DISEÑO DE UN SISTEMA INTEGRADO DE GESTION DE SEGURIDAD DE LA INFORMACION PARA LA EMPRESA QWERTY S.A

Ing. CARLOS ANDRES UBAQUE MAHECHA

Ing. GILBERTO ALEXIS MONTOYA TELLEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA –UNAD
VICERRECTORÍA ACADÉMICA Y DE INVESTIGACIÓN - VIACI
CIENCIAS BASICAS TECNOLOGIA E INGENIERIA BOGOTA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTA
2019

DISEÑO DE UN SISTEMA INTEGRADO DE GESTION DE SEGURIDAD DE LA INFORMACION PARA LA EMPRESA CASO ESTUDIO QWERTY S.A.

Ingeniero CARLOS ANDRES UBAQUE MAHECHA

Ingeniero GILBERTO ALEXIS MONTOYA TELLEZ

Proyecto de grado para optar por el título de Especialista en Seguridad Informática

Director de Proyecto, Ing. Edgar Mauricio López Rojas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA –UNAD
VICERRECTORÍA ACADÉMICA Y DE INVESTIGACIÓN - VIACI
CIENCIAS BASICAS TECNOLOGIA E INGENIERIA BOGOTA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTA
2019

Nota de aceptación:

_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

DEDICATORIA

Este trabajo está dedicado a la familia quienes durante todos estos años de profesionalismo han estado pendiente del crecimiento personal y profesional. A los amigos, a Dios por permitirnos llegar alcanzar esta meta que es un escalón más en nuestras carreras profesionales.

AGRADECIMIENTOS

Agradecemos a los tutores de la universidad nacional abierta y a distancia UNAD por compartir con nosotros los conocimientos y ayudarnos a llegar a un nivel de nuestras carreras mucho más avanzado.

A nuestras familias por el apoyo a este proceso para lograr alcanzar este objetivo.

En general a todos los que estuvieron de alguna manera involucrados en el desarrollo de nuestra especialización.

TABLA DE CONTENIDO

DETALLE DE LAS FIGURAS DEL PROYECTO

DETALLE DE LAS TABLAS DEL PROYECTO

DETALLE DE LOS ANEXOS DEL PROYECTO

GLOSARIO

Activo: Es un bien de la empresa que tiene valor significativo y monetario que presta algún servicio y que genera ganancia.

Amenaza: Es la raíz de una acción que puede ocasionar un incidente a cualquier ítem de configuración (activo) de la empresa y que se puede materializar.

Análisis: Experiencia que se aporta en el proceso de búsqueda de riesgos en una organización.

Campañas: Reunión de personal de una empresa para dar a conocer información y realizar ejercicios de aprendizaje de aplicación de las políticas de la empresa.

Confidencialidad: Dimensión de la información la cual asegura que sea accesible por los usuarios autorizados de la empresa.

CONTROL: Salvaguarda para reducir la degradación de un activo ante un eventual riesgo, con la implementación de políticas, procesos, procedimientos, manuales e instructivos de carácter administrativo, técnico, de gestión o legal.

Disponibilidad: Dimensión del activo de una empresa que asegura que la información esté utilizable para ser accedida.

Empresa: Organización dedicada a construir los productos y entregarlos a sus clientes para darle solución a sus problemas y necesidades empresariales.

Ethical Hacking: Proceso de penetración hacía los diferentes sistemas en busca de vulnerabilidades que puedan ser explotadas por diferentes metodologías y técnicas conocidas.

Hardening: Proceso que se realiza a los sistemas operativos para cerrar puertos TCP/UDP que no son necesarios y cerrar accesos de usuarios por defecto.

Honeynet: Es una red compuesta por varios servidores de diferentes sistemas operativos el cual contienen información de señuelo para los hackers.

Honeypots: Dispositivo para atraer al atacante hacía un objetivo que sirve como anzuelo y hacer parecer al atacante que ha ganado acceso.

Infraestructura: Son recursos técnicos utilizados por la organización para desempeñar las labores de la empresa ya sea a nivel tecnológico, edificación o laboral.

Integridad: Dimensión de la información la cual garantiza que la información se mantiene completa sin modificaciones.

Inventario: Relación de activos que tiene la empresa la cual tiene un valor monetario o informático para la empresa.

ISO 27001: Normas para una buena gestión de la información que permite asegurarla y resguardarla para una mayor seguridad.

MAGERIT: Es una metodología para análisis de riesgos de una empresa la cual cuenta con la aplicación de las mejores prácticas de los estándares de seguridad de la información a nivel internacional.

Políticas: Conjunto de reglas aprobadas por la empresa para ser aplicadas y acatadas por los usuarios para mantener una regulación en los procesos diarios.

Procesos: Es una secuencia de pasos a seguir para iniciar una tarea y terminarla con los resultados esperados.

Riesgo: Posibilidad de que una amenaza se vuelva tangible o se haga real ya sea en un activo o en una empresa.

Seguridad de la información: Aseguramiento de los diversos activos (tangibles e intangibles) y de la información a por medio de salvaguardas que permiten mantener la información asegurada y resguardada.

SIGSI: Es el sistema de gestión de seguridad de la información que contiene los lineamientos de la empresa y los procesos que aplican basados en las normas internacionales. Para la empresa QWERTY este sistema se llamará **SIGSI.**

SLA (SERVICE LEVEL AGREEMENT): Por sus siglas en inglés es un acuerdo entre la empresa y un suscriptor el cual denota un nivel de servicio que un cliente espera de su suscriptor.

Software: Programa que realiza unas tareas específicas en la empresa y arroja resultados esperados.

Usuario: Persona que es parte de QWERTY y desempeña una tarea específica el cual tiene asignado un medio informático para su trabajo.

Vulnerabilidad: Es una falencia de un sistema el cual puede ser explotada por una amenaza.

RESUMEN

Sin lugar a dudas el activo más importante para una empresa es la información. En los últimos tiempos esta visión se ha ampliado dando una cobertura global, no solo a la información en sí misma, sino a todos los procesos que acompañan el tratamiento de dicha información a través de los sistemas actuales que están bajo las normas vigentes. La empresa QWERTY S.A. no posee dicho sistema, siendo vulnerable a diferentes ataques que se ven a diario en el mundo informático. Por esto se quiere “diseñar” un sistema de seguridad de la información que cumpla con las expectativas y se acomode al presupuesto de la empresa, con los objetivos de control referenciados en las normativas ISO-27001, y la metodología MAGERIT V.3.

Este sistema de seguridad se quiere diseñar e implementar para prevenir los delitos informáticos establecidos en la legislación colombiana “ley 1273-2009”. Por personajes como Hackers, Crackers o Lammers. Y educar en ingeniería social a los usuarios para que no permitan la perdida de datos indiscriminadamente.

Se requiere establecer una investigación cuantitativa que analice los datos de los CI (*ítems de configuración,* por sus siglas en inglés) actuales de la empresa, los procesos que se llevan a cabo sobre la información y la documentación de dichos procesos, las vulnerabilidades, las amenazas, el impacto de los riesgos a presentar, y el costo de no implementar este SIGSI para la empresa tanto monetariamente como funcionalmente.

A fin de establecer el alcance del sistema, en proporción a las necesidades básicas de seguridad identificadas, los controles que se pueden aplicar y el monitoreo de dichos controles a través del ciclo PHVA propuesto por Edwards Deming.

PALABRAS CLAVES: controls, ISO 27001, Magerit, PHVA, QWERTY S.A., SIGSI.

ABSTRACT

Information is the most precious asset of any company. In recent times, this vision extended to global coverage, to not only the information itself, but also every processes that accompany the treatment of this information through the current systems that are under current regulations. The company QWERTY S.A. does not have such a system, being vulnerable to different attacks what they are daily in the computer world. For this reason, we want to “design” an information security system that meets the expectations and fits the company's budget, with the control objectives referenced in the ISO-27001 regulations, under the COBIT reference framework and methodology MAGERIT V.3.

The security system that we want designed and implemented to prevent cybercrime established in the Colombian legislation "Law 1273-2009". By characters like Hackers, Crackers or Lamer. In addition, user will be educating in social engineering to prevent data lost indiscriminately.

It is necessary to establish a quantitative research, to analyze company’s current IC (configuration items) data. the processes that are carried out on the information and documentation of these processes, vulnerabilities, threats, risk’s impact to be presented, and the cost of not implementing this SIGSI for the company both monetarily and functionally.

In order to establish the scope of the system, in proportion to the basic security needs identified, the controls applied and the monitoring of this controls through the Edwards Deming’s PDCA’s cycle.

KEYWORDS: controls, ISO 27001, Magerit, PHVA, QWERTY S.A., SIGSI.

INTRODUCCIÓN

QWERTY S.A. es una empresa del sector informático, que busca el desarrollo tecnológico en comunidades colombianas a través del uso de las TI (tecnologías de la información), como cualquier empresa se encuentra expuesta a muchas vulnerabilidades y riesgos. Como consecuencia de ello la importancia de implementar un sistema de gestión de la seguridad de la información basado en normas conocidas como la ISO 27001, con el fin de identificar los riesgos y las vulnerabilidades.

Propendiendo el aseguramiento de los activos de la empresa se requiere un levantamiento de información de la situación actual, a través de la implementación metodologías cuantitativas para analizar los datos de los CI actuales de la empresa con sus respectivos procesos. Al fin de buscar una estrategia que permita proteger la información, ya que aparentemente esta no cuenta con los controles necesarios que mitigue los riesgos y vulnerabilidades.

Con la información obtenida se diseñará un sistema integrado de gestión de seguridad de la información (**SIGSI**) que permita gestionar la ciberseguridad a partir de buenas prácticas para el aseguramiento de la información.

1. PLANTEAMIENTO DEL PROBLEMA

Desde la evolución de las computadoras a mitad del siglo XX hasta nuestros días, la información de las empresas se ha convertido en un sin número de bytes en diferentes dispositivos electrónicos, dejando en muchas ocasiones de lado el papel impreso. En la actualidad estos bytes han tenido una organización que permiten accederlos, modificarlos y hasta eliminarlos por medio de estructurados – y en algunas ocasiones no tan seguros – sistemas de información. Por esto es imperativo que dichos sistemas posean una salvaguarda adecuada frente a las posibles intromisiones procedentes de las flaquezas existentes en sus precarios o inexistentes sistemas de seguridad.

La empresa QWERTY S.A. posee estas vulnerabilidades a nivel de infraestructura y políticas de seguridad que ponen en potencial riesgo la información de su empresa. A través de acciones punibles como la suplantación de identidad, el tratamiento de datos sin autorización, el fraude o la disrupción de un sistema informático o la red de comunicaciones. Para revelar estas vulnerabilidades y amenazas existentes en la empresa es necesario iniciar procesos de diagnóstico que permitan identificar el momento actual de la seguridad, teniendo en cuenta la normatividad vigente y los procesos de análisis y la evaluación de riesgos.

Entre los riesgos se tienen en la empresa en relación en su seguridad al no poseer un sistema biométrico o de monitoreo de las aplicaciones. Los riesgos asociados al no contar con locaciones que cumplan condiciones de climatización óptimas. El riesgo de ser atacado por una mala configuración de red, sin configuraciones propias para la autorización o denegación del servicio, el no poseer software actualizado y la no operación por parte del personal idóneo.

En el 2017 las empresas que poseían sistemas de seguridad como “telefónica” se vieron a perdidas por culpa de un ciberataque denominado “Wannacry” quien secuestraba la información de los equipos que infectaba y pedía rescate por ellas, haciendo prácticamente irrecuperable estos archivos si no se tenían copias de seguridad. En más de 10 países, el ataque afectó a más de 40.000 dispositivos ocasionando pérdidas por millones de dólares.

Lo cual llevó en el 2018 a que se incrementara en las empresas en 12% la inversión en seguridad informática siendo la mayor parte del en servicios de seguridad, seguidos por la protección de infraestructura y equipos de seguridad de red.[1]

Por esto cabe preguntarnos si ¿Se está haciendo una buena implementación de políticas de seguridad en la empresa QWERTY S.A.? ¿Se tienen los controles necesarios? ¿Se controlan las fugas de información? ¿los dispositivos que contienen los sistemas de información de la empresa están protegidos contra las amenazas? La mayoría de las respuestas a estas preguntas parecen ser no. Por lo cual se puede definir que en la actualidad la empresa posee unas condiciones precarias en lo referente a seguridad informática.

Las políticas de seguridad actualmente aceptadas por medio de la normatividad estandarizada en la ISO 27001 no se ven aplicadas por ninguna parte en la empresa, por lo que se evidencia que la seguridad informática no es su mayor prioridad, o el desconocimiento de la misma hace que en un mundo en que se visualizan a diario muchos más ataques no sea algo que se deba a tomar a la ligera como se está tomando actualmente en la empresa QWERTY S.A. por lo cual es necesario realizar un plan que permita el diseño del SIGSI en la empresa teniendo en cuenta los objetivos a cumplir en el mismo, el estado actual de los activos para

[1] Manuel Ángel Méndez. El confidencial. Así fue el primer ciberataque masivo que ha paralizado el mundo. https://www.elconfidencial.com/tecnologia/2017-05-13/ransomware-wannacry-ciberataque-hackeo-ciberseguridad-telefonica_1381986/

dimensionar sus vulnerabilidades, y los controles con base a la norma ISO 27001 que se espera se apliquen para realizar vigilancia y control en la reducción de las amenazas y los riesgos en la empresa.

Si estos planes no se cumplen, la empresa corre una alta probabilidad de sufrir riesgos que dejen pérdidas significativas en la misma, tanto a nivel organizacional, de información y monetarios que puedan llevar a una gran pérdida económica y sin exagerar hasta la desaparición de la misma por bancarrota o inoperancia. Así es que la empresa en la actualidad posee un problema que debe solucionarse a través de la implementación de un SIGSI.

2. FORMULACIÓN DEL PROBLEMA

¿Cuál es el grado de seguridad de los sistemas de información de la empresa QWERTY S.A. en relación a las normativas vigentes que permitan el diseño de un sistema de gestión de seguridad de la información en el cual se implementen controlen que ayuden a mitigar los riesgos de fallo en las dimensiones claves de la información?

3. JUSTIFICACIÓN

Diseñar un sistema de gestión de seguridad de la información (SIGSI) en un proceso de hetero-evaluación y autoevaluación que ayudará a resolver el problema que tiene la empresa QWERTY S.A. en el caso de método aplicado donde se evidencia que en la actualidad su seguridad es bastante frágil y casi nula. Ya que no se presta caso a los estándares actuales y al hecho de que la seguridad de la información y la seguridad informática de las empresas no es solo una responsabilidad de las áreas de tecnologías de la información, sino que involucra todas las áreas de la empresa de manera transversal para el desarrollo de los procesos y procedimientos, en pro de respaldar las tres dimensiones de la información como son su integridad, confidencialidad y disponibilidad.

Al ser seleccionados como líderes de la implementación del SIGSI en la empresa se mostrará de manera eficiente y eficaz como evaluar, medir y proponer acciones para mitigar los riesgos que posee la empresa QWERTY S.A. con el fin de optimizar o aplicar los controles por medio de la planeación de las estrategias de mejora, la ejecución de dichas estrategias, la evaluación de estas estrategias a través de los controles de la norma ISO 27002 y el ajuste necesario o la reevaluación de las acciones para mantener la continuidad del negocio. Que muestren resultados que puedan ser puestos a beneficio de otras empresas o vistos como caso de éxito que ayude al crecimiento personal y académico de la persona encargada de la ejecución del proyecto.

El realizar el diseño e implementación del SIGSI marca el inicio de una carrera como ingeniero de sistemas con especialización en seguridad informática con un logro de un trabajo bien realizado al mostrar resultados que permitan replicar o mejorar el modelo en diferentes partes o empresas de la sociedad. Mejorando y optimizando sus procesos para un mejor desempeño de las empresas a fin de que puedan seguir

brindando a la sociedad sus productos y servicios con mínimos riesgos de seguridad informática.

Medir lo que se tiene actualmente a través de la recolección de información, las observaciones de campo de lo que hay en la empresa y los testimonios de los servidores de la misma serán las pautas iniciales para lograr el objetivo de implementar el SIGSI en la organización con miras a cumplir con los estándares actuales de las normas vigentes en el marco de trabajo y la metodología escogida para esta labor.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Diseñar un sistema de gestión de seguridad de la información para la empresa caso de estudio QWERTY S.A, que permita gestionar la seguridad de la información a partir de buenas prácticas de un Sistema Integrado de Gestión de Seguridad de la Información.

4.2. OBJETIVOS ESPECIFICOS

- Analizar los procesos existentes en la empresa para generar un análisis de riesgo y listar los activos informáticos de la empresa evidenciando sus vulnerabilidades y su probabilidad de frecuencia de ocurrencia de riesgo en ellos QWERTY S.A.
- Implementar las mejores prácticas, que permita dar cumplimiento a la legislación en la seguridad de la información.
- Establecer controles para aplicar y evaluar la ejecución de los mismos para ver oportunidades de mejora.
- Definir las políticas de seguridad que se aplicarán en la empresa QWERTY S.A.

5. MARCO REFERENCIAL

5.1. MARCO TEÓRICO

Propósito del SIGSI

Debido a la falta de seguridad y desactualización en los procesos de la empresa QWERTY S.A, es primordial conocer los recursos de la empresa que necesitan protección, para así mismo, gestionar el acceso a los sistemas y los privilegios de los colaboradores al sistema de información. Los mismos procedimientos se aplican los procesos manuales realizados por personal ajeno al proceso.

La investigación quiere hacer una medición en cuanto amenazas y riesgos a las cuales está exteriorizada la empresa, de igual manera identificar las condiciones físicas donde se encuentra alojados los equipos de cómputo.

El éxito de lograr las mediciones y de las acciones asertivas para mitigar las amenazas se deben soportar sobre normas conocidas como lo es la norma ISO 27001 y las técnicas de investigación como las de Ethical Hacking.

Construcción de un SIGSI

En la implementación del SIGSI se contará con un equipo humano especializado que iniciará con el análisis de riesgo de la empresa y el reconocimiento de cada una de las áreas que se tendrán en cuenta durante el proceso de recolectar información necesaria para la construcción de unas políticas coherentes con el funcionamiento de la organización.

Se realizarán reuniones con cada jefe de área para conocer a fondo el trabajo realizado por cada uno los colaboradores y la documentación que manejan para el cumplimiento de sus labores diarias. Con la información recolectada se iniciará con

la construcción de un borrador con los procesos iniciales para luego socializarlos y mejorarlos a medida que cada persona contribuya y aporte su experiencia en el proceso.

Análisis infraestructura

Se debe realizar un análisis de vulnerabilidades a la infraestructura computacional que le permita visualizar el estado actual de las aplicaciones, servidores, equipos de redes y estaciones de trabajo para luego presentar un informe a la dirección general con su respectiva remediación. En estos análisis en algunas ocasiones se requiere inversiones en equipos de seguridad que les ayude a tomar decisiones o acciones sobre los riesgos en la infraestructura de TI. Los directivos deberán evaluar costo-beneficio de la solución o soluciones que se lleguen a proponer en el momento que surjan.

Adicional al análisis de vulnerabilidades se debe realiza un ethical hacking que permita establecer el nivel de penetración en la cual se establecerá el nivel vulnerabilidad de la infraestructura incluyendo aplicaciones.

El inventario de software licenciado teniendo en cuenta que hay controles dentro del ISO 27001 que se implementarían y se determinaría la cantidad de software pirata el cual tiene que ser removido de los equipos de la empresa o licenciarlos.

Reunión con los líderes de los procesos

Se establecerá dialogo con los colaboradores para entender el concepto que tienen cada uno con respecto a la seguridad informática y como les afectaría en llegado que se presentase un incidente de seguridad de la información.

Realizar auditorías a intervalos planificados de tiempo para determinar si los riesgos

han bajado o por el contrario han aparecido nuevos riesgos los cuales se tendría que realizar un plan de tratamiento de los mismos.

Campañas con los usuarios

Las campañas para la concienciación se deben llevar cabo por el grupo de SIGSI para que los usuarios conozcan los procesos que se construyeron durante el tiempo de ejecución del proyecto. Crear conciencia acerca de la información que manejan y a la cual tienen acceso teniendo en cuenta que existen 3 pilares en la seguridad de la información que son: confidencialidad, integridad y disponibilidad de la información. Utilizando carteleras digitales, medios de comunicación y concursos se mantendrán dinamismo por parte de los usuarios y un interés en el tema.

Entrega resultados

Presentación de resultados a las directivas de la organización para su aprobación.

Creación de ruta informática para que los usuarios puedan acceder a la documentación aprobada.

Aplicación de las políticas aprobadas para dimensionar el impacto en los usuarios de la organización.

Revisión de los resultados para consolidar indicadores que ayuden a identificar el nivel de efectividad de cada una de las políticas.

