos, equipos entre otras.

En un sistema de información existen dos cosas principales para tener en cuenta:

[15] MAGERIT, Magerit v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información {En línea}. {28/09/2019}. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XehG3ZNKjIU
[16] Ibíd.

- la información que se opera o procesa para su disposición
- y los servicios que se ofrecen o publican al cliente

Estos activos son una esencial pauta para establecer las necesidades de seguridad que necesita el resto del sistema. Es importante reconocer otros activos que sobresalen como subordinados a estos:

— Archivos digitales(datos) o físicos donde se soporta la información.
— El equipamiento auxiliar como complemento del sistema informático de la organización.
— Las redes de comunicaciones.
— Las instalaciones
— Los soportes de información (almacenamiento de datos).
— Las personas o trabajadores que hacen uso de estos componentes.
— Servicios auxiliares necesarios para el uso del sistema.
— Las aplicaciones y software para el manejo de los datos e información.
— Los equipos informáticos (Desktop, Servidores entre otros que permiten almacenar y procesar la información).

Es importante tener en cuenta que no todos los activos son de la misma categoría, dependiendo de múltiples factores como el tipo o ubicación se pueden dirimir diferentes amenazas y salvaguardas.

Dependencias[17]

Los principales activos son la información y los servicios que se brindan al cliente; pero por otra parte estos dependen directamente de otros activos que se pueden catalogar como mediáticos o de soporte, tales son los equipos de cómputo, las redes de comunicación, la infraestructura o instalaciones y los trabajadores o empleados que hacen uso, operan o manipulan este tipo de activos.

En cada caso se deben adoptar los objetos del análisis, estructurando los activos de manera subordinada, hallando relación entre sí como se muestra a continuación:

• Activos esenciales
  - Información que se procesa
  - Servicios que se disponen al cliente

• Servicios internos
  - Los dispuestos de manera ordenada para el sistema de información.

• El equipamiento informático
  - Software o Aplicaciones del sistema

[17] Ibíd.

- El Hardware (servidores, equipos, etc.)
- Las redes de comunicación
- Los soportes de la información (discos de almacenamiento, servidores de archivo, NAS, etc.)

• El entorno: Aquellos establecidos para dar soporte a los demás puntos.
- Suministros y equipamiento: servicios (Refrigeración y ventilación, energía, intendencia, etc.).

• Las instalaciones o infraestructura física

• El personal
- Usuarios, Operarios, Administradores o jefes de grupo, etc.

• Los servicios subcontratados a terceros (servicios de mantenimiento, servicios de soporte, etc.)

Valoración[18]

Aquí estableceremos la importancia del activo a proteger, se da un valor objetivo para la empresa y no precisamente de valor monetario sino de un valor perspectivo de seguridad y que tanto puede afectar a la empresa que este se vea afectado ante un inminente riesgo.

Dimensiones[19]

En este concepto, podemos estructurar el manejo de la protección de los activos desde diferentes perspectivas o dimensiones tales como:

En cuanto a su confidencialidad, es una apreciación muy arraigada a los datos, donde nos debemos preguntar el impacto que se daría si cayera en manos no debidas esta información.

Integridad, al igual es una propiedad común de los datos, donde deberemos analizar los perjuicios que traería como consecuencia la corrupción o daño de esta información.
Por último, la disponibilidad, el cual es un factor común aplicable a todos los servicios que se prestan, en donde su dimensión se enfatizaría en evaluar cuál es la magnitud del perjuicio que traería el no poderlos usar.

Por otro lado, en la gran mayoría de los sistemas organizacionales dedicados a prestar servicios electrónicos o digitales, el conocimiento de estas dimensiones es

[18] Ibíd.
[19] Ibíd.

fundamental para poder prestar un mejor servicio y corregir las fallas tanto estructurales como funcionales, por ello es pertinente evaluar otros aspectos:

• Autenticidad: En esta dimensión es pertinente preguntarnos, ¿Qué impacto causaría el no saber quién ejecuta o realiza cualquier acción dentro del sistema sin plena identificación?, es una valoración común en los servicios y datos para identificar quienes acceden y ejecutan acciones sobre estos.

• Trazabilidad del uso del servicio o acceso a los datos: es otra dimensión muy objetiva y valida, en donde debemos preguntarnos, ¿Quién presta un servicio o quién accede a los datos y que hace con ellos?

Así las cosas, podemos concluir en este aspecto, que el autor no solamente se limita en reconocer las dimensiones básicas que analizamos en principio, sino que nos traslada a otras importantes como lo son la autenticidad y la trazabilidad, que podrían ser traducidos dentro de las dimensiones básicas pero que son de importante análisis para tener en cuenta al momento de evaluar los activos.

Paso 2: Amenazas[20]

En este paso deberemos determinar que amenazas influyen o afectan cada uno de los activos a proteger.

Identificación de las amenazas

De origen natural: Son aquellas en donde el sistema de información se afecta directamente con fenómenos naturales como inundaciones, terremotos, tormentas eléctricas, etc.

Del entorno o de origen industrial: En estas el sistema es afectado por desastres o accidentes industriales improvistos y ajenos a la organización como descargas eléctricas, explosiones, contaminación, entre otras.

Desperfectos de las aplicaciones: Estas se catalogan como vulnerabilidades técnicas y se deben a fallas en el diseño, programación e implementación de los sistemas de la organización.

De origen accidental por personas o trabajadores propios: En esta el sistema o activo de la organización se ve afectado por la mala manipulación o error no intencional en las operaciones ejecutadas por parte de los empleados que tienen acceso a estos.

[20] Ibíd.

De origen intencional por parte de empleados de la organización o terceros: Por último, el autor nos ilustra que tanto empleados de la misma empresa, como terceros con acceso a los sistemas de información pueden ser la causa de afectación a los activos a través de ataques intencionales con el ánimo de beneficiares o causar daños a la organización.

Es importante tener en cuenta que no todas las amenazas inciden en todos los activos, sino que la clase de activo puede relacionarse con lo que podría ocurrir inminentemente.

Valoración de las amenazas[21]

En este concepto es preciso aclarar que cuando un activo se ve afectado por una amenaza, no siempre se ve afectado en su totalidad o en la misma magnitud de cuantía. Por ende, es justo valorar y determinar la influencia en el valor del activo en los siguientes contextos:

Degradación: Es la magnitud que mide el perjuicio sobre el valor del activo ante su afectación, este concepto caracteriza como una porción de valor del activo después de ser afectado en un supuesto de que fuese víctima de una amenaza, es por ello que se ve su calificación como "Totalmente degradado o degradado en una pequeña porción", el autor nos aclara que es importante tener en cuenta que este precepto es aplicable para aquellas amenazas no intencionales, puesto que su proporcionalidad se pierde cuando esta es intencional, ya que un atacante puede causar muchísimo daño selectivamente.

Probabilidad: Esta por el contrario es mucho más difícil de determinar o referenciar, a veces suele ser modelada cualitativamente por medio de escalas. Este concepto está arraigado a la magnitud de probabilidad o improbabilidad de ocurrencia de una amenaza.

Paso 3: Salvaguardas[22]

En este paso se debe analizar las salvaguardas desplegadas definidas como aquellos mecanismos tecnológicos o sistémicos que reducen los riesgos. Hay amenazas que pueden mitigar sencillamente organizándose de manera adecuada, otras por el contrario necesitan componentes técnicos (software o hardware) u otras seguridad estructural o políticas de usuario.

[21] Ibíd.
[22] Ibíd.

Selección de salvaguardas

Pueden existir muchas alternativas de salvaguardas, pero para ello es necesario hacer un análisis profundo de algunos aspectos para tener en cuenta para hacer una evaluación de lo que se tiene y lo que se necesita:

1. Se debe tener en cuenta el tipo de activo a proteger, puesto que cada uno se protege de forma diferente.
2. Verificar que dimensiones que requieren protección
3. Detectar y referenciar las amenazas ante las cuales debemos de protegernos.
4. Verificar si existen salvaguardas adicionales o alternativas.

Es importante de incluir el costo de implementación de estas medidas (salvaguardas), puesto que hay que considerar este factor proporcionalmente al riesgo o amenaza que se desea evitar.

Por último, para el Paso 4: impacto residual y Paso 5: riesgo residual, después de darse un grupo de salvaguardas a desplegar, queda un posible impacto y una situación de riesgo a la que se le denomina residual, que en si se origina desde un valor potencial a uno residual, en donde intervienen los conceptos de degradación y probabilidad.

4.5 MARCO LEGAL

- Constitución Política de Colombia de 1991.

- Ley 599 del 2000 - Por la cual se dispone el “Código penal colombiano”.

- Ley 603 de 2000 - Por la cual se dispone el “Control de Legalidad del Software”.

- Ley 962 de 2005 - Por la cual se dicta la “Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas”.

- Ley 1150 de 2007 - Por la cual se regula la “Seguridad de la información electrónica en contratación en línea”.

- Ley 1273 del 2009 - Por la cual se regula la “Protección de la información y de los datos”.

- Ley 1341 de 2009 - Por la cual se dicta las disposiciones sobre las “Tecnologías de la Información y aplicación de seguridad”.

- Ley 1480 de 2011 - Por la cual se dicta la “Protección al consumidor por medios electrónicos. Seguridad en transacciones electrónicas”.

- Norma ISO 9001:2015 - La cual determina los requisitos para el Sistema de Gestión de la Calidad.

- Norma Técnica Colombiana NTC ISO/IEC 27001:2013 – Requisitos para un Sistema de gestión de seguridad de la información.

- Norma GTC-ISO/IEC 27002:2015 – Código de práctica para controles de seguridad de la información.

- Norma NTC ISO/IEC 27005 – Gestión del riesgo en la seguridad de la información.

5 DISEÑO METODOLÓGICO

5.1 TIPO DE INVESTIGACIÓN

Con base a lo descrito por el autor *UNIVERSIA*, este proyecto se utilizará un tipo de investigación *cuantitativa*, el cual utiliza herramientas informáticas y matemáticas para obtener resultados concluyentes.

5.1.1 Investigación Descriptiva. Este tipo de investigación cuantitativa se utiliza para describir la realidad de situaciones y eventos para pretender analizarlos, plantea lo más relevante de un hecho o situación en concreta. El investigador debe definir su análisis y procesos que se involucrarán[23] en el estudio, midiendo y evaluando diversos aspectos o componentes a investigar.

En ese orden de ideas, podemos afirmar que para poner en práctica este tipo de investigación, deberemos describir una serie de aspectos relacionados con la seguridad de la información de la empresa QWERTY S.A., en donde se debe involucrar el análisis de la situación actual de seguridad de la empresa; definiendo finalmente procesos y mecanismos necesarios para fortalecer la protección de la información de esta entidad, a partir de los requerimientos normativos y técnicos que sirvan como guía para gestionar y salvaguardar sus activos de manera adecuada.

5.2.2 Recolección de Información. Para este trabajo se hará una investigación descriptiva partiendo del estudio y análisis de la *información secundaria*, que según el autor *GALLARDO DE PARADA*[24], es aquella que es obtenida mediante el contacto indirecto con el objeto de estudio, esta información ya existía de antemano o fue recolectada parcialmente por otros, por lo tanto, no hay posibilidad de controlar los errores cometidos durante el proceso de recolección de información, lo cual, no permitiría medir las variables refinadamente. Esto se determinó a partir de que la información sobre el estado actual de la empresa QWERTY S.A. se recolectó a través de las anotaciones y especificaciones entregadas en el documento del escenario 2 de la Universidad UNAD.

---

[23] UNIVERSIA, Costa Rica – Tipos de investigación: Descriptiva, Exploratoria y Explicativa {En línea}. {05 de Diciembre de 2019}. Disponible en: https://noticias.universia.cr/educacion/noticia/2017/09/04/1155475/tipos-investigacion-descriptiva-exploratoria-explicativa.html

[24] GALLARDO DE PARADA, Yolanda; MORENO GARZÓN, Adonay. APRENDER A INVESTIGAR. {En línea}. {05 de Diciembre de 2019}. Disponible en: http://www.unilibrebaq.edu.co/unilibrebaq/images/CEUL/mod3recoleccioninform.pdf

6 DESARROLLO DE LOS OBJETIVOS

6.1 DESARROLLO DE OBJETIVO 1

6.1.1 Diagnóstico de situación del problema. Con base en el análisis del estado de la seguridad de la empresa, podemos identificar la situación problema:

Figura 4. Diagnóstico del problema actual de la empresa QWERTY S.A

Fuente: “Elaboración propia”

6.1.2 Indicadores del problema. Los siguientes son los indicadores que se establecieron con el objetivo de poder identificar el estado actual de la situación de seguridad de la información con la que cuenta la empresa QWERTY S.A, para poder otorgar un análisis general del problema a abordar.

Cuadro 3. Indicadores y requerimientos

INDICADORES	REQUERIMIENTOS
Nivel de seguridad física y control de acceso a las instalaciones.	Implementar una metodología de seguridad para acceso a la infraestructura de la organización, donde se encuentran las oficinas, Base de datos, entre otros.
Eficacia en la implementación de la seguridad para los equipos, red y servicios.	Verificar la eficacia en la implementación de la seguridad para los equipos de cómputo, red y servicios a través de un software y hardware eficiente que blinde la organización en contra de vulnerabilidades y riesgos.
Nivel de capacitación y compromiso del personal que integra la entidad en relación con la seguridad de la información	Establecer un nivel de capacitación y compromiso, del personal que integra la entidad, con el fin de que estos adquieran conocimiento en el manejo y administración de los recursos de forma confidencial y confiable para beneficio de la organización y sus empleados.

Fuente: “Elaboración propia”

6.2 DESARROLLO DE OBJETVO 2

6.2.1 Formulación de requerimientos. Para llevar a cabo la formulación de los requerimientos de QWERTY S.A. con relación al Sistema de Gestión de Seguridad de la Información, se definió el alcance del proyecto.

6.2.1.1 Alcance. Con este proyecto se pretende diseñar el modelo del *Sistema de Gestión de Seguridad de la Información* basado las necesidades actuales de la empresa QWERTY S.A y en concordancia con la norma ISO/IEC 27001:2013 y el objetivo presentado para el desarrollo de este proyecto, se orientará para:

- **Corregir las fallas de seguridad** presentadas en la empresa con el fin de implementar los controles básicos de seguridad para apoyar la misionalidad de la organización.

- **Mejorar la imagen de la entidad**, recuperando y consolidando la confiabilidad que tiene el cliente o los usuarios en los servicios que presta la empresa QWERTY S.A**.**

- **Cumplimiento normativo**. Con el diseño y posterior implementación de un Sistema de Gestión de Seguridad de la Información se iniciará la

implementación del cumplimiento a la normatividad vigente para la protección de los activos de información de la empresa, lo cual generará una percepción de seguridad y confiabilidad en el cliente tanto interno como externo de la entidad.

- **Disminuir costos**. La implementación del SGSI permitirá a futuro a la empresa QWERTY S.A. reducir costos que se invertirían para dar solución en la materialización de riesgos y vulnerabilidades detectadas en la organización, por tanto, este sistema ayudará a predecir las debilidades y riesgos a con anticipación con el fin de mitigarlos y contrarrestarlos de forma contundente.

Teniendo en cuenta lo anterior, se espera realizar las siguientes actividades:

- Identificación de los activos de información con los que cuenta la empresa QWERTY S.A, sobre los cuales y teniendo en cuenta la norma ISO/27001:2013, se deben proyectar medidas de protección.

- Identificación de los riesgos y amenazas de seguridad.

- Análisis y evaluación de los riesgos y gestionar su tratamiento.

- Identificación de salvaguardas para los activos de información y definir las políticas de seguridad de la información a través de un manual del SGSI para la empresa.

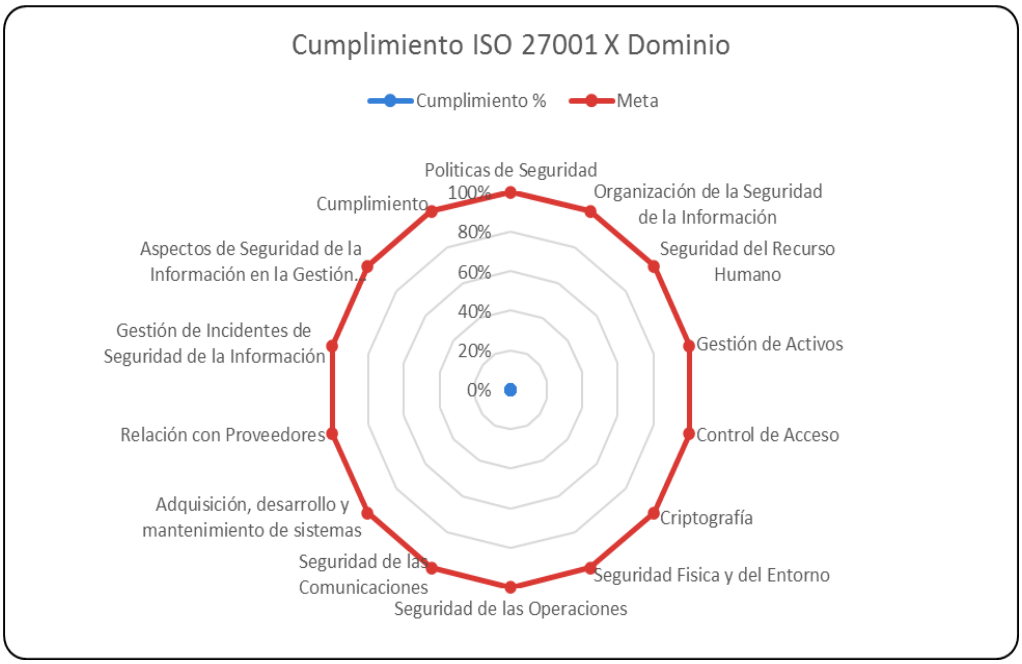
6.3 DESARROLLO DE OBJETIVO 3

6.3.1 Elección de metodología para realizar la gestión de riesgos. Para realizar la gestión de riesgos del sistema de información de QWERTY S.A., se ha elegido implementar la metodología *Magerit*, ya que nos permitirá analizar y evaluar los riesgos que soportan el sistema y su entorno, permitiéndonos recomendar las medidas de seguridad apropiadas que deben adoptarse para prevenir, controlar y contrarrestar los riesgos identificados, reduciendo su impacto o posibles perjuicios futuros sobre los activos de la empresa.

6.3.2 Análisis de implementación de los controles de la ISO 27001 en QWERTY S.A. El siguiente análisis se realizó con el objeto de establecer un contexto focalizado en datos, a partir de la gestión del riesgo en la seguridad de la información con el que cuenta inicialmente la organización, lo que finalmente nos permitirá establecer los criterios básicos para la implementación de controles necesarios en QWERTY S.A.

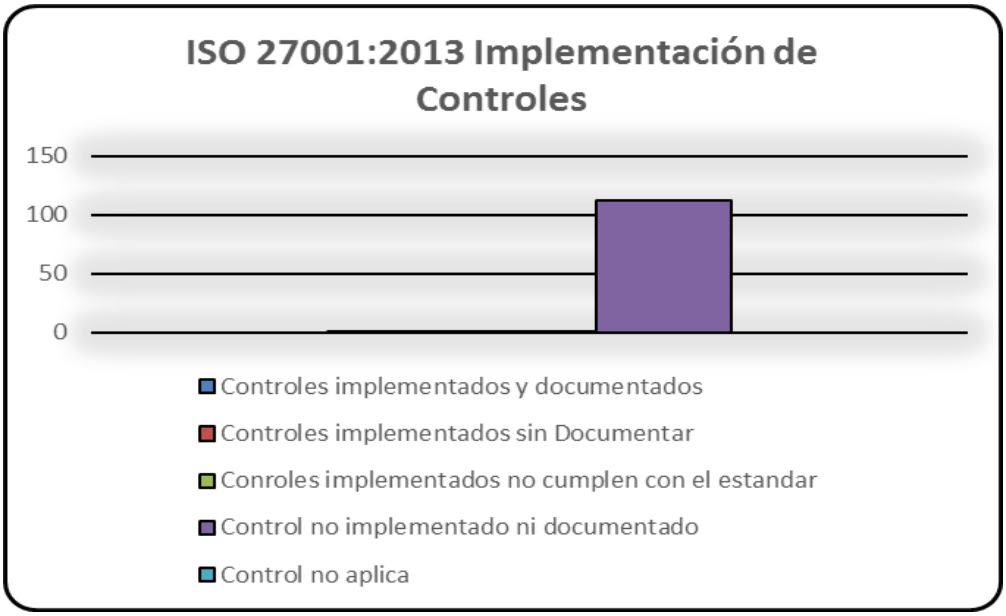
A continuación, verificaremos los aspectos iniciales en los que se encontraba la empresa QWERTY S.A. con referencia a la norma ISO 27001, ASÍ:

Figura 5. Gráfico del porcentaje de implementación de los controles de la norma ISO/IEC 27001



Fuente: Elaboración propia a partir del documento excel *"ISO27K_SOA_2013 – UNAD"*

Figura 6. Gráfico de los tipos de controles implementados por QWERTY S.A



Fuente: Elaboración propia a partir del documento excel "*ISO27K_SOA_2013 – UNAD"*

Podemos evidenciar en las anteriores *Figuras 5 y 6,* que la empresa de manera primigenia no tiene implementado los controles de la norma ISO 27001, por lo cual diferimos que no tenía un sistema de seguridad de la información que controlará y supervisará las actividades y procedimientos con el ámbito de gestión para sus activos de información, además no se contaban con un tratamiento de riesgos inherentes a estos.

6.3.3 Identificación de activos de información. Como punto de partida realizaremos la identificación de los activos de información de QWERTY S.A, mediante un proceso de clasificación de la información con sus respectivas características.

El Departamento de Sistemas tiene a cargo los siguientes activos de información:

Cuadro 4. Activos de información del departamento de sistemas de QWERTY S.A.

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

Cuadro 4. (Continuación)

	mensuales con capacidades de red alámbrica e inalámbrica. Impresora destinada para el servicio de directivos y administrativos y docentes		
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 Plan Máximo	Servicio contratado con la empresa Godaddy.com La página web tiene como objeto la publicación de contenido relacionado		1

Cuadro 4. (Continuación)

	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.		
Servidor de nómina y facturación Servidor marca dell en torre PowerEdge T440 Características de servidor Apache 2.4.25 PHP 5.6.30 - 7.1.1 MySQL 5.7.17 phpMyAdmin 4.6.6	Plataforma de desarrollo propio. Tiene como función el almacenamiento y la administración de la nómina y facturación de la empresa QWERTY S.A.		2
Servidor DHCP Servidor marca dell en torre PowerEdge T440	Servidor que asigna y administra de forma dinámica el direccionamiento dentro de la organización		1
Equipos de cómputo para gestión del desarrollo tecnológico	Equipos de cómputo donde se gestiona información online relacionada con el desarrollo del objeto social Presupuesto • Proveedores • Órdenes de compra • Inventarios	Dependencia de desarrollo tecnológico	3
Cortafuegos Cisco ASA 5505	Sistema de protección	Sistema de seguridad que está protegiendo a la red de datos, de intrusiones que se puedan presentar en la red	1

Cuadro 4. (Continuación)

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 Cómputo	Equipos destinados para el desarrollo del objeto social	Dependencia de prueba de software	5
Puntos de acceso alámbricos (hub)	Dispositivos de red encargados de la interconexión de la red de datos	Red de datos del centro	4
Switches cisco catalyst 2960	Dispositivos de red encargados de la interconexión de la red de datos	Red de datos del Centro	6
Técnicos de mantenimiento	Personal técnico encargado de realizar el mantenimiento preventivo a los equipos de computo	Departamento de Sistemas	2
Teléfonos IP	Sistema de comunicación a través de teléfonos Voz IP, que comunica las oficinas y departamentos del centro	Dependencias del centro	6
Puntos de acceso	Puntos de acceso al servicio de internet en el campus universitario	Departamento de sistemas	2

Fuente: Documento "*Escenario2_EnfoqueDirectivoAdministrativo – UNAD*"

En ese orden de ideas, a continuación, podemos realizar el siguiente desglose de activos de acuerdo con su importancia.

6.3.3.1 Activos primarios. Son todo el tipo de información electrónica, impresa y servicios que son de carácter central, los cuales son de vital importancia para la entidad.

De acuerdo con lo enunciado se identifican los siguientes activos de la empresa QWERTY S.A.

Cuadro 5. Activos primarios

Activo	Descripción
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.
Página web -Plan Máximo	Servicio contratado con la empresa Godaddy.com La página web tiene como objeto la publicación de contenido relacionado con el modelo negocio.
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.

Fuente: “Elaboración propia”

6.3.3.2 Activos de soporte. Son todo aquellos de los que dependen de los activos primarios, por tanto, brindan soporte para la ejecución de los procedimientos de la empresa.

Aunado a lo anterior, identificamos los siguientes activos de soporte en la entidad:

Cuadro 6. Activos de soporte

Activo	Descripción
Servidor DHCP Servidor marca dell en torre PowerEdge T440	Servidor que asigna y administra de forma dinámica el direccionamiento dentro de la organización
Equipos de cómputo para gestión del desarrollo tecnológico	Equipos de cómputo donde se gestiona información online relacionada con el desarrollo del objeto social: • Presupuesto • Proveedores • Órdenes de compra • Inventarios
Cortafuegos Cisco ASA 5505	Sistema de protección
Equipos de Computo Sistemas operativos win 10 Pro	Equipos destinados para el desarrollo del objeto social
Equipos de Computo Sistemas operativos win 10 Pro	Equipos destinados para el desarrollo del objeto social
Equipos de Cómputo	Equipos destinados para el desarrollo del objeto social
Puntos de acceso alámbricos (hub)	Dispositivos de red encargados de la interconexión de la red de datos
Switches cisco catalyst 2960	Dispositivos de red encargados de la interconexión de la red de datos
Técnicos de mantenimiento	Personal técnico encargado de realizar el mantenimiento preventivo a los equipos de computo
Teléfonos IP	Sistema de comunicación a través de teléfonos Voz IP, que comunica las oficinas y departamentos del centro
Puntos de acceso	Puntos de acceso al servicio de internet en el campus universitario
Servidor de Impresión: Servidor marca dell en torre PowerEdge T440	Equipo de cómputo que conecta dos impresoras destinadas a: Una (1) Impresora HP LaserJet Enterprise serie 600, activo que brinda el servicio para la dependencia de nómina y facturación. Permite la concurrencia

Cuadro 6. (Continuación)

	de hasta 25 usuarios y el volumen mensual de impresión es de 200 a 25000 páginas Una (1) Impresora SMART MultiXpress M4370LX, impresora que ofrece el servicio de escáner e impresión con un ciclo de trabajo de hasta 300000 páginas mensuales con capacidades de red alámbrica e inalámbrica. Impresora destinada para el servicio de directivos y administrativos y docentes.

Fuente: "Elaboración propia"

6.3.3.3 Caracterización de activos. Para caracterizar correctamente los activos en el inventario es importante clasificar su lugar en el sistema, para ello nos apoyaremos en seleccionar los activos con más incidencia en el sistema con los siguientes parámetros:

Categorización de los activos según su ubicación[25]:

[S] SERVICIOS
Son aquellos componentes que se entregan a los participantes del sistema

[D] DATOS
Es todo lo concernientes a la información que fluye por el sistema

[K] CLAVES CRIPTOGRÁFICAS
Son datos sensibles que tienen una capa de seguridad a nivel visualización

[SW] SOFTWARE
Son todas las aplicaciones y subprocesos automatizados que usen datos

[HW] EQUIPAMIENTO INFORMÁTICO
Es el inventario de activos por medio de los cuales opera la información

[COM] REDES DE COMUNICACIONES
Son las vías de transporte de los datos y de la información

[Media] SOPORTE DE INFORMACIÓN

[25] Documento Matriz de Análisis de Riesgos (Magerit) – UNAD

Son los medios físicos de almacenamiento de la información

[AUX] EQUIPAMIENTO AUXILIAR
Son los equipos que complementan a los activos en su funcionamiento

[L] INSTALACIONES
Es la infraestructura locativa en donde residen activos, información, equipos y personal

[P] PERSONAL
Son el talento humano que opera, administra, controla y vigila el sistema

Cuadro 7. Categorización de los activos de QWERTY S.A.

No.	DATOS DEL ACTIVO	TIPO									
	NOMBRE DEL ACTIVO DE INFORMACIÓN	[D] DATOS	[K] CLAVES CRIPTOGRÁFICAS	[S] SERVICIOS	[SW] SOFTWARE	[HW] EQUIPAMIENTO INFORMÁTICO	[COM] REDES DE COMUNICACIONES	[Media] SOPORTE DE INFORMACIÓN	[AUX] EQUIPAMIENTO AUXILIAR	[L] INSTALACIONES	[P] PERSONAL
1	Servidor de Impresión: Servidor marca Dell en torre PowerEdge T440					X					
2	Servidor de archivos FTP: Servidor marca Dell en torre PowerEdge T130						X				
3	Página web Plan Máximo			X							

Cuadro 7. (Continuación)

4	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				X						
5	Servidor DHCP Servidor marca Dell en torre PowerEdge T440				X						
6	Equipos de cómputo para gestión del desarrollo tecnológico					X					
7	Cortafuegos Cisco ASA 5505					X					
8	Equipos de Cómputo Sistemas operativos Win 10 Pro					X					
9	Equipos de Computo				X						
10	Equipos de Cómputo Sistemas operativos Win 10 Pro					X					
11	Puntos de acceso alámbricos (hub)					X					
12	Switches cisco Catalyst 2960					X					
13	Teléfonos IP					X					
14	Puntos de acceso					X					
15	Técnicos de mantenimiento										X

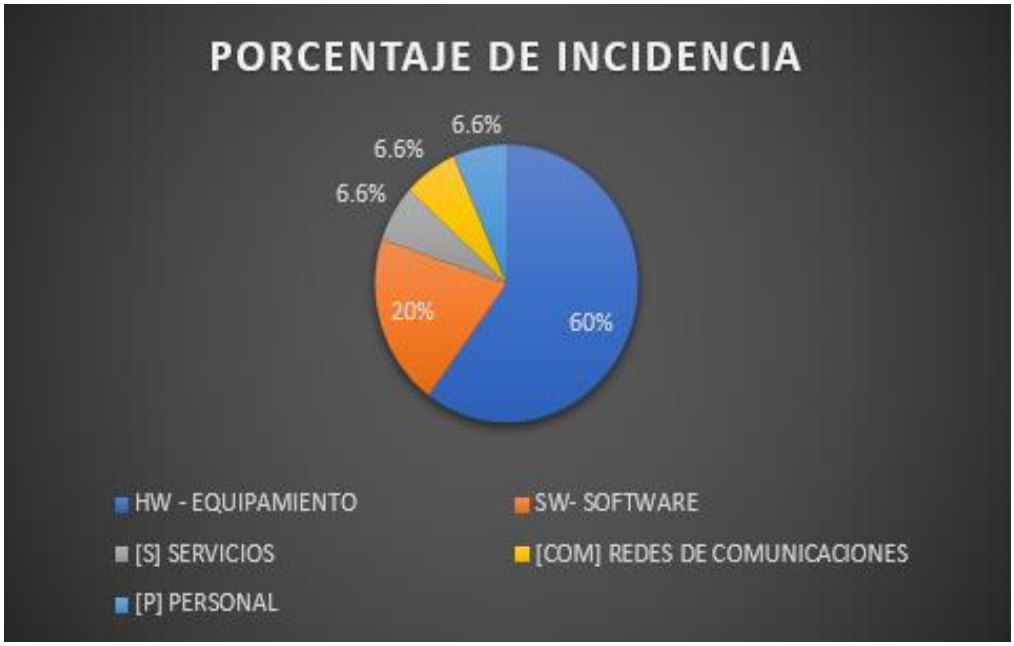
Fuente: Elaboración propia a partir del documento "*Matriz de Análisis de Riesgos (Magerit) – UNAD*"

Tabla 1. Categorización de activos de QWERTY S.A.

CATEGORIZACIÓN DEL ACTIVO	PORCENTAJE
HW - EQUIPAMIENTO	60%
SW- SOFTWARE	20%
[S] SERVICIOS	6.6%
[COM] REDES DE COMUNICACIONES	6.6%
[P] PERSONAL	6.6%

Fuente: “Elaboración Propia”

Figura 7. Categorización de activos



Fuente: “Elaboración propia”

Los activos con más incidencia en el sistema de acuerdo con el análisis que podemos apreciar a partir del *Cuadro 7* y la *Figura 7*, son HW – EQUIPAMIENTO de la empresa QWERTY S.A. con un 60% de incidencia, lo cual nos hace inferir que este activo el cual requiere más atención al momento de generar las correspondientes salvaguardas para diseñar el Sistema de Gestión de Información.