Modificación y actualización de las políticas en el momento que haya lugar a los escenarios donde la política esté presentando alguna inconsistencia.
Reuniones periódicas para mostrar el impacto en cifras de la aplicación de las políticas del SIGSI.

6. MARCO CONCEPTUAL

SISTEMA GESTION

Es el encargado de reunir todos los procesos y/o procedimientos que se ejecutan dentro de la empresa, partiendo de los estándares internacionales para una mejor tarea de la administración de la información dentro de la compañía.

ESTANDARES DE LA SEGURIDAD DE LA INFORMACIÓN

Las organizaciones internacionales dedicadas a documentar las mejores prácticas para la seguridad de la información han preparado varios documentos que han sido clasificados de acuerdo a los temas que se manejan y según el sector que se aplique, las normas ISO son las más utilizadas y desarrolladas para todo el tema de seguridad, ya sea de información, industrial, etc.

El SIGSI (Sistema integrado de gestión de seguridad de la información), está basado en las normas internacionales.

Dentro de estos estándares se encuentran las buenas prácticas para la seguridad de la información las cuales pueden ser aplicadas dentro de una organización.

Dependiendo de la documentación y los procesos se prepara un plan de homologación para llevarlos a las mejoras prácticas para la certificación del SIGSI.

NORMA ISO

La International Organization for Standardization - ISO e International Electrotechnical Commission – IEC son todo el conjunto de normas de la 27000 encargada de los procesos de seguridad en donde se plantean las mejores prácticas para la certificación de una empresa.

NORMA ISO 27000

Esta norma hace una descripción general del conjunto de normas que hacen parte del estándar de seguridad de la información con su respectivo alcance según la publicación. Indica cuales son los lineamientos que aportarán para construir un SIGSI, son los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SIGSI. Es aplicable para cualquier empresa pequeña, mediana o grande no importa si son públicas o privadas.

Este conjunto de normas tiene unos controles que son aplicables de acuerdo a los procesos a certificar.

ISO 27001

Esta norma tiene todo lo necesario para la construcción de un sistema de gestión de seguridad de la información y su mejora. Es la norma aplicada por los auditores para certificar los procesos de una empresa. Tiene un anexo con los controles necesarios para ser aplicados a todos los procesos de una empresa. Aunque dependiendo del alcance se determinan cuáles son los controles que aplican para el proceso de certificación.

El beneficio que tiene esta norma dentro de una organización es que genera mayor confiabilidad y un mejor manejo de la información haciendo que sus

clientes se sientan satisfechos con la aplicación de la seguridad para los datos resguardados dentro de la empresa.

El inicio de una auditoria de ISO 27001 comienza con el análisis de riesgos de los activos de la empresa la cual determina cuales las vulnerabilidades que pueden convertirse en amenazas dentro de la organización. Posterior a este proceso se prepara un plan para minimizar los riesgos o trasladar los riesgos a los dueños o a un tercero para que los gestione y tome las acciones necesarias para mitigarlos.

La 27001 no solo se enfoca en un área específica como por ejemplo TI, sino que tiene controles para ser aplicados a diferentes áreas que conforman una empresa. Por lo tanto, en muchas ocasiones la aplicación de todos los controles no es necesario.

ISO 27002

Está conformada por una guía que aplica una gran cantidad de controles basado en las mejores prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

Aunque esta norma está inmersa dentro de la 27001 en el anexo A, la 27002 no es certificable, es una guía de buenas prácticas a ser aplicadas dentro de la empresa para el resguardo y protección de la información.

CICLO PHVA

En la construcción de la política de la seguridad de información es importante tener en cuenta que se requiere de un modelo práctico para implementarlo, y así mismo comprobarlo de tal manera que se cumpla. El ciclo PHVA (Planificar, hacer, verificar y actuar) está basado en el ciclo de Deming, ayuda a construir el

camino para definir, ejecutar, hacer seguimiento, control y mantenimiento del sistema integrado de gestión de seguridad de la información.
En el estándar ISO 27001:2013 asume que muchas empresas ya tienen su propio ciclo de gestión empresarial que toma o no los lineamientos del PHVA. En el ámbito del desarrollo del SIGSI el ciclo de gestión que manejan dentro de las empresas difiere mucho o poco del ciclo PHVA, por eso la norma ISO 27001:2013 establece en el numeral 10.2 que el sistema integrado de gestión de seguridad de la información debe estar en un proceso de mejora constante para asegurar su eficacia y adecuación según el estándar internacional.

Dentro del ciclo PHVA se empieza por la planificación, realizando el diseño, el desarrollo y documentación de las políticas de seguridad. En esta fase, se plantean los objetivos, la documentación de los procesos y procedimientos partiendo desde el punto de vista de la seguridad de la información para asegurar una buena gestión de riesgos. La base de construcción de estas políticas se inicia con el análisis de riesgo teniendo en cuenta un análisis de costo-beneficio para la empresa. Dentro de las políticas hay que tener en cuenta la normatividad legal que aplica en cada uno de los lineamientos. En la fase de hacer, se implementa la política de seguridad acompañado de los procedimientos y medidas, se asignan responsabilidades en cada uno de los procesos. En la fase de revisar, se realizan auditorías internas evaluando si la política de información se está aplicando de manera correcta. En la fase de actuar, en llego caso que se tengan que aplicar controles nuevos se harán las modificaciones necesarias para que la política se ajuste. El ciclo PHVA es continuo y se encuentra dentro de SIGSI, se realizan auditorías a intervalos de tiempo determinado dentro de la organización.

COBIT

Es un estándar que se enfoca en el crecimiento de TI a nivel empresarial revisando el funcionamiento de las mejores prácticas basados en los estándares, revisando si necesita mejoras o nuevas formulaciones en búsqueda de la alineación de los objetivos comerciales con los objetivos TI, formando una relación entre los 2 y reduciendo el distanciamiento que pueda haber entre TI y las dependencias externas. El estándar COBIT se centra en el área de seguridad, la gestión de los riesgos y el gobierno de TI.

Se basa en 5 principios fundamentales: cumplir con las expectativas entre las partes interesadas, acaparar la empresa de un lado al otro, cumplir con un marco de referencia bajo un ámbito, construir un enfoque holístico para el negocio y dividir el gobierno dejando la administración a un lado.

MAGERIT

Es una metodología muy práctica para análisis y gestionar riesgos de los sistemas de información aplicada solamente a TI (Tecnologías de la información). Parte de un análisis de riesgo para detectar las vulnerabilidades, las amenazas y el impacto que estas generan dentro de una organización. La gestión de riesgos se basa en los resultados obtenidos durante el análisis, aplicando todos los controles y medidas de seguridad necesarios para mitigar, reducir o eliminar cada uno de los riesgos identificados. MAGERIT (Metodología de análisis y gestión de riesgos de los sistemas de información) se enfoca en estudiar todos los riesgos y hacer una gestión de los mismos para minimizar el efecto que esto tiene dentro de una organización, enruta a la empresa para prepararse para una certificación en ISO 27001, tiene 3 modelos básicos para seguir: entidades, eventos y procesos.

SEGURIDAD DE LA INFORMACIÓN

Es un conjunto de normas que se aplican para proteger y resguardar la información asegurando la confidencialidad, integridad y disponibilidad que son los pilares de la seguridad de la información.

Las empresas cada día acumulan información la cual se le debe dar un tratamiento para protegerla de vulnerabilidades y amenazas externas. La información puede estar almacenada en medios impresos, magnéticos, videos y audios, esta información es considerada valiosa y hace parte de los activos de la información las cuales se les debe dar un tratamiento para protegerla.

La información todos los días se está moviendo por lo que es accedida, modificada y guardada por el personal que tiene acceso, pero también puede ser objeto de amenazas. Las amenazas son las siguientes:

Externas: La información es expuesta por lo que los hackers inician procesos de intrusión violar los dispositivos de seguridad para acceder a ella para hacer lo que quieran provocando gran pérdida y confiabilidad de la empresa.

Internas: Son los puntos de ataque más frágiles que tiene una organización por lo que internamente dentro de ella están más cerca de la información para acceder a ella, la mayoría de las intrusiones dentro de la organización se presentan por los colaboradores ya sea a través de la red o llegando a ella por intermedio de los mismos empleados.

Naturales: Los fenómenos naturales también son elementos inevitables que la naturaleza de manera imprevista nos presenta, los huracanes, los terremotos y los desastres naturales.

IMPLEMENTACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La necesidad de la seguridad de la información le brinda a la empresa una mayor confiabilidad, posicionamiento, desempeño y competitividad. Genera ganancias en todos los sentidos colocando la empresa en las mejores en la rama que se desempeñan en el mercado.
La capacidad que tiene la empresa para enfrentar las amenazas son un gran reto cada día, los fenómenos que se presentan como los que imponen los hackers y los naturales hacen que le empresa piense en la manera de mantenerse vigente ante cualquier cambio en el medio donde se mueve la información.

Alistar la organización para cualquier proceso y/o procedimiento que involucre la seguridad de la información se requiere de un grupo de especialistas en la materia para realizar las operaciones necesarias para llevar a la empresa hacía el camino de la certificación o validación de la misma.

La evaluación de riesgos entrega información de la probabilidad de ocurrencia de que una amenaza se materialice.

Lo normatividad legal son elementos a tener en cuenta a la hora de la implementación de unas políticas de seguridad, en estas normas están los requerimientos y sanciones legales vigentes para el tratamiento de la información.

Como parte de la seguridad de la información se encuentra los equipos informáticos que prestan el servicio de acceso a los sistemas de información, para la protección de la información estos servicios deben estar monitoreados y protegidos por equipos de seguridad para minimizar los riesgos de intrusión y daño de la información.

POLITICA DE SEGURIDAD

Es el documento que rige lo necesario para el acceso a la información por parte de los usuarios, es el primer paso para dar conocer todo el sistema integrado de gestión de seguridad de la información.

Este documento lo debe conocer la dirección de la organización y ser aprobado. El documento firmado se anexa a la normativa para hacerse cumplir.

Este documento debe tener un lenguaje comprensivo y entendible para que los usuarios lo apliquen correctamente si llegar a caer en errores de comprensión de lectura.

7. MARCO LEGAL

Se tiene en cuenta las leyes colombianas que aplican para el tratamiento de la seguridad de la información como la ley 1581 del 2012 de protección de datos que contempla el derecho al tratamiento de los datos personales, la responsabilidad que tiene cada titular de las empresas y entidades para que dicha información no sea entregada a personas sin el consentimiento del dueño de los datos.

Considerando las siguientes definiciones a los diferentes datos (artículo 3 de la ley 1581 de 2012):

- **Dato público**: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio ya su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

- **Datos sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del *Titular* o cuyo uso indebido puede generar su discriminación, tales como aquello que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

- **Transferencia**: La transferencia de datos tiene lugar cuando el responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia,

envía la información o los datos personales a un receptor, que a su vez es responsable del Tratamiento y se encuentra dentro o fuera del país.

- **Transmisión**: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

Y que en su capítulo III habla de las políticas de tratamiento

- **Aviso de privacidad.**: En los casos en los que no sea posible poner a disposición del titular las políticas de tratamiento de la información, los responsables deberán informar por medio de un "Aviso de Privacidad" al titular sobre la existencia de tales políticas y la forma de acceder a las mismas, de manera oportuna y en todo caso a más tardar al momento de la recolección de los datos personales.

- **Contenido mínimo del aviso de privacidad**: El aviso de privacidad, como mínimo, deberá contener la siguiente información: 1. Nombre o razón social y datos de contacto del responsable del tratamiento. 2. El tratamiento al cual serán sometidos los datos y la finalidad del mismo. 3. Los derechos que le asisten al titular. 4. Los mecanismos dispuestos por el responsable para que el titular conozca la política de tratamiento de la información y los cambios sustanciales que se produzcan en ella o en el aviso de privacidad correspondiente. En todos los casos, debe informar al titular cómo acceder o consultar la política de tratamiento de información. No obstante, lo anterior, cuando se recolecten datos personales sensibles, el aviso de privacidad deberá señalar expresamente el carácter facultativo de la respuesta a las preguntas que versen sobre este tipo de datos. En todo caso, la divulgación del aviso de privacidad no eximirá al responsable de la obligación de dar a

conocer a los Titulares la política de tratamiento de la información, de conformidad con lo establecido en este decreto.

- Deber de acreditar puesta a disposición del aviso de **privacidad y las políticas de tratamiento de la información:** Los responsables deberán conservar el modelo del aviso de privacidad que utilicen para cumplir con el deber que tienen de dar a conocer a los titulares la existencia de políticas del tratamiento de la información y la forma de acceder a las mismas, mientras se traten datos personales conforme al mismo y perduren las obligaciones que de este se deriven. Para el almacenamiento del modelo, el responsable podrá emplear medios informáticos, electrónicos o cualquier otra tecnología que garantice el cumplimiento de lo previsto en la Ley 527 de 1999.

- **Medios de difusión**: del aviso de privacidad y de las políticas de tratamiento de la información. para la difusión del aviso de privacidad y de la política de tratamiento de la información, el responsable podrá valerse de documentos, formatos electrónicos, medios verbales o cualquier otra tecnología, siempre y cuando garantice y cumpla con el deber de informar al titular.

- **Procedimientos para el adecuado tratamiento de los datos personales**: Los procedimientos de acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización deben darse a conocer o ser fácilmente accesibles a los titulares de la información e incluirse en la política de tratamiento de la información.

- **Medidas de seguridad**: La Superintendencia de Industria y Comercio impartirá las instrucciones relacionadas con las medidas de seguridad en el tratamiento de datos personales.[2]

[2] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581 (18, octubre 2012) Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial Bogotá D.C., 2012 No. 48.587. p 1 – 301. Recuperado de: wsp.presidencia.gov.co

La ley 1273 del 2009 que contempla la confidencialidad, integridad y disponibilidad de la información en sistemas informáticos, así como los delitos informáticos conocidos y los ataques informáticos los cuales tienen una pena legal según se identifique el delito cometido. Los abusos cometidos a la infraestructura por parte de terceros son delitos que son castigables en la ley colombiana.
El capítulo segundo establece:

- **HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES**. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 del código penal, es decir, penas de prisión de tres (3) a ocho (8) años.
- **TRANSFERENCIA NO CONSENTIDA DE ACTIVOS**. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.[3]

[3] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (5, enero 2009) Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de

8. MARCO METODOLÓGICO

La información, tomada como activo de la empresa tiene muchos medios para ser administrada al interior de toda organización, entre ellos el papel impreso, la hablada en una reunión o conversación y por supuesto la que está por medio de la tecnología en la actualidad. La cual, se puede encontrar almacenada electrónicamente, transmitida por correo electrónico o imprimido. (NTP-ISO/IEC 17799) "La información debe protegerse cualquiera que sea la forma que tome o los medios por los que se comparta o almacene".

Y es precisamente en este medio en que la tecnología se hace participe, ya que desde mediados del siglo XX para acá se han venido creando dispositivos como disquetes, discos duros, CD, discos duros, memorias flash y muchos otros que han aparecido en la actualidad. Pero el mismo manejo de este tipo de medios ha permitido que la información se vea COMPROMETIDA al no poseer políticas o procedimientos y demás actividades que protejan la información.

La seguridad de la información debe considerarse un proceso de gestión y no un proceso tecnológico. Aunque la información resida en sistemas de cómputo (computadoras, servidores, enrutadores, medios, nube) como cualquier otro, requieren de protección, de igual forma la información; pues ya hacen parte de la red y como tal deben ser protegidos, de lo contrario equivaldría a dejar una puerta abierta a los delincuentes y esto no solo se logra al instalar un antivirus, que en otro momento muy seguramente tuvo éxito pero actualmente no, como se evidencia que más de la mitad de empresas de la región se vieron afectadas por diferentes códigos maliciosos[4].

---

la información y de los datos"-… Diario Oficial Bogotá D.C., 2009 No. 47.223. p 1 – 4. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[4] NAJAR, P. José y SUÁREZ, S. Nubia. La seguridad de la información: un activo valioso de la organización. En: Vínculos. Febrero 2015, vol 12, no 1, p 89-97. Disponible en Internet: https://revistas.udistrital.edu.co/index.php/vinculos/article/view/10518/11480

Es así que la alta dependencia de estos sistemas de información por parte de las empresas y en especial por parte de la empresa QWERTY S.A. es una preocupación para ellas dado los riesgos que se generan por la complejidad de estos sistemas, accidentes, errores humanos o ataques y la constante evolución de la tecnología[15] que hace que los dispositivos y el software que las empresas poseen se desactualice y se vuelvan foco de vulnerabilidades aprovechadas por los atacantes ya que entre más tiempo se quede dicho software en el mercado más tiempo poseen los atacantes.

Sin embargo, actualmente existen también muchas herramientas tecnológicas que ayudan a la reducción de estos riegos, desde la parte de infraestructura como de software y capacitaciones del personal. Pero desde la parte tecnológica ahora poseemos dispositivos como firewall, balanceadores, enrutadores, switches administrados, SAN, NAS, y a nivel de software también herramienta de monitoreo, herramientas DLP, herramientas de análisis de riesgos como Pilar y otra que permiten hacer una tarea sobre la información y los eventos de seguridad (SIEM). Además, software de protección de EndPoint y hasta WAF (Cortafuegos de aplicaciones web)

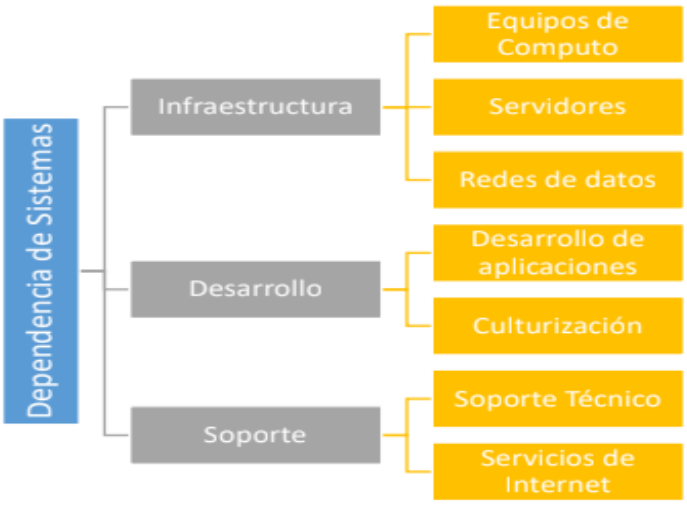
Desde este punto de vista, la tecnología está de la mano con los procesos de gestión de las organizaciones para ayudar a mantener la seguridad de la información, a punto que con el desarrollo de ataques desde principios de los 80 en el siglo pasado, también se han desarrollado tecnológicamente nuevas tendencias de hardware y software que apoyan la seguridad de la información para controlar el cumplimiento de las políticas y directrices que se definan en cada organización para minimizar los riesgos de la misma.

9. MARCO CONTEXTUAL

El proyecto se propone para implementar un SIGSI en la empresa QWERTY S.A. del sector tecnológico que busca el desarrollo tecnológico en comunidades colombianas a través del uso de TI (Tecnologías de Información). Actualmente cuenta con 120 colaboradores entre directivos, administrativos y operadores quienes consultan datos con frecuencia diaria a través de los medios de información que tiene la empresa.

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

Ilustración 1 Distribución dependencia de Sistemas de QWERTY S.A.



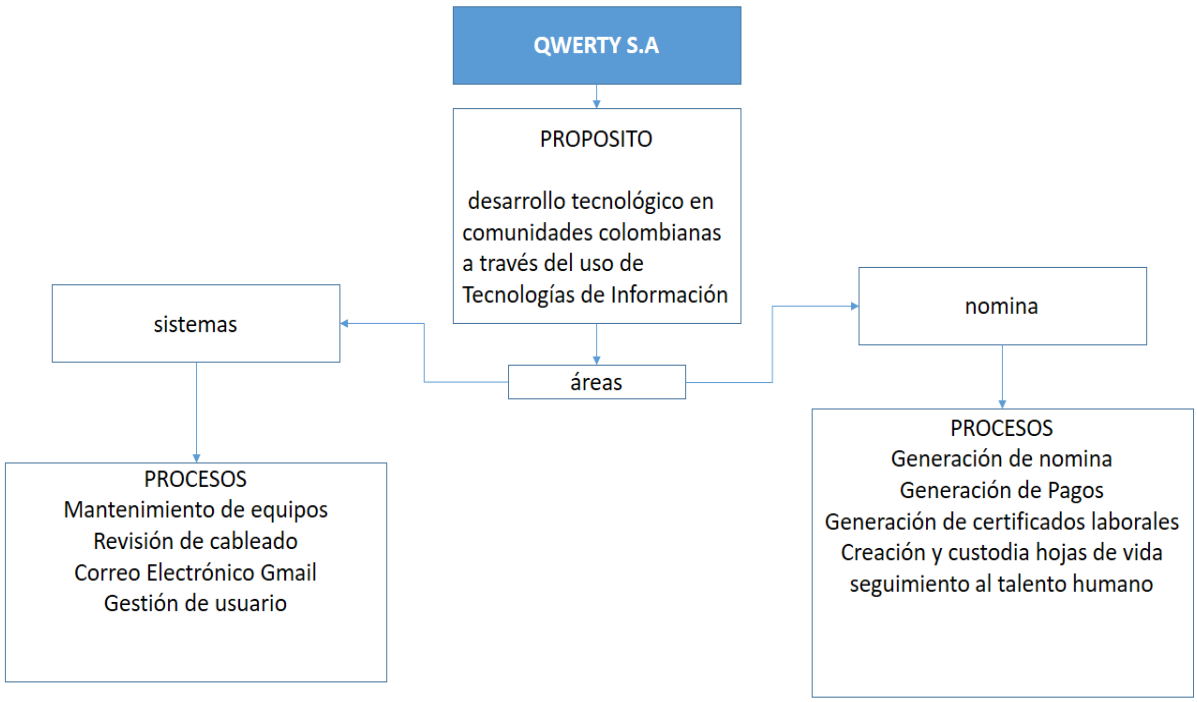
Fuente propia.