6.3.4 Valoración de activos. Tomamos como referencia la metodología *Magerit*, en la cual se tendrá en cuenta los criterios mostrados en los *Cuadros 8, 9, 10 y 11* en la que se relacionan parámetros de valorización tanto cuantitativos como cualitativos de los activos y que a continuación mostraremos, Los cuales nos

ayudaran a valorizar el riesgo de cada uno de los activos de la empresa QWERTY S.A.:

Cuadro 8.Probabilidad del riesgo - Magerit

PROBABILIDAD DEL RIESGO			
	Nomenclatura	**Categoría**	**Valoración**
Probabilidad	MA	**Prácticamente seguro**	5
	A	**Probable**	4
	M	**Posible**	3
	B	**Poco probable**	2
	MB	**muy raro**	1

Fuente: Documento *"Matriz de Análisis de Riesgos (Magerit) – UNAD"*

Cuadro 9. Impacto del riesgo - Magerit

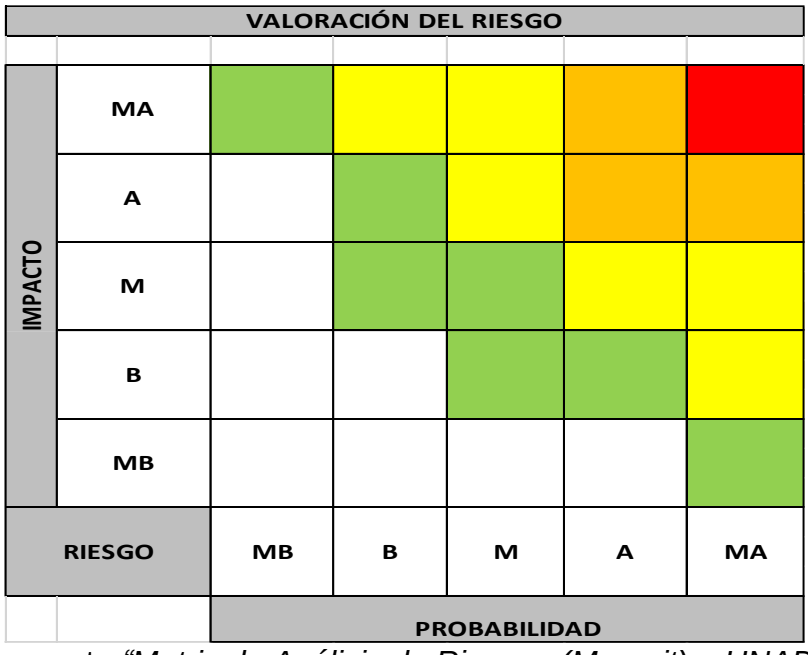
IMPACTO DEL RIESGO			
	Nomenclatura	**Categoría**	**Valoración**
Impacto	MA	**Muy Alto**	5
	A	**Alto**	4

Cuadro 9. (Continuación)

	M	**Medio**	3
	B	**Bajo**	2
	MB	**Muy Bajo**	1

Fuente: Documento *"Matriz de Análisis de Riesgos (Magerit) – UNAD"*

Cuadro 10. Valoración del riesgo (Impacto vs Probabilidad)



Fuente: Documento *"Matriz de Análisis de Riesgos (Magerit) – UNAD"*

Cuadro 11. Valoración del riesgo

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

Fuente: Documento *"Matriz de Análisis de Riesgos (Magerit) – UNAD"*

6.3.4.1 Valoración cualitativa. En esta valoración se evalúa aspectos tales como la Dimensión, Atributos y ubicación de cada activo:

Cuadro 12. Valoración de la dimensión y ubicación de los activos de QWERTY S.A

No.	DATOS DEL ACTIVO DE INFORMACIÓN	DIMENSIÓN					UBICACIÓN	
	Nombre del activo de información	Dimensión Autenticidad (B / M /A / MA/ MB)	Dimensión Trazabilidad (B / M /A / MA/ MB)	Dimensión Confidencialidad (B / M /A / MA/ MB)	Dimensión Integridad (B / M /A / MA/ MB)	Dimensión Disponibilidad (B / M /A / MA/ MB)	Físico	Electrónico
1	Servidor de Impresión: Servidor marca dell en torre PowerEdge T440	B	B	MA	B	MA	X	
2	Servidor de archivos FTP: Servidor marca dell en torre PowerEdge T130	B	B	MA	B	MA	X	
3	Página web Plan Máximo	A	B	A	A	B		X
4	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	A	M	M	M	MA		X
5	Servidor DHCP Servidor marca dell en torre PowerEdge T440	M	M	M	M	MA	X	
6	Equipos de cómputo para gestión del desarrollo tecnológico	M	A	A	M	MA	X	
7	Cortafuegos Cisco ASA 5505	M	M	MA	A	MA	X	

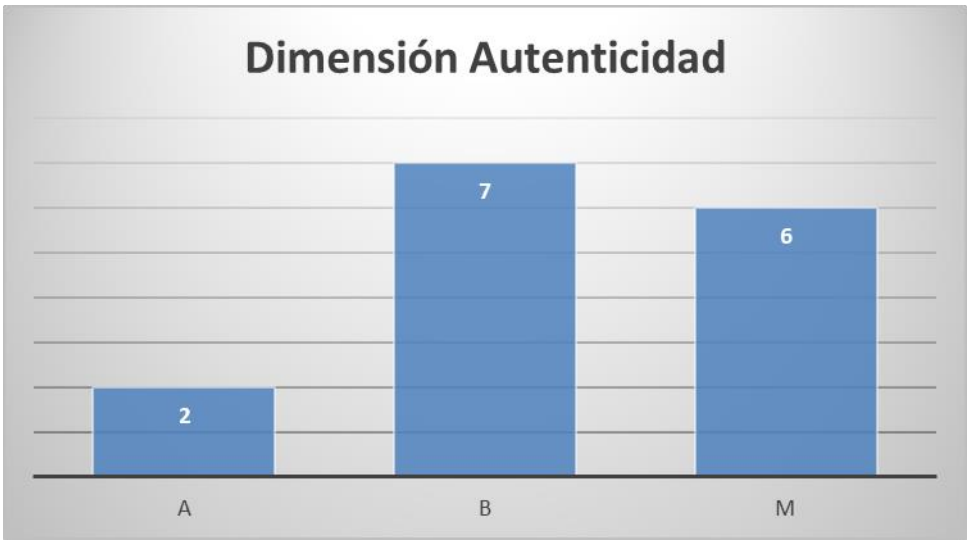
Cuadro 12. (Continuación)

8	Equipos de Cómputo Sistemas operativos Win 10 Pro	B	B	B	B	M	X	
9	Equipos de Cómputo	B	B	B	M	M		X
10	Equipos de Cómputo Sistemas operativos Win 10 Pro	B	B	B	B	M	X	
11	Puntos de acceso alámbricos (Hub)	M	M	MA	M	MA	X	
12	Switches cisco Catalyst 2960	M	M	MA	M	MA		
13	Teléfonos IP	B	B	B	B	M	X	
14	Puntos de acceso	M	B	MA	M	MA	X	
15	Técnicos de mantenimiento	B	M	B	B	M	X	

Fuente: "Elaboración propia a partir del Documento Matriz de Análisis de Riesgos (Magerit) – UNAD"

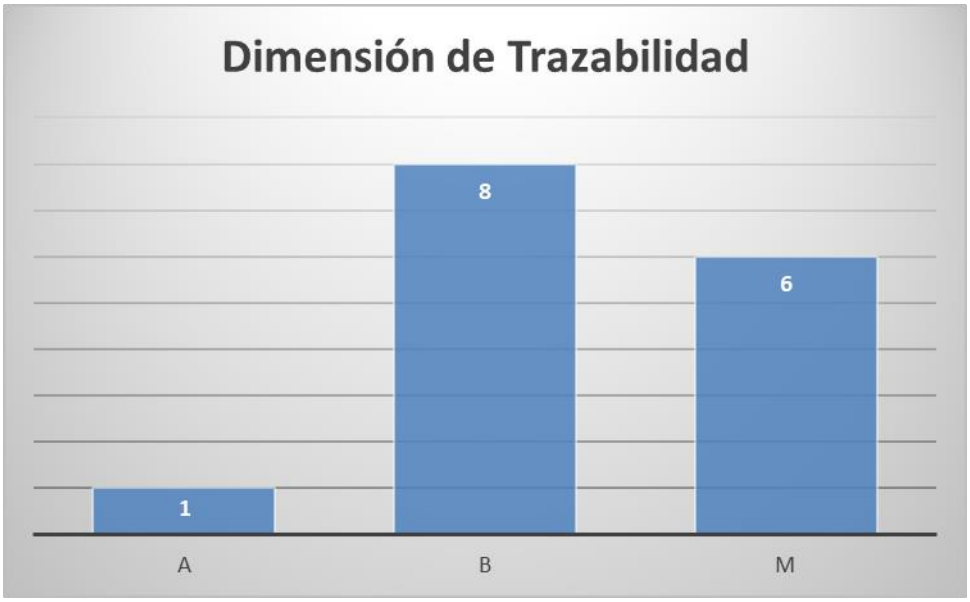
Análisis estadístico de la valoración cualitativa de las dimensiones:

Figura 8. Gráfica de la dimensión de autenticidad de los activos de QWERTY S.A.



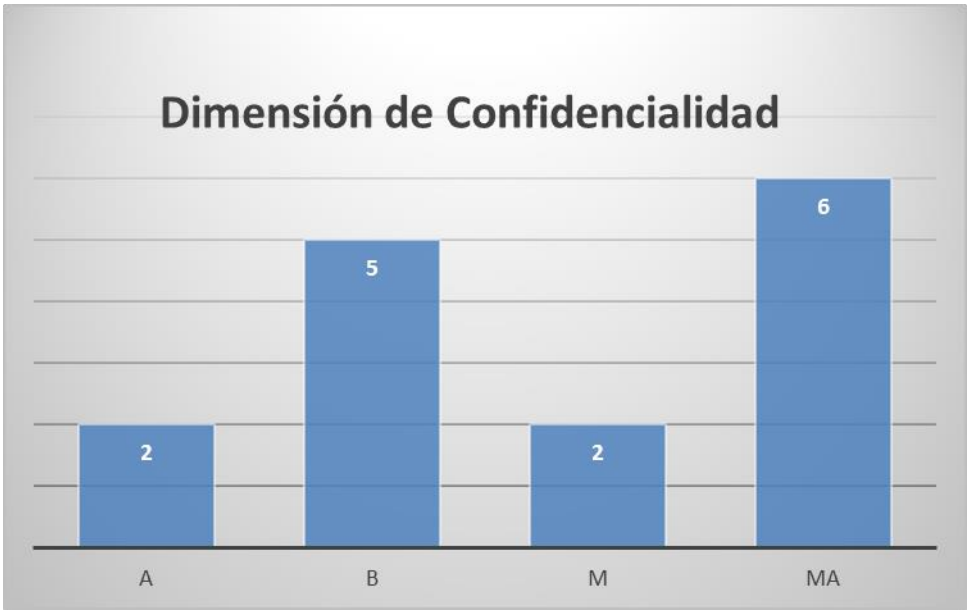
Fuente: "Elaboración propia"

Figura 9. Gráfica de la dimensión de trazabilidad de los activos de QWERTY S.A



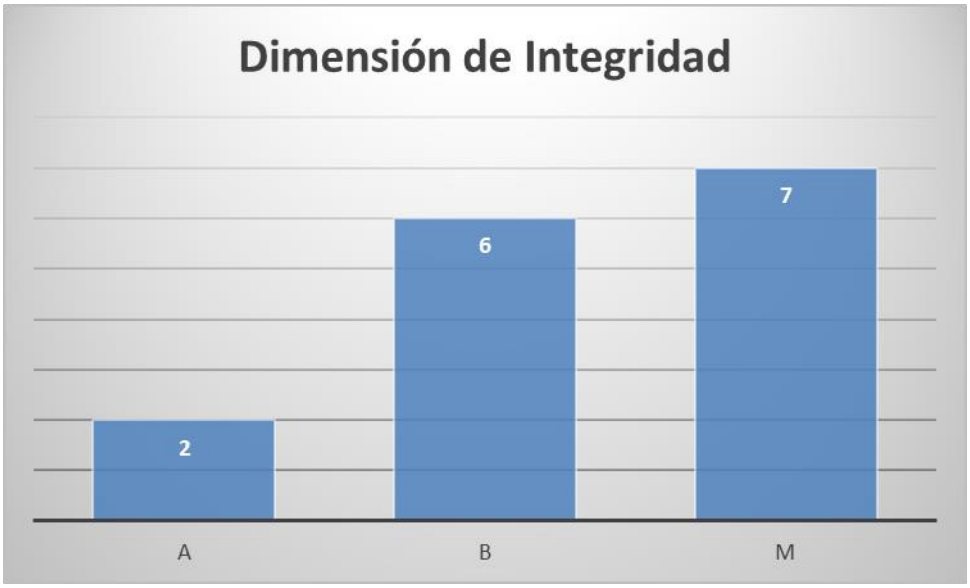
Fuente: “Elaboración propia”

Figura 10. Gráfica de la dimensión de confidencialidad de los activos de QWERTY S.A.



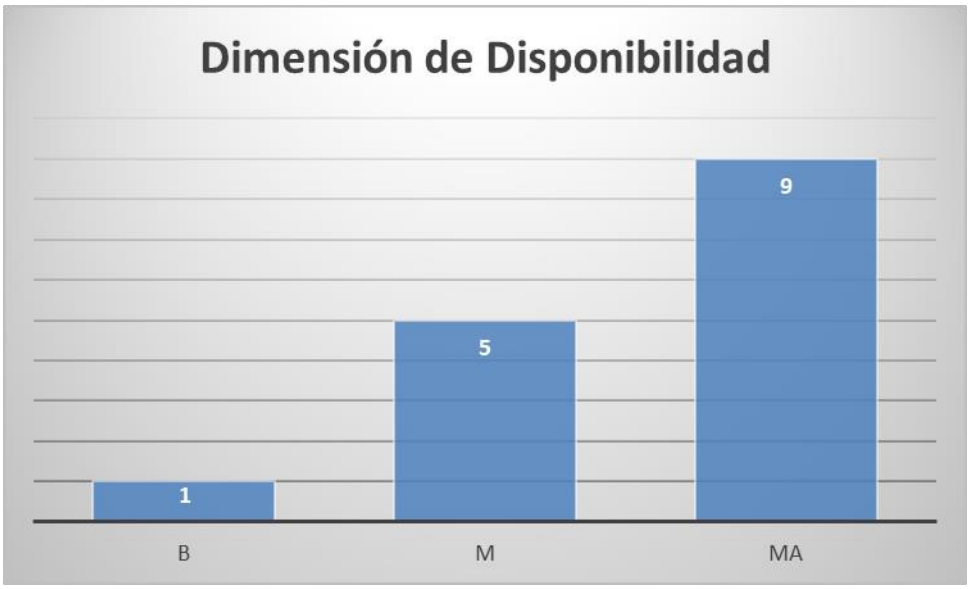
Fuente: “Elaboración propia”

Figura 11. Gráfica de la dimensión de Integridad de los activos de QWERTY S.A.



Fuente: “Elaboración propia”

Figura 12. Gráfica de la dimensión de disponibilidad de los activos de QWERTY S.A



Fuente: “Elaboración propia”

En las Figuras de la *8* a la *12*, podemos analizar que:

- En la dimensión de *Autenticidad*, los activos de la empresa QWERTY S.A tienen una valoración general de riesgo **B** "**Baja**" representando un **46,6%**, mientras que, por otro lado, el **40%** representa un nivel **M** "**Apreciable**"; por tanto, se debe tener en cuenta esta dimensión para ser incluida para la construcción del sistema.

- En la dimensión de *Trazabilidad*, los activos de la empresa tienen una valoración general de riesgo **B** "**Baja**" representando un **53,3%**, mientras que, por otro lado, el **40%** representa un nivel **M** "**Apreciable**"; por tanto, se debe tener en cuenta esta dimensión para ser incluida para la construcción del sistema.

- En la dimensión de *Confidencialidad*, los activos de la empresa tienen una valoración general de riesgo **MA** "**Crítico**" representando un **40%**, mientras que, por otro lado, el **33,3%** representa un nivel **B** "**Baja**"; por tanto, se debe incluir esta dimensión en la construcción del sistema, para contrarrestar todos los riesgos que afecten los activos con referencia a esta dimensión.

- En la dimensión de *Integridad*, los activos de la empresa QWERTY S.A tienen una valoración general de riesgo **M** "**Apreciable**" representando un **46,6%**, mientras que, por otro lado, el **40%** representa un nivel **B** "**Baja**"; por tanto, se debe tener en cuenta esta dimensión para ser incluida para la construcción del sistema.

- En la dimensión de *Disponibilidad*, los activos de la empresa tienen una valoración general de riesgo **MA** "**Crítico**" representando un **60%**, mientras que, por otro lado, el **33,3%** representa un nivel **B** "**Baja**"; por tanto, se debe incluir esta dimensión en la construcción del sistema, para contrarrestar todos los riesgos que afecten los activos con referencia a esta dimensión.

En conclusión, con referencia a las dimensiones de valoración cualitativa de los activos, la ***Confidencialidad*** y ***Disponibilidad*** son las más afectadas, sobre todo los activos con una ubicación ***física*** dentro de la organización, por lo cual requieren atención inmediata en el diseño del Sistema de Gestión de Seguridad de la Información para la empresa QWERTY S.A.

Cuadro 13. Valoración de los atributos de los activos de QWERTY S.A

No.	DATOS DEL ACTIVO DE INFORMACIÓN	ATRIBUTOS								
	Nombre del activo de información	¿Es activo de información de terceros o de clientes que debe protegerse?	¿Activo de información que debe ser restringido a un número limitado de empleados?	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes o corrupción	Activo de información que es muy crítico para las operaciones internas	Activo de información que es muy crítico para el servicio hacia terceros	Activo de información que, en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera:		
								Leve	Importante	Grave
1	Servidor de Impresión: Servidor marca Dell en torre PowerEdge T440	NO	SI	SI	SI	SI	NO		X	
2	Servidor de archivos FTP: Servidor marca dell en torre PowerEdge T130	NO	SI	SI	SI	SI	NO		X	
3	Página web Plan Máximo	SI	NO	NO	SI	SI	SI		X	
4	Servidor de nómina y facturación Servidor marca Dell en torre PowerEdge T440	SI	SI	SI	SI	SI	NO			X
5	Servidor DHCP Servidor marca Dell en torre PowerEdge T440	NO	SI	SI	SI	SI	NO		X	
6	Equipos de cómputo para gestión del desarrollo tecnológico	NO	SI	SI	SI	SI	NO		X	
7	Cortafuegos Cisco ASA 5505	NO	SI	SI	SI	SI	SI			X
8	Equipos de Cómputo Sistemas operativos Win 10 Pro	NO	NO	SI	SI	NO	NO	X		

Cuadro 13. (Continuación)

9	Equipos de Computo	NO	NO	SI	SI	NO	NO	X		
10	Equipos de Cómputo Sistemas operativos Win 10 Pro	NO	SI	SI	SI	NO	NO	X		
11	Puntos de acceso alámbricos (hub)	NO	SI	SI	SI	SI	NO		X	
12	Switches Cisco Catalyst 2960	NO	SI	SI	SI	SI	NO	X		
13	Teléfonos IP	NO	SI	SI	SI	SI	NO	X		
14	Puntos de acceso	NO	NO	SI	SI	SI	NO		X	
15	Técnicos de mantenimiento	NO	NO	SI	SI	NO	NO	X		

Fuente: "Elaboración propia a partir del Documento Matriz de Análisis de Riesgos (Magerit) – UNAD"

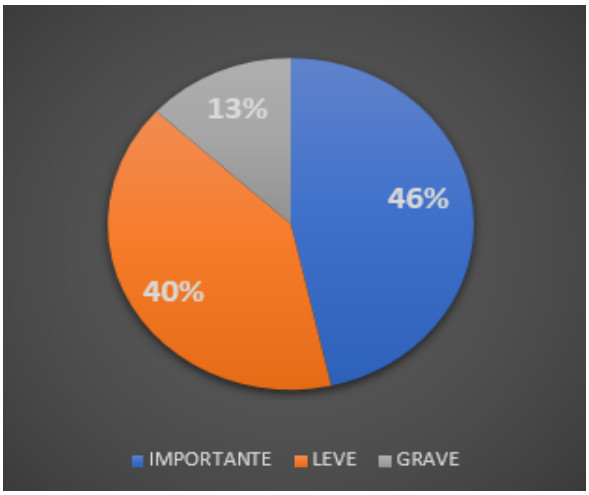
Al analizar el parámetro por el cual un "Activo de información que, en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera Leve, Importante o Grave", se obtuvo el siguiente resultado:

Tabla 2. Análisis del impacto ante modificaciones de los activos de QWERTY S.A

IMPACTO NEGATIVO ANTE MODIFICACIONES	PORCENTAJE
IMPORTANTE	46%
LEVE	40%
GRAVE	13%

Fuente: "Elaboración propia"

Figura 13. Gráfico del análisis del impacto ante modificaciones de los activos de la empresa QWERTY S.A



Fuente: "Elaboración propia"

De acuerdo con el anterior gráfico, podemos evidenciar que el impacto sería ***importante*** ante la modificación de los activos de la empresa QWERTY SA., por lo cual es importante buscar alternativas para blindarlos contra modificaciones no autorizadas que deben ser incluidas dentro del sistema.

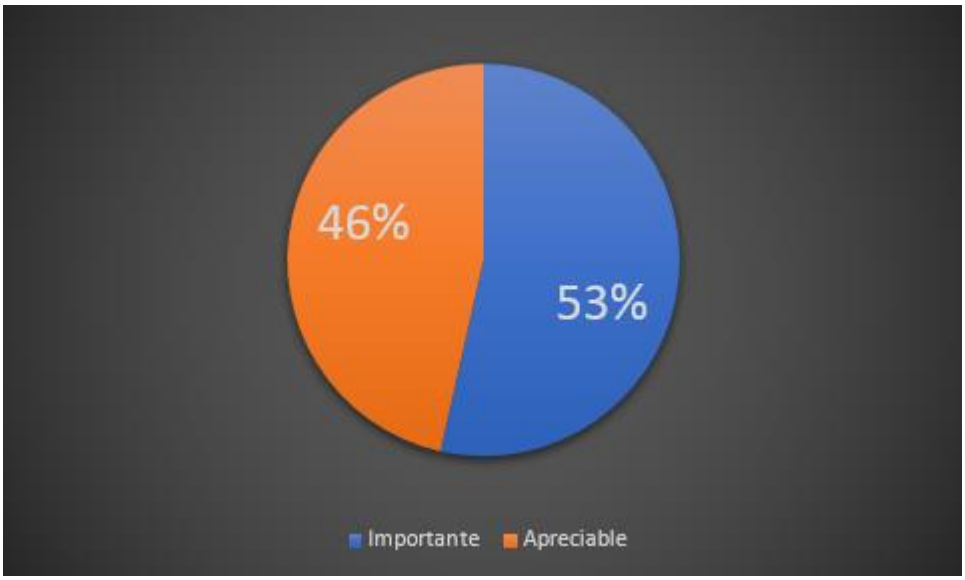
6.3.4.2 Valoración cuantitativa. En esta valoración se tuvo en cuenta los parámetros del *Cuadro 9***,** obteniendo los siguientes resultados en el análisis estadístico realizado:

Tabla 3. Valoración cuantitativa del riesgo de los activos de la empresa QWERTY S.A.

VALORACIÓN DEL RIESGO	PORCENTAJE
Importante	53%
Apreciable	46%

Fuente: "Elaboración propia"

Figura 14. Gráfico del análisis de la valoración cuantitativa del riesgo de los activos de la empresa QWERTY S.A



Fuente: "Elaboración propia"

La valoración cuantitativa nos muestra que el 53% de los activos tienen un riesgo ***importante***, donde los que se ven más vulnerables son: *Cortafuegos Cisco ASA 5505* con una valoración de riesgo de 20, seguido por los *Equipos de cómputo para la gestión del desarrollo*, *Puntos de acceso inalámbrico (Hub)*, *Switches Cisco Catalyst 2960* con una valoración de 19.

6.3.5 Enfoque de evaluación del riego. Es importante tener en cuenta que para la evaluación hay que entender que el enfoque de la evaluación del riesgo comprende las siguientes actividades:

- Identificación y caracterización de cada uno de los entornos que rodean el riesgo, cálculo del riesgo partiendo desde análisis de la amenaza y análisis de las vulnerabilidades que inciden sobre los activos de información de la empresa.

- Se debe realizar una valoración del riesgo ahondando en requisitos de aceptabilidad, tolerancia y seguridad para poder tratarlo o abordarlo según sea el caso.

Por último, Se debe realizar una evaluación del riesgo para que, junto a la dirección de la empresa se tomen decisiones a fin de tomar medidas para su prevención y mitigación.

6.3.6 Identificación de amenazas y vulnerabilidades. Realizando un estudio detallado de las amenazas y vulnerabilidades que pueden afectar cada uno de los activos de la empresa QWERTY S.A, se identificaron 33 posibles a las cuales se les realizó una parametrización en la Matriz de análisis y tratamiento de riesgos de la metodología *Magerit* como podemos ver a continuación:

Cuadro 14. Identificación de amenazas y vulnerabilidades – Magerit

Activos de información	**No. De Amenazas y Vulnerabilidades**	**Nombre del activo de información**	**Amenazas metodología Magerit**	**Vulnerabilidades**	**Probabilidad de vulneración**
[HW] EQUIPAMENTO INFORMÁTICO	1	Servidor de Impresión: Servidor marca dell en torre PowerEdge T440	[I5] Avería de origen físico o lógico	Falta de instrucciones de reacciones rápidas para la protección del hardware en caso de perjuicios ocasionados por el agua o por un incendio (restaurante y cocina)	3
[HW] EQUIPAMENTO INFORMÁTICO	2	Servidor de Impresión: Servidor marca dell en torre PowerEdge T440	[I5] Avería de origen físico o lógico	Envejecimiento del hardware	3
[HW] EQUIPAMENTO INFORMÁTICO	3	Servidor de Impresión: Servidor marca dell en torre PowerEdge T440	[I7] Condiciones inadecuadas de temperatura o humedad	Necesita climatización para funcionar	5
[HW] EQUIPAMENTO INFORMÁTICO	4	Servidor de Impresión: Servidor marca dell en torre	[I7] Condiciones inadecuadas de temperatura o humedad	Falta de hardware redundante	2

Cuadro 14. (Continuación)

		PowerEdge T440			
[S] SERVICIOS	5	Servidor de archivos FTP: Servidor marca dell en torre PowerEdge T130	[A5] Suplantación de la identidad del usuario	Posibilidad de gestionar el sistema en forma remota con herramientas de gestión no cifradas	4
[S] SERVICIOS	6	Servidor de archivos FTP: Servidor marca dell en torre PowerEdge T130	[A5] Suplantación de la identidad del usuario	Los recursos compartidos facilitan el uso del sistema por parte de personas no autorizadas	3
[S] SERVICIOS	7	Servidor de archivos FTP: Servidor marca dell en torre PowerEdge T130	[A24] Denegación de servicio	Falta de filtros que protejan al sistema contra saturaciones	4
[HW] EQUIPAMENTO INFORMÁTICO	8	Servidor de archivos FTP: Servidor marca dell en torre PowerEdge T130	[I5] Avería de origen físico o lógico	Envejecimiento del hardware	3

Cuadro 14. (Continuación)

[HW] EQUIPAMENTO INFORMÁTICO	9	Servidor de archivos FTP: Servidor marca dell en torre PowerEdge T130	[I7] Condiciones inadecuadas de temperatura o humedad	Necesita climatización para funcionar	5
[HW] EQUIPAMENTO INFORMÁTICO	10	Servidor de archivos FTP: Servidor marca dell en torre PowerEdge T130	[I7] Condiciones inadecuadas de temperatura o humedad	Falta de hardware redundante	2
[HW] EQUIPAMENTO INFORMÁTICO	11	Servidor de archivos FTP: Servidor marca dell en torre PowerEdge T130	[I11] Emanaciones electromagnéticas	Hardware sensible a las emisiones electromagnéticas (restaurante y cocina)	1
[S] SERVICIOS	12	Página web Plan Máximo	[A5] Suplantación de la identidad del usuario	Posibilidad de gestionar el sistema en forma remota	4
[SW] SOFTWARE	13	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	[E21] Errores de mantenimiento / actualización de programas (software)	Uso de una versión obsoleta de las aplicaciones	3

Cuadro 14. (Continuación)

[S] SERVICIOS	14	Servidor DHCP Servidor marca dell en torre PowerEdge T440	[A5] Suplantación de la identidad del usuario	Posibilidad de gestionar el sistema en forma remota con herramientas de gestión no cifradas	4
[S] SERVICIOS	15	Servidor DHCP Servidor marca dell en torre PowerEdge T440	[A24] Denegación de servicio	Falta de filtros que protejan al sistema contra saturaciones	4
[HW] EQUIPAMENTO INFORMÁTICO	16	Servidor DHCP Servidor marca dell en torre PowerEdge T440	[I5] Avería de origen físico o lógico	Falta de instrucciones de reacciones rápidas para la protección del hardware en caso de perjuicios ocasionados por el agua o por un incendio (restaurante y cocina)	3
[HW] EQUIPAMENTO INFORMÁTICO	17	Servidor DHCP Servidor marca dell en torre PowerEdge T440	[I5] Avería de origen físico o lógico	Envejecimiento del hardware	3
[HW] EQUIPAMENTO INFORMÁTICO	18	Servidor DHCP Servidor marca dell en torre PowerEdge T440	[I7] Condiciones inadecuadas de temperatura o humedad	Necesita climatización para funcionar	5

Cuadro 14. (Continuación)

[HW] EQUIPAMENTO INFORMÁTICO	19	Servidor DHCP Servidor marca dell en torre PowerEdge T440	[I7] Condiciones inadecuadas de temperatura o humedad	Falta de hardware redundante	2
[HW] EQUIPAMENTO INFORMÁTICO	20	Equipos de cómputo para gestión del desarrollo tecnológico	[I5] Avería de origen físico o lógico	Envejecimiento del hardware	3
[HW] EQUIPAMENTO INFORMÁTICO	21	Equipos de cómputo para gestión del desarrollo tecnológico	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de informes de las operaciones de mantenimiento	2
[HW] EQUIPAMENTO INFORMÁTICO	22	Cortafuegos Cisco ASA 5505	[I5] Avería de origen físico o lógico	Falta de instrucciones de reacciones rápidas para la protección del hardware en caso de perjuicios ocasionados por el agua o por un incendio (restaurante y cocina)	3
[HW] EQUIPAMENTO INFORMÁTICO	23	Cortafuegos Cisco ASA 5505	[I5] Avería de origen físico o lógico	Envejecimiento del hardware	3
[HW] EQUIPAMENTO INFORMÁTICO	24	Cortafuegos Cisco ASA 5505	[E2] Errores del administrador	Faltan normas técnicas de filtrado	4

Cuadro 14. (Continuación)

[HW] EQUIPAMENTO INFORMÁTICO	25	Equipos de Cómputo Sistemas operativos win 10 Pro	[I5] Avería de origen físico o lógico	Envejecimiento del hardware	3
[HW] EQUIPAMENTO INFORMÁTICO	26	Equipos de Cómputo Sistemas operativos win 10 Pro	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de informes de las operaciones de mantenimiento	2
[SW] SOFTWARE	27	Equipos de Cómputo Sistemas operativos win 10 Pro	[E21] Errores de mantenimiento / actualización de programas (software)	Uso de una versión obsoleta de las aplicaciones o componentes del sistema operativo	3
[HW] EQUIPAMENTO INFORMÁTICO	28	Equipos de Cómputo	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de informes de las operaciones de mantenimiento	3
[HW] EQUIPAMENTO INFORMÁTICO	29	Puntos de acceso alámbricos (hub)	[I5] Avería de origen físico o lógico	Envejecimiento del hardware	3
[HW] EQUIPAMENTO INFORMÁTICO	30	Switches cisco catalyst 2960	[I5] Avería de origen físico o lógico	Envejecimiento del hardware	3
[HW] EQUIPAMENTO INFORMÁTICO	31	Teléfonos IP	[I5] Avería de origen físico o lógico	Envejecimiento del hardware	3
[HW] EQUIPAMENTO INFORMÁTICO	32	Puntos de acceso	[I5] Avería de origen físico o lógico	Envejecimiento del hardware	3
[P] PERSONAL	33	Técnicos de mantenimiento	[E28] Indisponibilidad del personal	Ausencia del puesto de trabajo por enfermedad	3

Fuente: "Elaboración propia a partir del Documento Matriz de Análisis de Riesgos (Magerit) – UNAD"

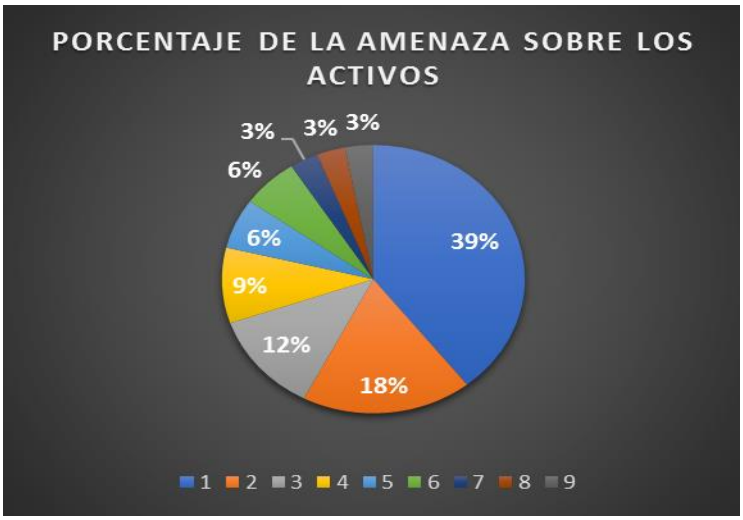
A continuación, vamos a realizar un análisis estadístico de la frecuencia de las amenazas que inciden sobre los activos de información de la empresa QWERTY S.A para lo cual realizamos la *Tabla 4* y el gráfico de la *Figura 15*, donde verificaremos cuales son las más frecuentes para tener en cuenta al momento de generar las salvaguardas y modelar el sistema de gestión seguridad de la información de la empresa QWERTY S.A.:

Tabla 4. Frecuencia de las amenazas que inciden sobre los activos de QWERTY S.A

No.	AMENAZA	FRECUENCIA	PORCENTAJE
1	[I5] Avería de origen físico o lógico	13	39%
2	[I7] Condiciones inadecuadas de temperatura o humedad	6	18%
3	[A5] Suplantación de la identidad del usuario	4	12%
4	[E23] Errores de mantenimiento / actualización de equipos (hardware)	3	9%
5	[A24] Denegación de servicio	2	6%
6	[E21] Errores de mantenimiento / actualización de programas (software)	2	6%
7	[E2] Errores del administrador	1	3%
8	[E28] Indisponibilidad del personal	1	3%
9	[I11] Emanaciones electromagnéticas	1	3%

Fuente: “Elaboración propia”

Figura 15. Gráfico del porcentaje de frecuencia de las amenazas sobre los activos de QWERTY S.A



Fuente: "Elaboración propia"

Aunado a lo anterior, tenemos que verificar la probabilidad de vulneración que tienen las amenazas sobre los activos de información de la empresa, con el fin de visionar que tipo de salvaguardas podemos emplear para prevenir y mitigar las amenazas y así reducir el riesgo, por tal motivo se establece el siguiente gráfico, para analizar este contexto:

Figura 16. Gráfico de probabilidad de vulneración de los activos

Fuente: "Elaboración propia"

En esta figura podemos observar, que de acuerdo con la probabilidad de vulneración donde la calificación de 1 corresponde a "Muy raro", 2 a "Poco

probable", 3 a "Posible", 4 a "Probable" y 5 a "Prácticamente seguro"; Las amenazas y vulnerabilidades que más requieren atención son el número de calificación 4 y 5, siendo estas las amenazas N° 3,5,7,9,12,14.15,18 y 24 que corresponden a:

Cuadro 15. Amenazas y vulnerabilidades que requieren atención Urgente para la empresa QWERTY S.A

ACTIVO	No. De Amenaza	Nombre del activo	Amenaza	Vulnerabilidad	Probabilidad de vulneración
[HW] EQUIPAMENTO INFORMÁTICO	3	Servidor de Impresión: Servidor marca Dell en torre PowerEdge T440	[I7] Condiciones inadecuadas de temperatura o humedad	Necesita climatización para funcionar	5
[S] SERVICIOS	5	Servidor de archivos FTP: Servidor marca Dell en torre PowerEdge T130	[A5] Suplantación de la identidad del usuario	Posibilidad de gestionar el sistema en forma remota con herramientas de gestión no cifradas	4
[S] SERVICIOS	7	Servidor de archivos FTP: Servidor marca Dell en torre PowerEdge T130	[A24] Denegación de servicio	Falta de filtros que protejan al sistema contra saturaciones	4
[HW] EQUIPAMENTO INFORMÁTICO	9	Servidor de archivos FTP: Servidor marca Dell en torre PowerEdge T130	[I7] Condiciones inadecuadas de temperatura o humedad	Necesita climatización para funcionar	5
[S] SERVICIOS	12	Página web Plan Máximo	[A5] Suplantación de la identidad del usuario	Posibilidad de gestionar el sistema en forma remota	4
[S] SERVICIOS	14	Servidor DHCP Servidor marca Dell en torre PowerEdge T440	[A5] Suplantación de la identidad del usuario	Posibilidad de gestionar el sistema en forma remota con herramientas de gestión no cifradas	4

Cuadro 16. (Continuación)

[S] SERVICIOS	15	Servidor DHCP Servidor marca Dell en torre PowerEdge T440	[A24] Denegación de servicio	Falta de filtros que protejan al sistema contra saturaciones	4
[HW] EQUIPAMENTO INFORMÁTICO	18	Servidor DHCP Servidor marca Dell en torre PowerEdge T440	[I7] Condiciones inadecuadas de temperatura o humedad	Necesita climatización para funcionar	5
[HW] EQUIPAMENTO INFORMÁTICO	24	Cortafuegos Cisco ASA 5505	[E2] Errores del administrador	Faltan normas técnicas de filtrado	4

Fuente: "Elaboración propia a partir del Documento Matriz de Análisis de Riesgos (Magerit) – UNAD"

Así las cosas, realizamos un diagrama de Pareto que nos traza la distribución de los activos que más se afectan en orden descendente de frecuencia, comparando este con un porcentaje total, en el cual podremos analizar cuáles son los más afectados con el fin de orientar las salvaguardas y el modelo del sistema.

Figura 17. Diagrama de Pareto de los activos más afectados

Fuente: "Elaboración propia"

Aquí en este gráfico observamos que el Servidor de archivos FTP y el Servidor DHCP son los activos con más riesgo dentro de la empresa QWERTY S.A. con una frecuencia de probabilidad de vulneración de 13 que representa cerca del 95%, lo

cual nos infiere que debemos enfocar principalmente las salvaguardas para estos activos.