La empresa cuenta con un servicio de internet de 25 Mb para el desarrollo de sus actividades diarias, monitoreado por el área de insfraestructura de la dependencia de sistemas. Además, la empresa cuenta con diferentes activos de información entre los cuales, encontramos *servidores, impresoras, servidor de archivos –como servicio– firewall, access point, página web –como servicio– DHCP, software de facturación, equipos de computo de usuario final, equipos para gestión del desarrollo tecnológico, puntos de acceso (Hub), Switches, personal tecnico de mantenimiento y telefonía Ip.*

Pero aun con todos estos activos, la empresa no tiene sistema de seguridad para el registro de los usuarios que permita monitorear el ingreso y egreso de los clientes externos e internos. De igual forma, no se cuenta con condiciones óptimas para mantener la temperatura en el lugar donde están los servidores.

Tampoco se ve que se tengan políticas de seguridad informática, o si se tienen no existen controles para verificar su aplicación, dado que pasan eventos como tener antivirus pero no saber si están actualizados o no, al igual que tampoco se tiene control sobre los usuarios que administran el flujo de información sobre el software de nómina y facturación.

Ilustración 2 Organigrama de QWERT S.A.



Fuente propia.

Propósito del SIGSI: Debido a la falta de seguridad y desactualización en los procesos de la empresa QWERTY S.A, es primordial conocer qué recursos de la empresa necesitan protección, lo que permitirá controlar el ingreso a las aplicaciones y los privilegios de los involucrados en el sistema de información. Los mismos procedimientos se emplean para los procesos manuales realizados por personal ajeno al proceso.

La investigación quiere hacer una medición en cuanto amenazas y riesgos a las cuales está expuesta la empresa, de igual manera identificar las condiciones naturales y físicas donde se encuentra alojados los equipos de cómputo.

El éxito de lograr las mediciones y de las acciones asertivas para mitigar las amenazas se deben soportar sobre normas conocidas como lo es la norma ISO 27001 y las técnicas de investigación como las de Ethical Hacking.

Construcción de un SIGSI: En la implementación del SIGSI se contará con un equipo humano especializado que iniciará con el análisis de riesgo de la empresa y el reconocimiento de cada una de las áreas que se tendrán en cuenta durante el proceso de recolectar información necesaria para la construcción de unas políticas coherentes con el funcionamiento de la organización.

Se realizarán reuniones con cada jefe de área para conocer a fondo el trabajo realizado por cada uno los colaboradores y la documentación que manejan para el cumplimiento de sus labores diarias. Con la información recolectada, se iniciará con la construcción de un borrador con los procesos iniciales, para luego socializarlos y mejorarlos a medida que cada persona contribuya y aporte su experiencia en el proceso.

Análisis infraestructura: Se debe realizar un análisis de vulnerabilidades a la infraestructura computacional que le permita visualizar el estado actual de las aplicaciones, servidores, equipos de redes y estaciones de trabajo para luego presentar un informe a la dirección general con su respectiva remediación. En estos análisis en algunas ocasiones se requiere inversiones en equipos de seguridad que les permita mitigar o disminuir los riesgos en la infraestructura de TI. Los directivos deberán evaluar costo-beneficio de la solución o soluciones que se lleguen a proponer en el momento que surjan.

Adicional al análisis de vulnerabilidades se debe realiza un ethical hacking que permita establecer el nivel de penetración en la cual se establecerá el nivel vulnerabilidad de la infraestructura incluyendo aplicaciones.

El inventario de software licenciado teniendo en cuenta que hay controles dentro del ISO 27001 que se implementarían y se determinaría la cantidad de software pirata el cual tiene que ser removido de los equipos de la empresa o licenciarlos.

Reunión con los líderes de los procesos: Se establecerá dialogo con los colaboradores para entender el concepto que tienen cada uno con respecto a la seguridad informática y como les afectaría en llegado que se presentase un incidente de seguridad de la información.

Efectuar auditorías con regularidad de tiempo para decretar si los riesgos han bajado o por el contrario han aparecido nuevos riesgos los cuales se tendría que realizar un plan de tratamiento de los mismos.

Campañas con los usuarios: Las campañas para la concienciación se deben llevar cabo por el grupo de SIGSI para que los usuarios conozcan los procesos que se construyeron durante el tiempo de ejecución del proyecto. Crear conciencia acerca de la información que manejan y a la cual tienen acceso teniendo en cuenta que existen 3 pilares en la seguridad de la información que son: confidencialidad, integridad y disponibilidad de la información. Utilizando carteleras digitales, medios de comunicación y concursos se mantendrán dinamismo por parte de los usuarios y un interés en el tema.

Realizar entregas de resultados trimestrales:

- Presentación de resultados a las directivas de la organización para su aprobación.
- Creación de ruta informática para que los usuarios puedan acceder a la documentación aprobada.
- Aplicación de las políticas aprobadas para dimensionar el impacto en los usuarios de la organización.
- Revisión de los resultados para consolidar indicadores que aprueben la medición del nivel efectividad de cada una de las políticas.
- Modificación y actualización de las políticas en el momento que haya lugar a los escenarios donde la política esté presentando alguna inconsistencia.
- Reuniones periódicas para mostrar el impacto en cifras de la aplicación de las políticas del SIGSI.

SISTEMA INTEGRADO DE GESTIÓN DE SEGURIDA DE LA INFORMACIÓN (SIGSI)

10.1. METODOLOGÍA DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS

Por medio de la metodología Magerit, el tratamiento de riesgos debe tomar algunas consideraciones para su aplicación, dependiendo de diversos factores:

- El peligro de que se materialice el impacto y/o riesgo.
- Las necesidades a las que la empresa debe responder de acuerdo a la ley.
- Las obligaciones a las que la empresa de acuerdo al sector donde se desenvuelve.
- Las obligaciones a las que la empresa esté sometida por obligación contractual.

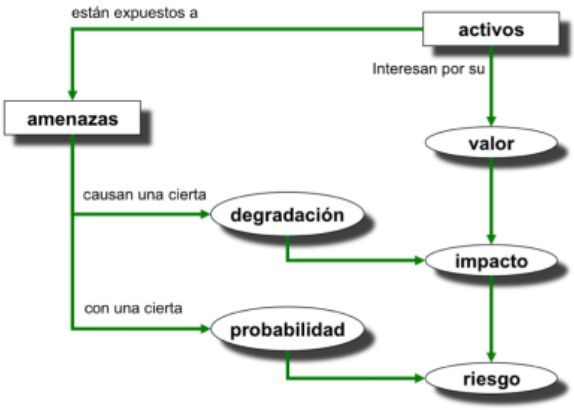
Posterior a esto, el análisis de riesgos es una aproximación a través de un método en una sucesión de pasos para determinar la exposición de los activos a dicho riesgo:

10.1.1. Identificación de los activos

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [UNE 71504:2008][5]

[5] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de riesgos de los Sistemas de Información. Libro I – Método. NIPO: 630-12-171-8. Madrid, España. 2012 127 p. Disponible en Internet: https://www.politecnicojic.edu.co/images/downloads/biblioteca/guias/NTC5613.pdf

Ilustración 3 Análisis de riesgos sobre un activo.



Fuente Magerit_v3_libro1.

En un sistema integrado de gestión de la seguridad de la información hay dos cosas esenciales que se debe tener en cuenta, la **información** que se maneja y los **servicios** que esta presta, por lo cual los activos son esenciales para fijar los demás componentes del sistema y por medio de esta clasificación se pueden determinar otros activos relevantes:

Tabla 1 Otros activos relevantes de una empresa

ACTIVOS RELEVANTES	
Datos	Que materializan la información
Servicios	Necesarios para la organización del sistema.
Aplicaciones Informáticas	(software) que permite manejar los datos
Equipos Informáticos	(Hardware) que permite hospedar los datos, aplicaciones y servicios.
Soportes de Información	Dispositivos para el almacenamiento de datos.
Equipamiento auxiliar	Que complementan el material informático
Redes de Comunicaciones	Que permiten el intercambio de datos.

ACTIVOS RELEVANTES	
Instalaciones	Que acogen los equipos informáticos y de comunicaciones
Personas	Que explotan u operan todos los elementos anteriormente citados.

Fuente: propia basada en el libro Magerit_v3_libro1

Estos activos son comunes en casi toda organización o empresa, aunque se puedan presentar cambios en una o en otra, muy a menudo se pueden estructurar el conjunto de activos en un orden.

Tabla 2 Conjunto de activos en capas

ACTIVOS	DESCRIPCIÓN
Activos Esenciales	• Información que se maneja • Servicios prestados
Servicios Internos	• Estructuran ordenadamente el sistema de información
Equipamiento Informático	• Aplicaciones (software) • Equipos Informáticos (hardware) • Comunicaciones • Soportes de información: discos, cintas, USB entre otros
entorno	• Equipamiento y suministros: energía, climatización • Mobiliario
Servicios subcontratados	• Outsourcing
Instalaciones físicas	• Edificios • Oficinas • Centros de datos en arriendo
Personal	• Usuarios

ACTIVOS	DESCRIPCIÓN
	• Operadores y administradores • Desarrolladores • Contratistas • empleados

Fuente: propia basada en el libro Magerit_v3_libro1

de estos activos, siempre es importante definir para todo sistema integrado de gestión de seguridad informática, se hace necesario evaluarlo en las tres dimensiones claves de la información, **confidencialidad** (¿qué daño causaría que lo conociera quien no debe?), **integridad** (¿qué perjuicio causaría que estuviera dañado o corrupto?) y **disponibilidad** (¿qué perjuicio causaría no tenerlo o no poder utilizarlo?) aunque pueden existir otras dimensiones como la autenticidad y la trazabilidad de uso del servicio y acceso a los datos. Nos enfocaremos en las tres principales.

Esta evaluación se realiza para dar cumplimiento a la ley 1581 de 2012, art 3 para proteger los datos personales de la empresa QWERTY S.A

Valoración de un Activo

Todo activo debe tener un valor, este valor está dado por la necesidad de preservar en relación a lo importante o imprescindible que este es para la empresa de QWERTY S.A. En relación a las dimensiones establecidas, se debe determinar el valor de este activo en el coste (monetario) que representaría para la empresa la recuperación de un incidente en el que el activo se viese involucrado. Hay muchos factores a considerar.

- Qué valor tiene reponerlo: adquisición e instalación.
- Quien lo repone: personal (especializado o técnico operativo)
- Perdida de ganancia: cuanto se deja de recibir por tener el activo en daño.

- Capacidad operativa: perdida de procesos y clientes, usuarios o proveedores por incapacidad de operar.
- Multas: incumplimiento de leyes o tiempos de entrega a obligaciones contractuales o de tiempos de demandas.
- Daños: a otros activos, a personas o medioambientales.

La valoración del activo se puede hacer desde una perspectiva cualitativa y una cuantitativa, siendo esta última la de mayor uso por las empresas.

10.1.2. Identificación de amenazas

Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008]

Tabla 3 Tipos de amenazas

TIPO DE AMENAZA	DESCRIPCIÓN
De origen natural	Terremotos, inundaciones, erupciones volcánicas entre otros, el sistema es pasivo, ya que no hay forma de que el sistema esté preparado para esto.
Del entorno (origen industrial)	Contaminación, fallas eléctricas, entre otros, el sistema está en estado pasivo, pero se puede estar preparados sin estar indefensos.
Defecto de las aplicaciones	Defectos en diseño o implementación, denominadas vulnerabilidades
Causadas por el personal de forma accidental	Errores por omisión o mal procedimiento no intencionados
Causadas por el personal de forma deliberada	Ataques, con ánimos lucrativos o solo por causar daños

Fuente: propia basada en el libro Magerit_v3_libro1

No todas las amenazas afectan todos los activos o no todos los activos están propensos a las mismas amenazas, se puede decir que existe una relación entre el tipo de activo y la amenaza que lo puede suceder, es por esto que después de determinar dicha relación hay que valorar como afecta la amenaza al activo dos dimensiones, la **degradación** (cuan perjudicado resultaría el [valor del] activo) y la **probabilidad** (que posibilidad existe de que la amenaza se vuelva real).

Tabla 4 Degradación del valor

Acrónimo	Valor del acrónimo	Degradación	Daño del activo
MA	Muy alta	Casi seguro	fácil
A	Alta	Muy alto	Medio
M	Media	Posible	Difícil
B	Baja	Poco probable	Muy difícil
MB	Muy baja	Muy raro	Extremadamente difícil

Fuente: propia basada en el libro Magerit_v3_libro1

Para la probabilidad de ocurrencia de que una amenaza se materialice se utiliza una escala de 1 año como tasa anual de frecuencia de que la amenaza se haga real.

Tabla 5 Probabilidad de ocurrencia

Acrónimo	Escala	Valoración	Ocurrencia
MA	100	Bastante frecuencia	Casi todos los días
A	10	Frecuente	Casi todos los meses
M	1	Normal	1 vez al año
B	1/10	Poco frecuente	Cada varios años
MB	1/100	Casi nunca ocurre	siglos

Fuente: propia basada en el libro Magerit_v3_libro1

10.1.3. Tipos de Impacto potencial

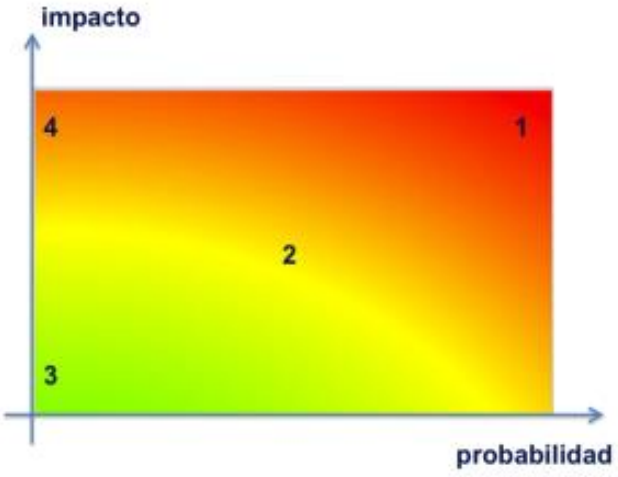
El impacto es el daño que ocasiona la materialización del riesgo sobre el activo en cualquiera o todas sus dimensiones al hacerse real la amenaza. En el sistema integrado de gestión de seguridad informática de QWERTY S.A. este impacto es medible sobre los activos en relación a la información que ellos manejan y los servicios que presta.

Existen dos tipos de impacto que se pueden dar sobre los activos, **impacto acumulado** el valor acumulado del activo al tener en cuenta los otros activos que dependen de este y las amenazas a las que está expuesto y el **impacto repercutido** el cual es calculado sobre un activo al tener en cuenta su valor propio y las amenazas a las que este se expone determinando las consecuencias sobre el sistema de información.

10.1.4. Clasificación del riesgo potencial

La clasificación del riesgo es una estimación que se realiza al evaluar el impacto que se tiene sobre los activos de la entidad y la probabilidad de ocurrencia de que la amenaza se materializase, dando una valoración cualitativa y cuantitativa del mismo al determinar zonas de mayor catástrofe para la entidad y otras en las cuales es posible aprender a mitigar o convivir con los riegos.

Ilustración 4 Zonas de Riesgos.



Fuente Magerit_v3_libro1.

B: Zona de riesgo *baja*: el riesgo se puede asumir riesgos improbables y de bajo impacto.

M: Zona de riesgo *moderada*: Asumir el riesgo, pero buscando la manera de mitigarlo o reducirlo.

A: Zona de riesgo alta: Reducir el riesgo, evitarlo, compartirlo o transferirlo. Riesgos improbables y de bajo impacto.

E: Zona de riesgo *extrema*: Evitar el riesgo. Riesgos muy probables y de muy alto impacto

10.1.5. Clase de controles o salvaguardas

Las salvaguardas son acciones (controles* de ahora en adelante) que se pueden tomar o llevar a cabo para reducir el impacto y el riesgo al que están expuestos los activos. En la actualidad no existe un sistema de información que no tenga algunos controles y QWERTY S.A. no es la excepción a la regla. Es por esto, aunque se

haya realizado una identificación de activos, de amenazas y de los riegos de los activos, es necesario también evaluar los controles para volver a revaluar los riesgos sobre los activos.

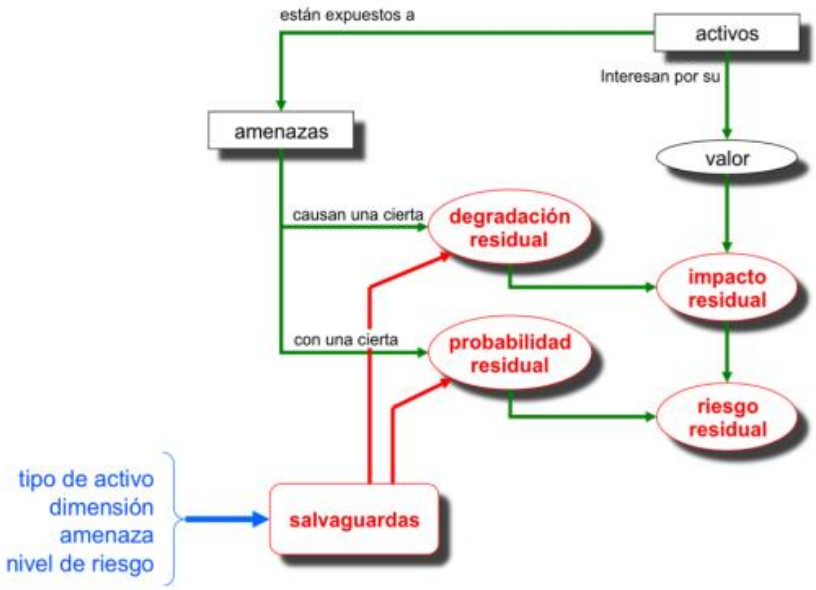
Estos controles se deben seleccionar con base en los siguientes aspectos.

1. Activos a proteger, para cada uno se definen controles específicos.
2. Dimensiones de seguridad a proteger (para el proyecto se han seleccionado la confidencialidad, integridad y disponibilidad).
3. Amenazas de los activos a proteger.
4. La cobertura o protección que puede brindar el control en proporción a la reducción, minimización, eliminación o aceptación del riesgo.

Estos controles pueden ser desde elementos técnicos (software o infraestructura de equipos de cómputo), seguridad física y políticas de seguridad para el personal.

Por esto para no tener en cuenta un control se debe validar dos aspectos importantes de los mismos como **no aplica** – técnicamente no es adecuada para el activo o no sirve para la dimensión del activo que se quiere proteger - o **no se justifica** – aplica, pero es desproporcionada al riesgo que se quiere evitar –

Ilustración 5 Análisis de riesgos de Activos con salvaguardas.



Fuente Magerit_v3_libro1.

Es así que se determinan el tipo de protección que los controles brindaran a los activos y a la información en ellos.

Tabla 6 Tipos de controles

Acrónimo	Nombre	Definición
[PR]	Prevención	Reduce la probabilidad de ocurrencia de una amenaza
[DR]	Disuasión	Disuade a los atacantes de aprovechar una vulnerabilidad
[EL]	Eliminación	No permite que una amenaza tenga lugar
[IM]	Minimización del Impacto	Limita el impacto acotando las consecuencias del incidente
[CR]	Corrección	Repara el daño que se ha ocasionado por la ocurrencia de un incidente
[RC]	Recuperación	Permite regresar a un estado anterior
[MN]	Monitorización	Permiten supervisar la ocurrencia en tiempo real y reducir los tiempos de respuesta

Acrónimo	Nombre	Definición
[DC]	Detección	Informa del ataque en tiempo real siendo proactivo el control
[AW]	Concienciación	Actividades de capacitación, formación y ayuda a mejorar los otros controles.
[AD]	Administración	Relacionadas con los componentes de seguridad.

Fuente: propia basada en el libro Magerit_v3_libro1

Estos controles también se pueden clasificar de acuerdo al efecto que producen sobre los activos y la organización a la hora de escogerse para ser aplicados.

Tabla 7 Clasificación de controles de acuerdo al efecto

EFECTO	TIPO
reduce la probabilidad de ocurrencia	[PR] preventivas [DR] disuasivas [EL] eliminatorias
acotan la degradación del activo	[IM] minimizadoras [CR] correctivas [RC] recuperativas
consolidan los efectos de las demás	[MN] monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Fuente: libro Magerit_v3_libro1

10.1.6. Formalización de actividades

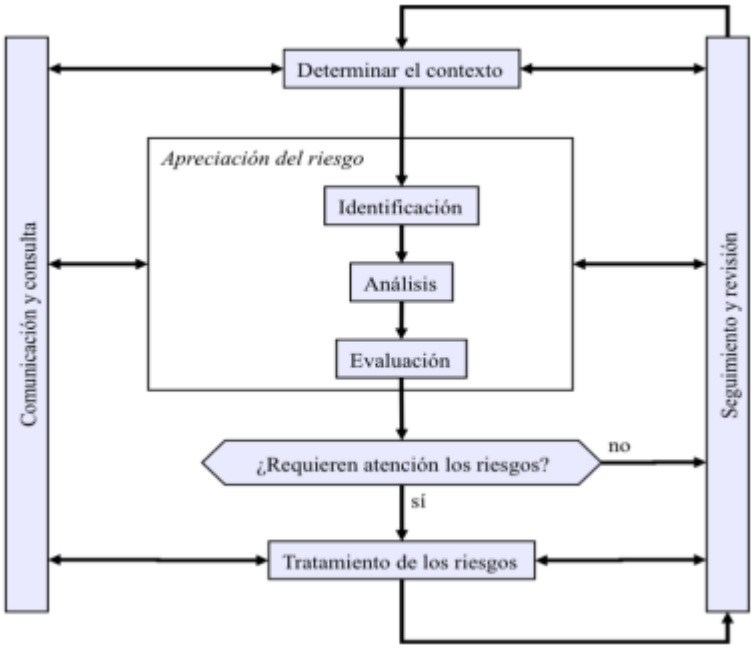
Los riesgos son ineludibles, están presentes y siempre pueden aparecer, identificarlos y alcanzar a las disposiciones que corresponde tomar en relación a ellos son las actividades condicionados por diversos factores (aparte de las enunciadas al principio de este plan) intangibles, pero también muy importantes para la empresa:

- Reputación: lo que piensa la comunidad de la empresa.
- Política interna: capacidad de contratación de personal idóneo, mantención de los mejores empleados, rotación de personal y capacidad de crecimiento personal y profesional.
- Relaciones con los proveedores.
- Relaciones con los clientes o usuarios, tales como capacidad de retención, capacidad de incrementar la oferta, capacidad de diferenciarse frente a la competencia
- Relaciones con otras empresas: alianzas estratégicas y nuevas oportunidades de negocio.

Estas consideraciones ayudan a socavar la calificación del riesgo con las siguientes determinaciones:

1. Crítico: requiere atención urgente.
2. Grave: requiere atención.
3. Apreciable: Es objeto de estudio para verificar su mejor tratamiento.
4. Asumible: no se toman acciones para detenerlo, simplemente acciones correctivas después de que ha acontecido el hecho.

Ilustración 6 Plan de tratamiento de riesgos.



Fuente ISO 31000.

10.1.6.1. Aceptación del riesgo

QWERTY S.A. tiene que establecer el valor de impacto y riesgo que aceptará, entendiendo la responsabilidad de aceptar la insuficiencia de las salvaguardas (controles) y de las vulnerabilidades de los activos para enfrentar estos riesgos. No es una decisión técnica, más bien administrativa. Esta aceptación se puede hacer por cada uno de los activos o por aglomeración de activos, entendiendo el tratamiento que se le ha de dar. Este tratamiento se puede dar de dos formas muy escogidas por la administración de la mayoría de las empresas, entre ellas:

Tratamiento: eliminación

Se realiza este tipo de tratamiento frente a riesgos que no son aceptables tenerlos en la empresa. Se puede prescindir de cierto tipo de activos, o emplear otros en vez

de esto por desactualización o EOL (*End Of Life*) del software o del hardware que compone un activo. Reordenar la arquitectura de un sistema de modo que se redistribuya el valor acumulado del activo por estar expuesto a grandes amenazas.

Tratamiento: mitigación

Se busca reducir la probabilidad de degradación del activo causado por una amenaza o reducir la probabilidad de que esta amenaza se materialice, mucho de los controles de tipo técnico está enfocado a este tipo de tratamiento.

Tratamiento: compartición

Transferir el riesgo, parcial o totalmente se define como compartirlo de forma cualitativa, en la cual se divide el sistema para que se repartan las responsabilidades, o de forma cuantitativa a través de la adquisición de seguros o subcontratación para contratar el grado de responsabilidad de las partes.

Tratamiento: financiación

Aceptación del riesgo, la empresa tiene que ahorrar fondos por la posibilidad de que el riesgo se haga real y deba responder a sus consecuencias. Puede crear un “fondo de contingencia” o comprar un seguro que le ayude a minimizar por lo menos la pérdida económica.

10.1.7. Plan de Implementación

Después de escoger los controles más convenientes para tener un nivel de riesgo tratable para el o los procesos y activos incluidos en SIGSI, es necesario identificar es importante definir los pasos para tratar estos riesgos, las acciones que se

implementarán y los responsables de esta implementación. Definido en el plan, cada acción, etapa y procedimiento logrando el monitoreo de la ejecución del mismo.

Este plan debe ser aprobado por cada uno de los administradores de los objetos sobre los que se puede dar cada riesgo, de un comité designado para lo mismo por parte de la empresa y la dependencia de sistemas.

10.1.8. Políticas de administración del riesgo.

Todo lo realizado hasta ahora es el camino para establecer las políticas de administración del riesgo, complementando así los resultados de SIGSI, justificando la declaración de aplicabilidad de los controles, por qué se escogieron dichos controles y los involucrados en estos procesos y procedimientos. Por esto también se deben definir las responsabilidades de estos actores y la periodicidad con la que se deben revisar los controles para mirar su correcta ejecución y en caso en que haya lugar realizar los cambios pertinentes para su mejora continua.

Las metodologías de evaluación de y tratamiento de riesgos son una cadena sucesiva de actividades realizadas con base en un marco de referencia que avala la seguridad en una empresa.

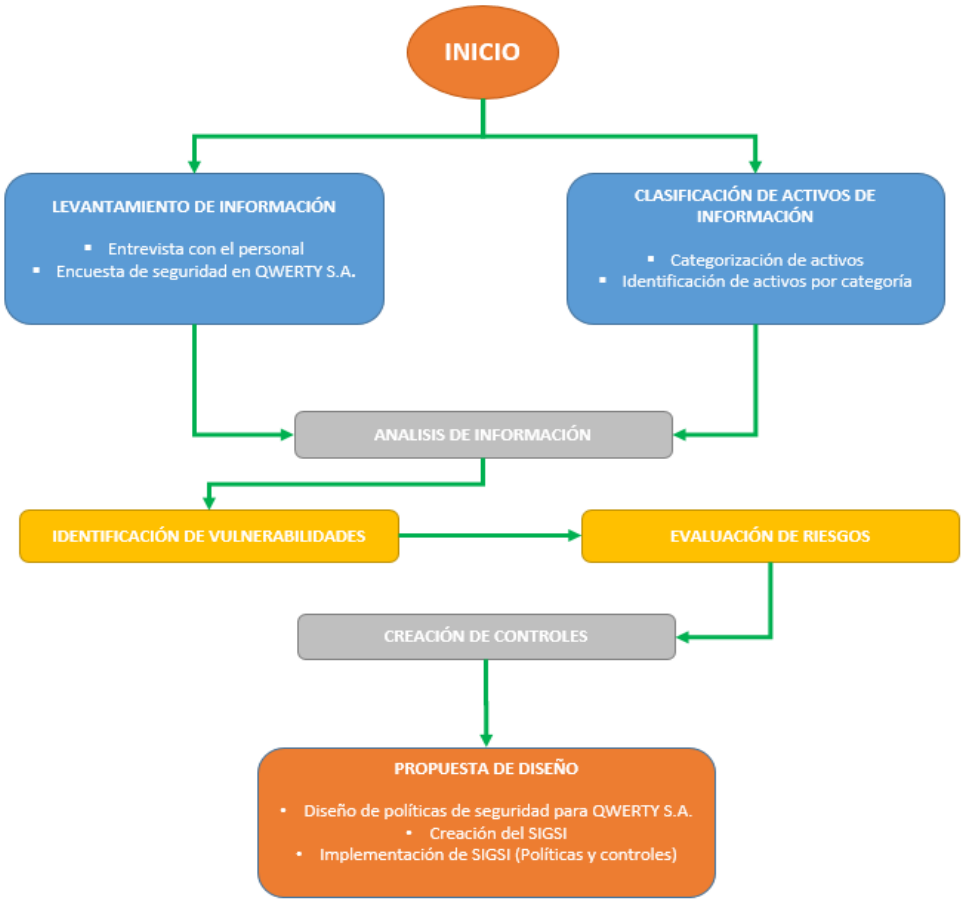
Estas metodologías se han diseñado con el fin de comprender como una empresa puede lograr sus objetivos y el beneficio de identificar sus riesgos y como gestionarlos. Desarrollándola en diferentes etapas que permitan concluir el estado en el que se encuentra la empresa. Por medio de darle un valor – ya que solo lo que se puede valorar y medir se puede controlar – a diferentes aspectos que ayudarán a identificar las amenazas y vulnerabilidades a las cuales está expuesta la empresa y lo acertado o débil de los controles que se implementan.

Todo esto con el fin de propender la protección de los pilares de la seguridad – disponibilidad, integridad y confidencialidad – de la información de QWERTY S.A.

Al poner en práctica esta metodología se quiere diseñar la base del estado de seguridad de la empresa identificando la etapa actual y lo necesario para la ejecución del SIGSI. El punto de partida de esta línea base será la medición inicial para entender la percepción que se tiene de seguridad por los empleados – especialmente la dependencia de sistemas – y su reacción a la implementación de este sistema de gestión de la seguridad informática.

Primariamente es necesario definir los pasos o fases del proyecto que se llevaran a cabo para lograr establecer el punto de partido y el desarrollo del modelo de este sistema de gestión de seguridad de la información.

Ilustración 7 Diagrama de flujo desarrollo del proyecto.



Fuente propia.

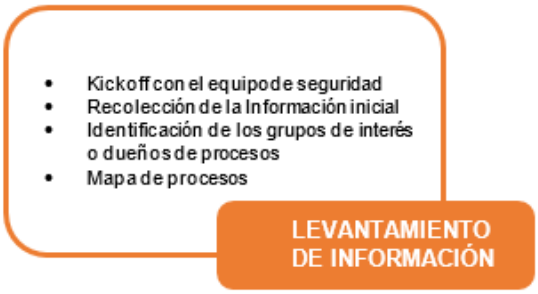
10.1.9. Levantamiento de Información

Se debe coleccionar la diferente información con cada una de las dependencias propias de la empresa – empezando por la dependencia de sistemas – a través de instrumentos de recolección como la entrevista y la encuesta identificando la percepción y la realidad del estado de la seguridad informática de la empresa para construir oportunidades de mejora. Además de realizar la categorización de los activos de la empresa QWERTY S.A. por medio de la observación y la identificación de estos activos categorizados.

La información recogida además de permitir la identificación de activos más importantes de la dependencia y su relación con los procesos – misionales o de apoyo – debe permitirnos reconocer el contexto para llevar la planeación de los objetivos de la empresa.

A las personas que se van a entrevistar, deben reconocer las partes esenciales de su empresa, el mapa de procesos, los manuales de seguridad de la información que existan, la metodología de riesgos, la identificación de amenazas y los planes de mitigación de los mismos, concibiendo esta información como la raíz para identificar la actualidad de la empresa en el ámbito de la seguridad.

Ilustración 8 Levantamiento de Información.



Fuente propia.

10.1.9.1. Revisión de Documentación

Es necesario revisar todos aquellos documentos –manuales, instructivos, procedimientos escritos, diapositivas – que puedan indicar un punto de partida acerca de la documentación que se tiene en QWERTY S.A. como principio de seguridad informática. A fin de determinar si es necesario un cambio, una actualización o una modificación para acoplar las políticas o procesos y sus controles a la actualidad y los riesgos propios de la época.

Esta revisión des muy importante, conllevando a entender el porqué de las medidas de seguridad adoptadas por la empresa, el sentido de pertenencia y conocimiento de estas medidas – procesos de seguridad – por el personal de la dependencia y de la empresa y de la responsabilidad de aplicarlas y mejorarlas.

10.1.9.2. Identificación de Amenazas

Es necesario realizar actividades que permitan conocer cómo se desarrollan los procedimientos en la dependencia, quienes están involucrados y/o ejecutan dichos procedimientos, los activos sobre los que se realizan y hasta la infraestructura y procesos que se ven involucrados durante la realización de la misma. Todo esto con el fin de poder determinar la posible causa de un riesgo o perjuicio de una mala educación para QWERTY S.A.

La calificación de estas evaluaciones ayudara a desplegar directrices de reducción de vulnerabilidades encontradas, para utilizar de mejor manera los recursos y los activos y la simplificación o automatización de los procesos que se operan con dichos elementos y los controles que se pueden aplicar para vigilar, reducir o mejorar en el tiempo su ciclo de vida.

Es por esto que para la identificación y clasificación de estas amenazas hay que cumplir con ciertas actividades como:

- Enlistar y categorizar los activos de la empresa, calificando su criticidad, sus supuestas falencias técnicas, operacionales y de gestión.
- Diseñar un cuadro comparativo con las amenazas potenciales, y sus inminentes formas de ataque.
- Estructurar acciones de reducción y mitigación para cada amenaza que se pueda volver real.

El resultado de esta evaluación ha de ser el SIGSI en su etapa inicial, a través de documentos, guías, listas, manuales y controles sugeridos que ayuden a la mitigación del riesgo y a mejorar la seguridad de la información.

10.1.9.3. Procesos y herramientas para la recolección de información

Para el desarrollo de la investigación se utilizará la metodología cuantitativa para realizar la correspondiente recolección de información con el fin de entender las condiciones actuales de seguridad en la que se encuentra la empresa.

La población a tomar es global ya que es toda la empresa QWERTY S.A.

La muestra va ser en relación a los activos de la empresa e ítems de configuración y a nivel de personal se tomará el 50% del personal, esto quiere decir a 60 personas escogidas de las diferentes áreas para cubrir todos los procesos y procedimientos de la empresa.

Las técnicas de recolección de información que se utilizara son encuestas al personal seleccionado donde se realizaran a través de la división de grupos de empleados, siendo los primeros operativos y los segundos administrativos.

Esto para propender la identificación de vulnerabilidades, amenazas y riegos de una manera más asertiva y precisa de la situación de seguridad actual de la empresa

Fuentes primarias

Mediante las encuestas y las entrevistas se analizará de manera oportuna cada una de los momentos que evidencian la vulnerabilidad en la empresa y de esta manera definir la solución de acuerdo a las mejores prácticas para dicha situación con base

en la norma ISO 27001:2013 y el marco de referencia MAGERIT en concordancia con las necesidades de la empresa QWERTY S.A.

Fuentes secundarias

Es indispensable que la investigación tenga material de apoyo como contenido multimedia, libros, ensayos científicos, páginas web de consulta, conferencias, tendencias y toda aquella información que sirva como herramienta y soporte a la solución de cada uno de los objetivos específicos planteados en el proyecto.

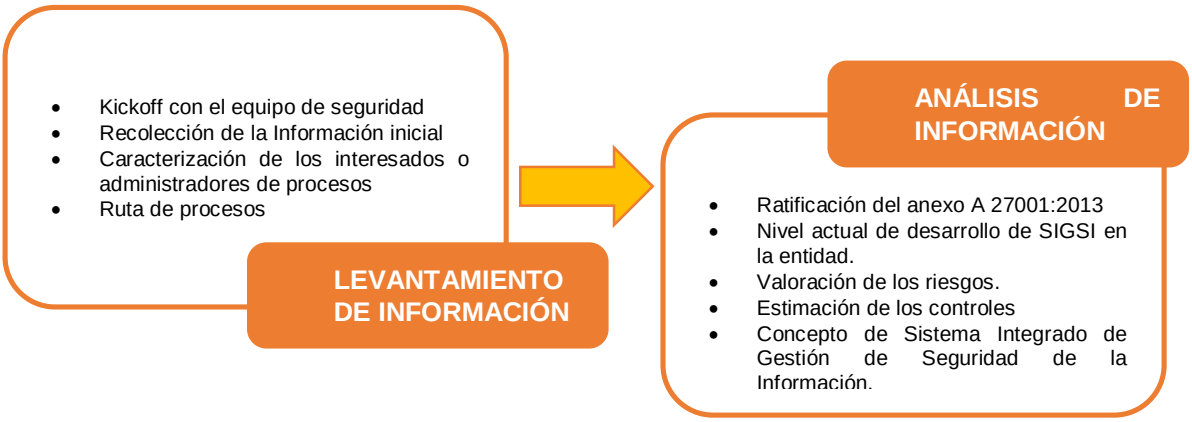
10.1.10. Análisis de la Información

Examinar la información recopilada en la fase anterior identificando las diferentes vulnerabilidades que la empresa posee a nivel de seguridad informática y seguridad de la información, así como dando a conocer los diversos riesgos a los que se encuentra expuesto por estar propenso a las amenazas que traen consigo estas vulnerabilidades.

Es necesario identificar estas amenazas como debilidades al no tener o tener precariamente implementado el modelo de seguridad actual de QWERTY S.A. y los controles que se tengas para ser reforzados o creados en la ausencia de estos

Para esto, la empresa debe revisar bajo de uno o varios marcos de trabajo (considerable el apéndice A de la ISO 27001:2013, el ciclo de vida de Deming) el nivel de avance de QWERTY S.A. para conseguir un punto inicial de madurez del concepto de seguridad integrado de los sistemas de información.

Ilustración 9 Etapas de levantamiento de Información y Análisis de Información.



Fuente propia.

Para realizar este análisis de información es necesario aplicar pruebas a la luz del anexo A, por medio de técnicas e instrumentos para comprobar el nivel de seguridad de QWERTY S.A., indispensablemente las pruebas sobre empleados y/o usuarios, procesos, procedimientos, aplicaciones y sistemas de la empresa para encontrar las vulnerabilidades.

10.1.10.1. Pruebas de Efectividad

Existen tres tipos de pruebas de efectividad, de acuerdo al conocimiento de los sistemas o infraestructuras de un objetivo a ser atacado.

- **Pruebas Con Desconocimiento por Completo Del Entorno**: Esta prueba se basará en un ataque real externo, sin conocimiento de la empresa o infraestructura.
- **Pruebas Con Desconocimiento Relevante Del Entorno:** Esta prueba tiene tipos de ataques como pentesting, se ha de conocer ciertas cosas del ambiente como tipo de infraestructura, algo del hardware o software de la

empresa y se maneja cierta información que ayuda a realizar el ataque. Simula una persona que ya ha traspasado las primeras barreras de la seguridad.

- **Pruebas Con Conocimiento Completo Del Entorno:** Es cuando el hacker tiene toda la información relacionada al sistema objetivo del ataque. Es generalmente para temas de auditoría.[6]

Para el caso del proyecto, se trabajarán las <<Pruebas con conocimiento Nulo Del Entorno>> dado que no se tiene mayor información que la proporcionada sobre la empresa en relación a la dependencia de sistemas.

10.1.10.2. Alcance de las pruebas

Todas las pruebas deben tener un entorno, un contorno y unas limitaciones, dado que extender o no realizar estas pruebas en ambientes controlados pueden ocasionar más males que remedios en la empresa. Es bueno para limitar este alcance definir los siguientes puntos:

1. **Plan de trabajo:** Tiempo en el que se realizarán las pruebas, los sistemas o aplicaciones involucradas sobre los que se realizarán las pruebas y los rollback en caso de dañar o afectar algo indebido.
2. **Insumos:** personal, ventanas de tiempo, infraestructura, equipos y otros objetos necesarios para las pruebas.
3. **Responsables:** Encargados de efectuar las pruebas
4. **Afectaciones:** Debe definirse los horarios y que tanto podría afectar la empresa si las pruebas se realizan en horario laboral, fin de mes entre otros.