6.3.6 Análisis y evaluación del riesgo. Para realizar un análisis y evaluación del riesgo para determinar que salvaguardas se van a implementar y orientar el modelo del sistema de gestión de seguridad de la información para la empresa QWERTY S.A. tomamos como punto primordial el *Cuadro 17***,** en la cual podremos apreciar la evaluación individual de cada amenaza donde podremos apreciar el Cálculo del riesgo neto (Magnitud que se relaciona proporcionalmente de la valoración del riesgo junto con la probabilidad de la vulneración), la Criticidad neta, la Calificación de gestión (donde se evalúa si existen los controles y qué tan eficaces son), Riesgo residual (Magnitud que se relaciona inversamente proporcional del riesgo neto sobre la calificación de la gestión), Criticidad residual y finalmente el nivel de aceptación del riesgo, donde la dirección de la empresa QWERTY S.A. determina que el nivel a tratar del riesgo será aquellos que sean Inaceptables.

Cuadro 16.Análisis y evaluación de riesgos

e Amenazas y Vulnerabilidades	**Amenazas Metodología** Magerit	**Vulnerabilidades**	**Cálculo del** riesgo neto (Valoración del riesgo * probabilidad de **vulneración)**	**Criticidad neta** (1 a 4 despreciable (d), 5 a 9 baja (B), 10 a 15 apreciable (a), 16 a 20 importante (i), 21 a 25 crítico(C))	**Calificación de Gestión (1 control** no existe, 2 existe, pero no efectivo, 3 efectivo, pero no documentado, 4 efectivo y documentado)	**Si la opción es 2 - 3 o 4 Indique el Control aplicado actual**	**Riesgo residual** (riesgo neto dividido entre la calificación de gestión)	**Criticidad residual** (1 a 4 despreciable (d), 5 a 9 baja (B), 10 a 15 apreciable (a), 16 a 20 importante (i), 21 a 25 crítico(C))	**Niveles de aceptación del riesgo** (1 a 5 aceptable (A), 6 a 15 moderado (M), 16 a 26 inaceptable(I))

Cuadro 16. (Continuación)

1	[I5] Avería de origen físico o lógico	Falta de instrucciones de reacciones rápidas para la	45	C	2	A.11.2.4 Mantenimiento de equipos (se	23	C	I

		protección del hardware en caso de perjuicios ocasionados por el agua o por un incendio (restaurante y cocina)				realiza mantenimiento; se desconocen los demás riesgos)			
2	[I5] Avería de origen físico o lógico	Envejecimiento del hardware	45	C	3	A.11.2.4 Mantenimiento de equipos (se realiza mantenimiento; no se cuenta con un control de los mismos)	15	A	I
3	[I7] Condiciones inadecuadas de temperatura o humedad	Necesita climatización para funcionar	75	C	1		75	C	I
4	[I7] Condiciones inadecuadas de temperatura o humedad	Falta de hardware redundante	30	C	1		30	C	I
5	[A5] Suplantación de la identidad del usuario	Posibilidad de gestionar el sistema en forma remota con herramientas de gestión no cifradas	60	C	1		60	C	I
6	[A5] Suplantación de la identidad del usuario	Los recursos compartidos facilitan el uso del sistema por parte de personas no autorizadas	45	C	1		45	C	I
7	[A24] Denegación de servicio	Falta de filtros que protejan al sistema contra saturaciones	60	C	2	A.13.1.2 Seguridad de los servicios de red (Cortafuegos sin configurar)	30	C	I
8	[I5] Avería de origen físico o lógico	Envejecimiento del hardware	45	C	3	A.11.2.4 Mantenimiento de equipos (se realiza mantenimiento; no se cuenta	15	A	I

Cuadro 16. (Continuación)

						con un control de los mismos)			
9	[I7] Condiciones inadecuadas de temperatura o humedad	Necesita climatización para funcionar	75	C	1		75	C	I
10	[I7] Condiciones inadecuadas de temperatura o humedad	Falta de hardware redundante	30	C	1		30	C	I
11	[I11] Emanaciones electromagnéticas	Hardware sensible a las emisiones electromagnéticas (restaurante y cocina)	15	A	1		15	A	I
12	[A5] Suplantación de la identidad del usuario	Posibilidad de gestionar el sistema en forma remota	64	C	3	A.13.1.2 Seguridad de los servicios de red (proveedor)	21	C	I
13	[E21] Errores de mantenimiento / actualización de programas (software)	Uso de una versión obsoleta de las aplicaciones	54	C	1		54	C	I
14	[A5] Suplantación de la identidad del usuario	Posibilidad de gestionar el sistema en forma remota con herramientas de gestión no cifradas	68	C	1		68	C	I
15	[A24] Denegación de servicio	Falta de filtros que protejan al sistema contra saturaciones	68	C	2	A.13.1.2 Seguridad de los servicios de red (Cortafuegos sin configurar)	34	C	I
16	[I5] Avería de origen físico o lógico	Falta de instrucciones de reacciones rápidas para la protección del hardware en caso de perjuicios	51	C	2	A.11.2.4 Mantenimiento de equipos (se realiza mantenimiento; se desconocen	26	C	I

Cuadro 16. (Continuación)

		ocasionados por el agua o por un incendio (restaurante y cocina)				los demás riesgos)			
17	[I5] Avería de origen físico o lógico	Envejecimiento del hardware	51	C	3	A.11.2.4 Mantenimiento de equipos (se realiza mantenimiento; no se cuenta con un control de los mismos)	17	I	I
18	[I7] Condiciones inadecuadas de temperatura o humedad	Necesita climatización para funcionar	85	C	1		85	C	I
19	[I7] Condiciones inadecuadas de temperatura o humedad	Falta de hardware redundante	34	C	1		34	C	I
20	[I5] Avería de origen físico o lógico	Envejecimiento del hardware	57	C	3	A.11.2.4 Mantenimiento de equipos (se realiza mantenimiento; no se cuenta con un control de los mismos)	19	I	I
21	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de informes de las operaciones de mantenimiento	38	C	3	A.11.2.4 Mantenimiento de equipos (se realiza mantenimiento; no se tiene documentado el seguimiento de los mismos)	13	A	M
22	[I5] Avería de origen físico o lógico	Falta de instrucciones de reacciones rápidas para la protección del hardware en caso de perjuicios ocasionados por el agua o por un incendio	60	C	2	A.11.2.4 Mantenimiento de equipos (se realiza mantenimiento; se desconocen los demás riesgos)	30	C	I

Cuadro 16. (Continuación)

		(restaurante y cocina)							
23	[I5] Avería de origen físico o lógico	Envejecimiento del hardware	60	C	3	A.11.2.4 Mantenimiento de equipos (se realiza mantenimiento; no se cuenta con un control de los mismos)	20	I	I
24	[E2] Errores del administrador	Faltan normas técnicas de filtrado	80	C	1		80	C	I
25	[I5] Avería de origen físico o lógico	Envejecimiento del hardware	30	C	3	A.11.2.4 Mantenimiento de equipos (se realiza mantenimiento; no se registra un control de los mismos)	10	B	M
26	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de informes de las operaciones de mantenimiento	20	I	3	A.11.2.4 Mantenimiento de equipos (se realiza mantenimiento; no se realiza informes de control y gestión)	7	B	M
27	[E21] Errores de mantenimiento / actualización de programas (software)	Uso de una versión obsoleta de las aplicaciones o componentes del sistema operativo	30	C	3	A.11.2.4 Mantenimiento de equipos (se realiza mantenimiento; no se tiene registro de estas actividades)	10	B	M
28	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de informes de las operaciones de mantenimiento	33	C	3	A.11.2.4 Mantenimiento de equipos (se realiza mantenimiento; no se registra	11	A	M

Cuadro 16. (Continuación)

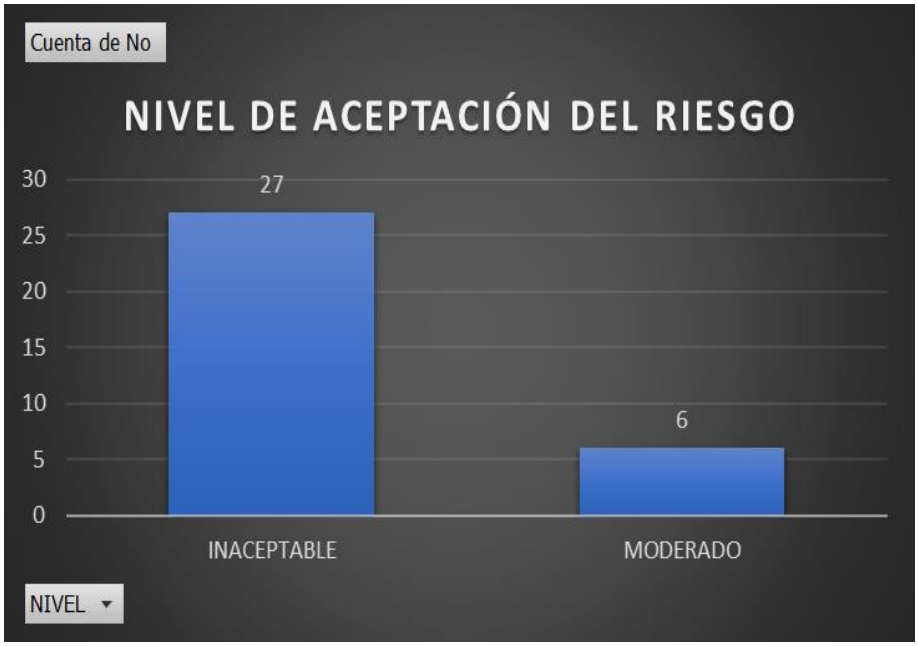
						un control de los mismos)			
29	[I5] Avería de origen físico o lógico	Envejecimiento del hardware	57	C	3	A.11.2.4 Mantenimiento de equipos (no se registra un control de los mismos)	19	I	I
30	[I5] Avería de origen físico o lógico	Envejecimiento del hardware	57	C	3	A.11.2.4 Mantenimiento de equipos (se realiza mantenimiento; no se registra un control de los mismos)	19	I	I
31	[I5] Avería de origen físico o lógico	Envejecimiento del hardware	30	C	3	A.11.2.4 Mantenimiento de equipos (se realiza mantenimiento; no se registra un control de los mismos)	10	B	M
32	[I5] Avería de origen físico o lógico	Envejecimiento del hardware	54	C	3	A.11.2.4 Mantenimiento de equipos (se realiza mantenimiento; no se registra un control de los mismos)	18	I	I
33	[E28] Indisponibilidad del personal	Ausencia del puesto de trabajo por enfermedad	33	C	1		33	C	I

Fuente: "Elaboración propia a partir del Documento Matriz de Análisis de Riesgos (Magerit) – UNAD"

Por lo anterior realizamos el siguiente gráfico en el cual podremos observar de manera objetiva el estado actual de la evaluación del riesgo en la empresa con relación de su nivel de aceptación y si hay riesgos que necesiten tratamiento de

manera primordial y así determinar las respectivas salvaguardas para la implementación del SGSI.

Figura 18. Gráfico del nivel de aceptación del riesgo



Fuente: “Elaboración propia”

En el gráfico podemos apreciar que 27 de las 33 amenazas identificadas tienen un nivel “Inaceptable”, por ende, deben ser sometidas a un tratamiento del riesgo excluyéndose así de acuerdo con los datos contenidos en el cuadro anterior las amenazas No. 21, 25, 26, 27, 28 y 31 que tienen un nivel “Moderado” de concordancia con los parámetros establecidos por la Dirección.

6.3.7 Salvaguardas y propuesta para la gestión del riesgo. De acuerdo con el anterior análisis y evaluación de amenazas y riesgos, se determinó las contramedidas o salvaguardas que podemos apreciar en el *Cuadro 18* teniendo en cuenta la metodología *Magerit*, las cuales obraran como mecanismos considerados efectivos para reducir y mitigar el riesgo identificado ante la dirección de la empresa QWERTY S.A.

Cuadro 17. Salvaguardas para la empresa QWERTY S.A.

CLASIFICACIÓN	SALVAGUARDA
Protecciones generales u horizontales	✓ **H.tools.IDS IDS/IPS** - Herramienta de detección / prevención de intrusión. ✓ **H.tools.TM** - Herramienta de monitorización de tráfico.
Protección de las aplicaciones (software)	✓ **SW.SC** - Se aplican perfiles de seguridad. ✓ **SW.CM** - Cambios (actualizaciones y mantenimiento).
Protección de las comunicaciones	✓ **COM** - Protección de las Comunicaciones.
Protección de los elementos auxiliares	✓ **AUX.AC** – Climatización.
Protección de los servicios	✓ **S.A** - Aseguramiento de la disponibilidad.
Seguridad física – Protección de las instalaciones	✓ **L.AC** - Control de los accesos físicos.
Salvaguardas relativas al personal	✓ **PS.AT** - Formación y concienciación.
Externalización	✓ **E.4** - Personal subcontratado.

Fuente: “Elaboración propia”

6.3.8 Plan de tratamiento de riesgos. Después de haber identificado, clasificado, valorado, y evaluado, junto con su probabilidad de que ocurran y su nivel de aceptación de cada una de las amenazas y riesgos que afectan a los activos de información de la empresa, se realizó un *plan de tratamiento de riesgos* el cual permite establecer medidas, procedimientos, actividades, recursos y responsabilidades en el tratamiento del riesgo (Véase la Cuadro 19 del Anexo B).

6.3.9 Informe de evaluación de riesgos.

6.3.9.1 Metodología aplicada. Este proceso se ha realizado de acuerdo con la Metodología de evaluación y tratamiento del riesgo de *Magerit*.

6.3.9.2 Proceso de evaluación y tratamiento de riesgo. En la evaluación y tratamiento de riesgos se utilizó la metodología escogida para poder cuantificar la posible ocurrencia de las amenazas identificadas sobre los activos de la empresa QWERTY S.A y su impacto y con base en ellos, poder modelar de forma correcta un sistema de gestión de seguridad de la información para prevenir y contrarrestar estas amenazas de manera eficaz.

6.3.9.3 Iniciativas para el tratamiento del riesgo. Las medidas para el tratamiento del riesgo después de la evaluación son los siguientes:

Mitigar: Aquí la organización define que el valor del riesgo es relevante, por tanto, se debe realizar una evaluación de las contra medidas o salvaguardas que debe aplicar según lo que requiera la organización y el presupuesto con el que se cuente, aquí se debe incluir aquellos riesgos que hayan salido calificados como “Riesgo Medio” o “Riesgo Alto”, buscando crear acciones que permitan reducir la probabilidad de que se materialice la amenaza.

Transferir: Se determina esta cuando la organización define el valor del riesgo implementando medidas de mitigación y aun cuando se aplican el valor resultante del riesgo es “Riesgo Alto” y aunque su probabilidad de materialización es baja, su impacto puede ser devastador.

Aceptar: Se determina cuando el valor del riesgo para la organización es irrelevante (BAJO) y se decide no tomar acciones, ya que este no puede causar gran impacto dentro de la compañía o en el producto que se ofrece.

Los controles que serán implementados para tratar los riesgos deben asegurar la reducción hasta un nivel aceptable de los mismos y están previamente referenciados en el Plan de Tratamiento de riesgos de la empresa.

6.3.9.4 control de efectividad. A fin de constatar la efectividad de los controles implementados para el sistema, se debe realizar un control de manera periódica y permanente, con el cual se pueda obtener el riesgo residual a partir de los riesgos identificados dentro de la organización.

6.3.9.5 Supervisión de la evaluación y tratamiento de riesgos. Es importante aclarar, que se debe implementar una valoración de los riesgos en intervalos de revisión planificada mínimo una vez al año o cuando sea conveniente, como cambios de estructura, actualizaciones tecnológicas y procesos del negocio.

Es preciso recalcar que el proceso de evaluación y valoración de riesgos debe conservar antecedentes de forma documentada para que obren como soportes. Adicionalmente los controles deben evaluarse de manera periódica, puesto que, si dan resultados inesperados, se debe aplicar las acciones de mejora a través del ciclo PHVA para corregirlo.

6.4 DESARROLLO OBJETIVO 4

6.4.1 Controles. Es en este punto donde definimos los controles adecuados para implementar en la empresa QWERTY S.A, orientando al igual cuáles serán los objetivos de los controles, su implementación y demás aspectos necesarios que

encaminarán el modelo del sistema de gestión de seguridad de la información de la empresa.

A partir de los datos relacionados en el *Cuadro 16*, podemos observar la aplicabilidad con la que contaba inicialmente la empresa con relación a los controles de la norma ISO 27001 en la columna de "Clasificación de la Gestión", adicionalmente nos ayuda a aprobar en las columnas contiguas la calificación del riesgo residual en pro definir la implementación de los controles finales para la empresa; por ello, se realizó el gráfico en la *Figura 19*, en el cual vamos a evidenciar el nivel de cumplimiento inicial de la ISO 27001 dentro de la organización:

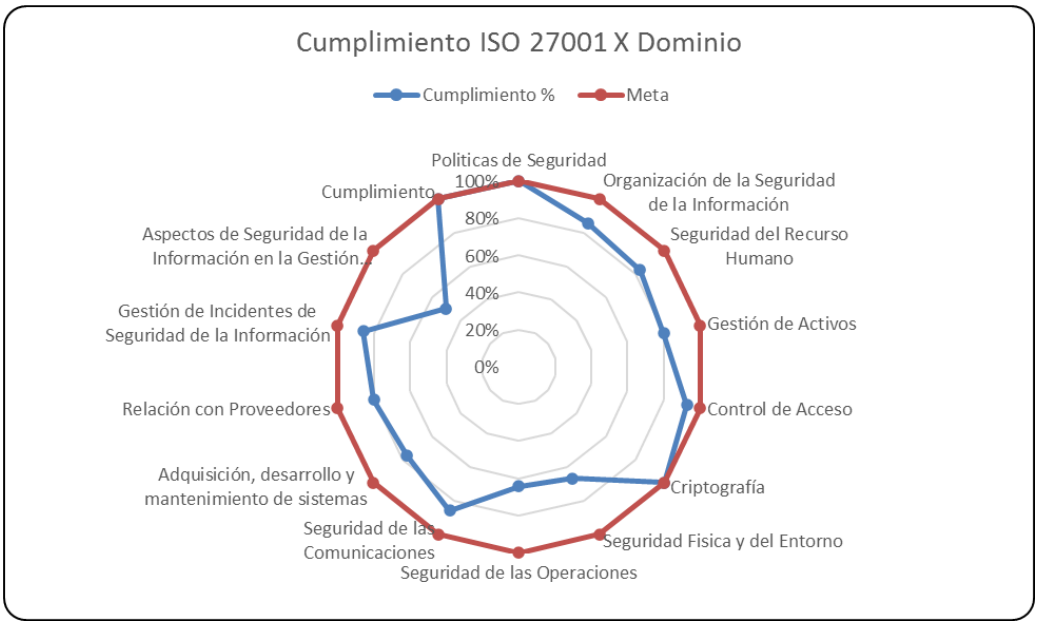
Figura 19. Gráfico de la Clasificación de la Gestión ISO 27001 de la empresa QWERTY S.A.

Fuente: "Elaboración propia"

En el anterior gráfico podemos analizar que aproximadamente el 39.4% de los activos de información de la empresa QWERTY S.A. no implementaba ningún control para salvaguardar sus activos, el resto se implementaban con falencias en su aplicación o no son efectivos.

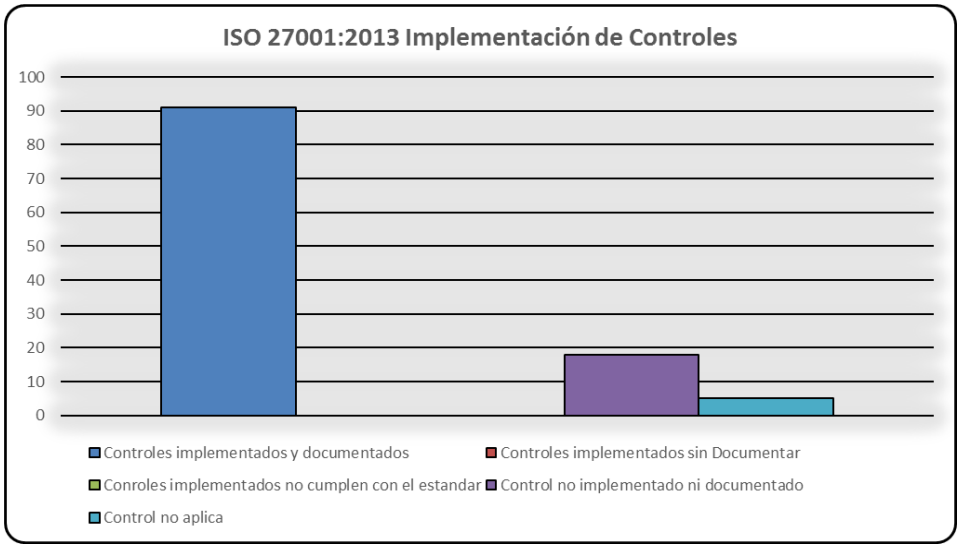
6.4.1.1 Implementación de los controles de la ISO 27001 en QWERTY S.A. Finalmente se realizó una reunión con la dirección de QWERTY S.A donde se dieron a conocer los controles necesarios de acuerdo con el resultado de la evaluación del riesgo, los cuales se referenciaron en el *Cuadro 20* del *Anexo C*. Así las cosas y con el objeto de ampliar la aplicabilidad de la norma ISO 27001, se determinó junto con la dirección de la empresa QWERTY S.A los requerimientos de seguridad y presupuesto para la implementación de los controles finales que se van a implementar en la entidad, los cuales se plasmaron en el *Cuadro 21* del *Anexo D*.

Figura 20. Gráfico de porcentaje de cumplimiento final de la empresa durante la aplicación del sistema



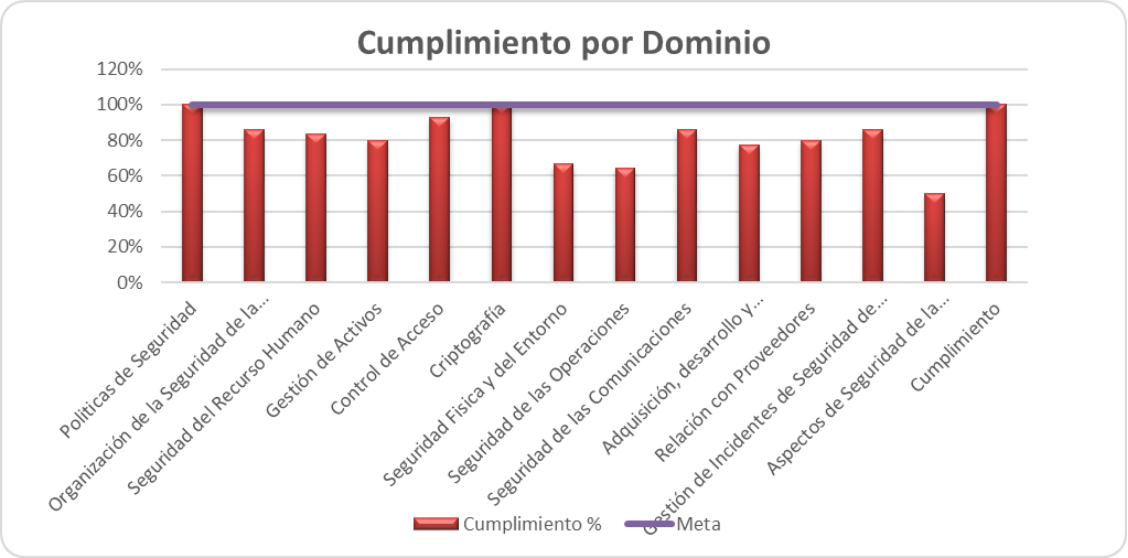
Fuente: Elaboración propia a partir del Documento excel *"ISO27K_SOA_2013 – UNAD"*

Figura 21. Gráfico de tipo de controles implementados de acuerdo con la norma ISO 27001



Fuente: Elaboración propia a partir del Documento excel *"ISO27K_SOA_2013 – UNAD"*

Figura 22. Gráfico de porcentaje de cumplimiento por dominio de los controles definidos



Fuente: Elaboración propia a partir del Documento excel ISO27K_SOA_2013 - UNAD

En las anteriores *figuras 20, 21 y 22* ser relacionan los resultados del cumplimiento de la norma, evidenciando varios aspectos positivos para QWERTY S.A entre los cuales observamos una amplia aplicación de los controles de la norma ISO 27001, que representa cerca del 91% de implementación de los controles dentro de la entidad; siendo las “Políticas de seguridad”, “Criptografía” y “Cumplimiento” los dominios que llegaron al 100% del cumplimiento.

Estos controles aprobados por la dirección de QWERTY S.A. darán una cobertura a la necesidad actual de la empresa en su abordaje o implementación inicial, debiéndose ampliar el cumplimiento con el paso del tiempo o cuando se amerite a través de los comités de seguimiento del sistema, donde se deberá realizar evaluaciones de la proyección de crecimiento y consecución de recursos necesarios para la protección de todos los activos de información, para así brindar tranquilidad y respaldo a los clientes y usuarios en los servicios que presta la organización.

6.4.2 Recomendaciones. Para la implementación del sistema proyectado en la empresa, es necesario adquirir los siguientes equipos y servicios:

- Implantación de un servicio de dominio para la gestión de usuarios y equipos en la red.
- Adecuación de las instalaciones
- Sistema de control ambiental (Climatización)

- Sistema de control de contraseñas
- Sistema de control de acceso Biométrico.
- Software de Borrado Seguro de la Información

Estos requerimientos se relacionan a continuación en el cálculo de costos para la adquisición de estos elementos y los necesarios para la implementación del sistema de gestión en la empresa.

6.4.3 Calculo de costos.

6.4.3.1 Costos de adquisición de equipos y servicios.

Tabla 5. Costos de adquisición de Equipos Tecnológicos y Servicios

TIPO	DESCRIPCIÓN	CANTIDAD	TOTAL
Servicio de dominio	• Servidor Rack • Licencia Windows Server 2019	1	$ 8´585.900
Sistema de control ambiental	Sistema de climatización (aires acondicionados, sistema de control, cableado, etc)	1	$32’700.000
Sistema de control de contraseñas	Software gestor de contraseñas	1 licencia /año	$150.000
Sistema de control biométrico	Sistema de control de acceso (servidor de huellas, electroimanes, torniquetes de paso, lectores biométricos)	1	$60.650.600
Software	Software de borrado seguro de la información	1 licencia /año	$600.000
Total Equipos y Servicios			**$ 102’146.500**

Fuente: “Elaboración propia”

6.4.3.2 Costos recursos humanos.

Tabla 6. Costos de Recursos Humanos

TIPO	DESCRIPCIÓN	VALOR - HORA	CANTIDAD	TOTAL
Tutor del SGSI	Asesoría de un profesional para la aplicación de una metodología adecuada sobre la Norma ISO 27001:2013	$ 50.000	120 Horas	$ 6’000.000
Analistas e implementadores	Se requiere 1 analista y 1 implementador para poner en marcha el SGSI	$ 28.000	10 Horas x 32 Semanas	$ 8’960.000
Total Recursos Humanos				**$ 14’960.000**

Fuente: “Elaboración propia”

6.4.3.3 Costos de recursos administrativos.

Tabla 7. Costos de Recursos Administrativos

RECURSO	DESCRIPCIÓN	VALOR UNITARIO	CANTIDAD	TOTAL
Capacitaciones	Capacitaciones sobre la Norma ISO 27001:2013 tanto para el personal administrativo como para los empleados de la entidad.	$ 370.000	3	$ 1’100.000

Publicidad educativa SGSI	Banner, afiches, videos académicos, entre otros	$2.000.000	2 (kit de 2 Banner, 3 afiches y 1 video educativo)	$4’000.000
Papelería y elementos	Impresiones, resmas de papel, fotocopias, entre otros.	$ 120.000	1	$ 120.000
Total Recursos Administrativos				**$ 5’230.000**

Fuente: “Elaboración propia”

6.4.3.4 Total de recursos.

Tabla 8. Costo total de recursos para la Implementación del SGSI

RECURSO	**VALOR**
Total Equipos y servicios	$ 102’146.500
Total Recursos Humanos	$ 14’960.000
Total Recursos Administrativos	$ 5’230.000
Total Recursos (Valor aproximado)	**$ 122’237.150**

Fuente: “Elaboración propia”

6.4.4 Cronograma de actividades para la implementación del SGSI en QWERTY S.A.

Tabla 9. Cronograma de actividades

Actividad	JUN	JUL	AGO	SEP	OCT	NOV	DIC
Revisión del alcance							
Implementación del ciclo PHVA							
Documentación de riesgos y amenazas							
Declaración de aplicabilidad							
Publicidad de las Políticas de							

SGSI							
Aplicación de los controles del SGSI en cada Área y Grupo							
Implantación y cumplimiento del SGSI en la empresa							

Fuente: “Elaboración propia”

6.4.5 Manual del sistema de gestión de seguridad de la información de QWERTY S.A. El sistema de gestión de seguridad de la información de QWERTY S.A estará guiado y parametrizado de acuerdo con el manual del sistema (*Ver Anexo E*), en el cual se encuentran plasmados los objetivos y políticas de seguridad para realizar el despliegue de controles del sistema de seguridad de la información.

6.4.6 Procedimientos documentados. De acuerdo con la norma ISO 9001 es un conjunto de instrucciones operativas o protocolos de actuación frente a una actividad especifica que requiera ser documentada, con los cuales se tiene por objeto reducir la variabilidad de las operaciones realizadas por el personal de la empresa y prevenir errores en su aplicación, estos son susceptibles de mejora y deben representarse de manera gráfica mediante diagramas de flujo.

Los procedimientos documentados para la aplicación de las políticas de seguridad de la información de la empresa QWERTY S.A. se relacionan en el *Anexo F.*

6.4.7 Formatos, Formularios y lista de chequeo. Los formatos, lista de chequeo y formularios (Cláusulas) se encuentran relacionados en el *Anexo G.*

7 CONCLUSIONES

La empresa QWERTY S.A. no cuenta con un sistema que blinde y garantice la seguridad de sus activos de información, por tanto, se hace necesario implementar un sistema de gestión de seguridad de la información, que minimice y reduzca el índice de vulnerabilidades que presenta en sus procesos de acuerdo con el problema planteado.

Para la implementación de seguridad de la información de una entidad se analizaron los riesgos y el nivel de seguridad con los que cuenta la entidad, con el fin de tomar como punto de partida los resultados del análisis para la toma de decisiones con respecto a la implementación de este sistema; evidenciando, que los pocos controles que se venían implementando, eran casi nulos, no existía una ruta o guía que estableciera parámetros acordes a las buenas prácticas, ni controles sobre la gran mayoría de activos, lo cual en evidencia ponía en riesgo los intereses de la empresa y sus clientes.

La evaluación de riesgos y amenazas nos sirvió como análisis para abordar de manera correcta la problemática presentada y presentar unas salvaguardas o contramedidas para proyectar de manera correcta los controles necesarios para la empresa.

Los controles proyectados para la implementación del sistema de gestión de seguridad de la información en la empresa QWERTY S.A., Otorgarán un soporte inicial para la implementación de este sistema, por lo cual la empresa deberá ampliar la cobertura de estos con el paso del tiempo para lograr la meta del 100%, dicha planeación se deberá proyectarse a través de reuniones del Comité de seguimiento del SGSI para realizar un abordaje de los controles necesarios que vaya requiriendo la empresa conforme se amplíe o cambie su estructura o misionalidad y los recursos para la inversión de los mismos.

8 RECOMENDACIONES

Como recomendación principal, se debe realizar una recolección de información de primera mano para este caso, puesto que este trabajo se centró en una investigación descriptiva a partir del análisis de “información secundaria”, lo cual expone a la investigación a la posibilidad de no controlar errores cometidos a la hora de haber recolectado esta información y con ello, haber dejado de lado algunos datos que podrían ser decisivos a la hora de realizar una planeación y análisis de situación, arrojándonos como consecuencia que el resultado de las variables no se definan de manera acorde a la problemática de la empresa QWERTY S.A y con ello que las necesidades en materia de Seguridad de los activos de información se cubran parcialmente, exponiendo parte de estos a posibles riesgos y vulnerabilidades no planteadas.

Para la planeación de la implementación de un SGSI en una entidad u organización, es pertinente tener en cuenta la clasificación de la empresa de acuerdo con el Decreto 957 del 05 de junio de 2019, con el fin de verificar el tamaño de la empresa y proyectar los recursos necesarios para la implementación del sistema, adicionalmente verificar la proyección de crecimiento de esta, con el fin de plantear de manera asertiva los recursos necesarios para dar cobertura a futuro

BIBLIOGRAFÍA

1. AL-RASHID, Ibrahim, NASIRUDDEEN, Vaseem y RADHAKRISHNAN, Sreechith, “Cómo COBIT 5 ayudó a Al Rajhi Bank a alcanzar los requerimientos de cumplimiento y regulatorios”, {En línea}. {04 de Febrero de 2019} disponible en: http://www.isaca.org/COBIT/focus/Pages/how-cobit-5-helped-al-rajhi-bank-to-meet- compliance-and-regulatory-requirements-spanish.aspx

2. Altamirano Di Luca M. Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso. (Spanish). Avances [Internet]. 2019 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edo&AN=135677506&lang=es&site=eds-live&scope=site

3. Altamirano Yupanqui JR, Bayona Oré S. Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento. (Spanish). RISTI: Iberian Journal on Information Systems & Technologies / Revista Ibérica de Sistemas e Tecnologias de Informação [Internet]. 2017 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edb&AN=128674523&lang=es&site=eds-live&scope=site

4. ÁLVAREZ RIAÑO, Jerzon Herley, “DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI BASADO EN LA NORMA ISO27001 PARA EL COLEGIO PROCOLOMBIANO DE LA CIUDAD DE BOGOTÁ, QUE INCLUYE: ASESORÍA, PLANEACIÓN”, {En línea}. {10 de Febrero de 2019} disponible en: https://repository.unad.edu.co/handle/10596/11950

5. Análisis de la preparación de las organizaciones Mapfre Perú Seguros y Kallpa Corredora de Seguros ante las amenazas de seguridad de la información en el medio empresarial y que podrían impactar en sus operaciones de negocio . {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.BA21D5F2&lang=es&site=eds-live&scope=site

6. Arévalo Moscoso FM. Elaboración y plan de implementación de políticas de seguridad de la información aplicadas a una empresa industrial de alimentos.

2017 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.BD25D475&lang=es&site=eds-live&scope=site

7. Armas Huamán AM, Perez Romero FR. Desarrollo de un sistema de gestión de seguridad de la información para minimizar riesgos en los activos de información en la sub gerencia de informática y telecomunicaciones de la Municipalidad Distrital de Independencia 2016. {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.5ECE1ADB&lang=es&site=eds-live&scope=site

8. Baca Flores VM. Diseño De Un Sistema De Gestión De La Seguridad De La Información Para La Unidad De Gestión Educativa Local - Chiclayo. 2016 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.9CEB9719&lang=es&site=eds-live&scope=site

9. BENAVIDES SEPÚLVEDA, A.; BLANDÓN JARAMILLO, C. Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico. Scientia et Technica, [s. l.], v. 23, n. 1, p. 85–92, {En línea}. {15 de Febrero de 2019} Disponible en: <http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=a9h&AN=130405186&lang=es&site=eds-live&scope=site>

10. Blumsztein EC. Implantación del Sistema de Gestión de Seguridad de la Información en una empresa compleja. Memoria de Trabajos de Difusion Cientifica y Técnica {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=zbh&AN=28340227&lang=es&site=eds-live&scope=site

11. Campos Cruz H ettorec04@cibnor. m. Fenomenología de la adopción de las Tecnologías de la Información y las Comunicaciones (TIC) en docentes de un Centro Público de Investigación. (Spanish). Dilemas Contemporáneos: Educación, Política y Valores [Internet]. 2019 Jan {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=eue&AN=134365757&lang=es&site=eds-live&scope=site

12. Cárdenas-Solano L-J leidy. cardenas2@correo. uis. edu. c., Martínez-Ardila H hugom@saber. uis. edu. c., Becerra-Ardila L-E lbecerra@uis. edu. c. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: REVISIÓN BIBLIOGRÁFICA. (Spanish). El Profesional de la Información. {En línea}. {10 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=aci&AN=119802423&lang=es&site=eds-live&scope=site

13. Carlos Encalada Loja, Diego Cordero Guzmán. Guía de auditoría para la evaluación del control interno de seguridad de la información con enfoque COBIT 5: caso Universidad Católica de Cuenca (UCACUE). Revista Científica y Tecnológica UPSE {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsdoj&AN=edsdoj.2affd4322ae54dec89809812f97f756b&lang=es&site=eds-live&scope=site

14. Celis Figueroa LA. Plan de seguridad de la información aplicado a la central hidroeléctrica Carhuaquero. 2018 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.9739F437&lang=es&site=eds-live&scope=site

15. Davila Villanueva MA. Evaluación de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001:2013, en la municipalidad distrital de José Crespo y Castillo - Aucayacu; 2018. 2018 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.D676681A&lang=es&site=eds-live&scope=site

16. DÍAZ, Andrés Fabián, COLLAZOS, Gloria Isabel, CORTEZ LOZANO, Hermes ORTIZ, Leidy Johanna y HERAZO PÉREZ, Gustavo Adolfo, “IMPLEMENTACION DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LA COMUNIDAD NUESTRA SEÑORA DE GRACIA, ALINEADO TECNOLÓGICAMENTE CON LA NORMA ISO 27001”, {En línea}. {12 de Febrero de 2019} disponible en: http://www.konradlorenz.edu.co/images/stories/articulos/SGSI.pdf

17. Diéguez M mauricio. dieguez@ceisufro. c., Cares C carlos. cares@ceisufro. c., Cachero C ccachero@dlsi. ua. e. Metodología para la Selección de Controles

de Seguridad de la Información. (Portuguese). CISTI (Iberian Conference on Information Systems & Technologies {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=aci&AN=127421046&lang=es&site=eds-live&scope=site

18. Diseño de un modelo de políticas basado en la norma ISO 27001, para mejorar la gestión de la seguridad de la información en la Municipalidad Distrital de Florida – Bongará – Amazona. 2018 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.5DF91D5F&lang=es&site=eds-live&scope=site

19. ENCICLOPEDIA DE CLASIFICACIONES. "Tipos de análisis". {En línea}. {06 de Diciembre de 2019}. Disponible en: https://www.tiposde.org/general/517-tipos-de-analisis/

20. Enríquez Collaguazo AA. Modelo de gestión de seguridad de la información para instituciones de salud, basado en las normas ISO 27799:2008, ISO/IEC 27005:2008 e ISO/IEC 27002:2013 aplicada a la clínica médica fértil. 2018 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.302900BF&lang=es&site=eds-live&scope=site

21. ERB, Markus. 7. Análisis de Riesgo. {En línea}. Fecha. {22/03/20}. Disponible en https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

22. FARFAN CORREA, Cesar Octavio, Jenith Marsella, “ANÁLISIS DEL NIVEL DE SEGURIDAD DE LOS ROLES Y PRIVILEGIOS, EN EL SISTEMA SAP ERP DE COLPENSIONES, TOMANDO COMO REFERENCIA LA NORMA ISO 27001 Y LAS GUÍAS DE SEGURIDAD DE SAP”, {En línea}. {10 de Febrero de 2019} disponible en: http://hdl.handle.net/10596/12852

23. Flores Barrios MCL, del Ángel MS, Camacho Díaz OD, Barrera Reyes MA. Evaluación Del Impacto De Los Sistemas De Gestion De Seguridad De La Información Bajo La Serie Iso/Iec 27001 en Empresas De La Ciudad De Tuxpan, Veracruz. Revista de la Alta Tecnología y Sociedad {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=tru

e&db=zbh&AN=67073510&lang=es&site=eds-live&scope=site

24. GALLARDO DE PARADA, Yolanda; MORENO GARZÓN, Adonay. APRENDER A INVESTIGAR. {En línea}. {05 de Diciembre de 2019}. Disponible en: http://www.unilibrebaq.edu.co/unilibrebaq/images/CEUL/mod3recoleccioninform.pdf

25. García Ospina BD. Análisis y diseño del sistema de gestión de seguridad de la información en la Cooperativa FAVI de la Universidad Tecnológica de Pereira. 2018 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.12EBACF8&lang=es&site=eds-live&scope=site

26. García Samamé SC. Modelo de seguridad de la información para contribuir en la gestión de las unidades ambientales de la región Lambayeque. 2018 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.3BCEE7AD&lang=es&site=eds-live&scope=site

27. Güillín Sanabria AA. Plan informático 2018 – 2022, basado en las normas ISO/IEC 27001:2013 para mejorar la seguridad de la información, procesos informáticos y recursos tecnológicos en la comisión de tránsito del ecuador UCT2 del cantón Santo Domingo. 2019 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.367DD538&lang=es&site=eds-live&scope=site

28. Implementación de los controles de la ISO/IEC 27002:2013 para la mejora del nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte. 2018 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.7FF04CC&lang=es&site=eds-live&scope=site

29. ISO27000.ES, “El portal de ISO 27002 en Español”, {En línea}. {09 de Febrero de 2019} disponible en: http://www.iso27000.es/iso27002.html

30. ISO27000.ES, “El portal de ISO 27001 en Español”, {En línea}. {09 de Febrero de 2019} disponible en: http://www.iso27000.es/sgsi.html

31. ISO27000.ES, “ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES”, {En línea}. {09 de Febrero de 2019} disponible en: http://iso27000.es/download/ControlesISO27002-2013.pdf

32. ISO 27000.es, “Sistema de Gestión de la Seguridad de la Información”, {En línea}. {04 de Febrero de 2019} disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

33. ISOTOOLS, “Cómo implementar un Sistema de Gestión de Seguridad de la Información”, {En línea}. {04 de Febrero de 2019} disponible en: https://www.isotools.org/2015/08/13/como-implementar-un-sistema-de-gestion-de- seguridad-de-la-informacion/

34. Lema Vinlasaca RC, Donoso Gallo DF. Implementación de un sistema de gestión de seguridad de información basado en la Norma ISO 27001:2013 para el control físico y digital de documentos aplicado a la empresa LOCKERS S.A. 2018 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.A2364073&lang=es&site=eds-live&scope=site

35. MAGERIT – versión 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro I - Método. 2012 {En línea}. {28 de Septiembre de 2019}. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XehG3ZNKjIU

36. MAGERIT – versión 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro II - Catálogo de Elementos. 2012 {En línea}. {28 de Septiembre de 2019}. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XehG3ZNKjIU

37. MAGERIT – versión 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro III - Guía de Técnicas. 2012 {En línea}. {28 de Septiembre de 2019}. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XehG3ZNKjIU

38. MERCADO PALENCIA, Yolima, “LEGISLACION Y NORMATIVA EN

SEGURIDAD INFORMATICA", {En línea}. {08 de Febrero de 2019} disponible en: https://repository.unad.edu.co/handle/10596/23527

39. MILTON, Sue, "Cómo COBIT 5 puede ayudar a reducir la probabilidad y el impacto de las 5 amenazas cibernéticas más importantes", {En línea}. {04 de Febrero de 2019} disponible en: http://www.isaca.org/COBIT/focus/Pages/how-cobit-5-can-help-reduce-the-likelihood-and-impact-of-the-top-5-cyberthreats-spanish.aspx

40. Monzón Escobar GA. El Teorema Inconcluso en el Proceso de la Seguridad de la Información (TIPSI) y la Implementación de la Estrategia de Ciberseguridad (IEC). {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.687A1EEA&lang=es&site=eds-live&scope=site

41. Muyón C, Guarda T, Vargas G, Ninahualpa Quiña G. Esquema Gubernamental de Seguridad de la Información EGSI y su aplicación en las entidades públicas del Ecuador. {En línea}. {14 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edb&AN=136334360&lang=es&site=eds-live&scope=site

42. Pardo Toledo VA. Plan informático 2018-2022 basado en la norma ISO/IEC 27001-2013 para mejorar la seguridad de la información e infraestructura tecnológica en el laboratorio clínico "LABPICHINCHA" en la ciudad de Santo Domingo. 2018 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.D342CE18&lang=es&site=eds-live&scope=site

43. Perugachi Espinosa CA. Modelo de seguridad de gestión de la información basado en la norma ISO 27001, para el data-center de la facultad de Ingeniería en Ciencias Aplicadas, en la Universidad Técnica del Norte. 2018 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.723B1C1F&lang=es&site=eds-live&scope=site

44. Pizarro Sánchez IA. Diseño de un modelo de gestión de seguridad de la información con un enfoque en el factor humano para el ICPNA Región Centro en el año 2017. 2018 [cited 2019 May 22]; Available from: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=tru

e&db=edsbas&AN=edsbas.AB2A796E&lang=es&site=eds-live&scope=site

45. PRANDINI, Patricia y SZUSTER, Rodolfo, “RE-EVOLUCIÓN COBIT”, {En línea}. {04 de Febrero de 2019} disponible en: http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT5-and-InfoSec-Spanish.ppt

46. PULIDO BARRETO, Ana Milena y MANTILLA RODRÍGUEZ, Jenith Marsella, “MODELO PARA LA IMPLEMENTACIÓN DEL SISTEMA GENERAL DE SEGURIDAD INFORMÁTICA Y PROTOCOLOS DE SEGURIDAD INFORMÁTICA EN LA OFICINA TIC DE LA ALCALDÍA MUNICIPAL DE FUSAGASUGÁ, BASADOS EN LA GESTIÓN DEL RIESGO INFORMÁTICO”, {En línea}. {10 de Febrero de 2019} disponible en: https://repository.unad.edu.co/handle/10596/6327

47. Ramos Y, Urrutia O, Bravo A, Ordoñez D. Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO/IEC 27002:2013 para la Cooperativa Codelcauca. 2017 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.5A47F8C6&lang=es&site=eds-live&scope=site

48. Reglamento de Ejecución (UE) 2018/151 de la Comisión, de 30 de enero de 2018, por el que se establecen normas para la aplicación de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo en lo que respecta a la especificación de los elementos que han de tener en cuenta los proveedores de servicios digitales para gestionar los riesgos existentes para la seguridad de las redes y sistemas de información, así como de los parámetros para determinar si un incidente tiene un impacto significativo. España, Europa. {En línea}. {15 de Febrero de 2019}. Disponible en: <http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.75B8D4C1&lang=es&site=eds-live&scope=site>.

49. RIVERA-GUERRERO, C. B.; FELIPE-REDONDO, A. M.; NUÑEZ-CÁRDENAS, F. J. Scheme of ISO 27001 Information Security Management System ; Esquema de ISO 27001 Sistema de Gestión de la Seguridad de la Información. [{En línea}. {15 de Febrero de 2019}. Disponible en: <http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.F189314E&lang=es&site=eds-live&scope=site>..

50. RUIZ PEÑA, José Higinio, “DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BAJO LA NORMA ISO/IEC 27001:2013, EN LA COOPERATIVA MULTIACTIVA DEL PERSONAL DEL SENA, EN BOGOTÁ”, {En línea}. {10 de Febrero de 2019} disponible en: https://repository.unad.edu.co/handle/10596/17300

51. Seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del Ministerio de Educación, 2018. 2019 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.AE6EE20B&lang=es&site=eds-live&scope=site

52. Sistema de Gestión de la Seguridad de la Información en una entidad financiera. 2018 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.EDCFA294&lang=es&site=eds-live&scope=site

53. Sussy B sbayonao@hotmail. co., Wilber C wchauca@gmail. co., Milagros L mlopezvf@gmail. co., Carlos M cmaldonado55@yahoo. co. Implementación de la NTP ISO/IEC 27001 en las Instituciones Publicas:Caso de Estudio. (Spanish). CISTI (Iberian Conference on Information Systems & Technologies / Conferência Ibérica de Sistemas e Tecnologias de Informação) Proceedings {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=aci&AN=114061092&lang=es&site=eds-live&scope=site

54. Tacza Valverde IR. Cumplimiento del plan de seguridad de la información con relación a la norma ISO 27000 en la Universidad Nacional Tecnológica de Lima Sur. año 2017. 2018 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.12D941D7&lang=es&site=eds-live&scope=site

55. TESSIN, Peter C., “Marco GEIT trabajando, Parte 1: Identificación del problema”, {En línea}. {04 de Febrero de 2019} disponible en: http://www.isaca.org/COBIT/focus/Pages/geit-framework-at-work-part-1-identifying- the-problem-spanish.aspx

56. Tola Franco DE. Implementacion de un Sistema de Gestion de Seguridad de la Informacion para una empresa de consultoria y auditoria, aplicando la norma

ISO/IEC 27001. 2015 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.7B7E830E&lang=es&site=eds-live&scope=site

57. Torres León MR. Diseño de un sistema de gestión de la seguridad de la información (SGSI), basada en la norma ISO/IEC 27001:2013, para el proceso de servicio post-venta de un integrador de soluciones en Telecomunicaciones. 2018 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.1EADF996&lang=es&site=eds-live&scope=site

58. UNIVERSIA, Costa Rica – Tipos de investigación: Descriptiva, Exploratoria y Explicativa {En línea}. {05 de Diciembre de 2019}. Disponible en: https://noticias.universia.cr/educacion/noticia/2017/09/04/1155475/tipos-investigacion-descriptiva-exploratoria-explicativa.html

59. Valencia-Duque FJ, Orozco-Alzate M. Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000 [Internet]. 2017 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edssci&AN=edssci.S1646.98952017000200006&lang=es&site=eds-live&scope=site

60. Villalba Romero JJ, Jiménez Toledo RA, Torres Burbano ÁR. Evaluación de la seguridad de la información en la Clínica Hispanoamérica de Pasto, basada en la norma ISO/IEC 27001. 2016 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.BB4AE531&lang=es&site=eds-live&scope=site

61. Viloria O, Blanco W. Modelo Sistémico De La Seguridad De La Información en Las Universidades. 2016 {En línea}. {15 de Febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.3704F5C6&lang=es&site=eds-live&scope=site

62. Yupanqui JRA, Oré SB. Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento {En línea}. {15 de Febrero de 2019}. Disponible en:

http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edssci&AN=edssci.S1646.98952017000500009&lang=es&site=eds-live&scope=site

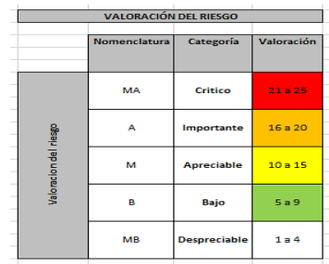
ANEXOS

Anexo A. Valoración cuantitativa de activos

Tabla 10. Activos y valoración cuantitativa

ACTIVO	Riesgo	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
Servidor de Impresión: Servidor marca dell en torre Pov	APRECIABLE	9	9	25	9	25	15
Servidor de archivos FTP: Servidor marca dell en torre	APRECIABLE	9	9	25	9	25	15
Página web Plan Máximo	IMPORTANTE	20	9	20	20	9	16
Servidor de nómina y facturación Servidor marca dell e	IMPORTANTE	20	15	15	15	25	18
Servidor DHCP Servidor marca dell en torre PowerEdge	IMPORTANTE	15	15	15	15	25	17
Equipos de cómputo para gestión del desarrollo tecno	IMPORTANTE	15	20	20	15	25	19
Cortafuegos Cisco ASA 5505	IMPORTANTE	15	15	25	20	25	20
Equipos de Computo Sistemas operativos win 10 Pro	APRECIABLE	9	9	9	9	15	10
Equipos de Computo	APRECIABLE	9	9	9	15	15	11
Equipos de Computo Sistemas operativos win 10 Pro	APRECIABLE	9	9	9	9	15	10
Puntos de acceso alámbricos (hub)	IMPORTANTE	15	15	25	15	25	19
Switches cisco catalyst 2960	IMPORTANTE	15	15	25	15	25	19
Teléfonos IP	APRECIABLE	9	9	9	9	15	10
Puntos de acceso	IMPORTANTE	15	9	25	15	25	18
Técnicos de mantenimiento	APRECIABLE	9	15	9	9	15	11

Fuente: Elaboración propia a partir del Documento Matriz de Análisis de Riesgos (Magerit) – UNAD



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

Anexo B. Plan de tratamiento de Riesgos

Cuadro 18. Plan de tratamiento de riesgos de los activos de la empresa QWERTY S.A.

Activos de Información	No. De Amenazas y Vulnerabilidades	Nombre del activo de información	Amenazas Metodología Magerit	Plan de Tratamiento							
				Transefir	Aceptar	Mitigar	Si el plan de tratamiento es MITIGAR, Indique el control aplicar a partir de la norma ISO 27001			Descripción de la aplicación del control	Eliminar
[HW] EQUIPAMIENTO INFORMÁTICO	1	Servidor de Impresión: Servidor marca dell en torre PowerEdge T440	[I5] Avería de origen físico o lógico			X	A11.2.1	Ubicación y protección de los equipos	Se debe ubicar un sitio seguro para contener los equipos y asegurar su protección contra cualquier amenaza y accesos no autorizados	IMPLANTAR Se debe implantar una seguridad física contra amenazas de cualquier índole natural y humana	
[HW] EQUIPAMIENTO INFORMÁTICO	2	Servidor de Impresión: Servidor marca dell en torre PowerEdge T440	[I5] Avería de origen físico o lógico			X	A11.2.4	Mantenimiento de equipos	Los equipos deben contar con un mantenimiento adecuado para asegurar su disponibilidad	IMPLANTAR Realizar mantenimiento preventivo de equipos	

Cuadro 18. (Continuación)

[HW] EQUIPAMIENTO INFORMÁTICO	3	Servidor de Impresión: Servidor marca dell en torre PowerEdge T440	[I7] Condiciones inadecuadas de temperatura o humedad			X	A11.2.1	Ubicación y protección de los equipos	Se debe ubicar un sitio seguro para contener los equipos y asegurar su protección contra cualquier amenaza y accesos no autorizados	IMPLANTAR Implantar un sistema de climatización optima de aire acondicionado y sistemas de refrigeración en cuarto de servidores	
[HW] EQUIPAMIENTO INFORMÁTICO	4	Servidor de Impresión: Servidor marca dell en torre PowerEdge T440	[I7] Condiciones inadecuadas de temperatura o humedad		X		A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Las instalaciones de esta índole deben asumir e implementar una redundancia adecuada para asegurar su disponibilidad	ASUMIR	
[S] SERVICIOS	5	Servidor de archivos FTP: Servidor marca dell en torre PowerEdge T130	[A5] Suplantación de la identidad del usuario			X	A13.1.1	Controles de redes	Las redes deben contar con controles de protección.	IMPLANTAR Definir perfiles dentro de la aplicación Agregar doble Factor de Autenticación Establecer una sesión segura de transporte para cifrar los datos que viajan por el medio	
[S] SERVICIOS	6	Servidor de archivos FTP: Servidor marca dell en torre PowerEdge T130	[A5] Suplantación de la identidad del usuario			X	A9.1.2	Acceso a redes y a servicios en red	Se debe restringir el acceso a la red a usuarios que no deban tenerlo	IMPLANTAR Definir perfiles dentro de la aplicación Agregar doble Factor de Autenticación Establecer una sesión segura de transporte para cifrar los datos que viajan por el medio	

Cuadro 18. (Continuación)

[S] SERVICIOS	7	Servidor de archivos FTP: Servidor marca dell en torre PowerEdge T130	[A24] Denegación de servicio			X	A13.1.2	Seguridad de los servicios de red	Se debe analizar los permisos a restringir en la red y los que se van a autorizar, diferenciando cuales se prestan internos y externos o cuales serán contratados	IMPLANTAR Limitar el número de conexiones concurrentes al servidor por unidad de tiempo Permitir el acceso al servidor solo al tráfico deseado Restringir el uso del ancho de banda por aquellos equipos que cometan violaciones Verificar si el equipo remoto terminó de establecer la conexión de TCP. Filtrar flags erróneos Parches y actualización del Servidor FTP	
[HW] EQUIPAMIENTO INFORMÁTICO	8	Servidor de archivos FTP: Servidor marca dell en torre PowerEdge T130	[I5] Avería de origen físico o lógico			X	A11.2.4	Mantenimiento de equipos	Los equipos deben contar con un mantenimiento adecuado para asegurar su disponibilidad	IMPLANTAR Realizar mantenimiento preventivo de equipos	
[HW] EQUIPAMIENTO INFORMÁTICO	9	Servidor de archivos FTP: Servidor marca dell en torre PowerEdge T130	[I7] Condiciones inadecuadas de temperatura o humedad			X	A11.2.1	Ubicación y protección de los equipos	Se debe ubicar un sitio seguro para contener los equipos y asegurar su protección contra cualquier amenaza y accesos no autorizados	IMPLANTAR Implantar un sistema de climatización optima de aire acondicionado y sistemas de refrigeración en cuarto de servidores	

Cuadro 18. (Continuación)

[HW] EQUIPAMIENTO INFORMÁTICO	10	Servidor de archivos FTP: Servidor marca dell en torre PowerEdge T130	[I7] Condiciones inadecuadas de temperatura o humedad		X		A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Las instalaciones de esta índole deben asumir e implementar una seguridad y redundancia adecuada para asegurar su disponibilidad	ASUMIR	
[HW] EQUIPAMIENTO INFORMÁTICO	11	Servidor de archivos FTP: Servidor marca dell en torre PowerEdge T130	[I11] Emanaciones electromagnéticas		X		A11.2.1	Ubicación y protección de los equipos	Se debe ubicar un sitio seguro para contener los equipos y asegurar su protección contra cualquier amenaza y accesos no autorizados	ASUMIR	
[S] SERVICIOS	12	Página web Plan Máximo	[A5] Suplantación de la identidad del usuario	X			A13.1.2	Seguridad de los servicios de red	Identificar los mecanismos de protección y los servicios de red a los que se accede tanto interna como externamente y verificar cuales usuarios tienen acceso y para qué.	TRANSFERIR a Godaddy.com Autorizar a cada usuario con un token antes de realizar el acceso a los datos Agregar doble Factor de Autenticación Establecer una sesión segura de transporte para cifrar los datos que viajan por el medio	
[SW] SOFTWARE	13	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	[E21] Errores de mantenimiento / actualización de programas (software)			X	A12.5.1	Instalación de software en los sistemas operativos	Implementar un mecanismo de control para que solo los administradores o técnicos de sistemas de la empresa puedan instalar software	IMPLANTAR Realizar mantenimiento preventivo de software Parches y actualización del software	

Cuadro 18. (Continuación)

[S] SERVICIOS	14	Servidor DHCP Servidor marca dell en torre PowerEdge T440	[A5] Suplantación de la identidad del usuario			X	A13.1.1	Controles de redes	Se debe realizar controles y restricciones de acceso a la red para proteger los sistemas de información y aplicaciones de la empresa.	IMPLANTAR Definir perfiles dentro de la aplicación Agregar doble Factor de Autenticación Establecer una sesión segura de transporte para cifrar los datos que viajan por el medio	
[S] SERVICIOS	15	Servidor DHCP Servidor marca dell en torre PowerEdge T440	[A24] Denegación de servicio			X	A13.1.2	Seguridad de los servicios de red	Se debe analizar los permisos a restringir en la red y los que se van a autorizar, diferenciando cuales se prestan internos y externos o cuales serán contratados	IMPLANTAR Limitar el número de conexiones concurrentes al servidor por unidad de tiempo Permitir el acceso al servidor solo al tráfico deseado Restringir el uso del ancho de banda por aquellos equipos que cometan violaciones Verificar si el equipo remoto terminó de establecer la conexión de TCP. Filtrar flags erróneos Parches y actualización del Servidor DHCP	

Cuadro 18. (Continuación)

[HW] EQUIPAMIENTO INFORMÁTICO	16	Servidor DHCP Servidor marca dell en torre PowerEdge T440	[I5] Avería de origen físico o lógico			X	A11.2.1	Ubicación y protección de los equipos	Se debe ubicar un sitio seguro para contener los equipos y asegurar su protección contra cualquier amenaza y accesos no autorizados	IMPLANTAR Se debe implantar un sistema de protección física contra las amenazas de cualquier índole.	
[HW] EQUIPAMIENTO INFORMÁTICO	17	Servidor DHCP Servidor marca dell en torre PowerEdge T440	[I5] Avería de origen físico o lógico			X	A11.2.4	Mantenimiento de equipos	Los equipos deben contar con un mantenimiento adecuado para asegurar su disponibilidad	IMPLANTAR Realizar mantenimiento preventivo de equipos	
[HW] EQUIPAMIENTO INFORMÁTICO	18	Servidor DHCP Servidor marca dell en torre PowerEdge T440	[I7] Condiciones inadecuadas de temperatura o humedad			X	A11.2.1	Ubicación y protección de los equipos	Se debe ubicar un sitio seguro para contener los equipos y asegurar su protección contra cualquier amenaza y accesos no autorizados	IMPLANTAR Implantar un sistema de climatización optima de aire acondicionado y sistemas de refrigeración en cuarto de servidores	
[HW] EQUIPAMIENTO INFORMÁTICO	19	Servidor DHCP Servidor marca dell en torre PowerEdge T440	[I7] Condiciones inadecuadas de temperatura o humedad		X		A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad	ASUMIR	
[HW] EQUIPAMIENTO INFORMÁTICO	20	Equipos de cómputo para gestión del desarrollo tecnológico	[I5] Avería de origen físico o lógico			X	A11.2.4	Mantenimiento de equipos	Los equipos deben contar con un mantenimiento adecuado para asegurar su disponibilidad	IMPLANTAR Realizar mantenimiento preventivo de equipos	
[HW] EQUIPAMIENTO INFORMÁTICO	21	Equipos de cómputo para gestión del desarrollo tecnológico	[E23] Errores de mantenimiento / actualización de equipos (hardware)			X	~~A11.2.4~~	Mantenimiento de equipos	Los equipos deben contar con un mantenimiento adecuado para asegurar su disponibilidad	IMPLANTAR Tener en cuenta el Sistema Integrado de Gestión - SIG - de la Institución para documentar los procesos de mantenimiento	

Cuadro 18. (Continuación)

[HW] EQUIPAMIENTO INFORMÁTICO	22	Cortafuegos Cisco ASA 5505	[I5] Avería de origen físico o lógico			X	A11.2.1	Ubicación y protección de los equipos	Se debe ubicar un sitio seguro para contener los equipos y asegurar su protección contra cualquier amenaza y accesos no autorizados	IMPLANTAR Se debe implantar un sistema de protección física contra las amenazas de cualquier índole.	
[HW] EQUIPAMIENTO INFORMÁTICO	23	Cortafuegos Cisco ASA 5505	[I5] Avería de origen físico o lógico			X	A11.2.4	Mantenimiento de equipos	Los equipos deben contar con un mantenimiento adecuado para asegurar su disponibilidad	IMPLANTAR Realizar mantenimiento preventivo de equipos	
[HW] EQUIPAMIENTO INFORMÁTICO	24	Cortafuegos Cisco ASA 5505	[E2] Errores del administrador			X	A13.1.2	Seguridad de los servicios de red	Se debe analizar los permisos a restringir en la red y los que se van a autorizar, diferenciando cuales se prestan internos y externos o cuales serán contratados	IMPLANTAR Limitar el número de conexiones concurrentes al servidor por unidad de tiempo Permitir el acceso al servidor solo al tráfico deseado Restringir el uso del ancho de banda por aquellos equipos que cometan violaciones Verificar si el equipo remoto terminó de establecer la conexión de TCP. Filtrar flags erróneos Parches y actualización de los Servidores	

Cuadro 18. (Continuación)

[HW] EQUIPAMIENTO INFORMÁTICO	25	Equipos de Cómputo Sistemas operativos win 10 Pro	[I5] Avería de origen físico o lógico			X	~~A11.2.4~~	Mantenimiento de equipos	Los equipos deben contar con un mantenimiento adecuado para asegurar su disponibilidad	IMPLANTAR Realizar mantenimiento preventivo de equipos	
[HW] EQUIPAMIENTO INFORMÁTICO	26	Equipos de Cómputo Sistemas operativos win 10 Pro	[E23] Errores de mantenimiento / actualización de equipos (hardware)			X	~~A11.2.4~~	Mantenimiento de equipos	Los equipos deben contar con un mantenimiento adecuado para asegurar su disponibilidad	IMPLANTAR Tener en cuenta el Sistema Integrado de Gestión - SIG - de la Institución para documentar los procesos de mantenimiento	
[SW] SOFTWARE	27	Equipos de Cómputo Sistemas operativos win 10 Pro	[E21] Errores de mantenimiento / actualización de programas (software)			X	~~A12.5.1~~	Instalación de software en los sistemas operativos	Implementar un mecanismo de control para que solo los administradores o técnicos de sistemas de la empresa puedan instalar software	IMPLANTAR Realizar mantenimiento preventivo de software Parches y actualización del software	
[HW] EQUIPAMIENTO INFORMÁTICO	28	Equipos de Computo	[E23] Errores de mantenimiento / actualización de equipos (hardware)			X	~~A11.2.4~~	Mantenimiento de equipos	Los equipos deben contar con un mantenimiento adecuado para asegurar su disponibilidad	IMPLANTAR Tener en cuenta el Sistema Integrado de Gestión - SIG - de la Institución para documentar los procesos de mantenimiento	
[HW] EQUIPAMIENTO INFORMÁTICO	29	Puntos de acceso alámbricos (hub)	[I5] Avería de origen físico o lógico			X	A11.2.4	Mantenimiento de equipos	Los equipos deben contar con un mantenimiento adecuado para asegurar su disponibilidad	IMPLANTAR Realizar mantenimiento preventivo de equipos	
[HW] EQUIPAMIENTO INFORMÁTICO	30	Switches cisco catalyst 2960	[I5] Avería de origen físico o lógico			X	A11.2.4	Mantenimiento de equipos	Los equipos deben contar con un mantenimiento adecuado para asegurar su disponibilidad	IMPLANTAR Realizar mantenimiento preventivo de equipos	

Cuadro 18. (Continuación)

[HW] EQUIPAMIENTO INFORMÁTICO	31	Teléfonos IP	[I5] Avería de origen físico o lógico			X	~~A11.2.4~~	Mantenimiento de equipos	Los equipos deben contar con un mantenimiento adecuado para asegurar su disponibilidad	IMPLANTAR Realizar mantenimiento preventivo de equipos	
[HW] EQUIPAMIENTO INFORMÁTICO	32	Puntos de acceso	[I5] Avería de origen físico o lógico			X	A11.2.4	Mantenimiento de equipos	Los equipos deben contar con un mantenimiento adecuado para asegurar su disponibilidad	IMPLANTAR Realizar mantenimiento preventivo de equipos	
[P] PERSONAL	33	Técnicos de mantenimiento	[E28] Indisponibilidad del personal		X		A6.1.2	Separación de deberes	Los deberes y responsabilidades sin importar cualquier causa o factor se deben separar a fin de evitar modificaciones no autorizadas o el uso indebido de los activos de la empresa	ASUMIR	

Fuente: Elaboración propia a partir del Documento Matriz de Análisis de Riesgos (Magerit) – UNAD

Anexo C. Controles necesarios de acuerdo con los resultados de la evaluación de riesgos y amenazas

Cuadro 19. Controles para la empresa QWERTY S.A. de acuerdo con la evaluación de amenazas y riesgos

CONTROL	OBJETIVO DEL CONTROL	RESPONSABLE
Separación de deberes	Evitar el uso indebido de los activos de la empresa, realizando la separación de deberes y responsabilidades del personal que labora en cada una de las áreas, esto para que, en momentos de ausencia y sobrecarga de trabajo, se delegue a un responsable suplente de la misma área o aprendiz que esté previamente calificado e instruido sobre el proceso a fin de mitigar cualquier amenaza que se avecine para el servicio.	Principal responsable Oficina de Recursos Humanos de QWERTY S.A. Jefes de cada área como instructores del personal que integra la dependencia y el personal aprendiz
Acceso a redes y a servicios en red	Controlar el acceso a la red permitiendo exclusivamente al personal autorizado el acceso a la red y los servicios conexos, mediante controles y reglas que blinden las conexiones y trasmisiones de datos no autorizados y que pongan en riesgo los activos de información de la organización.	Área de Infraestructura
Controles de acceso físicos	Implementar y asegurar las áreas que requieren seguridad física con los controles de acceso adecuados para el ingreso únicamente del personal autorizado y así asegurar los activos de información que contengan estos sitios.	Estará a cargo de las áreas de Infraestructura y Desarrollo
Ubicación y protección de los equipos	Ubicar de manera acorde y con todas las garantías necesarias de funcionamiento (Climatización, Seguridad, etc) de acuerdo con la norma, todos los equipos tecnológicos que lo requieran, a fin de ser protegidos contra la materialización de amenazas de toda índole que puedan afectar los activos de información de la organización.	Área de Infraestructura
Mantenimiento de equipos	Realizar planes o actividades tendientes a mantener correctamente los equipos tecnológicos y así asegurar la integridad y disponibilidad de los activos de información de la organización.	Área de Soporte

Cuadro 19. (Continuación)

Instalación de software en los sistemas operativos	Implementar procedimientos para controlar la instalación y actualizaciones de software en los sistemas operativos de los equipos tecnológicos de la empresa, estos deben contar con una supervisión y control del estado actual y los requerimientos que se lleguen a necesitar en esta materia, a fin de evitar cualquier riesgo relacionado para los activos de información.	Área de Soporte
Controles de redes	Gestionar y controlar las redes y su configuración, de forma acorde con la estructura de la empresa y sus necesidades de seguridad a fin de proteger la información en sistemas y aplicaciones.	Área de Infraestructura
Seguridad de los servicios de red	Identificar mecanismos de seguridad y necesidades de gestión de todos los servicios de red, incluyendo estos en todos los acuerdos de servicio, sin importar si son servicios internos o externos contratados a fin de asegurar la seguridad informática de la empresa.	Área de Infraestructura
Disponibilidad de instalaciones de procesamiento de información	Implementar instalaciones de procesamiento de información de manera redundante, que tengan los requisitos necesarios para dar una disponibilidad 24/7 de los servicios ofrecidos por la empresa.	Estará a cargo de las áreas de Infraestructura y Desarrollo

Fuente: “Elaboración propia”

Anexo D. Controles definidos para la implementación del SGSI

Cuadro 20. Controles definidos para la implementación del SGSI en la empresa QWERTY S.A.

Statement of Applicability

Current as of: 22/05/2020

Legenda (Para controles seleccionados y razones de selección del control)

LR: Requerimiento Legal **CO**: Obligación Contractual, **BR/BP**: Requerimiento de Negocio/Mejores prácticas, **RRA**: resultado de evaluación de riesgo

Legenda (Controles Existentes)

D: Control implementado y Documentado **MD**: Control Implementado sin Documentar **RD**: Control no cumple con el estándar

PND: Control no implementado **NA** Control no aplicable

ISO/IEC 27001:2013 Anexo A Controles			Control	Justificación de la exclusión	Razones para la selección del Control				Observaciones
					LR	CO	BR/BP	RRA	
Clausula	Sec	Objetivo de Control/Control							
	5,1	Management direction for information security							
5 Políticas de Seguridad	5.1.1	Políticas para la seguridad de la información	D		X				Se debe definir un conjunto de políticas para la seguridad de la información, que esté debidamente aprobada por la dirección, publicada para la consulta de todos los empleados y

Cuadro 20. (Continuación)

									partes externas que intervengan con QWERTY S.A.
	5.1.2	Revisión de las políticas para la seguridad de la información	D				X		Estas políticas de seguridad de la información se deben revisar con una temporalidad establecida y planeada o si ocurren cambios de cualquier índole interno o externo que ameriten replantearlas, con el fin de asegurar su adecuación y eficacia en QWERTY S.A.
6 Organización de la Seguridad de la Información	6.1	Organización Interna							
	6.1.1	Roles y responsabilidades para la seguridad de la Información	D		X				Se debe definir y establecer las responsabilidades de la seguridad de la información
	6.1.2	Separación de Deberes	D					X	Los deberes y áreas de responsabilidad en riesgo, se deben

Cuadro 20. (Continuación)

									dividir para evitar los errores no intencionales o modificaciones sin autorización que afecten los activos de QWERTY S.A.
	6.1.3	Contacto con las Autoridades	D				X		Se deben tener en cuenta los contactos con las autoridades pertinentes para la atención oportuna en caso de incidentes (Sospecha de violación de la ley entre otras).
	6.1.4	Contacto con grupos de interés especial	D				X		QWERTY S.A. debería mantener contactos apropiados en materia de asociaciones de profesionales especializados en materia de seguridad, para

Cuadro 20. (Continuación)

								asegurar mejores prácticas.
6.1.5	Seguridad de la Información en la gestión de proyectos	D				X		Independientemente del tipo de proyecto, QWERTY S.A deberá aplicar la seguridad de la información en la metodología de gestión de proyectos para identificar y tratar los riesgos asociados a este.
6.2	Dispositivos Móviles y Teletrabajo							
6.2.1	Política para Dispositivos Móviles	D				X		Se debe asegurar que no se comprometa la información de QWERTY S.A, Por tanto, se debe tener en cuenta y mitigar los riesgos de trabajar con dispositivos móviles en un entorno externo o no protegido por la empresa.