[6] 37. MINTIC. Guía 1 – Metodológica de Pruebas de Efectividad Bogotá D.C.: Ministerio, 2016, 28 p. Disponible en Internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf

5. **Sanciones:** En caso de no respetarse el alcance de las pruebas, se debe medir los gastos o sanciones disciplinarias que consigo traiga no cumplir con este alcance

10.1.10.3. Ejecución de las pruebas de efectividad

Existen pautas que deben llevarse paso a paso para realizar estas pruebas de efectividad.

a. Contextualización:

Es necesario identificar que se quiere lograr con las pruebas y cuáles van a ser los métodos y procesos para alcanzar estos objetivos, esto se puede hacer con preguntas que orienten a conocer lo que se quiere:

- ¿Cuáles serán los objetivos a evaluar?
- ¿Se harán las pruebas en horario hábil, no hábil o fin de semana?
- Si es vulnerado el sistema, que tipo de acciones posteriores deben hacerse (pruebas de vulnerabilidades, escalamiento de privilegios entre otros)
- Definir las fechas de las actividades
- ¿Hace parte la ingeniería social de estos procedimientos de manera válida para ser ejecutados?

Es prudente recordar que estas pruebas no solo deben llevar como objetivo identificar las amenazas de sistemas, activo o aplicación, sino que están enfocadas al bien mayor de reconocer los *riesgos de seguridad de la información y si los controles que se tienen son efectivos para la mitigación de los mismos.* Propendiendo tomar medidas efectivas/proactivas para reducir estos riesgos.

b. Reconocimiento del Objetivo

Posterior a la definición del alcance de las pruebas, es preferible acceder a tanta información como sea posible, a través de algunos métodos (enfocados a los sistemas de información)

- **NO ACTIVO:** No tiene acceso a la empresa. Es teórico recopilando información de otras partes que pueden ser muy similares a nuestra infraestructura.
- **SEMI-ACTIVO:** método realizado en la empresa, con simulación de tráfico, pero sin ser intrusivo para los sistemas.
- **ACTIVO:** Método realizado en la empresa, siendo completamente intrusivos a los sistemas de la misma, se realizan actividades como la verificación de puertos, revisión de vulnerabilidades de puertos, intersección de directorios, archivos y robo de información.

c. Modelado de Amenazas

Amenazas a la entidad: Busca definir el riesgo en la empresa y el estado de los activos que causan mayor impacto al verse afectados. ¿Qué pasa sí?

En dicha gestión es necesario incluir este tipo de activos:

- Datos De Empleados, clientes, usuarios, proveedores entre otros.
- Sistemas De Información privada y no privada
- Información Financiera y De Mercadeo
- Políticas, Planes y Procedimientos, e Información Técnica (Diseños de infraestructura de hardware y software, registros de configuración del sistema, cuentas de usuarios normales y con privilegios)
- Personas

- Información de los procesos de negocio.
- Información de software desarrollado (Investigación, desarrollo y patentes entre otros.)

Enfocado en el atacante: dirigido sobre aquellos personajes que podrían lanzar un ataque a la entidad.

Tabla 8 Posibles personajes que podrían lanzar un ataque a la organización

PERSONAJES	DESCRIPCIÓN
INTERNOS	Administradores, ejecutivos, de infraestructura, empleados, ingenieros, técnicos, desarrolladores, personal de soporte y personal remoto, así como contratistas
EXTERNOS	Sociedades, competidores, proveedores, crimen organizado, hackers, entre otros.

Fuente: propia

d. Evaluación de Vulnerabilidades

Por medio de este análisis se quiere encontrar todas las falencias y debilidades que se tengan en los sistemas y aplicaciones de QWERTY S.A. y puedan ser aprovechadas por las amenazas hacía la entidad o hacía los atacantes, dependiendo del enfoque que se tenga y a través de dos tipos de análisis, ya sea a un host (servidor) en específico o a toda una granja de servidores (servicio o entidad completa)

Análisis activo: se debe tener contacto directo con el objeto a probar. Se realiza automático o manual. Comúnmente se llama automático cuando se involucra un software que ayude a realizar los procedimientos sobre el objeto en cuestión.

Análisis pasivo: este método busca realizar análisis a través de archivos publicados en internet, evidencias registradas o investigaciones similares que ayuden a identificar las mismas amenazas. Se puede y comúnmente se hace a través de la investigación donde se obtiene información a través de las siguientes fuentes:

- Registros de las vulnerabilidades y amenazas conocidas. (CVE)
- Alarmas y avisos de proveedores de las casas de software.
- Bases de datos de tipos de ataques.
- Contraseñas por defecto de software o lenguajes específicos.
- Hardening para asegurar los sistemas operativos, cerrando accesos y puertos TCP/UDP.
- Desarrollo de acciones de prueba y error en máquinas virtuales y ambientes duplicados Honeypots.

e. Reporte:

Se prepara documento con las pruebas realizadas, para exponer los resultados de cada una de las etapas, enunciando la justificación pertinente de los resultados obtenidos. Para el reporte es necesario tener en cuenta la audiencia a la que se le va a presentar, para que el nivel de lenguaje técnico y reporte específico sea directamente proporcional a la audiencia que se le presenta.

Reporte Gerencial: Un reporte menos detallado, con introducción, objetivos y resultados de las pruebas, clasificación del riesgo y principio de las vulnerabilidades encontradas, a través de servidores no parchados, servicios activos no utilizados, puertos abiertos innecesarios o arquitecturas inseguras.

Reporte Técnico: este reporte contiene la información de un reporte gerencial, pero se aclaran y especifican detalles más importantes de forma técnica, ya que quienes

poseen este reporte son aquellas personas que pueden ayudar a subsanar las vulnerabilidades encontradas.

Posterior a los reportes, se espera que la empresa QWERTY S.A. tome en consideración las actividades propuestas para mitigar y reducir las amenazas y las vulnerabilidades a las que estén expuestos.

10.1.10.4. Clases de análisis

Con la información recolectada se procederá a realizar el análisis correspondiente para evaluar el estado actual de la seguridad informática de la empresa y así mismo listar las políticas y controles que se deberán aplicar para implementar el sistema de gestión de la seguridad.

Creación de SIGSI: como última etapa está la creación de controles que hagan parte de la propuesta del *sistema integrado de gestión de la seguridad informática* el cual tendrá los controles y las políticas de seguridad que requiere la empresa a ser diseñados, implementados y evaluados para el mejoramiento continuo de este nuevo sistema.

10.2. INVENTARIO DE ACTIVOS

En principio, se contaba con el listado de activos que poseía la entidad, el cual se relaciona a continuación, aportado por la empresa QWERTY S.A. y luego se realizó una visita a las instalaciones de la empresa para realizar las encuestas y las entrevistas a su personal administrativo y operativo para conocer su percepción y acciones en relación a la seguridad de su información.

Tabla 9 Activos de QWERTY S.A.

INVENTARIO DE ACTIVOS						
Identificador	**Nombre**	**Descripción**	**Responsable**	**Tipo**	**Ubicación**	**Crítico**
ID_0001	Página Web - Joomla versión 2.5, plan máximo Ver ficha técnica del proveedor	Servicio contratado con la empresa Godaddy.com La página web tiene como objeto la publicación de contenido relacionado con el modelo negocio. Está construida a partir del sistema gestor de contenidos dinámicos Joomla versión 2.5 El hospedaje web la infraestructura del servidor es Apache, PHP, MySQL.	externo Godaddy	Servidor (físico)	externo	Sí
ID_0002	Servicio de Correo Electrónico	Brindar a la empresa el servicio de mensajería electrónica	Dpto. sistemas. .	Router (físico)	datacenter	si
ID_0003	Servicio de gestión y mantenimiento	Dar Soporte a las a las salas de Cómputo	Dpto. sistemas. .	Servidor (físico)	Dpto. soporte	Sí
ID_0004	Servicio de Gestión de usuarios y contraseñas	Gestionar el ingreso a los sistemas de los usuarios internos y externos de la empresa	Dpto. sistemas.	servicio	Dpto. soporte	si
ID_0005	Servidor de Impresión: Servidor marca Dell en torre PowerEdge T440 Ver ficha técnica	Equipo de cómputo que conecta dos impresoras	Dpto. sistemas. .	Servidor (físico)	datacenter	si

ID_0006	Impresora HP LaserJet Enterprise serie 600 Ver ficha técnica	Activo que permite la concurrencia de hasta 25 usuarios y el volumen mensual de impresión es de 200 a 25000 páginas	nómina y facturación	Impresora (físico)	Dpto. nomina	no
ID_0007	Impresora SMART MultiXpress M4370LX Ver ficha técnica	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.	nómina y facturación	Impresora (físico)	Dpto. nomina	no
ID_0008	Servidor de archivos FTP: Servidor marca Dell en torre PowerEdge T130 Ver ficha técnica	Equipo de cómputo que tiene como función el almacenamiento y la administración de los archivos que se están generando en el interior de la organización como son: Digitalización de documento de entrada y de salida, audios generados en reuniones, asambleas y otro tipo de encuentros, video, generados por docentes y funcionarios Dentro de las políticas de uso, para este servidor solo pueden tener acceso las personas autorizadas para los fines correspondientes	Dpto. sistemas.	Servidor (físico)	datacenter	si
ID_0009	Servidor DHCP Servidor marca Dell en torre PowerEdge T440 Ver ficha técnica	Servidor que asigna y administra de forma dinámica el direccionamiento dentro de la organización	Dpto. sistemas.	Servidor (físico)	datacenter	si
ID_0010	Equipos de cómputo para gestión del desarrollo tecnológico Sistema Operativo Windows 10 Pro.	Equipos de cómputo donde se gestiona información online relacionada con el desarrollo del objeto social Presupuesto • Proveedores • Órdenes de compra • Inventarios	Dpto. infraestructura	pc (físico)	Dpto. infraestructura	no
ID_0011	Cortafuegos Cisco ASA 5505 Ver ficha técnica	Sistema de protección Sistema de seguridad que está protegiendo a la red de datos, de intrusiones que se puedan presentar en la red,	Dpto. sistemas.	firwall (físico)	datacenter	si

ID_0012	Punto de acceso alámbrico (Hub)	Dispositivos de red encargados de la interconexión de la red de datos	Dpto. sistemas.	hub (físico)	todos los dpto	si
ID_0013	Switches cisco catalyst 2960 Ver ficha técnica	Dispositivos de red encargados de la interconexión de la red de datos	Dpto. sistemas.	switch (físico)	datacenter	si
ID_0014	Técnicos de mantenimiento	Personal técnico encargado de realizar el mantenimiento preventivo a los equipos de cómputo	Dpto. soporte	personal	Dpto. soporte	si
ID_0015	Teléfonos IP	Sistema de comunicación a través de teléfonos Voz IP, que comunica las oficinas y departamentos del centro	centro	servicio	todos los dpto	no
ID_0016	Puntos de acceso inalámbrico	Puntos de acceso al servicio de Internet del campus universitario	Dpto. sistemas.	servicio	todos los dpto	si
ID_0017	Equipos de cómputo Sistema Operativo Windows 10 pro.	Equipos destinados para el desarrollo del objeto social	control y seguimiento	pc (físico)	Dpto. control y seguimiento	si
ID_0018	Equipos de cómputo Sistema Operativo Windows 10 pro.	Equipos destinados para el desarrollo del objeto social	pruebas y software	pc (físico)	Dpto. pruebas y software	
ID_0019	Servidor de nómina y facturación Servidor marca Dell en torre PowerEdge T440 Ver ficha técnica	Plataforma de desarrollo propio. Tiene como función el almacenamiento y la administración de la nómina y facturación de la empresa QWERTY S.A. Características de servidor Apache 2.4.25 PHP 5.6.30 - 7.1.1 MySQL 5.7.17 phpMyAdmin 4.6.6	Dpto. sistemas.	Servidor (físico)	datacenter	si
ID_0020	app] Apache 2.4.25	Aplicación que permite la presentación de contenido web en servidores de contenido en internet	nómina y facturación	aplicación (software)	datacenter	si
ID_0021	[app] PHP 5.6.30 - 7.1.1	Procesador de hipertexto que permite la visualización del código escrito en el lenguaje PHP en el navegador del cliente.	nómina y facturación	aplicación (software)	datacenter	si
ID_0022	dbms] MySQL 5.7.17	Base de datos libre en lenguaje MySQL	nómina y facturación	aplicación (software)	datacenter	si

ID_0023	app] phpMyAdmin 4.6.6	Administrador de base de datos de lenguaje MySQL de interfaz gráfica	nómina y facturación	aplicación (software)	datacenter	si
ID_0024	[sub] Helisa Cloud Plus	Software de gestión contable y de nómina	nomina y facturación	aplicación (software)	datacenter	si
ID_0025	[prov] Google - Proveedor Correo Electrónico	Proveedor del servicio de Correo electrónico de la entidad	externo Godaddy	aplicación (software)	externo	si
ID_0026	[Internet] Canal de ancho de banda 25 Megas dedicado	Servicio de interconexión para la navegación por la red de redes en canal dedicado.	Dpto. sistemas.	servicio	Dpto. sistemas.	si
ID_0027	[LAN] red local	Servicio de interconexión de equipos de cómputo dentro de las instalaciones de la entidad	Dpto. infraestructura	Dpto. infraestructura	Dpto. infraestructura	si
ID_0028	av] antivirus	Servicio de protección contra software malicioso y amenazas	Dpto. sistemas.	aplicación (software)	Dpto. sistemas.	si
ID_0029	[files] [r] Documentos digitalizados de entrada y de salida	Archivos de la entidad que manejan los usuarios.	Dpto. sistemas.	aplicación (software)	datacenter	si
ID_0030	[files] [r] Audios de reuniones y asambleas	Archivos multimedia que se tienen en los diferentes equipos de cómputo de la empresa	Dpto. sistemas.	aplicación (software)	datacenter	si
ID_0031	files] [r] Vídeos generados por empleados y funcionarios	Archivos multimedia que se tienen en los diferentes equipos de cómputo de la empresa	Dpto. sistemas.	aplicación (software)	datacenter	si
ID_0032	[int] [r] Base de datos del Sistema de empleados	Sistema de Gestión y administración de datos con información pública y/o privada de usuarios, proveedores y clientes de la empresa.	Dpto. sistemas.	aplicación (software)	datacenter	si
ID_0033	int] [r] Datos Personales	Datos de empleados, proveedores o clientes de la entidad.	Dpto. sistemas.	aplicación (software)	datacenter	si
ID_0034	[int] [r] Base de datos del Sistema de suministros	Datos de suministros de la empresa.	Dpto. sistemas.	aplicación (software)	datacenter	si

ID_0035	[local] Oficina de Infraestructura	Instalaciones de la oficina de la dependencia de sistemas	Dpto. sistemas.	infraestructura	Dpto. sistemas.	si
ID_0036	[local] Dependencia de nómina y facturación	Instalaciones de la oficina de Contabilidad de la empresa	Dpto. nómina y facturación	infraestructura	Dpto. nómina y facturación	si
ID_0037	[local] Dependencia de sistemas	Instalaciones de las oficinas de sistemas de la empresa	Dpto. sistemas.	infraestructura	Dpto. sistemas.	si
ID_0038	[local] Antigua oficina de sistemas	Instalaciones de las oficinas de sistemas de la empresa donde se encuentra ubicado el Data Center de la empresa	Dpto. sistemas.	infraestructura	Dpto. sistemas.	si
ID_0039	[local] Dependencia Directiva y administrativa	Instalaciones de la alta gerencia de la empresa QWERTY S.A.	Dpto. directiva y administrativa	infraestructura	Dpto. directiva y administrativa	si
ID_0040	[local] Oficina de Desarrollo Tecnológico	Instalaciones de las oficinas de desarrollo de software de la entidad	Dpto. desarrollo tecnológico	infraestructura	Dpto. desarrollo tecnológico	si
ID_0041	local] Oficina de Prueba de Software	Instalaciones de las oficinas de pruebas de software desarrollado de la empresa.	Dpto. pruebas y software	infraestructura	Dpto. pruebas y software	si
ID_0042	[local] Data Center QWERTY S.A.	Instalaciones donde se encuentran los servicios de la empresa	Dpto. sistemas.	infraestructura	datacenter	si
ID_0043	prov] Empresa Godaddy - Proveedor de hospedaje web	Proveedor de alojamiento de la página web de la entidad	externo Godaddy	aplicación (software)	externo	si
ID_0044	[local] Oficina de Soporte	Instalaciones de la oficina de soporte a software de la empresa	Dpto. soporte	infraestructura	Dpto. soporte	si
ID_0045	[adm] administradores de sistemas	Personal capacitado para desempeñarse como administrador de los sistemas de la empresa	Dpto. sistemas.	personal	Dpto. sistemas.	si
ID_0046	[adm] administradores de comunicaciones	Personal capacitado para desempeñarse como administrador de comunicaciones y redes de la empresa	Dpto. sistemas.	personal	Dpto. sistemas.	si
ID_0047	[adm] administradores de BBDD	Personal capacitado para desempeñar las funciones de administrador de los	Dpto. sistemas.	personal	Dpto. sistemas.	si

		sistemas de bases de datos de la empresa				
ID_0048	[adm] administradores de seguridad	Personal con el conocimiento para desempeñar funciones de administrador de seguridad de la empresa.	Dpto. sistemas.	personal	Dpto. sistemas.	si
ID_0049	sof] Sistemas Operativo Windows 10	Sistema operativo de los equipos de cómputo de la empresa	Dpto. sistemas.	aplicación (software)	Dpto. sistemas.	si

Fuente: propia basada en la investigación

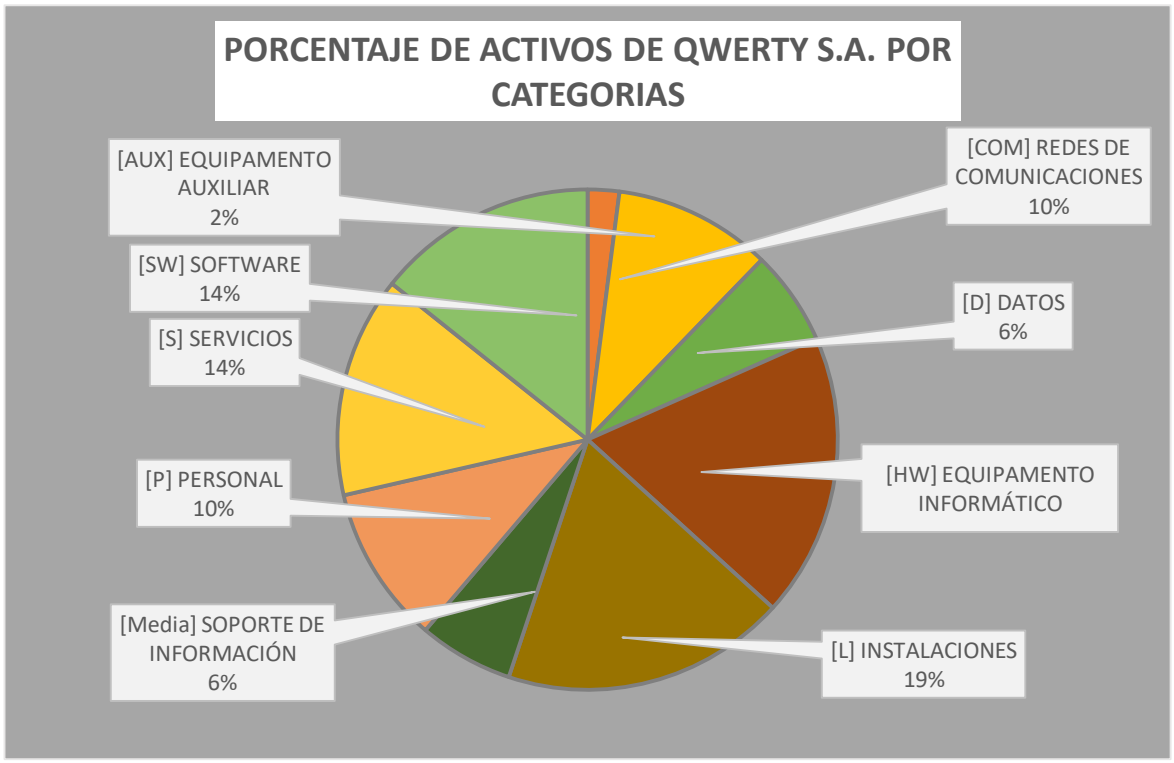
Para analizar estos activos se realiza un análisis de los mismos bajo la metodología Magerit, para categorizar cada uno de los activos en diferentes dominios.

Tabla 10 Cantidad de Activos por categoría

TIPO DE ACTIVOS	CANTIDAD
[AUX] EQUIPAMENTO AUXILIAR	1
[COM] REDES DE COMUNICACIONES	5
[D] DATOS	3
[HW] EQUIPAMENTO INFORMÁTICO	9
[L] INSTALACIONES	9
[Media] SOPORTE DE INFORMACIÓN	3
[P] PERSONAL	5
[S] SERVICIOS	7
[SW] SOFTWARE	7
Total, general	**49**

Fuente: propia

Ilustración 10 Porcentaje de activos por categoría.