Cuadro 20. (Continuación)

7 Seguridad del Recurso Humano	7.1	Antes de Asumir el Empleo							
	7.1.1	Selección	D		X				La verificación de todos los antecedentes de los candidatos a un empleo en QWERTY S.A. se deben llevar a cabo de acuerdo con las leyes y los reglamentos pertinentes, siendo proporcionales a los requisitos del negocio donde se incluyan varios aspectos sobre la información que se va a manipular o procesar y sus riesgos.
	7.1.2	Términos y condiciones del empleo	D		X				Los acuerdos y obligaciones contractuales para los empleados o contratistas deben establecerse a partir de las políticas de la

Cuadro 20. (Continuación)

									organización, donde se aclaren y suscriban los compromisos y sus responsabilidades en materia de seguridad de la información en QWERTY S.A.
	7.2	Durante el empleo							
	7.2.1	Responsabilidades de la Dirección	D	La dirección delegó esta responsabilidad a un funcionario supervisor que se encargará de exigir a quienes integran la entidad (empleados y contratistas) el deber y responsabilidad con la aplicación de la seguridad de la información de acuerdo con las políticas establecidas en QWERTY S.A e informará a la alta dirección de las actividades mediante informes y novedades, esto con el fin de tener un acercamiento más estrecho y un desarrollo más dinámico y eficaz en la implementación del sistema de gestión de			X		

Cuadro 20. (Continuación)

			seguridad de la información en la empresa.					
7.2.2	Toma de conciencia, educación y formación en Seguridad	D				X		Todos los integrantes de QWERTY S.A. deben recibir la educación y la formación en toma de conciencia apropiada de manera recurrente sobre las políticas en materia de seguridad de la información establecidas por la empresa.
7.2.3	Proceso Disciplinario	PND	La empresa no tiene implementado un proceso disciplinario formal, por tanto, este proceso se encuentra en construcción, ya que se tiene contemplado organizar de manera detallada los aspectos legales a nivel interno para su conformación e integración con la normatividad vigente.					Pendiente para aplicar este control
7,3	Terminación y cambio de Empleo							

Cuadro 20. (Continuación)

	7.3.1	Terminación o cambio de responsabilidades de Empleo	D			X			Para proteger los intereses de QWERTY S.A en el cambio o terminación del empleo, la empresa debe exigir y comunicar al empleado o contratista que los deberes y responsabilidades permanecen en materia de seguridad de la información.
8 Gestión de Activos	8.1	Responsabilidad por los Activos							
	8.1.1	Inventario de Activos	D				X		Se debe identificar todos los activos de información, elaborando un inventario de estos y mantenerlo para su consulta, estudio y protección pertinente
	8.1.2	Propiedad de los Activos	D				X		Los inventarios de los activos deberían

Cuadro 20. (Continuación)

								tener un propietario para la gestión de su ciclo de vida.
8.1.3	Uso aceptable de los activos	D				X		Se debe documentar e implementar reglas para el uso aceptable de los activos de información.
8.1.4	Devolución de Activos	D				X		Se debe exigir que todos los usuarios internos y externos de los activos de información, y que les fueron asignados mientras ejecuten sus funciones del cargo, que deben devolver estos a la empresa en iguales condiciones o mejor de cuando les fueron entregados.
8.2	Clasificación de la Información							
8.2.1	Clasificación de la Información	D		X				En función de los requisitos legales y

Cuadro 20. (Continuación)

								susceptibilidad, la información se debe clasificar en QWERTY S.A
	8.2.2	Etiquetado de la Información	D				X		Se debe desarrollar e implementar una metodología o proceso para etiquetar la información de acuerdo al esquema de clasificación establecida por QWERTY S.A.
	8.2.3	Manejo de Activos	D				X		Se debe establecer procedimientos de manejo de activos, de acuerdo con el esquema de clasificación de la información.
	8.3	Manejo de Medios							
	8.3.1	Gestión de medios removibles	D				X		Se deberían establecer procedimientos para la gestión de medios removibles de acuerdo con la

Cuadro 20. (Continuación)

									clasificación de la información establecida en QWERTY S.A
	8.3.2	Disposición de Medios	PND	Se encuentra en construcción y negociación un convenio con la empresa GIA VITARE para dar aplicabilidad del manejo de los RAEE´S para dar cumplimiento a la LEY 1672 DE 2013 y establecer un procedimiento adecuado para el tratamiento de estos elementos de manera segura. Se encuentra pendiente la consecución de recursos para su implementación.					Pendiente para aplicar este control
9 Control de Acceso	9.1	Requisitos del Negocio para el control de acceso							
	9.1.1	Política del Control de Acceso	D				X		Se debe documentar y establecer una política para limitar el acceso a la información e instalaciones de procesamiento de la misma de manera apropiada.

Cuadro 20. (Continuación)

	9.1.2	Acceso a redes y servicios de red	D					X	Solo se debe permitir el acceso de los funcionarios de la empresa a la red o para quienes hayan sido autorizados mediante políticas acerca de uso.
	9.2	Gestión de acceso de Usuarios							
	9.2.1	Registro y cancelación de acceso de usuarios	D				X		Se debe implementar un proceso formal de registro y cancelación de usuarios y sus derechos de acceso en la empresa.
	9.2.2	Suministro de acceso de usuarios	D				X		Se debe establecer un proceso de suministro para asignación o revocación de derechos de acceso manteniendo un registro central y revisar periódicamente los accesos por parte

Cuadro 20. (Continuación)

									de los propietarios de los sistemas de información y servicios de QWERTY S.A
	9.2.3	Gestión de Derechos de acceso privilegiado	D				X		Se debe controlar y supervisar la asignación y uso de los accesos privilegiados.
	9.2.4	Gestión de la Información secreta de autenticación de los usuarios	D				X		Mediante un proceso de gestión formal, se debe asignar la información de autenticación secreta.
	9.2.5	Revisión de los derechos de acceso de los usuarios	D				X		Los propietarios de los activos deben realizar una revisión recurrente de los derechos de acceso de los usuarios.
	9.2.6	Retiro o ajuste de los derechos de los usuarios	D				X		Cuando finalice el empleo o contrato suscrito con los empleados y contratistas, se deben eliminar los

Cuadro 20. (Continuación)

									accesos a las instalaciones de procesamiento de la información.
	9.3	Responsabilidades de los usuarios							
	9.3.1	Uso de información de autenticación secreta	D				X		Se debe exigir a los funcionarios (Empleados o contratistas) las prácticas de la organización para el uso de información secreta de autenticación.
	9.4	Control de acceso a sistemas y aplicaciones							
	9.4.1	Restricción de acceso a la información	D				X		El acceso a la información y servicios que prestan los sistemas de información de la entidad debe estar restringidos cumpliendo con la política de control de acceso.
	9.4.2	Procesamiento de Ingreso Seguro	D				X		Se debe controlar el acceso a los sistemas mediante

Cuadro 20. (Continuación)

									una política de ingreso seguro
	9.4.3	Sistema de Gestión de contraseñas	D				X		QWERTY S.A debe implementar interactividad en los sistemas de gestión de contraseñas para asegurar la calidad de estas.
	9.4.4	Uso de programas utilitarios privilegiados	PND	QWERTY S.A no tiene implementado programas utilitarios privilegiados que anulen sus sistemas y controles de aplicaciones de manera desmedida, sin embargo, se aconseja implementar a la alta dirección este control con el fin de anteceder futuros riesgos en esta materia.					Pendiente para aplicar este control
	9.4.5	Control de acceso a códigos fuente de programas	D						QWERTY S.A debe restringir el acceso a los códigos fuente de los programas.
10 Criptografía	10.1	Controles Criptográficos							
	10.1.1	Política sobre el uso de controles criptográficos	D				X		Se debe implementar una

Cuadro 20. (Continuación)

									política sobre el uso de controles criptográficos para la protección de la información.
	10.1.2	Gestión de llaves	D				X		QWERTY S.A debe desarrollar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas.
11 Seguridad Física y del Entorno	11.1	Áreas Seguras							
	11.1.1	Perímetro de Seguridad Física	PND	La alta dirección de QWERTY S.A se encuentra evaluando la estructura de las instalaciones para que cumplan con las consideraciones y recomendaciones de este control. Se encuentra pendiente la consecución de recursos para su implementación.					Pendiente para aplicar este control
	11.1.2	Controles de acceso Físicos	D					X	Se deben establecer controles para la protección de las áreas seguras

Cuadro 20. (Continuación)

	11.1.3	Seguridad de oficinas, recintos e instalaciones	D				X		Se debe diseñar y aplicar seguridad física a las Oficinas, espacios de trabajo e instalaciones.
	11.1.4	Protección contra amenazas externas y ambientales	D				X		Se debe diseñar y aplicar protección física contra fenómenos naturales, ataques intencionales o accidentales.
	11.2	Equipos							
	11.2.1	Ubicación y protección de los equipos	D					X	QWERTY S.A debe prevenir la pérdida, daño, robo o cualquier situación donde se comprometan los activos y se causen interrupciones de las operaciones de la empresa.
	11.2.2	Servicios de suministro	D				X		Los equipos de QWERTY S.A se deben proteger contra fallas de energía y otras causadas por fallas

Cuadro 20. (Continuación)

									en los servicios de suministro
	11.2.3	Seguridad del cableado	D				X		El cableado de energía y telecomunicaciones que da el soporte a los servicios de información deberá ser protegido contra interrupciones o daño, reo
	11.2.4	Mantenimiento de equipos	D					X	Los equipos deben mantenerse en buenas condiciones de funcionamiento para asegurar la disponibilidad e integridad de manera continua.
	11.2.5	Retiro de activos	D				X		Pese a que no se tiene establecido el modelo de teletrabajo dentro de la empresa, los equipos, información o software no se deben retirar de las

Cuadro 20. (Continuación)

									instalaciones de QWERTY S.A sin autorización previa.
	11.2.6	Seguridad de equipos y activos fuera de las instalaciones	D				X		Se debe aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de QWERTY S.A
	11.2.7	Disposición segura o reutilización de equipos	D				X		Se debe verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar cualquier dato sensible o software licenciado antes de su reúso o nueva disposición.
	11.2.8	Equipo de usuario desatendido	PND	QWERTY S.A se encuentra realizando las coordinaciones pertinentes para la adquisición de software necesario para atender la protección de equipos desatendidos. Se encuentra					Pendiente para aplicar este control

Cuadro 20. (Continuación)

				pendiente la consecución de recursos para su implementación.					
	11.2.9	Pantalla de escritorio limpio y pantalla limpia	PND	QWERTY S.A se encuentra realizando las coordinaciones pertinentes para la adquisición de software necesario para atender este control y estructurar la política para su implementación. Se encuentra pendiente la consecución de recursos para su implementación.					Pendiente para aplicar este control
12 Seguridad de las Operaciones	12.1	Procedimientos operacionales y responsabilidades							
	12.1.1	Procedimientos de operación documentados	D				X		Los procedimientos de operación se deben documentar y publicar para la consulta de todos los empleados.
	12.1.2	Gestión de cambios	D				X		Se deben controlar los cambios en la organización, en los procesos del negocio, en las instalaciones y sistemas que

Cuadro 20. (Continuación)

								afecten la seguridad de la información en QWERTY S.A
12.1.3	Gestión de capacidad	D				X		Se debe hacer seguimiento al uso de los recursos, hacer ajustes y proyecciones para asegurar el desempeño de los sistemas.
12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	D				X		Se debe separar los ambientes de desarrollo, pruebas y producción para reducir riesgos.
12.2	Protección contra códigos maliciosos							
12.2.1	Controles contra códigos maliciosos	D				X		QWERTY S.A debe asegurarse que las instalaciones de procesamiento de información estén protegidas contra malware o código malicioso.
12.3	Copias de Respaldo							
12.3.1	Respaldo de la Información	D				X		Se debe realizar copias de seguridad

Cuadro 20. (Continuación)

								o respaldo de la información y software, poniendo estas a prueba de manera regular estableciendo una política para su control.
12.4	Registro y monitoreo							
12.4.1	Registro de eventos	PND	QWERTY S.A tiene en proceso la adquisición de un sistema para registrar los eventos (Logs) y generar evidencia de manera acorde.					Pendiente por aplicar el control
12.4.2	Protección de la Información de Registro	PND	QWERTY S.A tiene en proceso la adquisición de un sistema para registrar los eventos (Logs) y generar evidencia de manera acorde.					Pendiente por aplicar el control
12.4.3	Registros del administrador y del operador	PND	QWERTY S.A tiene en proceso la adquisición de un sistema para registrar los eventos (Logs) y generar evidencia de manera acorde.					Pendiente por aplicar el control
12.4.4	Sincronización de relojes	D				X		Los relojes de todos los sistemas de procesamiento de la información de QWERTY S.A deben

Cuadro 20. (Continuación)

								sincronizarse con una única fuente de referencia de tiempo
12.5	Control de Software Operacional							
12.5.1	Instalación de software en sistemas operativos	D					X	Se debe implementar procedimientos para limitar la instalación de software en sistemas operativos por parte de los usuarios
12.6	Gestión de la Vulnerabilidad Técnica							
12.6.1	Gestión de las Vulnerabilidades técnicas	PND	QWERTY S.A aún no tiene conocimiento de las vulnerabilidades técnicas y por ende, aún tiene pendiente definir los roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas (proveedor y administradores de los sistemas). Se encuentra pendiente realizar la gestión para convocar mesas de trabajo.					Pendiente por aplicar el control

Cuadro 20. (Continuación)

	12.6.2	Restricciones sobre la instalación de software	D				X		QWERTY S.A deberá definir una política para hacerla cumplir con relación al tipo de software que pueden instalar los usuarios.
	12.7	Consideraciones sobre auditorias de sistemas de Información							
	12.7.1	Controles de auditorías de sistemas de Información	PND	QWERTY S.A se encuentra estableciendo un sistema de auditoría adecuado para no afectar la disponibilidad de los sistemas de la empresa. Se encuentra pendiente la consecución de recursos para su implementación.					
13 Seguridad de las Comunicaciones	13.1	Gestión de la seguridad de las redes							
	13.1.1	Controles de Redes	D					X	QWERTY S.A debe implementar la gestión y control de las redes con el fin de proteger los sistemas y aplicaciones.
	13.1.2	Seguridad de los servicios de Red	D					X	Se deberá identificar los mecanismos de

Cuadro 20. (Continuación)

									seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, tanto en servicios internos como externos contratados.
	13.1.3	Separación de las Redes	D				X		Los grupos de servicios de información de la empresa se deben separar en la red.
	13.2	Transferencia de Información							
	13.2.1	Políticas y procedimientos de transferencia de Información	D				X		Se deberá contar con políticas, procedimientos y controles de transferencia formal de información en todo tipo de instalaciones de comunicación.
	13.2.3	Mensajería Electrónica	D				X		Se debe proteger la información incluida en la mensajería

Cuadro 20. (Continuación)

									electrónica de QWERTY S.A
	13.2.4	Acuerdos de Confidencialidad o no divulgación	D				X		Si bien no se cuenta con acuerdos con partes externas, QWERTY S.A debe identificar, revisar y documentar los requisitos para los acuerdos de confidencialidad a los empleados de la organización.
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	14.1	Requisitos de Seguridad de los Sistemas de Información							
	14.1.1	Análisis y especificación de requisitos de seguridad de la Información	D				X		QWERTY S.A debe establecer los requisitos de seguridad de la información para sus empleados, informando a los operadores y usuarios sus deberes y responsabilidades.
	14.1.2	Seguridad de servicios de aplicaciones en redes Publicas	D				X		La información involucrada en los servicios de

Cuadro 20. (Continuación)

									aplicaciones que pasan por redes públicas, se debe proteger de actividades fraudulentas, divulgación y modificación no autorizada.
	14.1.3	Protección de los servicios de las aplicaciones transaccionales	D				X		La información transferida por medio de los servicios de las aplicaciones se deberá proteger para evitar la trasmisión incompleta o errada y alteraciones en los mensajes e interceptación y reproducción no autorizada.
	14.2	Seguridad de los procesos de desarrollo y soporte							
	14.2.1	Política de desarrollo seguro	D				X		Se debe establecer reglas para el desarrollo de software y sistemas

Cuadro 20. (Continuación)

									dentro de la empresa.
	14.2.2	Procedimientos de control de cambios en sistemas	PND	QWERTY S.A no tiene un procedimiento formal para el control de cambios dentro del ciclo de vida de desarrollo. Se recomienda implementar este control a la empresa.					Pendiente por aplicar el control
	14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	PND	QWERTY S.A no tiene un procedimiento formal para el control de cambios dentro del ciclo de vida de desarrollo. Se recomienda implementar este control a la empresa.					Pendiente por aplicar el control
	14.2.4	Restricción en los cambios a los paquetes de software	D				X		Se debe desalentar las modificaciones a los paquetes de software, limitando los cambios los cuales se deben controlar estrictamente.
	14.2.5	Principios de construcción de sistemas seguros	D				X		Se debe establecer principios para la construcción de sistemas seguros
	14.2.6	Ambiente de desarrollo seguro	D				X		QWERTY S.A debe establecer y proteger

Cuadro 20. (Continuación)

									adecuadamente los ambientes de desarrollo seguro con la compresión de ciclos de vida.
	14.2.8	Pruebas de seguridad en sistemas	D				X		Durante el desarrollo se deben realizar pruebas de funcionalidad de la seguridad a los sistemas de QWERTY S.A
	14.2.9	Pruebas de aceptación de sistemas	D				X		Se deben establecer pruebas de aceptación para los sistemas de información nuevos.
15 Relación con los proveedores	15.1	Seguridad de la Información en la relación con los proveedores							
	15.1.1	Política de seguridad de la información para las relaciones con los proveedores	D				X		Se deben mitigar los riesgos asociados con el acceso de proveedores a los activos de QWERTY, realizando acuerdos y se deben documentar.

Cuadro 20. (Continuación)

	15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	D				X		Se debe establecer y acordar requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso a los componentes de infraestructura de TI para la información de la empresa.
	15.1.3	Cadena de Suministro de tecnología de información y comunicaciones	PND	QWERTY S.A no tiene establecido acuerdos con los proveedores asociados con la cadena de suministro de productos y servicios de tecnología de la información y comunicación, se encuentra estableciendo los parámetros jurídicos para su implementación, ya que no ha tiene contemplado aun la compra de este tipo de suministros para la empresa.					Pendiente por aplicar el control
	15.2	Gestión de la prestación de servicios de proveedores							
	15.2.1	Seguimiento y revisión de los servicios de los proveedores	D				X		QWERTY S.A debe auditar de manera recurrente y hacer

Cuadro 20. (Continuación)

									seguimiento a la prestación de servicios suministrados por proveedores.
	15.2.2	Gestión de cambios en los servicios de los proveedores	D				X		Se debe gestionar los cambios en los suministros de servicios por parte de los proveedores para tener en cuenta aspectos como la revaloración de los riesgos y la mejora de políticas que beneficien a ambas partes.
16 Gestión de Incidentes de Seguridad de la Información	16.1	Gestión de incidentes y mejoras en la seguridad de la Información							
	16.1.1	Responsabilidades y procedimientos	D				X		Se debe establecer las responsabilidades y procedimientos de gestión para el aseguramiento de las respuestas a los incidentes de

Cuadro 20. (Continuación)

									seguridad de la información.
	16.1.2	Reporte de eventos de seguridad de la información	D				X		Los eventos de seguridad deben ser informados por medio de canales apropiados para su tratamiento.
	16.1.3	Reportes de debilidades de seguridad de la información	D				X		QWERTY S.A debe exigir a todo el personal que integra la empresa, que reporten de manera oportuna cualquier debilidad de seguridad de la información observada en los sistemas de información.
	16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	D				X		Los eventos de seguridad de la información se deben evaluar para decidir si se clasificarán como incidentes de seguridad.

Cuadro 20. (Continuación)

	16.1.5	Respuesta a incidentes de seguridad de la Información	D				X		Se deberá dar respuesta a los incidentes de seguridad de la información de acuerdo a los procedimientos documentados debidamente en QWERTY S.A
	16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la Información	D				X		La experiencia adquirida al analizar y dar solución a los incidentes de seguridad de la información se debe utilizar para mitigar los impactos de incidentes futuros.
	16.1.7	Recolección de Evidencia	PND	QWERTY S.A no cuenta con personal idóneo para la recolección de evidencia, por tanto, la empresa se encuentra en la consecución de presupuesto para implementar capacitaciones al personal que debe ser					Pendiente por aplicar el control

Cuadro 20. (Continuación)

				seleccionado para esta actividad.					
17 Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio	17.1	Continuidad de Seguridad de la Información							
	17.1.1	Planificación de la continuidad de la seguridad de la Información	D				X		La continuidad de la seguridad de la información se debe incluir en los sistemas de gestión de la continuidad del negocio de QWERTY S.A
	17.1.2	Implementación de la continuidad de la Seguridad de la Información	PND	QWERTY S.A no cuenta con la estructura de gestión adecuada para prepararse para responder a un evento y ejecutar una recuperación ante desastres, se encuentra realizando la consecución de recursos para implementar este control.					Pendiente por aplicar el control
	17.1.3	Verificación, revisión y evaluación de la continuidad de seguridad de la Información	PND	QWERTY S.A no cuenta con la estructura de gestión adecuada para prepararse para responder a un evento, por ende, no tiene un control adecuado para realizar las verificaciones generales de seguridad de la continuidad					Pendiente por aplicar el control

Cuadro 20. (Continuación)

				del negocio, se encuentra realizando la consecución de recursos para implementar este control de manera adecuada.					
	17.2	Redundancias							
	17.2.1	Disponibilidad de instalaciones de procesamiento de información	D					X	Las instalaciones de procesamiento de la información se deben establecer con redundancias suficientes para otorgar las condiciones de disponibilidad en QWERTY S.A
18 Cumplimiento	18.1	Cumplimiento de requisitos legales y contractuales							
	18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	D		X				La empresa debe evitar el incumplimiento de las obligaciones legales o contractuales relacionadas con seguridad de la información y cualquier requisito

Cuadro 20. (Continuación)

								de seguridad establecido.
	18.1.2	Derechos de propiedad Intelectual	D		X			Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales o contractuales sobre derechos de propiedad intelectual y software patentados.
	18.1.3	Protección de Registros	D		X			La protección de registros se debe efectuar de acuerdo a los requisitos legales o contractuales del negocio.
	18.1.4	Privacidad y protección de información de datos personales	D		X			De acuerdo a la legislación de protección de datos, se debe asegurar la privacidad y

Cuadro 20. (Continuación)

								protección de la información de datos personales cuando sea aplicable.
	18.1.5	Reglamentación de Controles Criptográficos	D				X		Se debe establecer controles criptográficos en cumplimiento de los acuerdos y legislación pertinente.
	18.2	Revisiones de Seguridad de la Información							
	18.2.1	Revisión Independiente de la Seguridad de la Información	D				X		QWERTY S.A debe asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos de la empresa.
	18.2.2	Cumplimiento con las políticas y normas de seguridad	D				X		Los responsables de cada área de la empresa, debe realizar una revisión regular del cumplimiento de los procedimientos

Cuadro 20. (Continuación)

									y normas de seguridad apropiadas.
	18.2. 3	Revisión del cumplimiento técnico	D				X		Los sistemas de información de QWERTY S.A se deben revisar con regularidad para verificar el cumplimiento técnico con las normas de seguridad de la información.

Fuente: Elaboración propia a partir del Documento excel ISO27K_SOA_2013 - UNAD

Anexo E. Manual del sistema

MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA QWERTY S.A.

INTRODUCCIÓN

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.

Por tal motivo publica el presente documento, definido como el Manual del Sistema de Gestión de Seguridad de la Información de acuerdo con la posición de la dirección de QWERTY S.A. para la implementación de este sistema como apoyo a la protección de los activos de información en el cual se publican sus políticas y procedimientos acordes a la norma ISO/IEC 27001.

QWERTY S.A en cumplimiento a su visión, misión y objetivos apegados a Ley del estado colombiano, se acoge a la normativa de Seguridad de la Información en la organización con el objeto de:

- Establecer políticas, procedimientos e instructivos con relación a la seguridad de la información dentro de la empresa.
- Proteger los activos de información pertenecientes a la empresa y a sus clientes.
- Implementar el sistema de seguridad de la información para la empresa.
- Minimizar el riesgo y su impacto en cada uno de sus activos de información.
- Mantener la confianza de sus clientes.
- Garantizar la continuidad del negocio contrarrestando todo tipo de incidentes.
- Fortalecer la cultura dentro de este contexto en los integrantes de la empresa.

PROPÓSITO

El presente documento identifica las responsabilidades estableciendo las políticas y objetivos pertinentes para la protección de los activos de información de la empresa QWERTY S.A, buscando reducir el riesgo accidental o intencional en el uso indebido de los activos de información, orientando así la administración de seguridad y proveyendo las bases para la gestión de cada proceso de la entidad de manera acorde a la normatividad.

MARCO NORMATIVO

- Constitución Política de Colombia de 1991.

- Ley 599 del 2000 - Por la cual se dispone el “Código penal colombiano”

- Ley 603 de 2000 - Por la cual se dispone el “Control de Legalidad del Software”

- Ley 962 de 2005 - Por la cual se dicta la “Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas”

- Ley 1150 de 2007 - Por la cual se regula la “Seguridad de la información electrónica en contratación en línea”

- Ley 1273 del 2009 - Por la cual se regula la “Protección de la información y de los datos”

- Ley 1341 de 2009 - Por la cual se dicta las disposiciones sobre las “Tecnologías de la Información y aplicación de seguridad”

- Ley 1480 de 2011 - Por la cual se dicta la “Protección al consumidor por medios electrónicos. Seguridad en transacciones electrónicas”

- Norma Técnica Colombiana NTC ISO/IEC 27001:2013 - Por la cual se publica la Norma técnica de sistemas de gestión de seguridad de la información.

GENERALIDADES DEL SISTEMA

En este manual se describen las políticas de seguridad las cuales aplicarán a todos los activos que requieren ser protegidos, en su todo su procesamiento (creación, organización, transporte, almacenamiento, entrega y eliminación). Aunado a ello, están dirigidas a garantizar la apropiada utilización y manejo de los equipos tecnológicos empleados por la entidad para cada ejecutar cada uno de sus procesos y servicios.

La información producida y usada para el desarrollo de la misionalidad de QWERTY S.A, es propiedad exclusiva de la entidad, por ende, todos aquellos que tengan un vínculo directo (empleados y miembros) e indirecto (terceros en prestación de servicios o contratistas) están obligados a protegerla.

Los usuarios y clientes serán conscientes de sus responsabilidades de hacer cumplir las políticas de la empresa y cuyas dudas e inquietudes sobre las mismas, serán resultas directamente por el promotor de seguridad del sistema SGSI de la empresa o quien haga sus veces.

OBJETIVOS DE SEGURIDAD

- Identificar y proporcionar el cumplimiento de los requerimientos legales y normativos, adquiridos por la empresa QWERTY S.A

- Salvaguardar toda información procesada por la empresa QWERTY S.A por medio de la ejecución de controles con base en la normatividad vigente.

- Vigilar y controlar el correcto uso y protección de los activos de información de la empresa QWERTY S.A.

- Capacitar y concientizar al personal que integra directa o indirectamente a la empresa en temas que giran en contorno a la seguridad de la información.

- Gestionar de manera adecuada los incidentes de seguridad, que pongan en riesgo la continuidad del negocio, con el objeto de establecer parámetros que permitan superar y mejorar los procesos de la entidad.

- Prevenir y contrarrestar los riesgos de seguridad siguiendo los parámetros establecidos por la dirección de la empresa, con el objeto de preservar la integridad, confidencialidad y disponibilidad de la información de propiedad de esta entidad.

POLÍTICA GENERAL PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE QWERTY S.A.

La empresa QWERTY S.A, tiene pleno conocimiento que el activo más importante que debe ser salvaguardado de toda amenaza, es la Información, reconociendo que la seguridad de esta es un eje fundamental para la continuidad del negocio. Por ende, establecen protocolos y estrategias dentro del marco del Sistema, conformando así un sistema integrado de mejora continua que asegure la correcta disposición y empleo de los recursos requeridos para la prestación de los diferentes servicios en cumplimiento a su misionalidad.

Así las cosas, QWERTY S.A se responsabiliza de gestionar y verificar el cumplimiento de todos los requisitos legales para garantizar que todo el componente del talento humano que la integran es concientice sobre la importancia de la aplicación de la seguridad de la información, en pro de generar una mejor prestación de los servicios y proteger sus intereses.

ALCANCE

La empresa QWERTY S.A. define su alcance para el Sistema en las actividades que a continuación relaciona: Crear y aplicar los principios y políticas de acuerdo con las normas del sector tecnológico para Colombia, entregando un servicio responsable y seguro relacionado con la búsqueda de desarrollo tecnológico en comunidades colombianas a través de tecnologías de la información.

POLÍTICAS DE SEGURIDAD

REVISIÓN DE LAS POLÍTICAS

La revisión de las políticas del Sistema de Gestión de Seguridad de la Información estará a cargo del Comité de Seguimiento del SGSI de QWERTY S.A. haciéndolo una vez al año o cuando ocurra un cambio a nivel directivo o sea convocado por este, o cuando haya una actualización en el marco legal y normativo de ser requerido. Estas acciones estarán soportadas mediante acta del comité para que obren como antecedente de las acciones allí tomadas.

POLÍTICA DE ORGANIZACIÓN INTERNA DE LA SEGURIDAD DE LA INFORMACIÓN

ROLES Y RESPONSABILIDADES

Todo persona natural o jurídica que tenga acceso a la información de QWERTY S.A, será responsable de salvaguardar su integridad y confidencialidad, a fin de cumplir con las políticas relacionadas en el presente manual:

- Responsabilidades individuales: todos aquellos que deban cumplir la política de seguridad de la información de la empresa, son responsables de su implementación y deberán verificar la efectividad y eficacia del sistema acorde a los objetivos y lineamientos de la empresa, administrando el uso adecuado de las herramientas tecnológicas y activos de información de la entidad. Todos deberán suscribir las correspondientes cláusulas de responsabilidad del SGSI.

- El promotor de seguridad de la información estará a cargo de la asesoría y vigilancia en la implementación del Sistema de Gestión de Seguridad de la Información dentro de la organización, realizará las correspondientes actividades tendientes a la toma de conciencia, educación y formación en seguridad, además hará la supervisión de los controles y aplicación de la norma ISO/IEC 27001 y demás funciones que le sean delegadas por el Comité de Seguimiento del SGSI de QWERTY S.A.

- Los jefes de área o grupo deberán implementar, supervisar y difundir a su personal las políticas de seguridad del sistema, las cuales serán evaluadas a través de listas de chequeo, en aras de verificar el cumplimiento de estas.

SEPARACIÓN DE DEBERES

Los cargos donde se ejecuten procedimientos susceptibles a errores, fugas de información o afectación directa a la seguridad de los activos de información de la empresa, deberán ser segregados en distintas tareas ejecutadas por varios empleados o contratistas debidamente avalados e instruidos para que estos se hagan responsables del buen manejo y supervisión, para así reducir el mal uso de estos activos que pongan en peligro los intereses y el buen servicio de la empresa.

Este proceso que deberá quedar documentado y archivado como antecedente.

CONTACTO CON LAS AUTORIDADES O CON GRUPOS DE INTERÉS ESPECIAL

Cada una de las áreas o dependencias de la empresa QWERTY S.A, realizará y tendrán a la mano en medio físico o digital un listado de contactos con las diferentes autoridades locales a las cuales debe acudir en caso de algún incidente, desastre natural o inducido, incluyendo a las empresas de servicios públicos, de salud y seguridad.

El promotor de seguridad de la información, en su proceso de gestión mantendrá contacto con los grupos de interés especial, esto a fin de mantener la empresa actualizada ante cualquier advertencia de seguridad o actualizaciones ante inminentes riesgos o vulnerabilidades en las que se incluya el software y firmware utilizado por QWERTY S.A

SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS

Cuando QWERTY S.A, planee e implemente nuevos proyectos relacionados con la compra o actualización de medios tecnológicos de cualquier índole, deberá hacer un estudio de conveniencia y oportunidad en el cual deberá incluir adicionalmente a los documentos de ley, cláusulas de firma de acuerdos de confidencialidad y estudios de confiabilidad donde se realicen consideraciones de los riesgos jurídicos y desarrollo del proyecto a convenir.

POLÍTICA DE DISPOSITIVOS MÓVILES

Los dispositivos móviles de propiedad de QWERTY S.A que sean utilizados dentro o fuera de las instalaciones de la empresa, deberán ser únicamente usados para actividades de carácter empresarial o relacionados con la misma, y estos a su vez,

deberán tener la seguridad igual o superior a la que ostentan los equipos de escritorio de propiedad de la misma. Por ende, se deberá seguir los siguientes parámetros:

a) No está permitido el uso de equipos de cómputo personales o ajenos a la empresa y su conexión a la red de la entidad, por tanto, se implementarán mecanismos de seguridad tales como Firewall, antivirus, entre otros aprobados por la dirección de QWERTY S.A, para garantizar su implementación y protección.

b) Las estaciones de trabajo y equipos portátiles deberán contar únicamente con: Software licenciado, Cifrado de disco duro, software de protección o antivirus, entre otros que sean avalados por la empresa.

c) Los equipos de cómputo de la empresa y la información contenida o gestionada a través de estos son propiedad de QWERTY S.A, por tanto, estos activos deberán ser supervisados, auditados o usados en el modo que se disponga o cuando lo requiera la empresa. Por tanto, cuando se termine el vínculo laboral o prestación de servicio, estos deberán ser devueltos en iguales condiciones a las que se entregaron para su servicio, siendo responsabilidad única y exclusiva del empleado al que se le fue conferido o asignado este elemento.

d) QWERTY S.A se reserva el derecho de inspeccionar y auditar los equipos tecnológicos (incluyendo servidores) y redes cuando sea requerido o cuando la dirección lo crea conveniente.

POLÍTICA DE SEGURIDAD DEL RECURSO HUMANO

SELECCIÓN, TÉRMINOS Y CONDICIONES PARA EL EMPLEO

QWERTY S.A. establece un procedimiento de selección y contratación del personal de planta y sus respectivos ascensos a nivel interno, a través de un proceso de comprobación de antecedentes, hoja de vida del aspirante o empleado, certificaciones académicas y profesionales que será responsabilidad del grupo de recursos humanos de la empresa; corroborando siempre el cumplimiento de la Ley 1581 de 2012 y la normatividad vigente aplicable para este proceso.

El aspirante o empleado una vez seleccionado para el empleo, deberá aceptar las responsabilidades con el sistema de seguridad de la información de la empresa, además de los términos y condiciones para el empleo, a través de cláusulas. Estas también serán aplicables para el personal de contratos de aprendizaje o quienes vayan a utilizar o manipular los activos de información de QWERTY S.A.

TOMA DE CONCIENCIA, EDUCACIÓN Y FORMACIÓN EN SEGURIDAD

La empresa QWERTY S.A delegará la responsabilidad a la Oficina de Recursos Humanos junto con el Promotor del sistema en Coordinación con el funcionario encargado de la publicidad de la empresa, para la realización de actividades de campañas educativas y de toma de conciencia, seminarios o cursos formativos sobre temas con referencia sobre la seguridad de la información las cuales estarán dirigidas al personal de planta de la empresa, clientes y quienes intervengan en el sistema. Este proceso se soportará mediante informes mensuales a la Dirección.