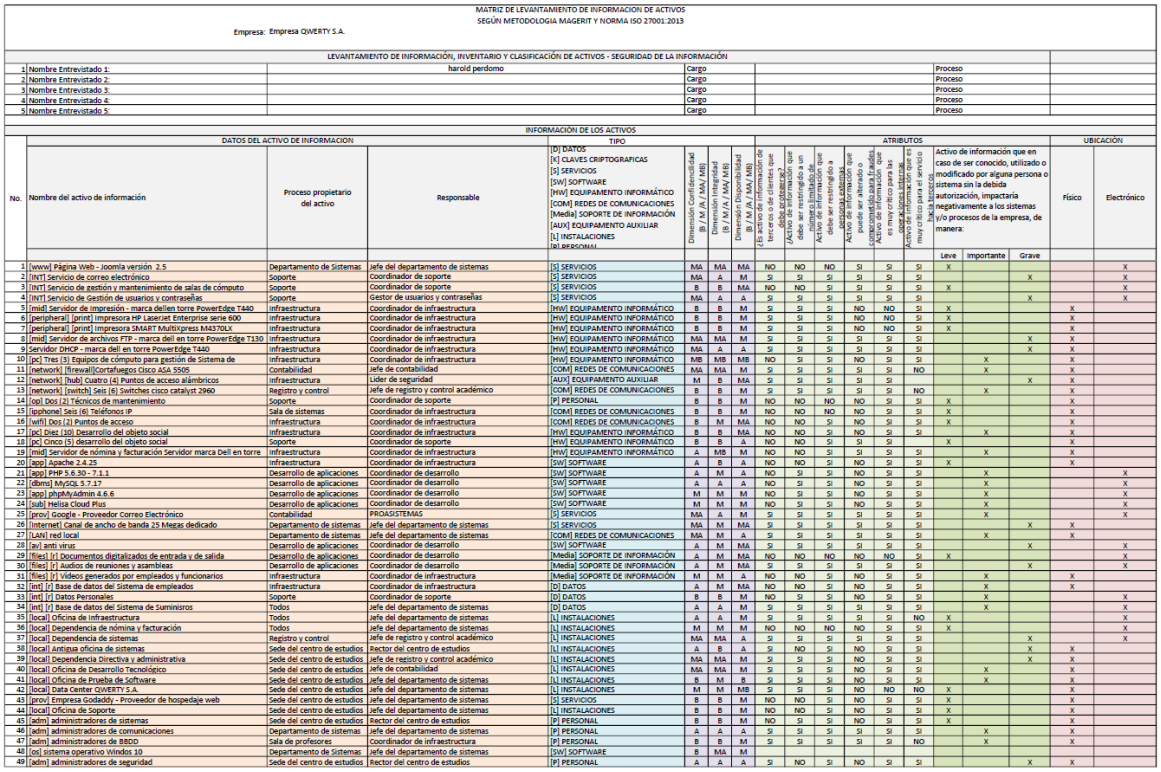


Fuente propia.

La mayor parte de los activos de la empresa los representa los dispositivos de cómputo informático (servidores y equipos de cómputo de la empresa) con el 19% al igual que las instalaciones que tiene la empresa. Seguido del software con el 14%, es por esto que tanto los activos físicos como electrónicos de la empresa, son tal vez los más esenciales para la empresa. Dado que solo existe una sede de la empresa, todas las instalaciones (oficinas) que están allí son esenciales, ya que en caso de que una amenaza –de orden natural, por ejemplo- se llegara a presentar, la empresa no tendría desde donde operar si sus servicios se ven afectados.

A continuación, se hace una clasificación cuantitativa de la criticidad del activo con base en su degradación y las encuestas realizadas al personal de la empresa bajo la metodología MAGERIT en sus dimensiones cualitativas y cuantitativas.

Ilustración 11 Clasificación cualitativa de los activos.



MATRIZ DE LEVANTAMIENTO DE INFORMACION DE ACTIVOS
SEGÚN METODOLOGIA MAGERIT Y NORMA ISO 27001:2013

Empresa: Empresa QWERTY S.A.

LEVANTAMIENTO DE INFORMACIÓN, INVENTARIO Y CLASIFICACIÓN DE ACTIVOS - SEGURIDAD DE LA INFORMACIÓN

1	Nombre Entrevistado 1:	harold perdomo	Cargo		Proceso
2	Nombre Entrevistado 2:		Cargo		Proceso
3	Nombre Entrevistado 3:		Cargo		Proceso
4	Nombre Entrevistado 4:		Cargo		Proceso
5	Nombre Entrevistado 5:		Cargo		Proceso

INFORMACIÓN DE LOS ACTIVOS

No.	DATOS DEL ACTIVO DE INFORMACION			TIPO	ATRIBUTOS										UBICACIÓN	
	Nombre del activo de información	Proceso propietario del activo	Responsable	[D] DATOS [K] CLAVES CRIPTOGRAFICAS [S] SERVICIOS [SW] SOFTWARE [HW] EQUIPAMIENTO INFORMÁTICO [COM] REDES DE COMUNICACIONES [Media] SOPORTE DE INFORMACIÓN [AUX] EQUIPAMENTO AUXILIAR [L] INSTALACIONES [P] PERSONAL	Dimensión Confidencialidad B / M / A / MA / MB	Dimensión Integridad B / M / A / MA / MB	Dimensión Disponibilidad B / M / A / MA / MB	¿Es activo de información de terceros o de clientes que debe ser protegido?	¿Activo de información que debe ser restringido a un número limitado de personas?	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes	Activo de información que es muy crítico para la operación	Activo de información que no puede ser conocido por 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:			Físico	Electrónico
															Leve	Importante	Grave		
1	[www] Página Web - Joomla versión 2.5	Departamento de Sistemas	Jefe del departamento de sistemas	[S] SERVICIOS	MA	MA	MA	NO	NO	NO	SI	SI	SI	X				X
2	[INT] Servicio de correo electrónico	Soporte	Coordinador de soporte	[S] SERVICIOS	MA	A	M	SI	SI	SI	SI	SI	SI			X		X
3	[INT] Servicio de gestión y mantenimiento de salas de cómputo	Soporte	Coordinador de soporte	[S] SERVICIOS	B	B	MA	NO	NO	SI	SI	SI	SI	X				X
4	[INT] Servicio de Gestión de usuarios y contraseñas	Soporte	Gestor de usuarios y contraseñas	[S] SERVICIOS	MA	A	A	SI	SI	SI	SI	SI	SI					X
5	[mid] Servidor de impresión - marca dellen torre PowerEdge T440	infraestructura	Coordinador de infraestructura	[HW] EQUIPAMIENTO INFORMÁTICO	B	B	M	SI	SI	SI	NO	NO	SI	X					X
6	[peripheral] [print] Impresora HP LaserJet Enterprise serie 600	infraestructura	Coordinador de infraestructura	[HW] EQUIPAMIENTO INFORMÁTICO	B	B	M	SI	SI	SI	NO	NO	SI	X					X
7	[peripheral] [print] Impresora SMART MultiXpress M4370LX	infraestructura	Coordinador de infraestructura	[HW] EQUIPAMIENTO INFORMÁTICO	B	B	M	SI	SI	SI	NO	NO	SI	X					X
8	[mid] Servidor de archivos FTP - marca dell en torre PowerEdge T130	infraestructura	Coordinador de infraestructura	[HW] EQUIPAMIENTO INFORMÁTICO	MA	MA	M	SI	SI	SI	SI	SI	SI				X		X
9	Servidor DHCP - marca dell en torre PowerEdge T440	infraestructura	Coordinador de infraestructura	[HW] EQUIPAMIENTO INFORMÁTICO	MA	A	A	SI	SI	SI	SI	SI	SI				X		X
10	[pc] Tres (3) Equipos de cómputo para gestión de Sistema de	infraestructura	Coordinador de infraestructura	[HW] EQUIPAMIENTO INFORMÁTICO	MB	MB	MB	NO	SI	SI	NO	SI	SI			X			X
11	[network] [firewall]Cortafuegos Cisco ASA 5505	Contabilidad	Jefe de contabilidad	[COM] REDES DE COMUNICACIONES	MA	MA	M	SI	SI	SI	SI	SI	NO			X			X
12	[network] [hub] Cuatro (4) Puntos de acceso alámbricos	infraestructura	Lider de seguridad	[AUX] EQUIPAMENTO AUXILIAR	M	B	MA	SI	SI	SI	SI	SI					X		X
13	[network] [switch] Seis (6) Switches cisco catalyst 2960	Registro y control	Jefe de registro y control académico	[COM] REDES DE COMUNICACIONES	B	B	M	SI	SI	SI	SI	SI	NO			X			X
14	[op] Dos (2) Técnicos de mantenimiento	Soporte	Coordinador de soporte	[P] PERSONAL	B	B	M	NO	NO	NO	NO	SI	SI	X					X
15	[ipphone] Seis (6) Teléfonos IP	Sala de sistemas	Coordinador de infraestructura	[COM] REDES DE COMUNICACIONES	B	B	M	NO	NO	NO	NO	SI	SI	X					X
16	[wifi] Dos (2) Puntos de acceso	infraestructura	Coordinador de infraestructura	[COM] REDES DE COMUNICACIONES	B	M	MA	NO	NO	SI	NO	SI	SI	X					X
17	[pc] Diez (10) Desarrollo del objeto social	infraestructura	Coordinador de infraestructura	[HW] EQUIPAMIENTO INFORMÁTICO	B	B	MA	NO	NO	SI	NO	SI	SI			X			X
18	[pc] Cinco (5) desarrollo del objeto social	Soporte	Coordinador de soporte	[HW] EQUIPAMIENTO INFORMÁTICO	B	B	A	NO	NO	SI	SI	SI		X					X
19	[mid] Servidor de nómina y facturación Servidor marca Dell en torre	infraestructura	Coordinador de infraestructura	[HW] EQUIPAMIENTO INFORMÁTICO	A	MB	M	NO	NO	SI	SI	SI	SI			X			X
20	[app] Apache 2.4.25	infraestructura	Coordinador de infraestructura	[SW] SOFTWARE	A	B	A	NO	NO	SI	NO	SI	SI	X					X
21	[app] PHP 5.6.30 - 7.1.1	Desarrollo de aplicaciones	Coordinador de desarrollo	[SW] SOFTWARE	A	M	A	NO	SI	SI	NO	SI	SI			X			X
22	[dbms] MySQL 5.7.17	Desarrollo de aplicaciones	Coordinador de desarrollo	[SW] SOFTWARE	A	A	A	NO	SI	SI	NO	SI	SI			X			X
23	[app] phpMyAdmin 4.6.6	Desarrollo de aplicaciones	Coordinador de desarrollo	[SW] SOFTWARE	M	M	M	NO	SI	SI	NO	SI	SI			X			X
24	[sub] Helisa Cloud Plus	Desarrollo de aplicaciones	Coordinador de desarrollo	[SW] SOFTWARE	M	M	M	NO	SI	SI	NO	SI	SI			X			X
25	[prov] Google - Proveedor Correo Electrónico	Contabilidad	PROASISTEMAS	[S] SERVICIOS	MA	A	M	SI	SI	SI	SI	SI	SI			X			X
26	[Internet] Canal de ancho de banda 25 Megas dedicado	Departamento de sistemas	Jefe del departamento de sistemas	[S] SERVICIOS	MA	M	MA	SI	SI	SI	SI	SI	SI				X	X	
27	[LAN] red local	Departamento de sistemas	Jefe del departamento de sistemas	[COM] REDES DE COMUNICACIONES	MA	M	A	SI	SI	SI	SI	SI	SI			X		X	
28	[av] anti virus	Desarrollo de aplicaciones	Coordinador de desarrollo	[SW] SOFTWARE	A	M	MA	SI	SI	SI	SI	SI	SI				X		X
29	[files] [r] Documentos digitalizados de entrada y de salida	Desarrollo de aplicaciones	Coordinador de desarrollo	[Media] SOPORTE DE INFORMACIÓN	A	M	MA	NO	NO	NO	NO	NO	SI	X					X
30	[files] [r] Audios de reuniones y asambleas	Desarrollo de aplicaciones	Coordinador de desarrollo	[Media] SOPORTE DE INFORMACIÓN	A	M	MA	SI	SI	SI	SI	SI	SI				X		X
31	[files] [r] Videos generados por empleados y funcionarios	infraestructura	Coordinador de infraestructura	[Media] SOPORTE DE INFORMACIÓN	M	M	A	NO	NO	SI	NO	SI	SI			X		X	
32	[int] [r] Base de datos del Sistema de empleados	infraestructura	Coordinador de infraestructura	[D] DATOS	A	M	MA	NO	NO	SI	NO	SI	SI			X		X	
33	[int] [r] Datos Personales	Soporte	Coordinador de soporte	[D] DATOS	B	B	M	NO	SI	SI	NO	SI	SI			X			X
34	[int] [r] Base de datos del Sistema de Suministros	Todos	Jefe del departamento de sistemas	[D] DATOS	A	A	M	SI	SI	SI	SI	SI	SI			X			X
35	[local] Oficina de Infraestructura	Todos	Jefe del departamento de sistemas	[L] INSTALACIONES	A	A	M	SI	SI	SI	SI	SI	NO	X					X
36	[local] Dependencia de nómina y facturación	Todos	Jefe del departamento de sistemas	[L] INSTALACIONES	M	M	M	NO	NO	NO	NO	SI	SI	X					X
37	[local] Dependencia de sistemas	Registro y control	Jefe de registro y control académico	[L] INSTALACIONES	MA	MA	A	SI	SI	SI	SI	SI	SI				X		X
38	[local] Antigua oficina de sistemas	Sede del centro de estudios	Rector del centro de estudios	[L] INSTALACIONES	A	B	A	SI	NO	SI	NO	SI	SI				X	X	
39	[local] Dependencia Directiva y administrativa	Sede del centro de estudios	Jefe de registro y control académico	[L] INSTALACIONES	MA	MA	M	SI	SI	SI	NO	SI	SI				X	X	
40	[local] Oficina de Desarrollo Tecnológico	Sede del centro de estudios	Jefe de contabilidad	[L] INSTALACIONES	MA	MA	M	SI	SI	SI	NO	SI	SI			X		X	
41	[local] Oficina de Prueba de Software	Sede del centro de estudios	Jefe del departamento de sistemas	[L] INSTALACIONES	B	M	B	SI	SI	SI	NO	SI	SI			X		X	
42	[local] Data Center QWERTY S.A.	Sede del centro de estudios	Jefe del departamento de sistemas	[L] INSTALACIONES	M	M	MB	SI	SI	SI	NO	NO	NO	X				X	
43	[prov] Empresa Godaddy - Proveedor de hospedaje web	Sede del centro de estudios	Jefe del departamento de sistemas	[S] SERVICIOS	B	B	M	NO	NO	SI	NO	SI	SI	X				X	
44	[local] Oficina de Soporte	Sede del centro de estudios	Jefe del departamento de sistemas	[L] INSTALACIONES	B	B	M	NO	NO	SI	NO	SI	SI	X				X	
45	[adm] administradores de sistemas	Departamento de sistemas	Rector del centro de estudios	[P] PERSONAL	B	B	M	NO	SI	SI	NO	SI	SI	X				X	
46	[adm] administradores de comunicaciones	Departamento de sistemas	Jefe del departamento de sistemas	[P] PERSONAL	A	A	A	SI	SI	SI	SI	SI	SI			X		X	
47	[adm] administradores de BBDD	Sala de profesores	Coordinador de infraestructura	[P] PERSONAL	B	B	M	SI	SI	SI	SI	SI	NO			X		X	
48	[os] sistema operativo Windos 10	Departamento de Sistemas	Jefe del departamento de sistemas	[SW] SOFTWARE	B	MA	M												
49	[adm] administradores de seguridad	Sede del centro de estudios	Rector del centro de estudios	[P] PERSONAL	A	A	A	SI	NO	SI	NO	SI	SI					X	X

Fuente propia.

C= Confidencialidad, I= Integridad, D= Disponibilidad

Tabla 11 Valoración de las dimensiones de seguridad de los activos

ITEM	NOMBRE DEL ACTIVO	IMPACTO	C	I	D	VALOR
1	[www] Página Web - Joomla versión 2.5	Importante	5	4	3	4
2	[INT] Servicio de correo electrónico	Importante	5	4	3	4
3	[INT] Servicio de gestión y mantenimiento de salas de cómputo	Apreciable	2	2	5	3
4	[INT] Servicio de Gestión de usuarios y contraseñas	Importante	5	4	4	4
5	[mid] Servidor de Impresión - marca dellen torre PowerEdge T440	Relevante	2	2	3	2
6	[peripheral] [print] Impresora HP LaserJet Enterprise serie 600	Relevante	2	2	3	2
7	[peripheral] [print] Impresora SMART MultiXpress M4370LX	Relevante	2	2	3	2
8	[mid] Servidor de archivos FTP - marca dell en torre PowerEdge T130	Importante	5	5	3	4
9	Servidor DHCP - marca dell en torre PowerEdge T440	Importante	5	4	4	4

ITEM	NOMBRE DEL ACTIVO	IMPACTO	C	I	D	VALOR
10	[pc] Tres (3) Equipos de cómputo para gestión de Sistema de contable - Plan Cloud Plus	Despreciable	1	1	1	1
11	[network] [firewall]Cortafuegos Cisco ASA 5505	Importante	5	5	3	4
12	[network] [hub] Cuatro (4) Puntos de acceso alámbricos	Apreciable	3	2	5	3
13	[network] [switch] Seis (6) Switches cisco catalyst 2960	Relevante	2	2	3	2
14	[op] Dos (2) Técnicos de mantenimiento	Relevante	2	2	3	2
15	[ipphone] Seis (6) Teléfonos IP	Relevante	2	2	3	2
16	[wifi] Dos (2) Puntos de acceso	Apreciable	2	3	5	3
17	[pc] Diez (10) Desarrollo del objeto social	Apreciable	2	2	5	3
18	[pc] Cinco (5) desarrollo del objeto social	Apreciable	2	2	4	3
19	[mid] Servidor de nómina y facturación Servidor marca Dell en torre PowerEdge T440	Apreciable	4	1	3	3
20	[app] Apache 2.4.25	Apreciable	4	2	4	3
21	[app] PHP 5.6.30 - 7.1.1	Importante	4	3	4	4
22	[dbms] MySQL 5.7.17	Importante	4	4	4	4
23	[app] phpMyAdmin 4.6.6	Apreciable	3	3	3	3
24	[sub] Helisa Cloud Plus	Apreciable	3	3	3	3
25	[prov] Google - Proveedor Correo Electrónico	Importante	5	4	3	4
26	[Internet] Canal de ancho de banda 25 Megas dedicado	Importante	5	3	5	4
27	[LAN] red local	Importante	5	3	4	4
28	[av] antivirus	Importante	4	3	5	4
29	[files] [r] Documentos digitalizados de entrada y de salida	Importante	4	3	5	4
30	[files] [r] Audios de reuniones y asambleas	Importante	4	3	5	4
31	[files] [r] Vídeos generados por empleados y funcionarios	Apreciable	3	3	4	3
32	[int] [r] Base de datos del Sistema de empleados	Importante	4	3	5	4
33	[int] [r] Datos Personales	Relevante	2	2	3	2
34	[int] [r] Base de datos del Sistema de suministros	Importante	4	4	3	4
35	[local] Oficina de Infraestructura	Importante	4	4	3	4
36	[local] Dependencia de nómina y facturación	Apreciable	3	3	3	3
37	[local] Dependencia de sistemas	Imprescindible	5	5	4	5
38	[local] Antigua oficina de sistemas	Apreciable	4	2	4	3
39	[local] Dependencia Directiva y administrativa	Importante	5	5	3	4
40	[local] Oficina de Desarrollo Tecnológico	Importante	5	5	3	4
41	[local] Oficina de Prueba de Software	Relevante	2	3	2	2
42	[local] Data Center QWERTY S.A.	Relevante	3	3	1	2
43	[prov] Empresa Godaddy - Proveedor de hospedaje web	Relevante	2	2	3	2

ITEM	NOMBRE DEL ACTIVO	IMPACTO	C	I	D	VALOR
44	[local] Oficina de Soporte	Relevante	2	2	3	2
45	[adm] administradores de sistemas	Relevante	2	2	3	2
46	[adm] administradores de comunicaciones	Importante	4	4	4	4
47	[adm] administradores de BBDD	Relevante	2	2	3	2
48	[os] sistema operativo Windows 10	Apreciable	2	5	3	3
49	[adm] administradores de seguridad	Importante	4	4	4	4

Fuente: propia

Tabla 12 Clasificación de los activos por criticidad

Criticidad del Activo	Número de Activos	Porcentaje
Imprescindible	1	4,08%
Importante	21	40,82%
Apreciable	13	26,53%
Relevante	13	26,53%
Despreciable	1	2,04%
TOTAL	**49**	**100%**

Fuente: propia

10.3. INFORME SOBRE EVALUACIÓN DE RIESGOS

Se definió la siguiente tabla como parámetro para determinar la calificación cuantitativa como cualitativa para todos los activos.