POLÍTICA DE GESTIÓN DE ACTIVOS

INVENTARIO DE ACTIVOS

Los inventarios de activos de información de la empresa QWERTY S.A. se harán en el despliegue de la implementación del sistema y cuando sea requerido nuevamente por cambio o adición de estos activos, cambio de Jefe de Área, Grupo o Director de la empresa; procedimiento el cual estará a cargo del Jefe de cada Área de la empresa en coordinación con el encargado del inventario del Área o Grupo y el levantamiento de esta información deberá ser sometido a Comité de Seguimiento del SGSI de la empresa, quienes deberán tener conocimiento pleno de los activos que hacen parte de la organización.

Es de anotar que este procedimiento se deberá realizar al menos una vez al año, con el fin de supervisarlos.

ASIGNACIÓN DE LOS ACTIVOS

La delegación de responsabilidad sobre los activos de información de propiedad de la empresa estará ligada de manera individual de acuerdo con el cumplimiento de las obligaciones del empleado o quien requiera acceder a estos (contratistas, aprendices o practicantes) y este procedimiento será ejecutado por el jefe del área al que pertenece el activo o quien sea delegado por este.

USO ACEPTABLE DE ACTIVOS

a) La información en cualquiera de sus presentaciones (física o digital), los medios, servicios y equipos tecnológicos de propiedad de QWERTY S.A son activos de la empresa y serán proporcionados a sus integrantes, empleados o terceros con el único fin de utilizarse para propósitos del negocio.

b) La información deberá ser manejada o procesada según su clasificación.

c) Los equipos tecnológicos adquiridos por la empresa deberán ser rotulados o etiquetados a fin de generar un control para su uso y asignación.

DEVOLUCIÓN DE ACTIVOS

Una vez se dé por terminado el vínculo laboral de un empleado, contratista o tercero, este deberá entregar los activos que le fueron asignados en las mismas condiciones en las que le fueron entregados, además se le deben retirar todos los permisos y derechos de acceso a los recursos y sistemas de información a los cuales estuvo autorizado por la empresa.

Es de anotar que esta devolución se deberá hacer de manera formal mediante un oficio o solicitud suscrita por la persona que devuelve los activos y deberá recibirla el personal autorizado del Área de Soporte.

CLASIFICACIÓN DE LA INFORMACIÓN

La empresa QWERTY S.A con base a la normatividad vigente, realiza una clasificación de la información, la cual será de obligatorio cumplimiento por parte de todos sus integrantes y terceras partes que hagan uso de sus activos de información, con el fin de garantizar su seguridad de la siguiente manera:

- **Dato Público:** son aquellos considerados de libre acceso o que pueden ser de conocimiento de todas las personas dentro o fuera de la empresa.

- **Dato interno:** Es aquella información que solo puede ser accesible a los miembros de la empresa o terceros en suscripción de cláusula de responsabilidad con la seguridad de la información, la cual solo es para uso con fines del negocio.

- **Dato Restringido:** Es aquella información que solo puede ser de conocimiento de los Jefes de Área y aquellos empleados autorizados a través de claves de acceso.

- **Dato Confidencial:** Por último, es aquella información de carácter restringida única y exclusivamente a la alta dirección de la empresa.

ETIQUETADO DE LA INFORMACIÓN Y MANEJO DE ACTIVOS

Todos los documentos físicos de la empresa QWERTY S.A será etiquetados y rotulados de acuerdo con los lineamientos de la gestión documental definida por la empresa en cumplimiento a la norma ISO 9000 y otorgando un ciclo de vida de estos documentos y procesamiento de estos de concordancia con las consideraciones de la Dirección.

GESTIÓN DE MEDIOS REMOVIBLES

QWERTY S.A verificando y controlando el uso de unidades de almacenamiento en la empresa establece:

- Se promueve el uso de carpetas compartidas a cambio de medios removibles o pendrive, a través del servicio FTP donde se estructura una organización de manera tal que se pueda compartir o intercambiar información al interior de la entidad según se requiera.

- El empleo de programas de cualquier índole en medios removibles sobre los equipos tecnológicos de la organización, están bloqueados desde la BIOS, el cual a su vez está protegido mediante contraseña.

- El software de protección antivirus está configurado para realizar un escaneo de manera automática a aquellos medios removibles que llegue a detectar conectados a estos equipos de manera preventiva.

POLÍTICA DE CONTROL DE ACCESO

CONTROL DE ACCESO

Se determina el ciclo de vida de los usuarios digitales empresariales a través de la herramienta de gestión de usuarios de la empresa QWERTY S.A. que son avalados por el grupo de recursos humanos previamente para su creación y habilitación de permiso de acceso a los sistemas de información.

Esta cuenta de usuario digital será intransferible y único para su uso, por tanto, la mala utilización o préstamo de mismo será objeto de investigaciones de tipo penal, disciplinarias o administrativas a la que hubiere lugar, ya que el uso irresponsable del mismo, pone en riesgo la integridad, confidencialidad y disponibilidad de la información de la empresa QWERTY S.A, por lo cual su alteración o degradación a causa de ello es únicamente responsabilidad del funcionario a quien se otorgó, por ende deberá seguir las recomendaciones dadas en la cláusula de responsabilidad suscrita ante el grupo de recursos humanos.

ACCESO A REDES Y SERVICIOS DE RED

En QWERTY S.A. las conexiones de red no seguras pueden afectar sus activos de información, por ende, se realiza un control a cargo del área de infraestructura en

donde esta desarrolla actividades tendientes a garantizar que los empleados tengan acceso a redes y servicios de red que no comprometan la seguridad así:

- Identificación de los equipos de cómputo y tecnológicos (servidores, entre otros) conectados a la red de la empresa, los cuales deben haber sido promovidos al dominio de QWERTY.

- El servicio de direccionamiento DHCP deberá realizar una reserva de los equipos en dominio con sus respectivas direcciones IP para identificar el uso del medio.

REGISTRO, CANCELACIÓN DE ACCESO EN LA GESTIÓN DE USUARIOS

El registro de creación de usuario corresponde a la cláusula suscrita en recursos humanos, quienes enviaran un correo firmado por el jefe de esa dependencia al área de infraestructura con el formato en digital para la creación del usuario digital empresarial.

Cuando el empleado o funcionario finalicen su vinculación laboral con la empresa QWERTY S.A, el grupo de recursos humanos hará llegar un correo electrónico al área correspondiente para la eliminación de acceso a los recursos otorgados a la persona, adicionalmente esa misma oficina deberá informar las ausencias laborales de los funcionarios por el mismo medio, a fin de que se inhabiliten los permisos otorgados a los mismos.

GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADO

QWERTY S.A controla la asignación y restricción del uso de acceso privilegiado a los sistemas de información mediante las siguientes directrices:

- Autenticación de usuarios para conexiones a través de servicios SSL, Canales de datos y VPN son contemplados por la empresa para su conexión a la red institucional de manera exclusiva y con fines de las actividades que sean autorizadas por la Dirección.

- Se realizará una protección de los puertos de configuración para el acceso remoto, lo cual permitirá dar soporte remoto a los equipos en red dentro de la organización, este estará restringido a los administradores de red y servidores.

- El acceso remoto a los equipos empresariales únicamente estará autorizado por el Área de Infraestructura.

RESPONSABILIDADES DE LOS USUARIOS

En las responsabilidades de los usuarios dentro de la empresa QWERTY son plenamente suscritas en la cláusula de responsabilidad con el sistema de gestión de seguridad de la información de QWERTY S.A. donde se integran las siguientes responsabilidades:

1. Observar el cumplimiento de cada una de las políticas suscritas en el manual del sistema de gestión de seguridad de la información de QWERTY S.A.

2. Comprometerse a Informar cualquier novedad ocurrida con los activos de información de la empresa.

3. Comprometerse a no conectar equipos tecnológicos no empresariales a las redes de éste, sin previa autorización.

4. Comprometerse a no ingresar o autorizar el ingreso de personas ajenas o sin autorización a áreas restringidas y /o lugares donde se procesa información sensible.

5. Comprometerse a acatar las normas de seguridad industrial evitando vender, comer o beber cualquier tipo de alimentos cerca a los equipos tecnológicos.

6. Cumplir en todo momento con las medidas apropiadas para la protección y conservación de la información y/o activos de información de la empresa.

7. Cumplir con las medidas para el almacenamiento seguro de información impresa, la cual debe permanecer con llave al terminar la jornada laboral o cuando no requiera su uso con el fin de asegurar su protección.

8. Evitar el uso de la red de datos de la empresa para crear, manipular o replicar material comercial, publicitario o mensajes que puedan poner en velo la reputación de la empresa o sus empleados.

9. Cuando por necesidades del servicio que presta la empresa, deba realizar otras labores de apoyo en cumplimiento de la misionalidad de esta, accederé a la información de otras áreas o grupos siempre observando y cumpliendo el deber de reserva y confidencialidad de esta, evitando la mala manipulación u otras acciones que puedan poner en peligro la integridad y disponibilidad de esta.

10. Proteger siempre la reputación de la empresa y sus empleados dentro y fuera de la plataforma tecnológica de la organización.

11. Hacer un buen y adecuado uso de los recursos y activos de información de la empresa, solamente para las actividades del servicio y en pro del cumplimiento de la misionalidad de esta.

12. Hacer un buen y adecuado uso del usuario digital empresarial.

13. No utilizar los equipos de cómputo para almacenar archivos o datos que no tengan que ver con la empresa o sus actividades misionales como videos, música, etc.

14. Hacer uso exclusivo de los equipos tecnológicos que me sean asignados y me responsabilizaré por su protección y cuidado, informando cualquier novedad con los mismos.

15. Acatar los protocolos y controles de acceso físico a las instalaciones de la empresa mediante la utilización de carné, autenticación biométrica y acompañamiento de personas visitantes.

CONTROL DE ACCESO A SISTEMAS Y APLICACIONES

Para este control, se hará el mismo procedimiento anterior de “registro y cancelación de acceso”, donde el grupo de recursos humanos hará una solicitud mediante correo electrónico empresarial, sobre la concesión de acceso a sistemas y aplicaciones de la empresa requeridos para el empleado o funcionario, los cuales serán soportados mediante cláusula de responsabilidad escaneada y anexa al mismo correo, a fin de que obren como antecedente.

RESTRICCIÓN DE ACCESO A LA INFORMACIÓN Y PROCESAMIENTO DE INGRESO SEGURO

Este control de acceso a la información se realizará mediante aprobación y previa solicitud del grupo de recursos humanos, quienes anexarán a los anteriores procedimientos, los privilegios que tendrá el empleado, autorizando el acceso a información tanto física como digital en las áreas donde estén contenidos, la cual será implementada y registrada en los servicios de acceso físico y digital a cargo del área de infraestructura.

Las condiciones de privacidad de esta información, estará a cargo de cada área o grupo de la empresa, previa solicitud ante el comité de seguimiento del SGSI.

Los sistemas de información revisarán los controles de acceso a la información, a través del procesamiento de ingreso seguro, el cual será definido por el Área de Desarrollo previo aval por parte de la dirección, definiendo este como un lineamiento seguro para el acceso y procesamiento de la información dentro de la organización.

SISTEMA DE GESTIÓN DE CONTRASEÑAS

El sistema de gestión de contraseña de la empresa QWERTY S.A es la herramienta administrativa adquirida por la empresa para realizar los siguientes controles en la gestión de la autenticación de usuarios y contraseñas:

- Permitir a los usuarios gestionar sus propias contraseñas
- Exigir de manera segura los caracteres que integren una contraseña de calidad.
- Forzar a los usuarios cambiar las contraseñas con un ciclo de vida adecuado no mayor de dos meses
- Llevar un compendio temporal de contraseñas utilizadas por los usuarios para impedir su reúso constante en los sistemas.
- Almacenar y registrar de manera segura las contraseñas
- No develar las contraseñas en el registro de a los sistemas de información de la empresa.

CONTROL DE ACCESO A CÓDIGOS FUENTE DE PROGRAMAS

En QWERTY S.A el acceso al código fuente y demás características de los sistemas de información empresariales están protegidos de acceso o cambios no autorizados a través de los siguientes controles:

- Suministro exclusivo al área de desarrollo y los funcionarios que la integran, el código fuente para modificaciones, con el objeto de garantizar la fuente y el ejecutable de estos.
- Se debe tener historial de las versiones de código fuente y sistemas de información.
- Se deben registrar todos los sistemas y programas en uso, indicando el nombre de estos, su programador y responsable de las autorizaciones de modificación o cambio e histórico de estas acciones.
- El personal de soporte debe tener acceso restringido a las librerías de las fuentes de los programas de la empresa.
- Se debe garantizar que no más de una persona realice las modificaciones de estos programas.

- Se debe evitar que programas fuentes históricos se almacenen en ambientes de producción.

- Se deben realizar con regularidad pertinente las copias de respaldo de los programas fuentes.

POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS Y GESTIÓN DE LLAVES

QWERTY S.A. utilizará sistemas y técnicas de criptografías para la protección de la información de acuerdo con su clasificación plenamente establecida en este documento, de acuerdo con el análisis de riesgos para procurar por su adecuada seguridad.

El uso estos controles se realizarán de acuerdo con las siguientes consideraciones:

a. Se utilizarán los controles criptográficos cuando se requiera:

- Protección de contraseñas en el acceso a los servicios y sistemas que requieran controles de acceso seguro.

- Servicios empresariales que recopilen información de terceros con el fin de salvaguardar su integridad.

- Mensajería empresarial instantánea

- Firma digital de documentos o correos electrónicos debidamente autorizados vía web.

- Trasmisión de información sensible al interior o fuera de la empresa.

Las llaves criptográficas deben ser cambiadas anualmente o cada vez que se ponga en tela de juicio la confidencialidad de estas, por otro lado, para el caso de los certificados SSL se deberá realizar su cambio con la periodicidad no mayor de 1 año o de acuerdo con la disponibilidad de presupuesto con la que cuenta la organización.

La administración de las llaves criptográficas y certificados estará a cargo del Área de Desarrollo quienes velaran por su adecuada implementación dentro de la empresa.

Todos los funcionarios responsables de tokens bancarios asignados deberán almacenar estos bajo llave cuando no se encuentren en uso, el adecuado uso y seguridad de estos serán supervisados por directamente por los jefes de cada dependencia a la cual pertenecen.

POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

CONTROLES DE ACCESO FÍSICO

Las áreas de infraestructura y desarrollo implementarán un sistema de control de acceso físico adecuado para restringir el ingreso de personal y empleados a las áreas seguras que contienen activos de información sensibles de la empresa. Adicionalmente, se tendrá un sistema de seguridad biométrico para registrar el ingreso de clientes y personal externo ajeno a la empresa, con el fin de llevar un control y monitoreo de las actividades que este personal realizará en las instalaciones.

SEGURIDAD DE OFICINAS, RECINTOS E INSTALACIONES

La seguridad del ingreso a las oficinas, recintos e instalaciones de la empresa QWERTY S.A estará a cargo del servicio de seguridad privada y del Área de infraestructura, en donde se implementarán sistemas de acceso aplicando controles para su ingreso, adicionalmente se establecerán restricciones que se deban tomar para algunos lugares que manejen información sensible de acuerdo las necesidades que se detecten deberán ser supervisados o cumplir con los siguientes aspectos:

- Las áreas que cuenten con controles de entrada asistidas por dispositivos biométricos, deberán ser verificados mensualmente por el personal autorizado del Área de Soporte.

- El ingreso a las instalaciones y áreas, deberán llevar un registro digital o físico en el cual se relacione fecha, hora de ingreso y salida de la persona, y para los visitantes se llevará un registro adicional de cuál es su motivo de la visita.

- Todas las personas y empleados deberán portar un tipo de identificación visible, el cual facilite la identificación de la persona por parte del personal de seguridad y control del personal que se encuentra dentro de las instalaciones.

PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES

QWERTY S.A socializará a través de los grupos de seguridad, emergencia o brigadistas los planes de evacuación al menos cada trimestre, además deberán ser publicados a través de medios audiovisuales o impresos estos planes al personal visitante de la empresa, como medio de prevención y reacción en caso de cualquier materialización de los riesgos de esta categoría.

UBICACIÓN Y PROTECCIÓN DE EQUIPOS TECNOLÓGICOS

Los equipos tecnológicos (computadores de escritorio, servidores, etc) serán ubicados de tal manera que se asegure su protección contra cualquier riesgo ocasionado por amenazas de cualquier origen, teniendo en cuenta los siguientes aspectos:

- Los equipos de cómputo deberán estar ubicados de tal manera que la información contenida no pueda ser visualizada o se genere oportunidades de acceso no autorizado.

- El acceso a áreas de almacenamiento de información o servidores, deben estar agrupados en un solo lugar, además su acceso deberá estar sujeto a un control de trazabilidad de acceso físico por medio de sistemas biométricos.

- Los centros de datos o áreas que contengan servidores deberán implementar controles ambientales o sistemas de climatización necesarios para el funcionamiento seguro en estas condiciones de acuerdo con la normatividad vigente.

SEGURIDAD DE SUMINISTRO

La empresa cuenta con un sistema de alimentación ininterrumpida redundante (UPS) la cual asegura la prestación de los diferentes servicios de QWERTY S.A ante cualquier fallo del suministro de energía, este sistema se encuentra conectado adicionalmente a una planta eléctrica que presta el soporte a este sistema en el caso que sea requerido.

SEGURIDAD DE EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES

El uso de equipos y activos fuera de las instalaciones de QWERTY S.A. estará restringido a equipos móviles y portátiles, su seguridad será igual o más robusta a la que ostentan los equipos tecnológicos ubicados dentro de las instalaciones de la entidad, por tanto, deberán cumplir los siguientes lineamientos para su uso externo:

- No podrán ser conectados a redes desconocidas o inseguras en lugares públicos.

- Los usuarios de estos deberán ser empresariales y los usuarios locales o por defecto del equipo deben ser bloqueados o deshabilitados.

- El software o programas instalados en estos equipos empresariales deben ser

totalmente licenciados.

- Deberán contar con controles criptográficos con el objeto de asegurar la confidencialidad e integridad de la información que allí se contiene.

SEGURIDAD DEL CABLEADO

La seguridad del cableado del servicio de energía eléctrica y redes de comunicación deben protegerse contra daño o interrupciones de cualquier origen, por tanto:
Se debe cumplir el estándar de calidad ISO 11801 o la normatividad vigente relacionada.

Se debe cumplir el reglamento RETIE expedido por el Ministerio de Minas y Energía de Colombia, para las instalaciones eléctricas y sus aspectos relacionados.

MANTENIMIENTO DE EQUIPOS

El mantenimiento de los equipos tecnológicos de la empresa otorga las condiciones necesarias para asegurar los activos de información de esta, por consiguiente, se deben realizar los siguientes controles y procesos por parte del área de soporte:

- El mantenimiento preventivo de los equipos tecnológicos se deberá realizar de acuerdo con las recomendaciones realizadas por el proveedor, dichos mantenimientos registrando los mismos en la planilla de control de equipos. El mantenimiento de los equipos de cómputo permitirá realizar un seguimiento de las actualizaciones y estado de los programas allí instalados.

- Solo el personal técnico del Área de Soporte puede realizar las reparaciones de los equipos y documentar mediante informes al grupo correspondiente administrativo y financiero, las solicitudes en los casos que se requiera un contrato de mantenimiento u orden de suministros para la reparación de estos.

- El responsable técnico es el encargado de registrar las reparaciones, fallas, necesidades, retiro de los activos de las instalaciones para reparaciones y reinstalación de programas por mantenimiento a través de la planilla de control de equipos.

RETIRO DE ACTIVOS

Los equipos, información o programas de QWERTY S.A no pueden retirarse de las instalaciones de la empresa sin previa autorización del propietario o quien sea delegado por la entidad para su supervisión, para lo cual se debe realizar un documento de soporte (acta u orden de mantenimiento), especificando para que va

a salir y por cuanto tiempo, se deben supervisar de manera periódica para detectar retiros no autorizados de estos elementos.

DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS

Este control establece que cuando el equipo se encuentre en buenas condiciones de funcionamiento, podrá ser asignado a otra persona revisando que se le haya realizado el correspondiente respaldo de la información. Para aquellos dispositivos que cumplan con su ciclo de vida útil, se le hará el proceso de disposición segura, realizando destrucción de elemento de almacenamiento o disco duro, documentando el proceso mediante los formatos.

POLÍTICA DE SEGURIDAD DE LAS OPERACIONES

PROCEDIMIENTOS DE OPERACIÓN DOCUMENTADOS

Todos los procesos y controles identificados en este manual que tengan que estar documentados, deberán estar avalados por el Comité de seguimiento del Sistema de Seguridad de la Información de QWERTY S.A, quienes mediante las actas de reunión de comité avalan su utilización y manejo dentro de la organización.

GESTIÓN DE CAMBIOS

En el proceso de negocio, en las instalaciones y sistemas de procesamiento de QWERTY S.A, toda modificación que se realice y afecte la seguridad de la información, debe emplearse os siguientes requisitos mínimos de gestión de cambios que se ajustan a las decisiones de arquitecturas seguras contemplando los siguientes puntos:

- Identificación y registros de cambios.
- Planificación y puesta de pruebas de los cambios.
- Valoración de los impactos potenciales, incluidos los impactos de esto cambios en la seguridad de información empresarial.
- Aprobación formal del cambio en reunión o comité de cambios de la empresa.
- Verificación de compromisos y requisitos de seguridad de la información.
- Comunicación de los cambios y detalles a las partes intervinientes.
- Procedimientos y protocolos de cancelación del cambio en casos fallidos.

- Verificación de los resultados del cambio realizado.

GESTIÓN DE CAPACIDAD

El proceso de desarrollo de la empresa QWERTY S.A, realiza un análisis detallado, quien junto con una planeación realiza una proyección de los requisitos para las necesidades futuras de crecimiento en talento humano, procesamiento, almacenamiento y trasmisión de los servicios e información prestados por la entidad, con el objeto de asegurar un adecuado desempeño.

SEPARACIÓN DE LOS AMBIENTES DE DESARROLLO, PRUEBAS Y PRODUCCIÓN

Los ambientes de desarrollo, pruebas y producción están separados de forma física y virtual, con el fin de evitar problemas operacionales, siendo documentado a través de informes documentales la transferencia de software aplicando los siguientes controles:

- Se debe ejecutar software de desarrollo y producción en ambientes de trabajo diferentes.

- Las diversas actividades de desarrollo y pruebas se deben ejecutar en ambientes separados.

- Los compiladores, editores y oras herramientas de desarrollo o utilidades del sistema no deben ser accesibles desde sistemas de producción cuando no se requiere.

- Lo datos sensibles no deben copiarse en ambientes de pruebas, ya que no se cuenta con controles equivalentes para sistemas de pruebas.

CONTROLES CONTRA CÓDIGOS MALICIOSOS

Con base en la prevención de códigos maliciosos o malware, se definen los siguientes controles los cuales se basan en software de antivirus así:

- Supervisa y verifica antes de la apertura de cualquier archivo, la posible presencia de virus o cualquier código malicioso oculto en este o contenido dentro del equipo.

- No se permite las instalaciones o uso de software no autorizado por el Área de soporte.

- No se permite el envío o intercambio de archivos planos por medio de los puertos de los equipos de cómputo, con el fin de salvaguardar la información de la empresa.

- El programa realiza una actualización automática de los paquetes disponibles para mantenerse al día con los datos que suministra el proveedor para brindar la seguridad robusta en el sistema contra cualquier amenaza.

RESPALDO DE LA INFORMACIÓN

La realización de las actividades tendientes a las copias y recuperación de la información estará a cargo del Área de soporte, quienes garantizarán las condiciones de seguridad necesarias para la disponibilidad e integridad de estos respaldos e información contenida de todas las áreas de la empresa, las cuales estará soportadas en el servidor FTP y su acceso será concedido por esta área de acuerdo con el requerimiento mediante correo electrónico de las áreas que requieran el acceso de su personal a este recurso.

SINCRONIZACIÓN DE RELOJES

QWERTY S.A para garantizar la exactitud de los registros de auditoría, dispone de servicio de red NTP que sincroniza a su vez con la hora legal Colombiana como única fuente de referencia de tiempo para toda la plataforma tecnológica de la entidad.

INSTALACIÓN DE SISTEMAS OPERATIVOS

El área encargada de la instalación de sistemas operativos es la de Soporte, en plena coordinación con el Área de desarrollo en los casos que esta requiera la instalación de algún software necesario para poner en producción una aplicación que fue avalada previamente por el Comité de Seguimiento del SGSI.

RESTRICCIÓN SOBRE LA INSTALACIÓN DE SOFTWARE

Para este control, se estableció una política a nivel de administrador de dominio, el cual es de responsabilidad y uso exclusivo del personal del Área de soporte, no permitiendo así que los usuarios puedan instalar programas o hagan cambios en los sistemas operativos de los equipos de cómputo de la empresa.

POLÍTICA DE SEGURIDAD DE LAS COMUNICACIONES

CONTROLES DE REDES

Para este control, se hace necesario cumplir con el estándar ISO/IEC 18028, el cual referencia las recomendaciones y parámetros para la implementación segura de las redes en la empresa.

SEGURIDAD EN SERVICIOS DE RED

En este proceso es importante supervisar e implementar los controles necesarios para asegurar los niveles de servicio y requerimientos de seguridad de la red, entre los cuales deberán estar el seguimiento del tráfico de red, monitoreo permanente y restricciones de los puertos de red, Las supervisión y respaldo de los logs de información que obrarán como antecedentes ante inminentes riesgos y amenazas que lleguen a materializarse dentro de la organización.

SEPARACIÓN DE REDES

Es fundamental asegurar las redes de la empresa y sus conexiones, Por ello se implementará por medio de protocolos seguros, a través de un sistema de protección o cortafuegos la configuración correspondiente para tal fin.

Aunado a lo anterior, se controlará el acceso a los servicios de red a través del servidor DCHP será segmentado, apartando los servicios de acuerdo con las necesidades de la empresa con el fin de evitar el acceso no autorizado estos o evitando que se materialicen riesgos y amenazas que pongan en peligro los activos de información de la empresa.

POLÍTICAS Y PROCEDIMIENTOS DE TRANSFERENCIA DE INFORMACIÓN

Para el intercambio de información, se hará uso de acuerdos de revelación de información de carácter confidencial y deber de reserva, adicionalmente se harán controles contemplando sistemas de información, uso de equipos y redes de comunicación, uso de modelos de control de acceso e implementación de servicios web con autenticación.

MENSAJERÍA ELECTRÓNICA

Este es un servicio está contratado con Google por ende este será utilizado para comunicación interna, compartir archivos previamente autorizados por la entidad, recibir comunicados oficiales, brindar espacio de almacenamiento ilimitado debidamente contratado, dar prioridad de las actividades para el desarrollo del programa académico.

Por lo anterior, no está permitido el intercambio de información empresarial a través de otras plataformas de mensajería electrónica instantánea, a fin de asegurar la seguridad de la información de QWERTY S.A.

POLÍTICA PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

ANÁLISIS Y ESPECIFICACIÓN DE REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN

QWERTY S.A con el objeto de realizar análisis y especificación de requisitos de seguridad de la información en la adquisición de productos con las características de seguridad y procesos formales de pruebas para la evaluación de ofertas, deberá contemplar los siguientes aspectos de seguridad de la información:

- Nivel de confianza con relación de la identificación declarada a los usuarios, para obtener requisitos de autenticación.

- Informar a los usuarios y operadores sobre los deberes y responsabilidades.

- Requisitos de los procesos del negocio, tales como registros de transacciones, seguimiento y no repudio.

- Necesidades los activos involucrados, observando su disponibilidad, confidencialidad e integridad.

- Los requisitos exigidos por otros controles tales como las interfaces de ingreso, seguimiento o sistemas de detección de fugas de información o datos.

SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS

La información de carácter publica de la empresa, esta resguardada de modificaciones no autorizadas que puedan afectar la imagen y la seguridad de la empresa, por ende, se creó un protocolo interno para autorizar la publicación de información ante los diferentes medios publicitarios previamente autorizados por la dirección de QWERTY S.A.

Lo anterior con el fin de cumplir las leyes sobre el tratamiento de datos y la demás normatividad que en relación se refiera.

PROTECCIÓN DE TRANSACCIONES DE LOS SERVICIOS DE LAS APLICACIONES

Aquellas dependencias donde se realicen transacciones en línea deberán cumplir las siguientes consideraciones de seguridad:

- Emplear y exigir uso de firmas electrónicas por parte de cada parte involucrada en el procedimiento.

- Las comunicaciones en cualquiera de las vías, deberá estar debidamente cifrada.

POLÍTICAS DE DESARROLLO SEGURO

QWERTY S.A reconoce que los sistemas de información son un soporte esencial para el cumplimiento de su misionalidad y en búsqueda de brindar seguridad a sus aplicaciones y programas establece los siguientes lineamientos:

- Con el fin de prevenir y minimizar el riesgo de uso no autorizado o fallos de cambios no previstos, todos los sistemas de información contarán con un módulo de auditoria que administrará el almacenamiento de registros y Logs de las actividades realizadas por usuarios o herramientas dentro del sistema.

- Se asegurará la independencia del inicio de una actividad y la autorización de la ejecución para prevenir y contrarrestar la conspiración de fraude.

- Se deberá dividir o segregar las funciones de desarrollo, producción e implementación o producción de los sistemas de información a fin de evitar cualquier materialización de los riesgos asociados a este.

- Se deberá documentar el motivo por el cual no se puede segregar las funciones, para que este obre como antecedente ante una posible auditoria.

RESTRICCIÓN SOBRE CAMBIO EN LOS PAQUETES DE SOFTWARE

Las restricciones de modificaciones de paquetes de software por parte de los proveedores deben contemplar los siguientes aspectos:

- Análisis de los términos y condiciones de las licencias, en los cuales deberán estar incluidos los cambios o modificaciones permitidas a estos, además analizar qué tan conveniente son estas modificaciones para la empresa y el proveedor.

- Evaluar el impacto a asumir el cambio de personal de la empresa

- Guardar copias del software que se modificará y se deberá documentar las modificaciones realizadas.

PRINCIPIOS DE DESARROLLO SEGURO

Las aplicaciones y sistemas de información como soporte importante para QWERTY S.A en los servicios misionales que presta a sus usuarios, busca brindar seguridad de la información que allí se procesa y entrega a sus clientes, por tanto, se establecen los siguientes principios a partir de la valoración de los riesgos asociados con las labores de desarrollo de sistemas individuales y sus ambientes, en los cuales se incluye las personas, procesos y tecnología asociados con el desarrollo e integración de estos sistemas, así:

- Se debe considerar el carácter sensible de los datos que el sistema va a procesar, almacenar o trasmitir.

- Todos los sistemas de información contarán con una auditoría para almacenar los registros de interfaces de usuarios y las transacciones ejecutadas por los mismos.

- Se controlará el acceso al ambiente de desarrollo.

- Se deben almacenar en lugares seguros fuera de sitio, las copias de respaldo.

- Se deberá considerar la confiabilidad del personal que trabaja en cada ambiente.

- Se deberá asegurar la independencia de inicio de la actividad y autorización para evitar posibilidad de fraude en los procesos.

AMBIENTES DE DESARROLLO

QWERTY S.A establece como ambientes de desarrollo, las oficinas del área de desarrollo de la organización en las cuales se encontrarán subdivididas en tres módulos independentes (Desarrollo, Pruebas y Producción) y con la seguridad biométrica adecuada y requerida para el acceso a estos, en donde se incluyen los ambientes acordes para incluir las persona, procesos y tecnología asociados al desarrollo e integración de los sistemas.

DESARROLLO CONTRATADO EXTERNAMENTE

La tercerización del desarrollo de software debe seguir las siguientes recomendaciones:

- Se deberá cumplir con lo normado en la ley 23 de 1982 sobre los derechos de autor y la normatividad sobre los delitos de propiedad intelectual e industrial en Colombia.

- Se deberá someter las aplicaciones y software desarrollado a pruebas de calidad que permitan determinar si cumplen con los requerimientos establecidos y la seguridad, entre otros aspectos que se consideren pertinentes.

- Dentro de las especificaciones, se debe contar con la garantía, así como el acuerdo de custodia de los códigos fuentes del software desarrollado externamente, en caso de necesitar algún cambio o modificación de este.

PRUEBAS DE SEGURIDAD Y ACEPTACIÓN DE SISTEMAS

El área de desarrollo de QWERTY S.A realizará pruebas de seguridad y funcionamiento de los sistemas antes de la salida a producción teniendo en cuenta lo siguiente:

- Analizar cómo afecta el nuevo sistema o sus actualizaciones la capacidad de procesamiento y almacenamiento los recursos actuales.

- Todos los sistemas tanto nuevos como actualizados serán sometidos a pruebas y verificación de la seguridad la cual será realizada inicialmente por el equipo de desarrollo de los sistemas.

- Se debe garantizar la recuperación ante errores.

- Los sistemas deben contar con mecanismos de restauración del sistema a su estado inicial antes del cambio.

- Las pruebas de aceptación y seguridad serán llevadas a cabo en un ambiente de pruebas realistas, para asegurar que no introducirá vulnerabilidades al ambiente de la organización y que estas son confiables.

- Capacitar a los nuevos usuarios de los sistemas sobre su uso.

POLÍTICAS DE RELACIÓN CON PROVEEDORES

POLÍTICA DE SEGURIDAD PARA LA RELACIÓN, TRATAMIENTO, SEGUIMIENTO Y REVISIÓN CON PROVEEDORES

QWERTY S.A establece los lineamientos de control en sus relaciones con terceros proveedores de bienes o servicios, quienes suscribirán a través de los contratistas

de la empresa avalados por la dirección, contratos y acuerdos que cumplan los siguientes aspectos:

- Los contratos deberán tener incluidos los acuerdos y contemplaciones de especificaciones técnicas de manera clara y concisa.

- Anexo a los contratos, se deberá suscribir o incluir las cláusulas de responsabilidad con el sistema de gestión de seguridad de la información de la empresa.

- Estos contratos se deben someter a un estudio de confiabilidad y credibilidad para certificar su responsabilidad.

- De manera primigenia, antes de la entrega de información, se deberá realizar una evaluación del riesgo por parte de la empresa y el supervisor del contrato delegado por esta, para establecer su viabilidad y salvaguardar la protección e integridad de esta.

- La empresa deberá delegar a un supervisor o responsable de supervisar el personal externo, contratistas o terceros mientras ejecutan las actividades para las cuales fueron contratados a fin de asegurar el cumplimiento de las labores y condiciones debidamente suscritas como debe corresponder.

POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

RESPONSABILIDADES Y PROCEDIMIENTOS

La responsabilidad de la gestión de incidentes de seguridad de la información y los procedimientos de tratamiento de este, estarán sujetos al Comité de Seguimiento del SGSI de la empresa QWERTY S.A. a quienes se pondrá en conocimiento los incidentes que se llegasen a conocer de primera mano, previo análisis mediante informe realizado por parte del Promotor de seguridad de la información sobre los eventos que se registren en la empresa.

REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

Este reporte es responsabilidad del promotor de seguridad de la información de la empresa, quien deberá plasmar el análisis y dictamen técnico de los eventos que se llegasen a presentar y que según su juicio deban ser de pleno conocimiento del Comité de Seguimiento de la empresa para la evaluación del procedimiento a seguir para su correspondiente tratamiento.

EVALUACIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN Y DECISIONES SOBRE ELLOS

El comité de seguimiento del SGSI será el encargado de realizar la evaluación de los eventos de seguridad que se llegasen a presentar en la empresa y tomará las decisiones para su tratamiento de acuerdo con la normatividad vigente, dejando registro de estas acciones en el acta del comité.

RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

El comité delegará un grupo de integrantes de este o en su defecto contratará de ser necesario a personal idóneo en la materia, para contrarrestar e implementar acciones tendientes a dar respuesta a los incidentes de seguridad de la información que se llegasen a conocer. Por tal motivo, ante este control se deberán rendir informe de las acciones implementadas y resultados obtenidos ante el comité para su correspondiente evaluación y acciones tengan lugar.