Escala de valoración

Tabla 13 Escala de Valoración del impacto de los activos

Valor		Criterio
1	**Insignificante**	Daño Irrelevante: (La interrupción es casi nula, afecta a un individuo y es probable que el riesgo o degradación del activo pueda ser asumido por la empresa)
2	**Menor**	Daño menor (interrupción parcial de un grupo de individuos o menos de un día)
3	**Moderado**	Importante (interrupción parcial de un grupo de individuos en 1 día o más)

4	**Mayor**	Grave (interrupción a toda la organización en un tiempo menor a un día)
5	**Catastrófico**	Extremadamente grave (interrupción a toda la organización en más de un día o afecta a otras organizaciones)

Fuente: propia

Esta escala fue aplicada a todos los activos identificados, tanto Esenciales como a otros relevantes en aquellas características que representa las condiciones de la información en: Confidencialidad (C), Integridad (I), Disponibilidad (D).

El segundo parámetro que se estableció tiene que ver con la calificación de la probabilidad de ocurrencia de las amenazas identificadas a cada activo así:

Tabla 14 Probabilidad de Ocurrencia de un riesgo

PROBABILIDAD DEL RIESGO			
	Nomenclatura	**Categoría**	**Valoración**
Probabilidad	MA	**Casi Seguro**	5
	A	**Probable**	4
	M	**Posible**	3
	B	**Improbable**	2
	MB	**Raro**	1

Fuente: propia

10.3.1. Valoración de los activos

Se realiza una estimación de cada uno de los activos de la empresa QWERTY S.A. en las tres dimensiones de la seguridad de la información, Confidencialidad (C), Integridad (I), Disponibilidad (D). para medir el impacto de afectación que puede tener cada uno de los activos de la entidad.

Tabla 15 Valoración de los Activos de acuerdo a su impacto.

ITEM	NOMBRE DEL ACTIVO	IMPACTO	C	I	D	VALOR
1	[www] Página Web - Joomla versión 2.5	MODERADO	2	2	5	3
2	[INT] Servicio de correo electrónico	MAYOR	5	4	3	4
3	[INT] Servicio de gestión y mantenimiento de salas de cómputo	MODERADO	2	2	5	3
4	[INT] Servicio de Gestión de usuarios y contraseñas	MAYOR	5	4	4	4
5	[mid] Servidor de Impresión - marca Dell torre PowerEdge T440	MENOR	2	2	3	2
6	[peripheral] [print] Impresora HP LaserJet Enterprise serie 600	MENOR	2	2	3	2
7	[peripheral] [print] Impresora SMART MultiXpress M4370LX	MENOR	2	2	3	2
8	[mid] Servidor de archivos FTP - marca Dell en torre PowerEdge T130	MAYOR	5	5	3	4
9	Servidor DHCP - marca Dell en torre PowerEdge T440	MAYOR	5	4	4	4
10	[pc] Tres (3) Equipos de cómputo para gestión de Sistema de contable - Plan Cloud Plus	INSIGNIFICANTE	1	1	1	1
11	[network] [firewall]Cortafuegos Cisco ASA 5505	MAYOR	5	5	3	4
12	[network] [hub] Cuatro (4) Puntos de acceso alámbricos	MODERADO	3	2	5	3
13	[network] [switch] Seis (6) Switches cisco catalyst 2960	MENOR	2	2	3	2
14	[op] Dos (2) Técnicos de mantenimiento	MENOR	2	2	3	2
15	[ipphone] Seis (6) Teléfonos IP	MENOR	2	2	3	2
16	[wifi] Dos (2) Puntos de acceso	MODERADO	2	3	5	3
17	[pc] Diez (10) Desarrollo del objeto social	MODERADO	2	2	5	3
18	[pc] Cinco (5) desarrollo del objeto social	MODERADO	2	2	4	3
19	[mid] Servidor de nómina y facturación Servidor marca Dell en torre PowerEdge T440	MODERADO	4	1	3	3
20	[app] Apache 2.4.25	MODERADO	4	2	4	3
21	[app] PHP 5.6.30 - 7.1.1	MAYOR	4	3	4	4
22	[dbms] MySQL 5.7.17	MAYOR	4	4	4	4
23	[app] phpMyAdmin 4.6.6	MODERADO	3	3	3	3
24	[sub] Helisa Cloud Plus	MODERADO	3	3	3	3
25	[prov] Google - Proveedor Correo Electrónico	MENOR	2	2	3	2
26	[Internet] Canal de ancho de banda 25 Megas dedicado	MAYOR	5	3	5	4
27	[LAN] red local	MAYOR	5	3	4	4
28	[av] antivirus	MAYOR	4	3	5	4
29	[files] [r] Documentos digitalizados de entrada y de salida	MAYOR	4	3	5	4

ITEM	NOMBRE DEL ACTIVO	IMPACTO	C	I	D	VALOR
30	[files] [r] Audios de reuniones y asambleas	MAYOR	4	3	5	4
31	[files] [r] Vídeos generados por empleados y funcionarios	MODERADO	3	3	4	3
32	[int] [r] Base de datos del Sistema de empleados	MAYOR	4	3	5	4
33	[int] [r] Datos Personales	MENOR	2	2	3	2
34	[int] [r] Base de datos del Sistema de suministros	MAYOR	4	4	3	4
35	[local] Oficina de Infraestructura	MAYOR	4	4	3	4
36	[local] Dependencia de nómina y facturación	MODERADO	3	3	3	3
37	[local] Dependencia de sistemas	MODERADO	3	3	3	3
38	[local] Antigua oficina de sistemas	MODERADO	4	2	4	3
39	[local] Dependencia Directiva y administrativa	MAYOR	5	5	3	4
40	[local] Oficina de Desarrollo Tecnológico	MAYOR	5	5	3	4
41	[local] Oficina de Prueba de Software	MENOR	2	3	2	2
42	[local] Data Center QWERTY S.A.	MENOR	3	3	1	2
43	[prov] Empresa Godaddy - Proveedor de hospedaje web	MENOR	2	2	3	2
44	[local] Oficina de Soporte	MENOR	2	2	3	2
45	[adm] administradores de sistemas	MENOR	2	2	3	2
46	[adm] administradores de comunicaciones	MAYOR	4	4	4	4
47	[adm] administradores de BBDD	MENOR	2	2	3	2
48	[os] sistema operativo Windows 10	MODERADO	2	5	3	3
49	[adm] administradores de seguridad	MAYOR	4	4	4	4

Fuente: propia

En cuanto a la definición de las amenazas se utilizó como referente la codificación que presenta la metodología MAGERIT, en el libro II Catalogo de elementos pagina 25 a 47. Los cuales se relacionan en la columna amenaza.

Tabla 16 Amenazas, descripción metodología MAGERIT

TIPO AMENAZA	AMENAZA	Cant. De Activos
[N] Desastres naturales	[N1] Fuego	40
	[N2] Daños por agua	40
	[N*] Desastres naturales	40
[I] De origen industrial	[I1] Fuego	40
	[I2] Daños por agua	40
	[I*] Desastres industriales	40
	[I3] Contaminación mecánica	25
	[I4] Contaminación electromagnética	15
	[I5] Avería de origen físico o lógico	25
	[I6] Corte del suministro eléctrico	25
	[I7] Condiciones inadecuadas de temperatura o humedad	15
	[I8] Fallo de servicios de comunicaciones	8
	[I9] Interrupción de otros servicios y suministros esenciales	10
	[I10] Degradación de los soportes de almacenamiento de la información	15
	[I11] Emanaciones electromagnéticas	15
[E] Errores y fallos no intencionados	[E1] Errores de los usuarios	6
	[E2] Errores del administrador	4
	[E3] Errores de monitorización (log)	4
	[E4] Errores de configuración	25
	[E7] Deficiencias en la organización	4
	[E8] Difusión de software dañino	25
	[E9] Errores de [re-]encaminamiento	4
	[E10] Errores de secuencia	4
	[E14] Escapes de información	25
	[E15] Alteración accidental de la información	4
	[E18] Destrucción de información	25
	[E19] Fugas de información	8
	[E20] Vulnerabilidades de los programas (software)	25
	[E21] Errores de mantenimiento / actualización de programas (software)	25

TIPO AMENAZA	AMENAZA	Cant. De Activos
	[E23] Errores de mantenimiento / actualización de equipos (hardware)	25
	[E24] Caída del sistema por agotamiento de recursos	8
	[E25] Pérdida de equipos	40
	[E28] Indisponibilidad del personal	8
[A] Ataques intencionados	[A3] Manipulación de los registros de actividad (log)	4
	[A4] Manipulación de la configuración	4
	[A5] Suplantación de la identidad del usuario	N/D
	[A6] Abuso de privilegios de acceso	8
	[A7] Uso no previsto	8
	[A8] Difusión de software dañino	25
	[A9] [Re-]encaminamiento de mensajes	4
	[A10] Alteración de secuencia	8
	[A11] Acceso no autorizado	N/D
	[A12] Análisis de tráfico	6
	[A13] Repudio	N/D
	[A14] Interceptación de información (escucha)	6
	[A15] Modificación deliberada de la información	4
	[A18] Destrucción de información	6
	[A19] Divulgación de información	12
	[A22] Manipulación de programas	12
	[A23] Manipulación de los equipos	12
	[A24] Denegación de servicio	1
	[A25] Robo	40
	[A26] Ataque destructivo	40
	[A27] Ocupación enemiga	40
	[A28] Indisponibilidad del personal	N/D
	[A29] Extorsión	N/D
	[A30] Ingeniería social (picaresca)	N/D

Fuente: libro Magerit_v3_libro2

10.3.2. Valoración del riesgo

Para estimar el riesgo potencial al que se ven enfrentados los activos se construyó la siguiente matriz en donde se relacionan impacto y probabilidad para obtener la calificación del riesgo

Tabla 17 Matriz de Riesgo Probabilidad vs Impacto

IMPACTO	**PROBABILIDAD**				
	Raro (1)	Improbable (2)	Posible (3)	Probable (4)	Casi seguro (5)
Catastrófico (5)	A	A	E	E	E
Mayor (4)	M	M	A	A	E
Moderado (3)	M	M	M	A	E
Menor (2)	B	B	M	A	A
Insignificante (1)	B	B	B	M	M

B: Zona de riesgo *baja*: el riesgo se puede asumir riesgos improbables y de bajo impacto.
M: Zona de riesgo *moderada*: Asumir el riesgo, pero buscando la manera de mitigarlo o reducirlo.
A: Zona de riesgo alta: Reducir el riesgo, evitarlo, compartirlo o transferirlo. riesgos improbables y de bajo impacto.
E: Zona de riesgo *extrema*: Evitar el riesgo. Riesgos muy probables y de muy alto impacto

Fuente: propia basada en el libro Magerit_v3_libro3

Ya que se calificó el impacto para las tres variables (confidencialidad, integridad y disponibilidad) para aplicar la valoración del riesgo se tomará el elemento de más alto impacto para determinar el nivel de riesgo.

Tabla 18 Valoración del Riesgo

VALORACIÓN DEL RIESGO			
	Nomenclatura	**Categoría**	**Valoración**
Valoración del riesgo	MA	**EXTREMO**	20 a 25
	A	**ALTO**	10 a 19
	M	**MODERADO**	5 a 9
	B	**BAJO**	1 a 4

Fuente: propia basada en el libro Magerit_v3_libro3

Teniendo las amenazas, la escala de valoración de los riesgos, y la definición de la valoración de los activos, es necesario calcular el valor de cada riesgo de acuerdo a la matriz de probabilidad. Se aclara nuevamente la escala de valoración del **Impacto** [Insignificante (1), Menor (2), Moderado (3), Mayor (4) y Catastrófico (5)] y de la **Probabilidad** [Muy baja (1), Baja (2), Medio (3), Alta (4) y Muy Alta (5)] de riesgo para la de tabla de valoración del riesgo de los activos.

Tabla 19 Valoración del riesgo en los activos

Tipo de Activo	**Activo**	**Amenazas**	**Vulnerabilidades**	**IMPACTO**	**PROBABILIDAD**	**RIESGO**
[AUX] EQUIPAMENTO AUXILIAR	[network] [hub] Cuatro (4) Puntos de acceso alámbricos	[E4] Errores de configuración	Reglas mal configuradas que no permiten acceder a internet.	3	3	M: MODERADO = 9

Tipo de Activo	Activo	Amenazas	Vulnerabilidades	IMPACTO	PROBABILIDAD	RIESGO
[COM] REDES DE COMUNICACIONES	[network] [firewall]Cortafuegos Cisco ASA 5505	[E21] Errores de mantenimiento / actualización de programas (software)	Instalación de programas sin licenciamiento	4	2	M: MODERADO = 8
	[network] [switch] Seis (6) Switches cisco catalyst 2960	[E21] Errores de mantenimiento / actualización de programas (software)	Instalación de programas sin licenciamiento	2	3	M: MODERADO = 6
	[ipphone] Seis (6) Teléfonos IP	[E21] Errores de mantenimiento / actualización de programas (software)	Instalación de programas sin licenciamiento	2	4	M: MODERADO = 8
	[wifi] Dos (2) Puntos de acceso	[I6] Corte del suministro eléctrico	Ausencia de UPS.	3	4	A: ALTO = 12
	[LAN] red local	[E28] Indisponibilidad del personal	Personal en reunión con los jefes.	4	2	M: MODERADO = 8
[D] DATOS	[int] [r] Base de datos del Sistema de empleados	[I6] Corte del suministro eléctrico	Ausencia de UPS.	4	3	A: ALTO = 12
	[int] [r] Datos Personales	[E4] Errores de configuración	Configuración de licenciamiento vencido.	2	3	M: MODERADO = 6

Tipo de Activo	Activo	Amenazas	Vulnerabilidades	IMPACTO	PROBABILIDAD	RIESGO
	[int] [r] Base de datos del Sistema de suministros	[I2] Daños por agua	Fuga de agua en el sitio por manipulación de líquidos derramables.	4	2	M: MODERADO = 8
[HW] EQUIPAMENTO INFORMÁTICO	[mid] Servidor de Impresión - marca Dell torre PowerEdge T440	[A23] Manipulación de los equipos	Acceso al servidor por parte de personal con permisos de administrador	2	3	M: MODERADO = 6
	[peripheral] [print] Impresora HP LaserJet Enterprise serie 600	[A23] Manipulación de los equipos	Impresora apagada por parte de personal no autorizado.	2	3	M: MODERADO = 6
	[peripheral] [print] Impresora SMART MultiXpress M4370LX	[A23] Manipulación de los equipos	Impresora apagada por parte de personal no autorizado.	2	3	M: MODERADO = 6
	[mid] Servidor de archivos FTP - marca Dell en torre PowerEdge T130	[A23] Manipulación de los equipos	Acceso al servidor por parte de personal con permisos de administrador	4	3	A: ALTO = 12
	Servidor DHCP - marca Dell en torre PowerEdge T440	[A23] Manipulación de los equipos	Acceso al servidor por parte de personal con permisos de administrador	4	3	A: ALTO = 12

Tipo de Activo	Activo	Amenazas	Vulnerabilidades	IMPACTO	PROBABILIDAD	RIESGO
	[pc] Tres (3) Equipos de cómputo para gestión de Sistema de contable - Plan Cloud Plus	[A23] Manipulación de los equipos	Acceso al servidor por parte de personal con permisos de administrador	1	3	B: BAJO = 3
	[pc] Diez (10) Desarrollo del objeto social	[I6] Corte del suministro eléctrico	Ausencia de UPS.	3	4	A: ALTO = 12
	[pc] Cinco (5) desarrollo del objeto social	[A28] Indisponibilidad del personal	Personal en reunión con los jefes.	3	3	M: MODERADO = 9
	[mid] Servidor de nómina y facturación Servidor marca Dell en torre PowerEdge T440	[E4] Errores de configuración	Personal no autorizado con conocimiento de las claves de autenticación de las extensiones.	3	3	M: MODERADO = 9
[L] INSTALACIONES	[local] Oficina de Infraestructura	[I5] Avería de origen físico o lógico	Manipulación por parte de terceros con permiso acceso.	4	2	M: MODERADO = 8
	[local] Dependencia de nómina y facturación	[I5] Avería de origen físico o lógico	Manipulación por parte de terceros con permiso acceso.	3	2	M: MODERADO = 6
	[local] Dependencia de sistemas	[E15] Alteración accidental de la información	Ingreso de personal no autorizado que tiene usuario y	5	3	A: ALTO = 15

Tipo de Activo	Activo	Amenazas	Vulnerabilidades	IMPACTO	PROBABILIDAD	RIESGO
			contraseña de administrador.			
	[local] Antigua oficina de sistemas	[N*] Desastres naturales	Ubicación del sitio en terreno inestable.	3	2	M: MODERADO = 6
	[local] Dependencia Directiva y administrativa	[E19] Fugas de información	Ingreso de personal no autorizado.	4	4	A: ALTO = 16
	[local] Oficina de Desarrollo Tecnológico	[E14] Escapes de información	Ingreso de personal no autorizado.	4	4	A: ALTO = 16
	[local] Oficina de Prueba de Software	[E25] Pérdida de equipos	Ingreso de personal no autorizado.	2	2	B: BAJO = 4
	[local] Data Center QWERTY S.A.	[E25] Pérdida de equipos	Ingreso de personal no autorizado.	2	3	M: MODERADO = 6
	[local] Oficina de Soporte	[E25] Pérdida de equipos	Ingreso de personal no autorizado.	2	3	M: MODERADO = 6
[Media] SOPORTE DE INFORMACIÓN	[files] [r] Documentos digitalizados de entrada y de salida	[A24] Denegación de servicio	Seguridad anti DDoS ausente.	4	3	A: ALTO = 12
	[files] [r] Audios de reuniones y asambleas	[E24] Caída del sistema por agotamiento de recursos	Asignación de recursos de hardware limitada para el volumen de peticiones.	4	4	A: ALTO = 16

Tipo de Activo	Activo	Amenazas	Vulnerabilidades	IMPACTO	PROBABILIDAD	RIESGO
	[files] [r] Vídeos generados por empleados y funcionarios	[I8] Fallo de servicios de comunicaciones	Canal de comunicaciones saturado por consumo de ancho de banda por parte de los usuarios.	3	3	M: MODERADO = 9
[P] PERSONAL	[op] Dos (2) Técnicos de mantenimiento	[E21] Errores de mantenimiento / actualización de programas (software)	Instalación de programas sin licenciamiento	2	4	M: MODERADO = 8
	[adm] administradores de sistemas	[E14] Escapes de información	Ingreso de personal no autorizado.	2	3	M: MODERADO = 6
	[adm] administradores de comunicaciones	[A24] Denegación de servicio	Seguridad anti DDoS ausente.	4	2	M: MODERADO = 8
	[adm] administradores de BBDD	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Partes de hardware reutilizadas defectuosas.	2	3	M: MODERADO = 6
	[adm] administradores de seguridad	[E2] Errores del administrador	Perdida de Información	4	2	M: MODERADO = 8
[S] SERVICIOS	[www] Página Web - Joomla versión 2.5	[A24] Denegación de servicio	Apache desactualizado	4	2	M: MODERADO = 8

Tipo de Activo	Activo	Amenazas	Vulnerabilidades	IMPACTO	PROBABILIDAD	RIESGO
	[INT] Servicio de correo electrónico	[E2] Errores del administrador	Problemas con la actualización de la plataforma	4	3	A: ALTO = 12
	[INT] Servicio de gestión y mantenimiento de salas de cómputo	[A28] Indisponibilidad del personal	Personal en reunión con los jefes	3	3	M: MODERADO = 9
	[INT] Servicio de Gestión de usuarios y contraseñas	[E4] Errores de configuración	Manipulación por parte de terceros que tiene usuario y contraseña del directorio activo.	4	4	A: ALTO = 16
	[prov] Google - Proveedor Correo Electrónico	[E4] Errores de configuración	Sistema operativo desactualizado.	4	1	B: BAJO = 4
	[Internet] Canal de ancho de banda 25 Megas dedicado	[E28] Indisponibilidad del personal	Personal en reunión con los jefes.	4	2	M: MODERADAO = 8
	[prov] Empresa Godaddy - Proveedor de hospedaje web	[E25] Pérdida de equipos	Ingreso de personal no autorizado.	2	3	M: MODERADO = 6
[SW] SOFTWARE	[app] Apache 2.4.25	[I5] Avería de origen físico o lógico	Cable de datos que conecta el AP con la red física defectuoso.	3	2	M: MODERADO = 6
	[app] PHP 5.6.30 - 7.1.1	[E4] Errores de configuración	Sistema operativo desactualizado.	4	4	A: ALTO = 16

Tipo de Activo	Activo	Amenazas	Vulnerabilidades	IMPACTO	PROBABILIDAD	RIESGO
	[dbms] MySQL 5.7.17	[E4] Errores de configuración	Sistema operativo desactualizado.	4	4	A: ALTO = 16
	[app] phpMyAdmin 4.6.6	[E4] Errores de configuración	Sistema operativo desactualizado.	3	4	A: ALTO = 12
	[sub] Helisa Cloud Plus	[E4] Errores de configuración	Sistema operativo desactualizado.	3	4	A: ALTO = 12
	[av] anti virus	[A24] Denegación de servicio	Seguridad anti DDoS ausente.	4	3	A: ALTO = 12
	[os] sistema operativo Windows 10	[I6] Corte del suministro eléctrico	Sistema de transferencia de la planta eléctrica defectuoso.	3	2	M: MODERADO = 6

Fuente: propia

Para dar soluciones y recomendaciones en el plan de tratamiento del riesgo, se seleccionaron los tipos de activos, los activos afectados, el nivel del riesgo con su grado de prioridad, y se procedió a controlar mediante algunos mecanismos prácticos y las medidas a las que hay que llegar con el fin de minimizar los riesgos. De lo que se obtuvo el siguiente cuadro

Tabla 20 Recomendaciones de tratamiento de Riesgos

TIPO DE ACTIVO	ACTIVO	RIESGO	CONTROLES	RECOMENDACIONES	MEDIDAS
[AUX] EQUIPAMENTO AUXILIAR	[network] [hub] Cuatro (4) Puntos de acceso alámbricos	M: MODERADA= 9	Control de redes, definición de contraseña WPA	Establecer política y registro de equipos de conexión inalámbrica y permisos de conexión	Atomizar, dispersar y asumir el riesgo.