POLÍTICA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

DISPONIBILIDAD DE INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN

La interrupción del servicio puede ocasionar daños incalculables y catastróficos para la empresa, en consecuencia, es fundamental que el Comité de seguimiento del SGSI de la empresa realice las siguientes acciones tendientes a preservar este control:

- Analizar las amenazas que pueden ocasionar interrupción a las actividades y procesos de la empresa.

- Evaluar los riesgos determinando su posible impacto ante estas interrupciones al servicio.

- Determinar controles preventivos.

- Desarrollar un plan de continuidad del negocio en el cual se reflejen estos aspectos estableciendo un enfoque integral para que la empresa pueda continuar con sus actividades ante posibles amenazas y mientras se restablece el servicio.

- El insumo de este control deberá implementarse mediante acta de comité para ser aprobada por el mismo y proyectar así el plan de continuidad del negocio.

POLÍTICA DE CUMPLIMIENTO

DERECHOS DE PROPIEDAD INTELECTUAL

QWERTY S.A en cumplimiento a las normas y leyes legales del estado colombiano, implementará algunas pautas en busca de la protección de la propiedad intelectual de la siguiente forma:

- En los activos de información de la empresa, solo se usarán los programas o software debidamente licenciados y autorizados por el Área de Soporte de la empresa.

- El área de soporte tiene la responsabilidad de instalar y verificar programas y software adquiridos por la empresa, velar por el mantenimiento de actualizaciones y licenciamiento de este y que utilice la empresa para el cumplimiento de su misionalidad, velar por el buen uso de los programas adquiridos y auditar e informar de manera oportuna el incumplimiento de las normas establecidas por parte de los empleados o funcionarios de esta empresa en el que se vean involucrados los activos de información de la misma.

- El software desarrollado por QWERTY S.A o suministrado por su fabricante deberá ser usado de acuerdo con las condiciones, términos acordados y el cumplimiento de la normatividad vigente.

- Todo miembro de la empresa se abstendrá de violar las normas de derechos de autor y aquellos relacionados.

PROTECCIÓN DE REGISTROS

Se deberán proteger de cualquier perdida, modificación no autorizada, falsificación y destrucción los registros críticos de QWERTY S.A. por ende deberán estar parametrizados mediante el lineamiento de gestión documental que aplica la empresa, donde están parametrizados los tiempos de almacenamiento de acuerdo con los requerimientos legales y normativos que soportan los procesos realizados por la empresa, y los cuales además siguen los siguientes parámetros:

- El sistema de almacenamiento de información es seleccionado de modo que los datos pueden recuperarse de forma tal que se admita en formato y demás características que cualquier empresa o entidad lo requiera.

- Las llaves criptográficas relacionadas con archivos cifrados se disponen de manera segura para el uso por parte de aquellas personas que estén

autorizadas.

- Si se establecen medios de almacenamiento electrónico, se deberá garantizar que hay capacidad para el acceso a la información por un periodo de tiempo determinado con el objeto de resguardarlos contra perdidas ocasionales o cambios futuros.

- Se debe garantizar una clasificación de los registros dentro del sistema de almacenamiento, además debe permitirse la destrucción de los registros adecuadamente cuando hayan cumplido su tiempo de almacenamiento o cuando sea necesario.

REGLAMENTACIÓN DE CONTROLES CRIPTOGRÁFICOS

El uso de certificados y firmas digitales para ser utilizadas en el intercambio de información con otras organizaciones o entidades diferentes a QWERTY S.A, se realizarán de acuerdo con la Ley 527 de 1999 “Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales…” por ende la empresa utilizará firmas y certificados digitales que son expedidos por entidades certificadoras para el intercambio de información de acuerdo a las actividades que lo requieran en cumplimiento a su misionalidad.

REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN

Un organismo externo auditor, realizará las evaluaciones y revisiones independientes sobre el cumplimiento de los controles y políticas de seguridad de la información de la empresa QWERTY S.A cuando sea requerido mediante solicitud para una futura certificación del sistema o cuando sea requerido para auditar los servicios de la empresa por parte de entes del estado.

CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD

QWERTY S.A a través de la planeación empresarial garantiza el cumplimiento de las políticas de seguridad de la información definidas en el presente manual, buscando el mejoramiento continuo del sistema, toda la organización deberá velar por el cumplimiento de la política de seguridad basada en las buenas prácticas y fortalecimiento de los procesos de cada una de las áreas de la entidad, verificando constantemente el seguimiento mediante auditorías internas sobre el estado de implementación y madurez del sistema de gestión de seguridad de la información, elaborando los respectivos planes de mejora continua.

REVISIÓN DEL CUMPLIMIENTO TÉCNICO

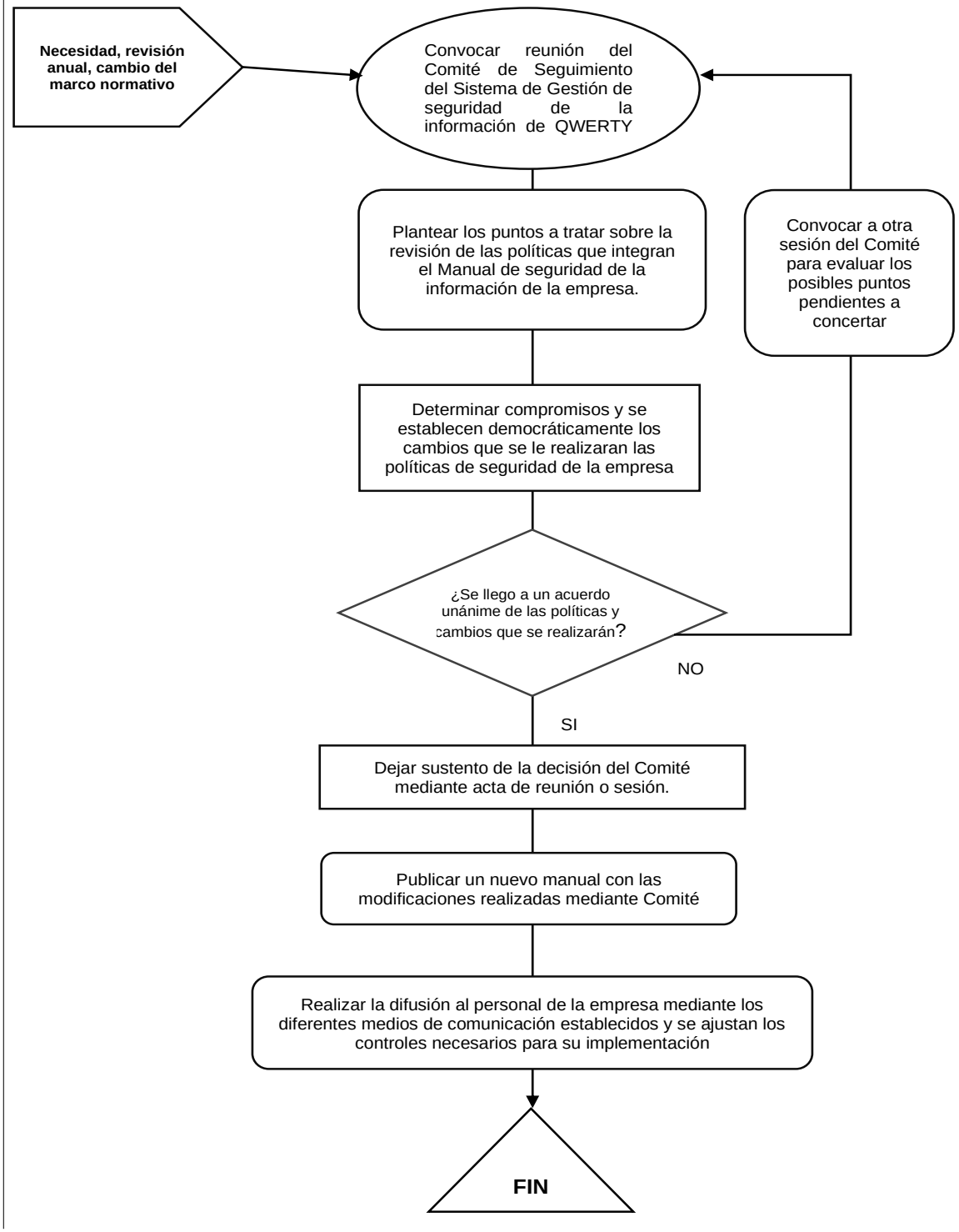
El promotor de seguridad de la información o los funcionarios delegados por el Comité de Seguimiento de seguridad de la información, verificarán cada uno de los sistemas de información, equipos tecnológicos y demás recursos de la empresa para supervisar que estos cumplan con los requisitos de seguridad básicos de manera primigenia, donde se deberán tener en cuenta las solicitudes y validación de las pruebas de penetración, los cuales son una manera de mejorar los controles, pero nunca eximirán el análisis de riesgos sobre los activos de información de QWERTY S.A.

Anexo F. Procedimientos documentados

PROCEDIMIENTO DOCUMENTADO

EMPRESA QWERTY S.A.

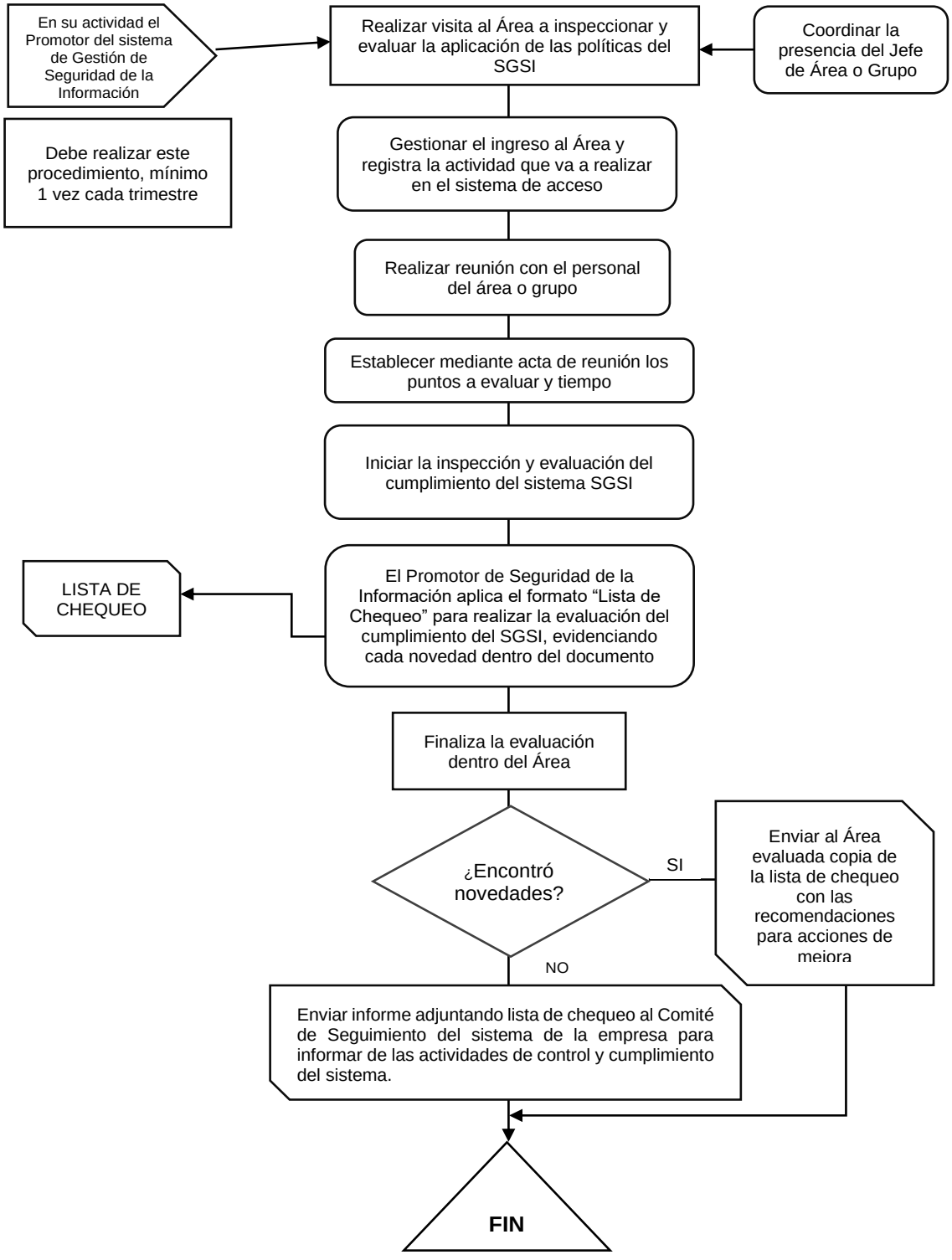
REVISIÓN DE POLÍTICAS



PROCEDIMIENTO DOCUMENTADO

EMPRESA QWERTY S.A.

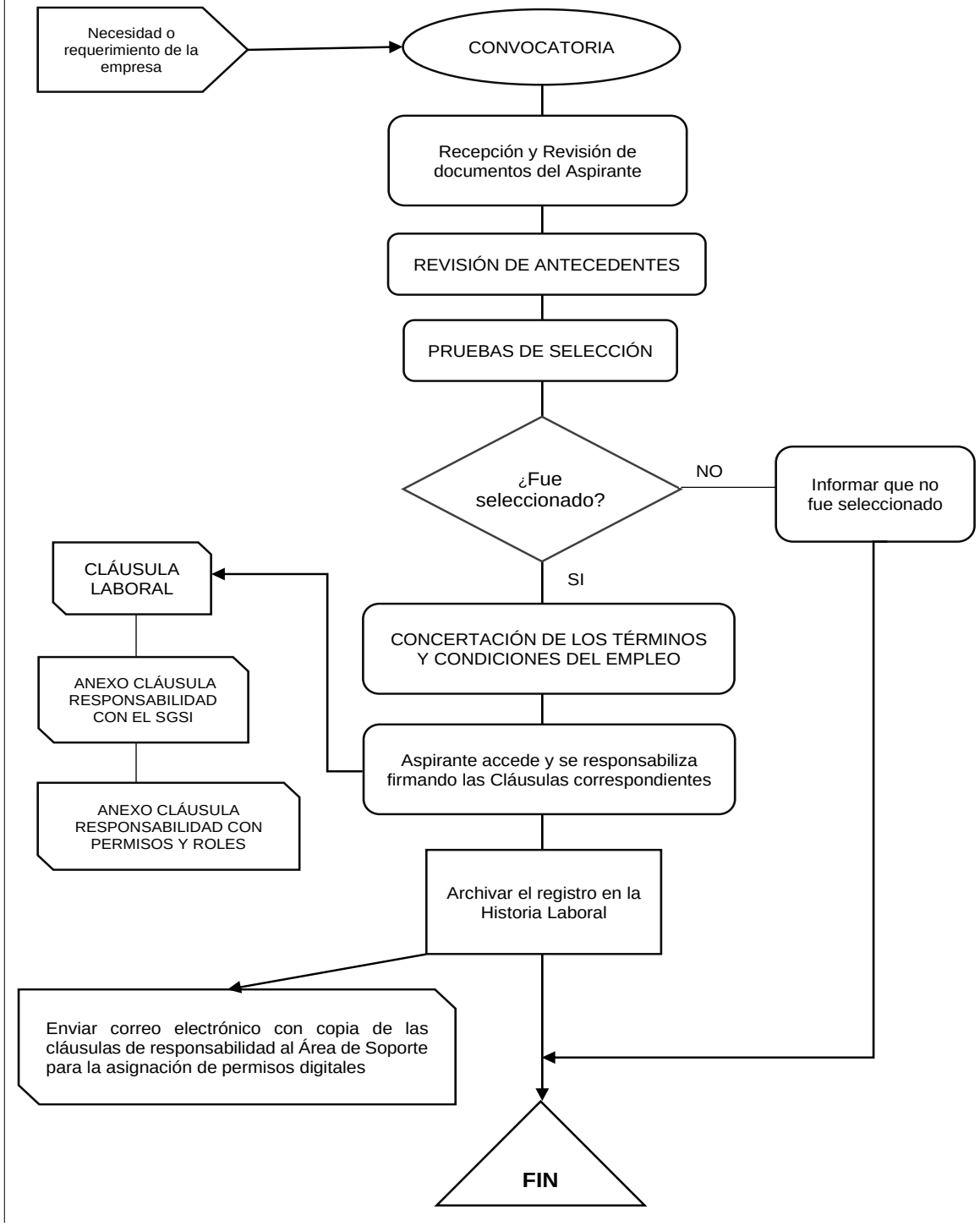
REVISIÓN DE ROLES Y RESPONSABILIDADES



PROCEDIMIENTO DOCUMENTADO

GRUPO DE RECURSOS HUMANOS

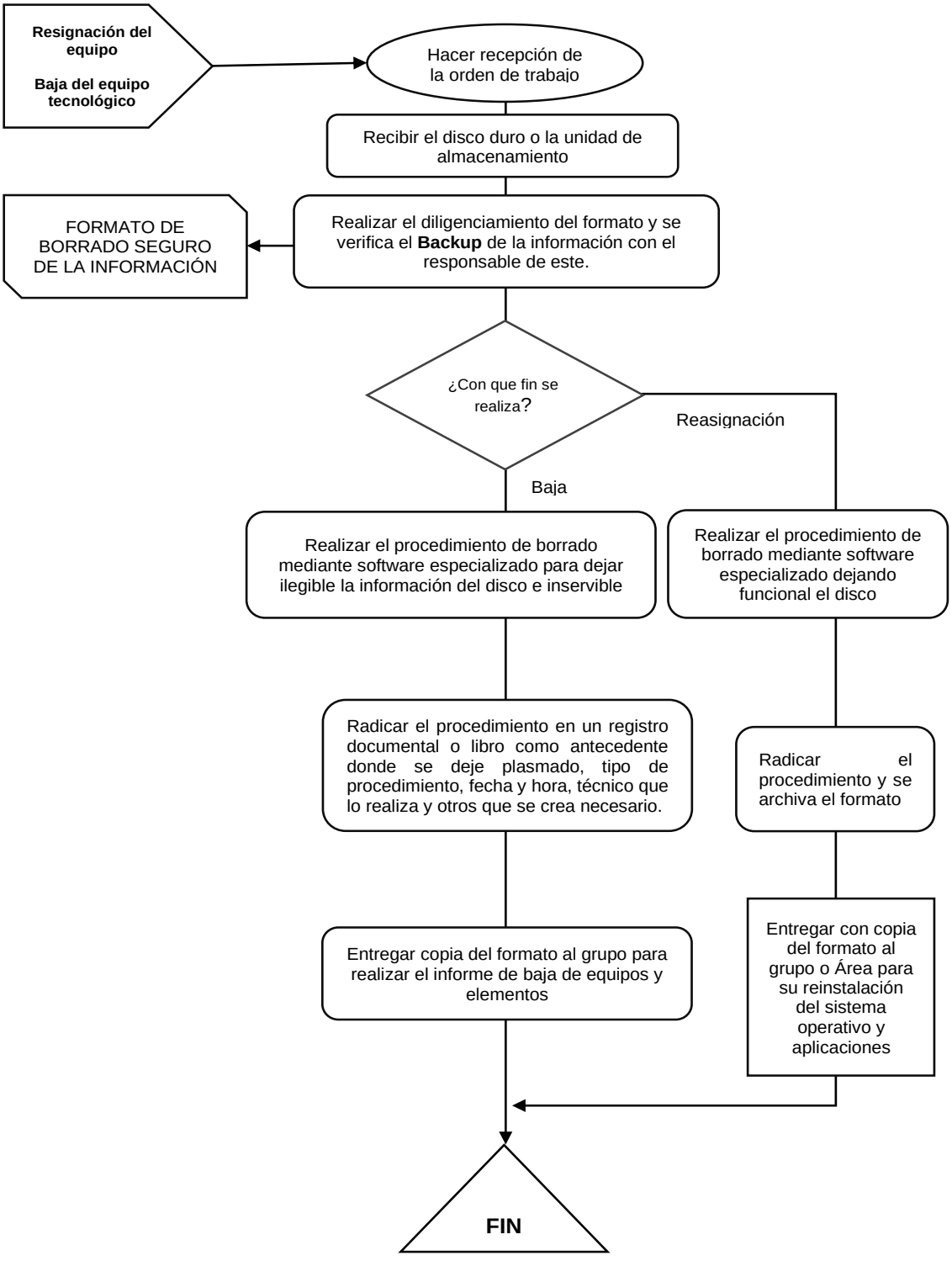
SELECCIÓN, TÉRMINOS Y CONDICIONES PARA EL EMPLEO



PROCEDIMIENTO DOCUMENTADO

ÁREA DE SOPORTE

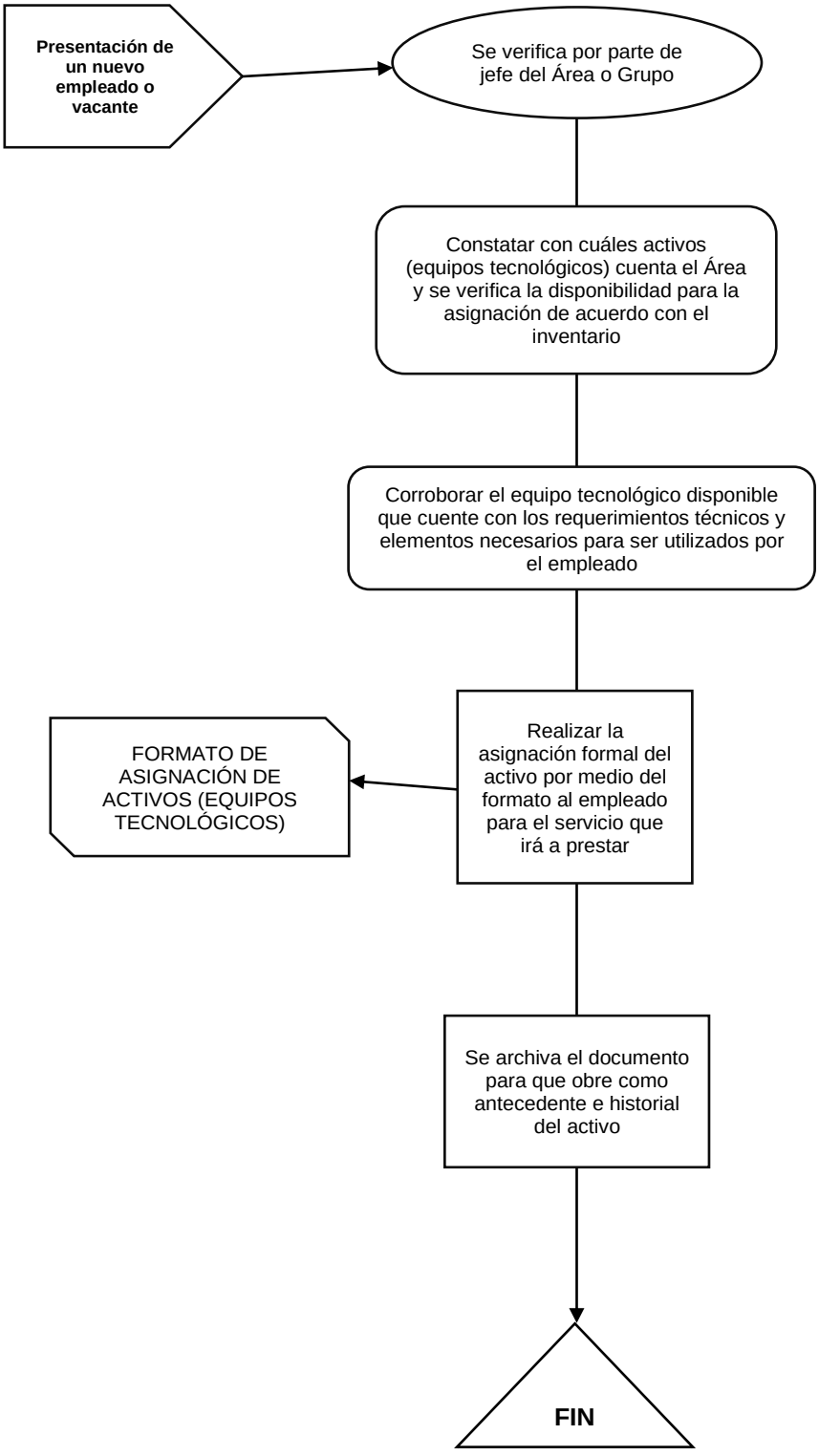
BORRADO SEGURO DE LA INFORMACIÓN - DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS



PROCEDIMIENTO DOCUMENTADO

ÁREA DE SOPORTE

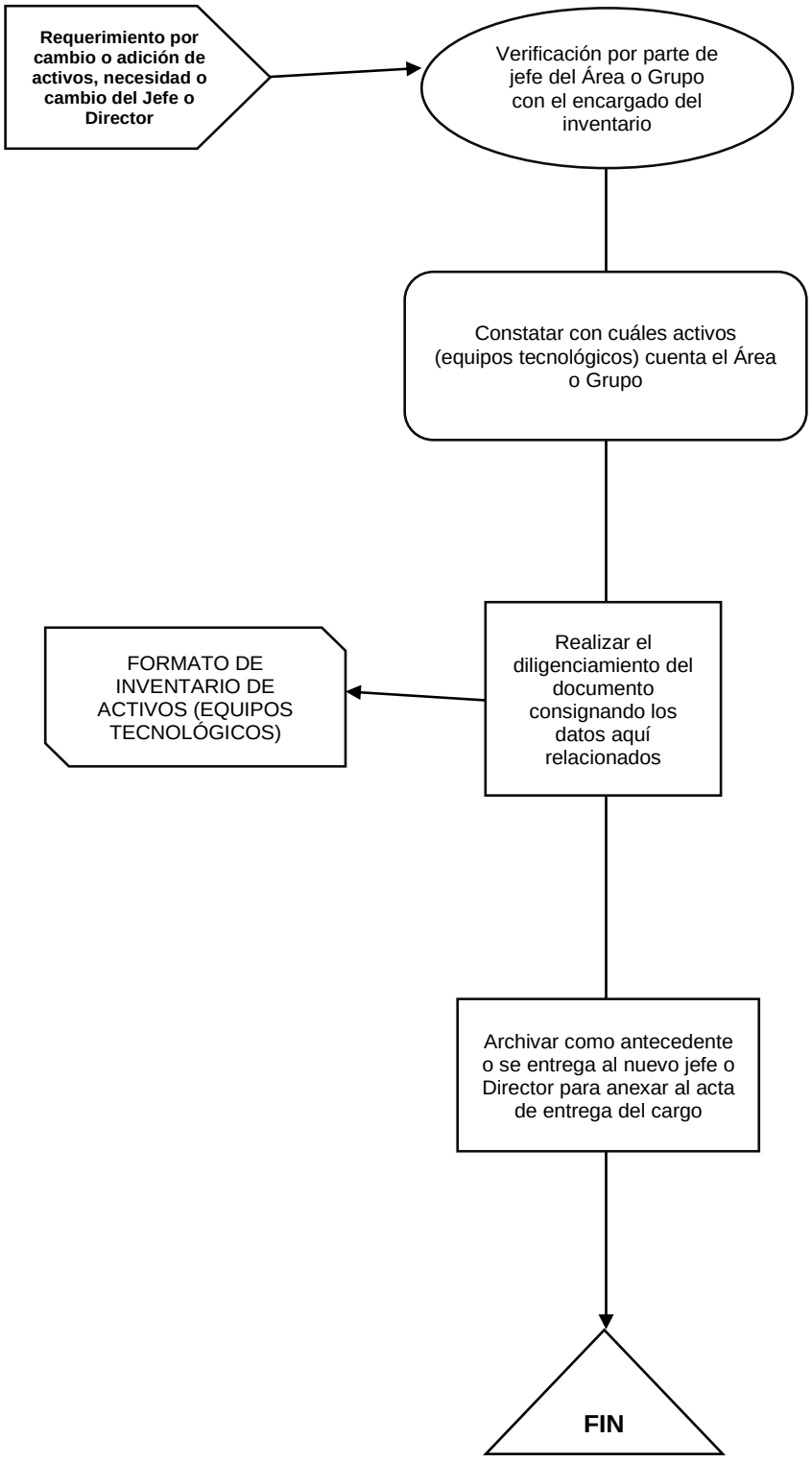
ASIGNACIÓN DE ACTIVOS



PROCEDIMIENTO DOCUMENTADO

EMPRESA QWERTY S.A

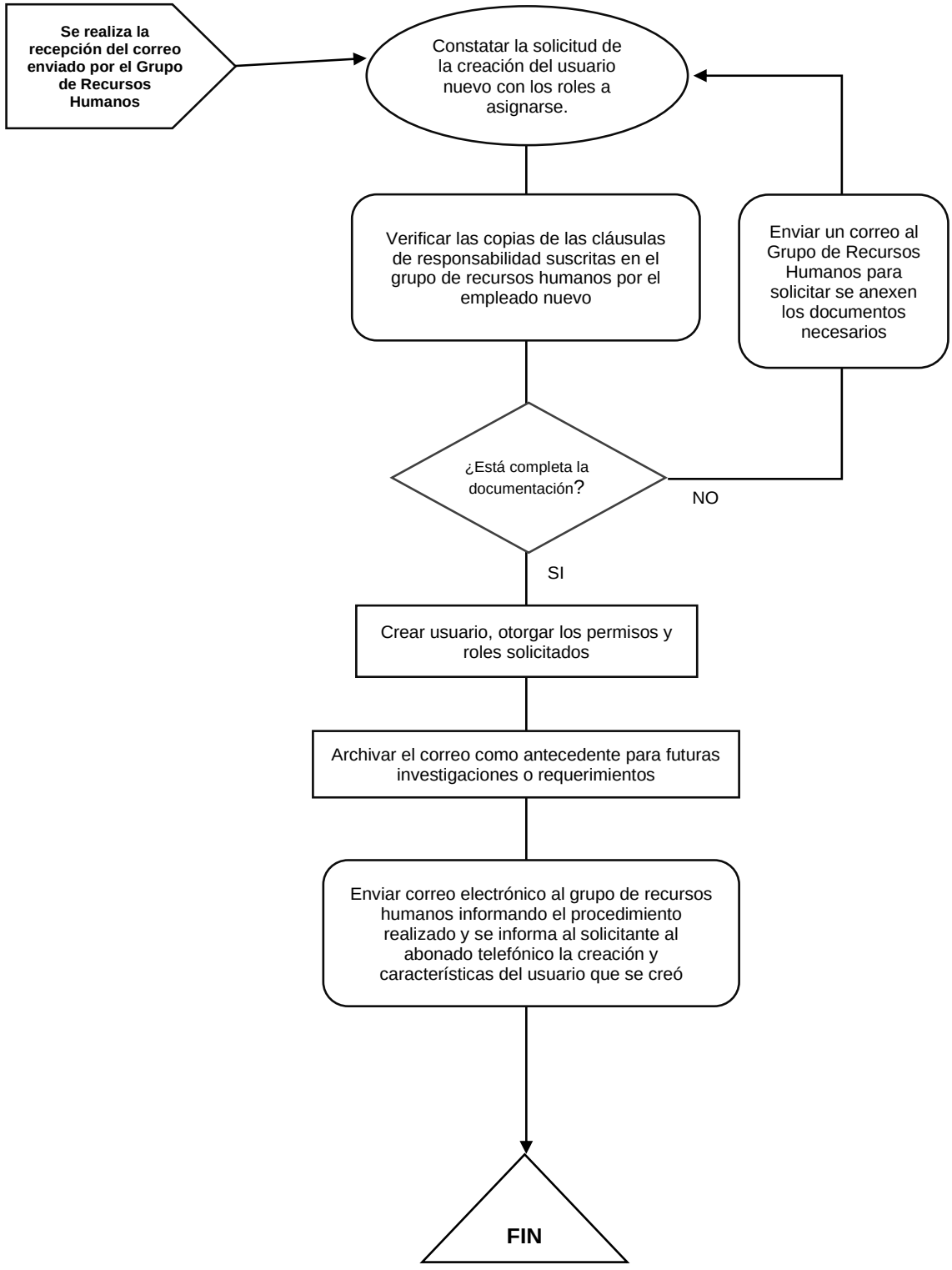
INVENTARIO DE ACTIVOS



PROCEDIMIENTO DOCUMENTADO

ÁREA DE INFRAESTRUCTURA

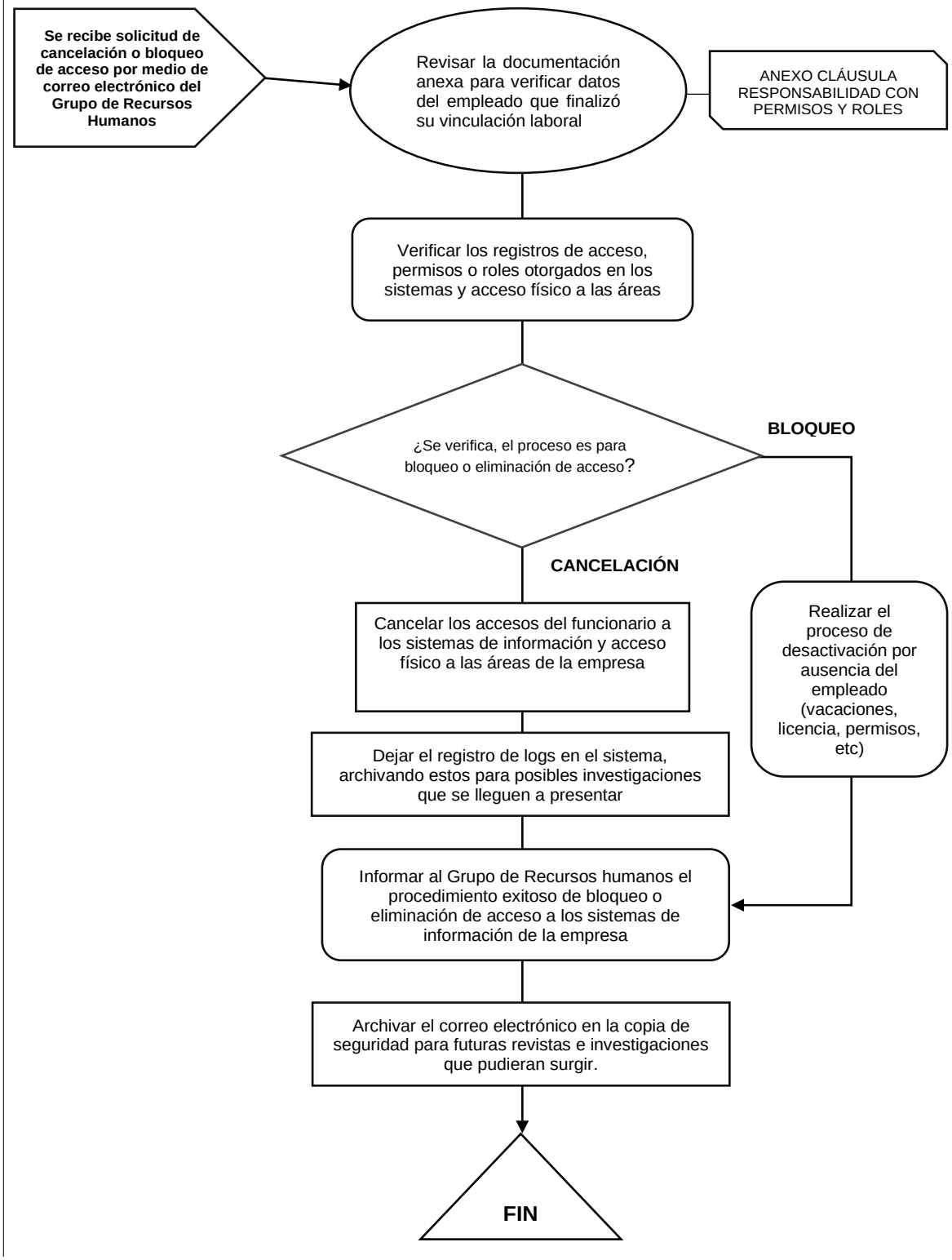
CONTROL DE ACCESO Y CREACIÓN DE USUARIOS



PROCEDIMIENTO DOCUMENTADO

ÁREA DE INFRAESTRUCTURA

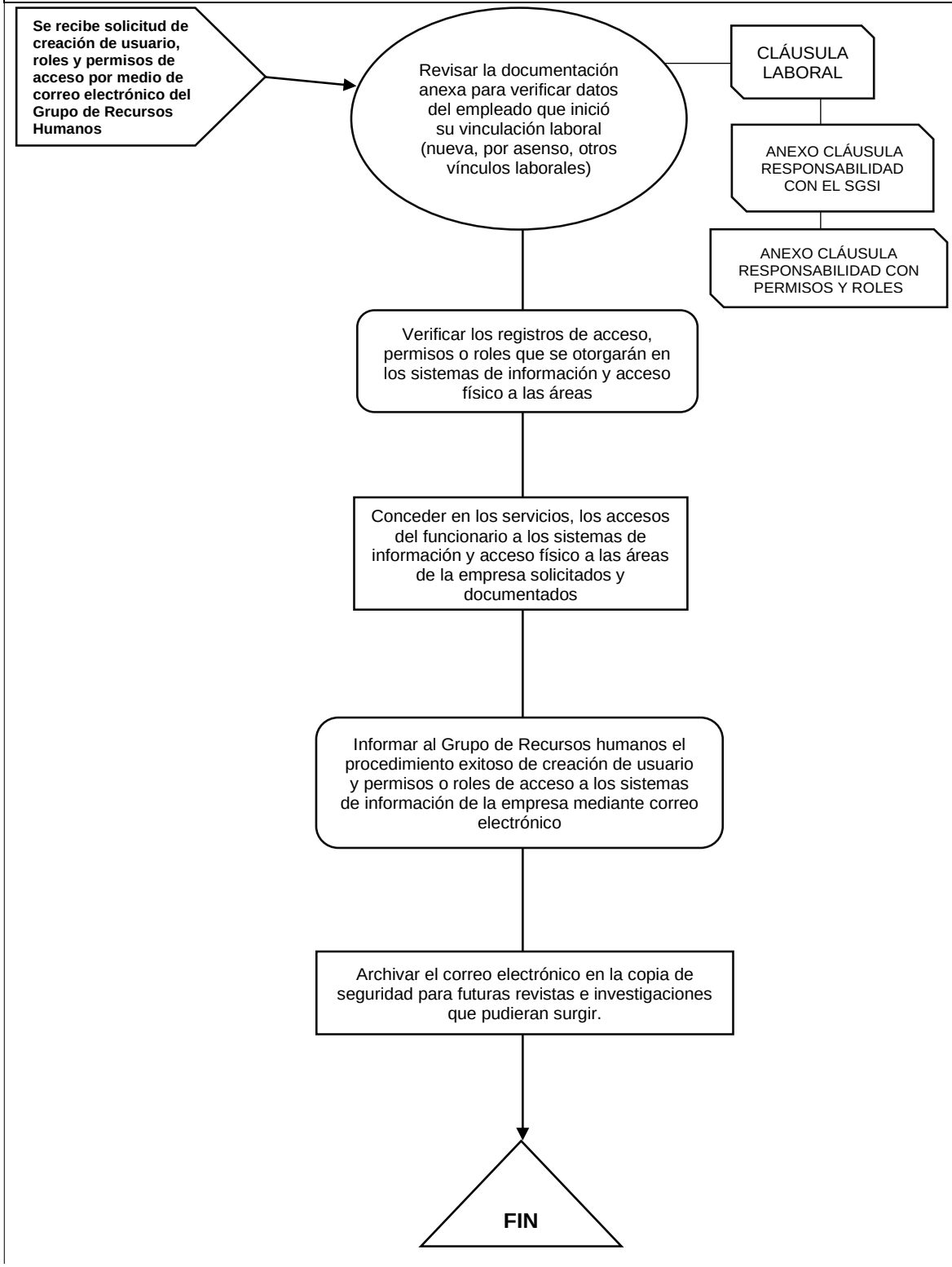
REGISTRO Y CANCELACIÓN DE ACCESO



PROCEDIMIENTO DOCUMENTADO

ÁREA DE INFRAESTRUCTURA

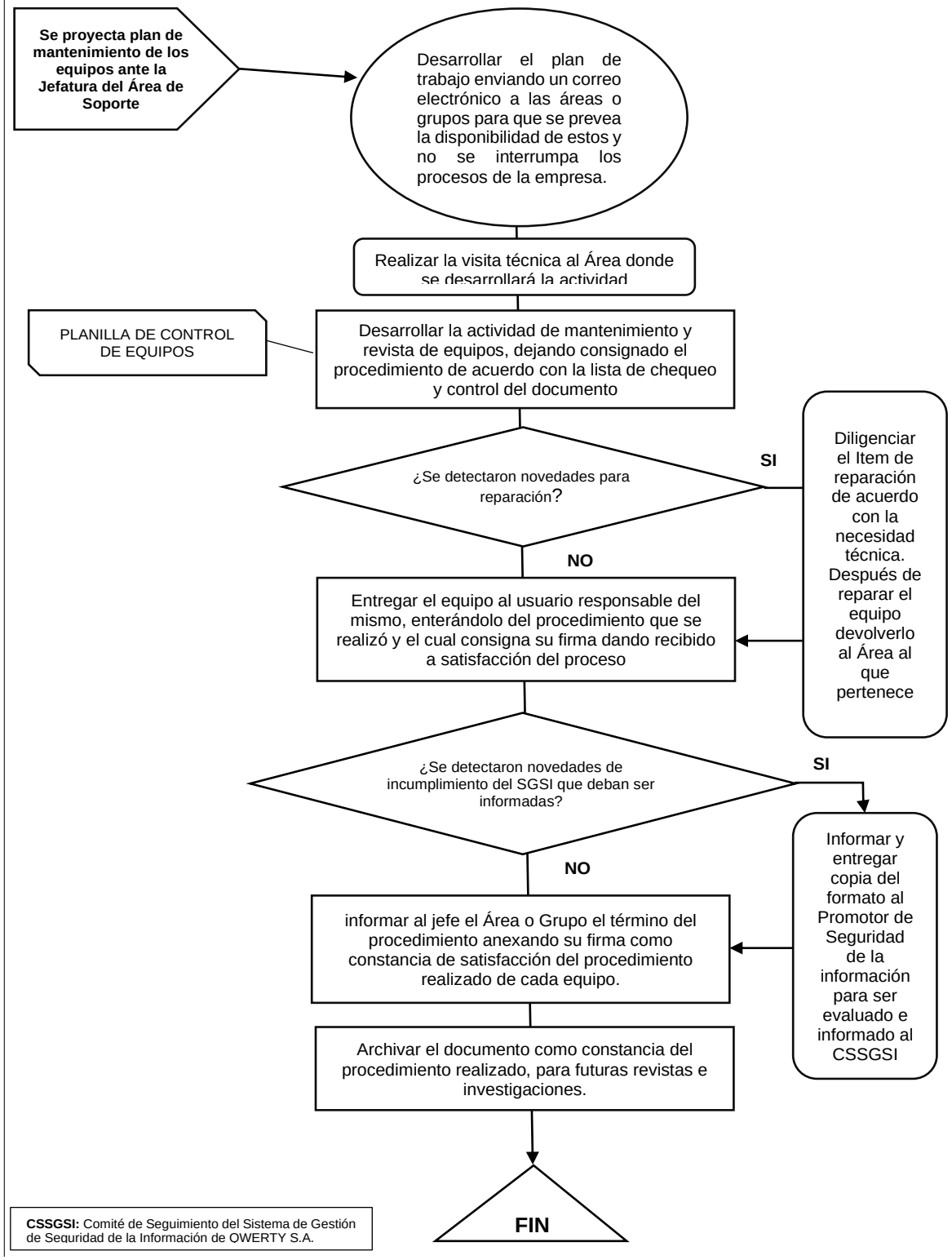
CONTROL DE ACCESO A SISTEMAS Y APLICACIONES



PROCEDIMIENTO DOCUMENTADO

ÁREA DE INFRAESTRUCTURA

MANTENIMIENTO Y REVISTA DE EQUIPOS

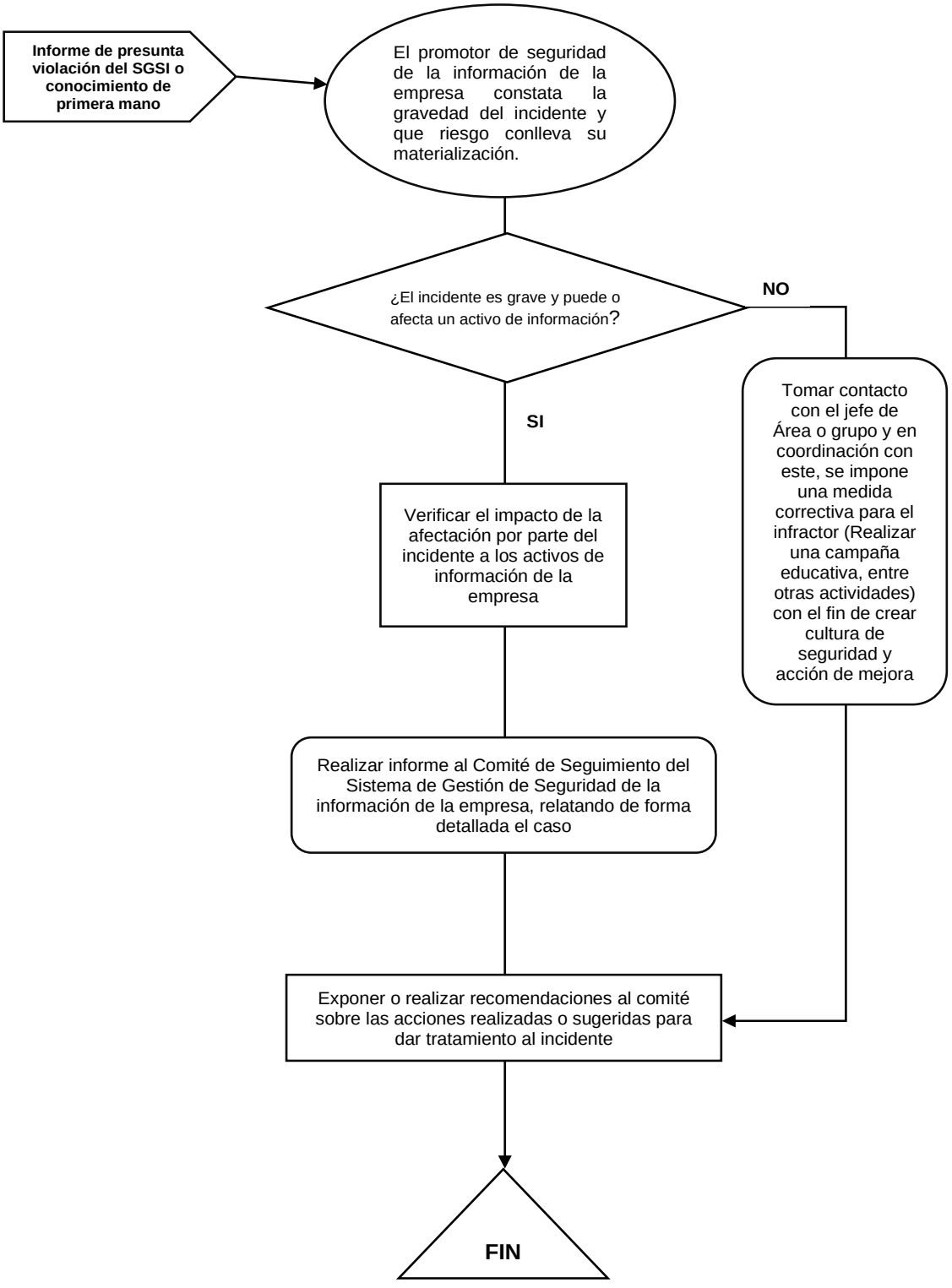


CSSGSI: Comité de Seguimiento del Sistema de Gestión de Seguridad de la Información de QWERTY S.A.

PROCEDIMIENTO DOCUMENTADO

EMPRESA QWERTY S.A.

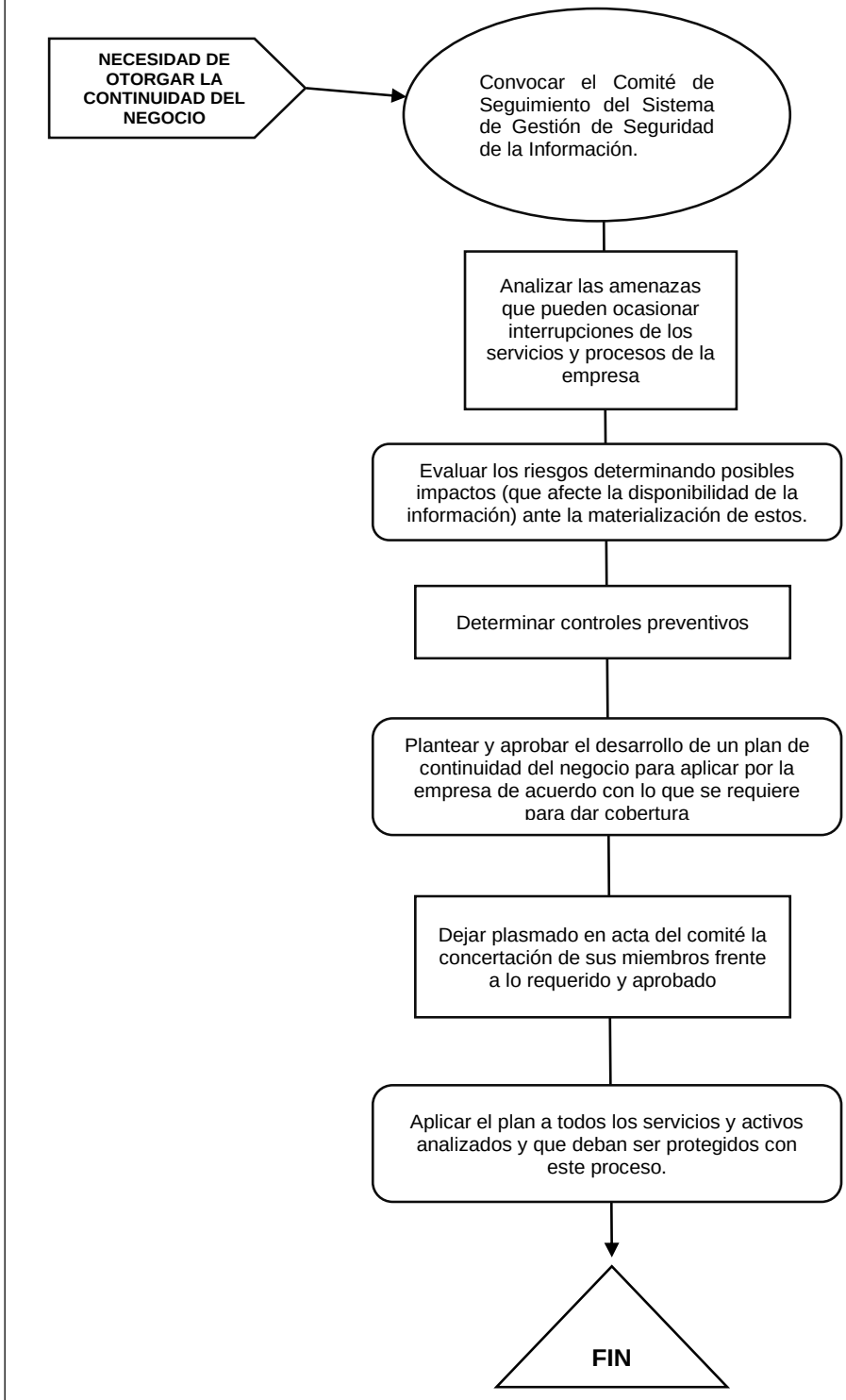
REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN



PROCEDIMIENTO DOCUMENTADO

ÁREA DE SOPORTE

DISPONIBILIDAD DE INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN



Anexo G. Formatos Y Formularios

ANEXO A LA CLAUSULA LABORAL AVALADO MEDIANTE ACTA No. XXXX - XX/XX/2020 DEL CSSGSI PARA LA EMPRESA QWERTY S.A.

CLAUSULA DE RESPONSABILIDAD CON EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFOMACIÓN DE QWERTY S.A.

El empleado suscribe de manera voluntaria absoluta reserva profesional sobre cualquier información que llegase a conocer, manipular o procesar de propiedad de QWERTY S.A, comprometiendose además de cumplir con sus actividades de carácter laboral para las cuales fue contratado en el marco de la normatividad vigente, a cumplir y hacer cumplir las políticas del sistema de gestion de seguridad de la información de QWERTY S.A sujetas al manual del sistema, y adicionalmente se compromete a cumplir las siguientes responsabilidades avaladas por el CSSGSI de QWERTY S.A así:

1. Observaré el cumplimiento de cada una de las políticas suscritas en el manual del sistema de gestion de seguridad de la información de QWERTY S.A
2. Me comprometo a Informar cualquier novedad ocurrida con los activos de información de la empresa.
3. Me comprometo a no conectar equipos tecnológicos no empresariales a las redes de éste, sin previa autorización.
4. Me comprometo a no ingresar o autorizar el ingreso de personas ajenas o sin autorización a áreas restringidas y /o lugrares donde se procesa información sensible
5. Me comprometo a actar las normas de seguridad industrial evitando vender, comer o beber cualquier tipo de alimentos cerca a los equipos tecnloógicos.
6. Cumpliré en todo momento con las medidas apropiadas para la protección y conservación de la información y/o activos de información de la empresa.
7. Cumpliré con las medidas para el almacenamiento seguro de información impresa, la cual debe permanecer con llave al terminar la jornada laboral o cuano no requiera su uso con el fin de asegurar su protección.
8. Evitaré el uso de la red de datos de la empresa para crear, manipular o replicar material comercial, publicitario o mensajes que puedan poner en velo la reputación de la empresa o sus empleados.
9. Cuando por necesidades del servicio que presta la empresa, deba realizar otras labores de apoyo en cumplimiento de la misionalidad de esta, accederé a la información de otras áreas o grupos siempre observando y cumpliendo el deber de reserva y confidencialidad de la misma, evitando la mala manipulación u otras acciones que puedan poner en peligro la integridad y disponibilidad de esta.
10. Protejeré siempre la reputación de la empresa y sus empleados dentro y fuera de la plataforma tecnológica de la organización.
11. Haré un buen y adecuado uso de los recursos y activos de informacion de la empresa, solamente para las actividades del servicio y en pro del cumplimiento de la misionalidad de esta.
12. Haré un buen y adecuado uso del usuario digital empresarial.
13. No utilizaré los equipos de computo para almacenar archivos o datos que no tengan que ver con la empresa o sus actividades misionales como videos, musica, etc.
14. Haré uso exclusivo de los equipos tecnológicos que me sean asignados y me responsabilizaré por su protección y cuidado, informando cualquier novedad con los mismos.
15. Acataré los protocolos y controles de acceso fisico a las instalaciones de la empresa mediante la utilización de carné, autenticación biometrica y acompañamiento de personas visitantes.

ADICIONAL A LO ANTERIOR EL EMPLEADO DEBE:

- Memorizar su usuario digital empresarial y su contraseña, cambiando esta última con una periocidad no mayor de 45 dias e implementando caracteres seguros de su elección de mínimo 8 unidades en longitud para estas.
- Cerrar o bloquear el equipo de computo antes de dejarlo solo.
-Tomar las medidas necesarias para que se prevenga que por su intermedio terceros o personas no autorizadas accedan a información de carácter confidencial de la empresa.
- Informar de cualquier novedad administrativa al grupo de recursos humanos para su bloqueo inmediato de acceso del usuario digital a los sistemas de informacion de la empresa.
- Evitar escribir su usuario y contraseña en papeles o cualquier documento donde alguien pueda acceder a estos.
-Extraer por cualquier medio información sensible sin autorización que pueda poner en riesgo la empresa o sus intereses.
- Evitar instalar sotware no autorizado o sin licencia que atente contra la ley de derechos de autor o las políticas de seguridad de la empresa.
- Acatar las instrucciones que le sean notificadas o instruidas por el personal del sistema SGSI frente a la protección de cualqiuier activo de información de la empresa.

De acuedo a lo anterior y en cumplimiento a la normatividad vigente, me comprometo con lo aquí acordado teniendo pleno conocimiento que el incumplimiento acarreará sanciones de tipo penal, disciplinario y administrativo:

Firma del empleado CC. No.	Firma del empleador CC. No.

Firma del Jefe de Recursos Humanos
CC. No.

ANEXO A LA CLAUSULA LABORAL AVALADO MEDIANTE ACTA No. XXXX - XX/XX/2020 DEL CSSGSI PARA LA EMPRESA QWERTY S.A.

CLAUSULA DE RESPONSABILIDAD CON LOS PERMISOS Y ROLES DE ACCESO QUE SE OTORGARÁN AL USUARIO

USUARIO DIGITAL EMPRESARIAL:	SI	NO	**ENROLAMIENTO BIOMETRICO PARA ACCESO A LAS SIGUIENTES ÁREAS:**	
REQUIERE PERMISOS EN APLICACIONES	SI	NO	PORTERIA Y ENTRADA PRINCIPAL	
¿Cuales?			DIRECCION Y SECRETRIA PRIVADA	
			OFICINA DE RECURSOS HUMANOS	
			ÁREA DE INFRAESTRUCTURA	
			ÁREA DE SOPORTE	
			ÁREA DE DESARROLLO	
			SERVIDORES	
			RACK DE REDES DE COMUNICACIONES	

REQUIERE ACCESO A LAS CARPETAS DEL SERVIDOR FTP DEL ÁREA:	
REQUIERE ROLES DE **ADMINISTRACIÓN**:	SI:___ No:____ SISTEMA A ADMINISTRAR:_____

De acuerdo a lo suscrito en la CLAUSULA DE RESPONSABILIDAD CON EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFOMACIÓN DE QWERTY S.A. y las responsabilidades legales a las que hubiere lugar de acuerdo a la normatividad vigente; de las cuales es conciente el empleado aquí firmante, confirmando su compromiso por el cual le serán concedidos los anteriores permisos y roles en los sistemas de información de la empresa, con el único objeto de cumplir con sus labores y actividades para las cuales fue contratado por la empresa y para dar cumplimiento a la misionalidad de la misma así:

En la ciudad de _____, a los _____ del mes de _____ del año _____,

_____ Firma del empleado CC. No.	_____ Firma del empleador CC. No.

_____
Firma del Jefe de Recursos Humanos
CC. No.

FORMATO DE CONTROL Y MANTENIMIENTO DE ACTIVOS (EQUIPOS TECNOLÓGICOS) AVALADO MEDIANTE ACTA No. XXXX - XX/XX/2020 DEL CSSGSI PARA LA EMPRESA QWERTY S.A.

PLANILLA DE CONTROL DE EQUIPOS

FECHA Y HORA:				ÁREA Y GRUPO:				
NOMBRES DEL EMPLEADO RESPONSABLE DEL EQUIPO:								
CÉDULA No.			CARGO:					
NOMBRE DEL TÉCNICO:				MOTIVO:	Revista	Mantenimiento	Reparación	Concepto para dar de baja el equipo

DATOS DEL EQUIPO

TIPO DE EQUIPO:	Servidor	Computador	Otro:		MARCA:		NOMBRE EN DOMINIO:	
SERIAL:		DISCO DURO:		PROCESADOR:		RAM:	IP:	

ACTIVIDADES DE REVISTA

CONTROL	SI	NO	¿CUÁL O POR QUÉ?	ACCIÓN	CONTROL	SI	NO	CUÁL O POR QUÉ	ACCIÓN
Usuario Digital Emp.					En Dominio				
Antivirus Actualizado					Unidad CD				
Periféricos o disp.					Usa Clave				
Paquete Office					Usa Huella				
Lector de Huella					Musica				
Aplicativos					Videos				
Equipo compartido					Juegos				
Equipo en servicio					**Consta de una buena ubicación Física:** SI:___ NO:___ **Requiere reubicación:** SI:___ NO:___				

REVISTA DE REPARACIONES					
Equipo fue reparado	SI:____ NO:____	¿FUE SOLUCIONADO EL PROBLEMA?:	SI:_____ NO:_____	SE INFORMÓ SOBRE EL ESTADO:	SI:_____ NO:_____
OBSERVACIONES:					

ACTIVIDAD DE MANTENIMIENTO Y REPARACIÓN

LIMPIEZA:	SI	NO	REVISIÓN TECNICA INTERNA	SI	NO	REVISIÓN DE ACTUALIZACIONES DEL SOFTWARE:		SI:_____	NO:_____
MATENIMIENTO TRIMESTRAL DEL:			Primer Trimestre	Segundo Trimestre		Tercer Trimestre		Cuarto Trimestre	
REQUIERE REPARACIÓN:	SI:_____	NO:_____	¿CUÁL?:						
REQUIERE ADQUISICIÓN DE PARTES O COMPONENTES ELECTRÓNICOS:				SI:___	NO:___	¿CUÁL?:			
EL DAÑO FUE CAUSADO POR EL EMPLEADO:			SI:_____	NO:_____		FECHA POSIBLE DE ENTREGA DEL EQUIPO (SI DEBE SER REPARADO):			
SE REPARÓ EL EQUIPO									
OBSERVACIONES:									

DAR DE BAJA EQUIPOS TECNOLÓGICOS

SE REALIZÓ **BACKUP** DE LA INFORMACIÓN: **SI:____ NO:____ NO APLICA:____**					SE REALIZÓ BORRADO SEGURO DEL DISCO DURO:			SI:____ NO:____ NO APLICA:____	
CONDICIÓN DEL ACTIVO A CONCEPTUAR POR:									
INSERVIBLE	OBSOLESCENCIA	HURTO	AVERÍA	REPARACIÓN ANTIECONÓMICA	ROTURA	SINIESTRO	MERMA	DESUSO	CASO FORTUITO
EL CUAL FUE DISPUESTO A REVISIÓN TÉCNICA DE FUNCIONAMIENTO Y SE CONSIDERA COMO **NO APTO** PARA EL SERVICIO POR LOS SIGUINTES MOTIVOS:									
Se conceptua para darsele disposición final adecauda de acuedo a la normatividad vigente ante:									

_____	_____	_____
FIRMA DE TÉNICO	FIRMA DEL JEFE DE ÁREA	FIRMA DEL EMPLEADO O RESPONSABLE DEL EQUIPO
CC. No.	CC. No.	CC. No.

FORMATO DE CERTIFICACIÓN DE BORRADO SEGURO DE INFORMACIÓN AVALADO MEDIANTE ACTA No. XXXX - XX/XX/2020 DEL CSSGSI PARA LA EMPRESA QWERTY S.A.

FORMATO DE BORRADO SEGURO DE LA INFORMACIÓN

FECHA Y HORA:				ÁREA Y GRUPO:			
NOMBRES DEL EMPLEADO RESPONSABLE DEL EQUIPO:							
CÉDULA No.			CARGO:				
NOMBRE DEL TÉCNICO:				MOTIVO DEL BORRADO:	REASIGNACIÓN	BAJA DEL EQUIPO TECNOLÓGICO	
DATOS DEL EQUIPO							
TIPO DE EQUIPO:	Servidor	Computador	Otro:	MARCA:		NOMBRE EN DOMINIO:	
SERIAL:		DISCO DURO:		NUMERO DE SERIE DISCO:		RADICADO DEL PROCEDIMIENTO:	
SE REALIZÓ BACK UP DE LA INFORMACIÓN:		SI:_____ NO:_____		PERSONA QUE REALIZA EL BACK UP:			
UBICACIÓN DEL BACK UP:				FIRMA Y CEDULA DE QUIEN REALIZA BACK UP:	_____ CC. No.		

Observaciones del procedimiento de borrado seguro:

DE ACUERDO A LO ANTERIOR, SE CERTIFICA QUE EL TÉCNICO FIRMANTE, BAJO SUPERVISIÓN DE SU PROCEDIMIENTO REALIZÓ BORRADO SEGURO DE LA INFORMACIÓN CONTENIDA EN EL DISCO DURO DE LAS CARACTERÍSTICAS AQUÍ CONSIGNADAS Y CON SOFTWARE AUTORIZADO POR LA ENTIDAD:

_____ CC.No._____ TÉCNICO ASIGNADO PARA EL BORRADO SEGURO	_____ CC. NO._____- JEFE DE ÁREA DE SOPORTE O DELEGADO

FORMATO DE ASIGNACIÓN DE ACTIVOS (EQUIPOS TECNOLÓGICOS) AVALADO MEDIANTE ACTA No. XXXX - XX/XX/2020 DEL CSSGSI PARA LA EMPRESA QWERTY S.A.

FORMATO DE ASIGNACIÓN DE ACTIVOS (EQUIPOS TECNOLÓGICOS)

FECHA Y HORA:				ÁREA Y GRUPO:						
NOMBRES DEL EMPLEADO QUIEN RECIBE EL ACTIVO:										
CÉDULA No.			CARGO:							
DATOS DEL EQUIPO										
TIPO DE EQUIPO:	Servidor	Computador	Otro:			MARCA:			NOMBRE EN DOMINIO:	
SERIAL:			DISCO DURO:		PROCESADOR:		RAM:		IP:	
ACCESORIOS										

En cumplimiento a la normatividad vigente, el manual de seguridad de la información y las políticas del sistema de gestion de a la información de QWERTY S.A, adicional al cumplimiento de las: CLÁUSULA DE RESPONSABILIDAD CON EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFOMACIÓN DE QWERTY S.A. y CLÁUSULA DE RESPONSABILIDAD CON LOS PERMISOS Y ROLES DE ACCESO QUE SE OTORGARÁN AL USUARIO, se asigna el activo (equipo tecnológico) al empleado firmante de este documento, quién se hará responsable de su protección y buen uso, entendiendo las responsabilidades penales, disciplinarias y administrativas que causan el daño, mal uso o perdida del elemento bajo su responsabilidad, así:

_____	_____
CC.No._____	CC. NO._____
RESPONSABLE DEL ACTIVO	JEFE DE ÁREA O DELEGADO QUIEN HACE LA ENTREGA

FORMATO DE INVENTARIO DE ACTIVOS (EQUIPOS TECNOLÓGICOS) AVALADO MEDIANTE ACTA No. XXXX - XX/XX/2020 DEL CSSGSI PARA LA EMPRESA QWERTY S.A.

FORMATO DE INVENTARIO DE ACTIVOS (EQUIPOS TECNOLÓGICOS)

FECHA Y HORA:		ÁREA Y GRUPO:		
NOMBRES DEL EMPLEADO QUE REALIZA EL INVENTARIO:				
CÉDULA No.		CARGO:		
MOTIVO:	ACTIALIZACIÓN	REVISTA	ADICCIÓN	CAMBIO DE JEFE DE ÁREA O DIRECTOR

DATOS

TIPO DE ACTIVO	NUMERO DE SERIE	MARCA	ESTADO	VALOR DEL ACTIVO

_____	_____
CC.No._____	CC. NO._____
RESPONSABLE DEL INVENTARIO	JEFE DE ÁREA RESPONSABLE O QUIEN RECIBE EL INVENTARIO DE ACTIVOS

FORMATO DE LISTA DE CHEQUEO RESPONSABILIDADES CON EL SGSI AVALADO MEDIANTE ACTA No. XXXX - XX/XX/2020 DEL CSSGSI DE LA EMPRESA QWERTY S.A.

LISTA DE CHEQUEO

RESPONSABILIDADES CON LA SEGURIDAD DE LA INFORMACIÓN

Fecha: DD_____/ MM_____/ AA_____ ÁREA O GRUPO: _____

Nombre del Jefe de Área: _____ C.C.No.: _____

Promotor del SGSI: _____ C.C.No.: _____

No	CONTROLES DE SEGURIDAD DE LA INFORMACIÓN	¿CUMPLE?	
1	Instalación y utilización de software licenciado y autorizado por el Área de Soporte de la empresa.	SI	NO
2	Utilización de dispositivos de almacenamiento masivo autorizados por el Jefe de Área o Promotor de Seguridad de la información.	SI	NO
3	Conexión y utilización de cualquier equipo tecnológico no empresariales a la red de datos de la Empresa, con autorización del Jefe de Área o Promotor de Seguridad del SGSI.	SI	NO
4	Uso adecuado de los usuarios digitales empresariales	SI	NO
5	Apagado de los equipos de cómputo asignados, en horas no laborales.	SI	NO
6	El Almacenamiento de información en los equipos de cómputo empresariales se encuentra respaldada en el servidor FTP.	SI	NO
7	Acceso a carpetas o información de otras áreas o grupos con autorización del Jefe de Área o Grupo.	SI	NO
8	Se evita la difusión de material comercial y mensajes masivos que puedan interrumpir los procesos de la empresa o atentar contra la imagen de la empresa o sus empleados.	SI	NO
9	Autorización de ingreso de personas a las áreas restringidas o donde se procese información sensible de la empresa con previa autorización y registro del acceso.	SI	NO
10	Protección bajo llave de documentos impresos con información empresarial, al terminar la jornada laboral o cuando se ausente el funcionario de su puesto.	SI	NO
11	Se cumple las normas de seguridad industrial absteniéndose de comer, beber o comercializar cualquier tipo de alimentos cerca a los equipos tecnológicos empresariales.	SI	NO
12	Se otorga el acceso a los activos de información a empleados o personas previamente autorizadas por el Promotor de seguridad de la información o Jefe de Área.	SI	NO
13	Realización de cambios en la Plataforma Tecnológica de la Empresa, con autorización de la Oficina de sistemas.	SI	NO
14	Cuidado de elementos o equipos tecnológicos, entregados para actividades propias de la empresa y están plenamente asignados mediante formatos al personal.	SI	NO
15	Se viene recomendando y estableciendo al personal de empleados, el cierre o bloqueo de sesión ante ausencias en su puesto de trabajo.	SI	NO
16	Los equipos empresariales se encuentran con reserva en el dominio de la empresa	SI	NO
17	Se utilizan los roles como administrador, únicamente para actividades propias de la empresa.	SI	NO
18	Los equipos tecnológicos tienen instalado software actualizado y con la seguridad necesaria para proteger la información contenida dentro de los mismos.	SI	NO
19	Se firmaron las correspondientes cláusulas de responsabilidad necesarias para el cumplimiento de la política de seguridad de la información de la Empresa antes de tener cualquier tipo de acceso a los sistemas de información de la empresa.	SI	NO
20	Se reportan de novedades laborales como licencias, vacaciones, excusas, terminación de contrato, entre otras, ante el grupo de recursos humanos o correspondiente área para el bloqueo inmediato del usuario al acceso de los sistemas de información de la empresa.	SI	NO
21	Se solicita la realización de borrado seguro para reasignar o baja de un equipo tecnológico asignado al área o grupo.	SI	NO
22	Se utiliza la infraestructura tecnológica de la empresa, únicamente para realizar actividades laborales o relacionados con esta.	SI	NO
23	Se cuenta con controles de acceso físico a las áreas a través de validación biométrica, carné y acompañamiento de personas ajenas a la empresa (previamente autorizadas)	SI	NO

FORMATO DE LISTA DE CHEQUEO RESPONSABILIDADES CON EL SGSI AVALADO MEDIANTE ACTA No. XXXX - XX/XX/2020 DEL CSSGSI DE LA EMPRESA QWERTY S.A.

LISTA DE CHEQUEO

RESPONSABILIDADES CON LA SEGURIDAD DE LA INFORMACIÓN

No	CONTROLES DE SEGURIDAD DE LA INFORMACIÓN	¿CUMPLE?	
24	El personal conoce y aplica las recomendaciones de emplear contraseñas seguras en los usuarios digitales empresariales.	SI	NO
25	Se cumple con otros protocolos establecidos por la empresa para la seguridad del área.	SI	NO

Este documento obra como instrumento de evaluación de las responsabilidades con el Sistema de Gestión de Seguridad de la Información y las políticas de seguridad empresariales deben ser aplicadas en cada una de las áreas de la empresa QWERTY S.A, por tanto, ante este se suscribe que la información contenida en este es verídica y será mostrará ante el Comité de Seguimiento del SGSI para su correspondiente evaluación y acciones correspondientes,

Promotor del Seguridad de la Información
C.C. No.

Jefe del Área o Grupo
C.C.No.

Anexo H. Difusión en la empresa QWERTY S.A.