TIPO DE ACTIVO	ACTIVO	RIESGO	CONTROLES	RECOMENDACIONES	MEDIDAS
[COM] REDES DE COMUNICACIONES	[network] [firewall]Cortafuegos Cisco ASA 5505	M: MODERADA=8	Políticas de control de navegación y acceso	Definir grupos de navegación, páginas permitidas, reglas de conexión, cifrar información sensible y aislar zonas	Evitar, transferir y reducir o mitigar el riesgo
	[network] [switch] Seis (6) Switches cisco catalyst 2960	M: MODERADA=6	Control de redes y administración, definición de Vlan y segmentación de redes	Crear la segmentación de redes, definir switches de distribución, switches de borde y switches de Core	Evitar, atomizar, dispersar y mitigar el riesgo.
	[ipphone] Seis (6) Teléfonos IP	M: MODERADA=8	Establecer identificación de las extensiones y condiciones de la terminal	Mantenimiento preventivo y correctivo de equipos de telecomunicaciones	Evitar, transferir y reducir los riesgos.
	[wifi] Dos (2) Puntos de acceso	A: ALTA=12	Control de redes, definición de contraseña WPA	Establecer política y registro de equipos de conexión inalámbrica y permisos de conexión	Atomizar, dispersar y asumir el riesgo.
	[LAN] red local	M: MODERADA=8	Verificar direccionamiento de red local y dispositivos interconectados	Realizar monitoreo de ping y trazabilidad de paquetes	Transferir, dispersar y mitigar el riesgo.
[D] DATOS	[int] [r] Base de datos del Sistema de empleados	A: ALTA=12	Copias de respaldo de información	Definir política de copia de respaldo de la información para ejecutar periódicamente y almacenamiento en nube o un lugar diferente	Dispersar y atomizar el riesgo.

TIPO DE ACTIVO	ACTIVO	RIESGO	CONTROLES	RECOMENDACIONES	MEDIDAS
	[int] [r] Datos Personales	M: MODERADA= 6	Copias de respaldo de información	Definir política de copia de respaldo de la información para ejecutar periódicamente y almacenamiento en nube o un lugar diferente	Dispersar y atomizar el riesgo.
	[int] [r] Base de datos del Sistema de suministros	M: MODERADA= 8	Copias de respaldo de información	Definir política de copia de respaldo de la información para ejecutar periódicamente y almacenamiento en nube o un lugar diferente	Dispersar y atomizar el riesgo.
[HW] EQUIPAMENTO INFORMÁTICO	[mid] Servidor de Impresión - marca Dell torre PowerEdge T440	M: MODERADA= 6	Configuración de las impresoras y cierre de puertos innecesarios	Verificar los roles y servicios del servidor y los accesos que se tienen al mismo	Dispersar, evitar y asumir el riesgo
	[peripheral] [print] Impresora HP LaserJet Enterprise serie 600	M: MODERADA= 6	Mantenimiento Preventivo y correctivo de Equipos	Crear, llenar y mantener bitácora de fallas, reemplazo de partes y suministros, y mantenimientos preventivos y correctivos	Evitar, transferir y asumir el riesgo
	[peripheral] [print] Impresora SMART MultiXpress M4370LX	M: MODERADA= 6	Mantenimiento Preventivo y correctivo de Equipos	Crear, llenar y mantener bitácora de fallas, reemplazo de partes y suministros, y mantenimientos preventivos y correctivos	Evitar, transferir y asumir el riesgo

TIPO DE ACTIVO	ACTIVO	RIESGO	CONTROLES	RECOMENDACIONES	MEDIDAS
	[mid] Servidor de archivos FTP - marca Dell en torre PowerEdge T130	A: ALTA=12	Protección de la información y asignación de permisos por carpeta o archivos	Definir control de acceso a los archivos del FTP	Mitigar, evitar y transferir el riesgo.
	Servidor DHCP - marca Dell en torre PowerEdge T440	A: ALTA=12	Protección de la información y vigilancia de la asignación de Ip	Se debe proteger el servidor y conocer la asignación de Ip a los dispositivos de la red interna y externa	Evitar, asumir, dispersar y atomizar el riesgo.
	[pc] Tres (3) Equipos de cómputo para gestión de Sistema de contable - Plan Cloud Plus	B: BAJA = 3	Servicio de suministro de partes y disponibilidad del activo	Los PC deben tener protección a fallos de corriente, alarmas de funcionamiento deficiente y stock te partes para reemplazo	Transferir, mitigar y asumir el riesgo
	[pc] Diez (10) Desarrollo del objeto social	A: ALTA=12	Servicio de suministro de partes y disponibilidad del activo	Los PC deben tener protección a fallos de corriente, alarmas de funcionamiento deficiente y stock te partes para reemplazo	Transferir, mitigar y asumir el riesgo
	[pc] Cinco (5) desarrollo del objeto social	M: MODERADA= 9	Servicio de suministro de partes y disponibilidad del activo	Los PC deben tener protección a fallos de corriente, alarmas de funcionamiento deficiente y stock te partes para reemplazo	Transferir, mitigar y asumir el riesgo
	[mid] Servidor de nómina y facturación Servidor marca Dell en torre PowerEdge T440	M: MODERADA= 9	Restricción al acceso de información por personal autorizado	Controlar y verificar los derechos de acceso, verificar usuarios activos y permisos	Evitar, reducir y/o transferir los riesgos.

TIPO DE ACTIVO	ACTIVO	RIESGO	CONTROLES	RECOMENDACIONES	MEDIDAS
[L] INSTALACIONES	[local] Oficina de Infraestructura	M: MODERADA=8	Tener sistema de control de incendios, control de inundaciones, control de sismo-resistencia, realizar revisiones periódicas y cumplir las normas de seguridad ambiental y perimetral	Mantener los sistemas de desastres naturales, identificador de usuarios (sistema de control de acceso) y realizar pruebas periódicas de funcionamiento	Mitigar, reducir y asumir el riesgo.
	[local] Dependencia de nómina y facturación	M: MODERADA=6	Tener sistema de control de incendios, control de inundaciones, control de sismo-resistencia, realizar revisiones periódicas y cumplir las normas de seguridad ambiental y perimetral	Mantener los sistemas de desastres naturales, identificador de usuarios (sistema de control de acceso) y realizar pruebas periódicas de funcionamiento	Mitigar, reducir y asumir el riesgo.
	[local] Dependencia de sistemas	A: ALTA=15	Tener sistema de control de incendios, control de inundaciones,	Mantener los sistemas de desastres naturales, identificador de usuarios (sistema de control de acceso) y	Mitigar, reducir y asumir el riesgo.

TIPO DE ACTIVO	ACTIVO	RIESGO	CONTROLES	RECOMENDACIONES	MEDIDAS
			control de sismo-resistencia, realizar revisiones periódicas y cumplir las normas de seguridad ambiental y perimetral	realizar pruebas periódicas de funcionamiento	
	[local] Antigua oficina de sistemas	M: MODERADA=6	Tener sistema de control de incendios, control de inundaciones, control de sismo-resistencia, realizar revisiones periódicas y cumplir las normas de seguridad ambiental y perimetral	Mantener los sistemas de desastres naturales, identificador de usuarios (sistema de control de acceso) y realizar pruebas periódicas de funcionamiento	Mitigar, reducir y asumir el riesgo.
	[local] Dependencia Directiva y administrativa	A: ALTA=16	Tener sistema de control de incendios, control de inundaciones, control de sismo-resistencia, realizar revisiones periódicas y	Mantener los sistemas de desastres naturales, identificador de usuarios (sistema de control de acceso) y realizar pruebas periódicas de funcionamiento	Mitigar, reducir y asumir el riesgo.

TIPO DE ACTIVO	ACTIVO	RIESGO	CONTROLES	RECOMENDACIONES	MEDIDAS
			cumplir las normas de seguridad ambiental y perimetral		
	[local] Oficina de Desarrollo Tecnológico	A: ALTA=16	Tener sistema de control de incendios, control de inundaciones, control de sismo-resistencia, realizar revisiones periódicas y cumplir las normas de seguridad ambiental y perimetral	Mantener los sistemas de desastres naturales, identificador de usuarios (sistema de control de acceso) y realizar pruebas periódicas de funcionamiento	Mitigar, reducir y asumir el riesgo.
	[local] Oficina de Prueba de Software	B: BAJA = 4	Tener sistema de control de incendios, control de inundaciones, control de sismo-resistencia, realizar revisiones periódicas y cumplir las normas de seguridad ambiental y perimetral	Mantener los sistemas de desastres naturales, identificador de usuarios (sistema de control de acceso) y realizar pruebas periódicas de funcionamiento	Mitigar, reducir y asumir el riesgo.

TIPO DE ACTIVO	ACTIVO	RIESGO	CONTROLES	RECOMENDACIONES	MEDIDAS
	[local] Data Center QWERTY S.A.	M: MODERADA= 6	Tener sistema de control de incendios, control de inundaciones, control de sismo-resistencia, realizar revisiones periódicas y cumplir las normas de seguridad ambiental y perimetral, poseer sistema de aire acondicionado para regular temperatura	Mantener los sistemas de desastres naturales, identificador de usuarios (sistema de control de acceso) y realizar pruebas periódicas de funcionamiento	Mitigar, reducir y asumir el riesgo.
	[local] Oficina de Soporte	M: MODERADA= 6	Tener sistema de control de incendios, control de inundaciones, control de sismo-resistencia, realizar revisiones periódicas y cumplir las normas de seguridad ambiental y perimetral	Mantener los sistemas de desastres naturales, identificador de usuarios (sistema de control de acceso) y realizar pruebas periódicas de funcionamiento	Mitigar, reducir y asumir el riesgo.

TIPO DE ACTIVO	ACTIVO	RIESGO	CONTROLES	RECOMENDACIONES	MEDIDAS
[Media] SOPORTE DE INFORMACIÓN	[files] [r] Documentos digitalizados de entrada y de salida	A: ALTA=12	Respaldo de información y software DLP, EndPoint y protección de datos. Software de encriptación	Prohibir el uso de software no autorizado, la creación de copias indebidas, actualización de software antivirus, antispyware entre otros.	Evitar, mitigar, reducir el riesgo
	[files] [r] Audios de reuniones y asambleas	A: ALTA=16	Respaldo de información y software DLP, EndPoint y protección de datos. Software de encriptación	Prohibir el uso de software no autorizado, la creación de copias indebidas, actualización de software antivirus, antispyware entre otros.	Evitar, mitigar, reducir el riesgo
	[files] [r] Vídeos generados por empleados y funcionarios	M: MODERADA=9	Respaldo de información y software DLP, EndPoint y protección de datos. Software de encriptación	Prohibir el uso de software no autorizado, la creación de copias indebidas, actualización de software antivirus, antispyware entre otros.	Evitar, mitigar, reducir el riesgo
[P] PERSONAL	[op] Dos (2) Técnicos de mantenimiento	M: MODERADA=8	Verificar conocimiento, información y acuerdos de confidencialidad	Mantener la confidencialidad de la empresa, y confirmar el vínculo laboral	Evitar y reducir el riesgo
	[adm] administradores de sistemas	M: MODERADA=6	Verificar conocimiento, participación en transferencia de conocimiento	Definir permisos y rol, mantener acuerdos de confidencialidad a nivel empresarial y vínculo laboral	Evitar y reducir el riesgo

TIPO DE ACTIVO	ACTIVO	RIESGO	CONTROLES	RECOMENDACIONES	MEDIDAS
	[adm] administradores de comunicaciones	M: MODERADA=8	Verificar conocimiento, participación en transferencia de conocimiento	Definir permisos y rol, mantener acuerdos de confidencialidad a nivel empresarial y vínculo laboral	Evitar y reducir el riesgo
	[adm] administradores de BBDD	M: MODERADA=6	Verificar conocimiento, participación en transferencia de conocimiento	Definir permisos y rol, mantener acuerdos de confidencialidad a nivel empresarial y vínculo laboral	Evitar y reducir el riesgo
	[adm] administradores de seguridad	M: MODERADA=8	Verificar conocimiento, participación en transferencia de conocimiento	Definir permisos y rol, mantener acuerdos de confidencialidad a nivel empresarial y vínculo laboral	Evitar y reducir el riesgo
[S] SERVICIOS	[www] Página Web - Joomla versión 2.5	8 MODERADO	Definición de las políticas de acceso	Limitar el acceso a un solo administrador, establecimiento de privilegios y roles	Evitar y transferir el riesgo a la empresa Godaddy
	[INT] Servicio de correo electrónico	A: ALTA=12	Políticas de Spam y control de acceso, definición de tiempo de no ingreso a la cuenta	Exigir contraseñas robustas, definir listas blancas y listas negras, controlar acceso a la administración	Reducir el riesgo, evitar
	[INT] Servicio de gestión y mantenimiento de salas de cómputo	M: MODERADA=9	Mantenimiento de equipos y actualización	Llevar bitácora de las fallas de los equipos, reemplazo de partes y mantenimientos preventivos y correctivos realizados	Evitar, transferir y asumir el riesgo

TIPO DE ACTIVO	ACTIVO	RIESGO	CONTROLES	RECOMENDACIONES	MEDIDAS
	[INT] Servicio de Gestión de usuarios y contraseñas	A: ALTA=16	Definición de políticas de contraseña segura	Exigir contraseña que incluyas mayúsculas, minúsculas, números, caracteres especiales, no caracteres repetidos consecutivamente	Evitar el riesgo
	[prov] Google - Proveedor Correo Electrónico	B: BAJA = 4	Definición de OLA, disponibilidad ininterrumpida	Firmar contrato con acuerdos definidos	Transferir el riesgo a la empresa proveedor a de correo
	[Internet] Canal de ancho de banda 25 Megas dedicado	M: MODERADA=8			
	[prov] Empresa Godaddy - Proveedor de hospedaje web	M: MODERADA=6	Mantener acuerdos OLA para disponibilidad	Crear y revisar el contrato de prestación de servicio	Transferir el riesgo
[SW] SOFTWARE	[app] Apache 2.4.25	M: MODERADA=6	Mantener software actualizado	Crear políticas de seguridad de uso y restricción de software	Evitar el riesgo, transferir o mitigar
	[app] PHP 5.6.30 - 7.1.1	A: ALTA=16	Mantener software actualizado	Crear políticas de seguridad de uso y restricción de software	Evitar el riesgo, transferir o mitigar
	[dbms] MySQL 5.7.17	A: ALTA=16	Mantener software actualizado	Crear políticas de seguridad de uso y restricción de software	Evitar el riesgo, transferir o mitigar
	[app] phpMyAdmin 4.6.6	A: ALTA=12	Mantener software actualizado	Crear políticas de seguridad de uso y restricción de software	Evitar el riesgo, transferir o mitigar

TIPO DE ACTIVO	ACTIVO	RIESGO	CONTROLES	RECOMENDACIONES	MEDIDAS
	[sub] Helisa Cloud Plus	A: ALTA=12	Mantener software actualizado	Crear políticas de seguridad de uso y restricción de software	Evitar el riesgo, transferir o mitigar
	[av] anti virus	A: ALTA=12	Mantener software actualizado	Crear políticas de seguridad de uso y restricción de software	Evitar el riesgo, transferir o mitigar
	[os] sistema operativo Windows 10	M: MODERADA=6	Ajustes al Firewall, control de versión de software y parches de seguridad, protección contra códigos maliciosos	No permitir software no autorizado, utilizar GPO para instalación de software y repositorio de software autorizado. Mantener sistema con actualizaciones de seguridad, mínimo la anterior a la última liberada	Evitar, transferir, mitigar y/o reducir el riesgo.

Fuente: propia

10.3.3. Verificación de Aplicabilidad de Controles

Tabla 21 Estado de los Controles de la declaración de Aplicabilidad

Clausula	Sección	Objetivos de Control	CRITERIO DE APLICABILIDAD
	A.5.1.	ORIENTACION DE LA DIRECCION PARA LA GESTION DE LA SEGURIDAD DE LA INFORMACION	

Clausula	Sección	Objetivos de Control	CRITERIO DE APLICABILIDAD
A5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	A 5.5.1.	Políticas de seguridad de la información	ND
	A 5.1.2.	Revisión de las políticas para la seguridad de la información	CNI
A6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	A.6.1.	ORGANIZACIÓN INTERNA	
	A.6.1.1	Roles y responsabilidades para la Seguridad de la Información	RD
	A.6.1.2	Separación de Deberes	RD
	A.6.1.3	Contacto con las Autoridades	CNI
	A.6.1.4	Contacto con los grupos de interés especial	CNI
	A.6.1.5	Seguridad de la Información en la Gestión de Proyectos	CNI
A.7. SEGURIDAD DE LOS RECURSOS HUMANOS	A.7.1	ANTES DE ASUMIR EL EMPLEO	
	A.7.1.1	Seguridad de los recursos humanos / Selección	RD
	A.7.1.2	Términos y Condiciones del empleo	RD
	A.7.2	DURANTE LA EJECUCIÓN DEL EMPLEO	
	A.7.2.1	Responsabilidades de la Dirección	CNI
	A.7.2.2	Concienciación, educación y formación en la Seguridad de la Información	CNI
	A.7.2.3	Proceso Disciplinario	CNI
	A.7.3	TERMINACIÓN Y CAMBIO DE EMPLEO	
	A.7.3.1	Terminación o cambio de responsabilidades de empleo	RD
A.8. GESTIÓN DE ACTIVOS	A.8.1	RESPONSABILIDAD POR LOS ACTIVOS	
	A.8.1.1	Inventario de Activos	RD
	A.8.1.2	Propiedad de los activos	ND
	A.8.1.3	Uso aceptable de los activos	CNI
	A.8.1.4	Devolución de los Activos	CNI
	A.8.2.	CLASIFICACIÓN DE LA INFORMACIÓN	
	A.8.2.1	Clasificación de la Información	ND
	A.8.2.2	Etiquetado y manejo de información	RD
	A.8.2.3	Manejo de Activos	CNI
	A.8.3	MANEJO DE MEDIOS	
	A.8.3.1	Gestión de Medios Removibles	CNI
	A.8.3.2.	Disposición de los Medios	ND
	A.8.3.3	Transferencia de Medios Físicos	CNI
A.9 CONTROL DE ACCESO	A.9.1	REQUISITOS DEL NEGOCIO	
	A.9.1.1	Política de control de Acceso	CNI

Clausula	Sección	Objetivos de Control	CRITERIO DE APLICABILIDAD
	A.9.1.2	Acceso a redes y servicios de red	CNI
	A.9.2	GESTIÓN DE ACCESO A USUARIOS	
	A.9.2.1	Registro y cancelación del registro de usuarios	ND
	A.9.2.2	Suministro de acceso a usuarios	ND
	A.9.2.3	Gestión de derechos de acceso privilegiado	RD
	A.9.2.4	Gestión de información de autenticación secreta de usuarios	RD
	A.9.2.5	Revisión de los derechos de Acceso de Usuarios	ND
	A.9.2.6	Retiro o ajuste de derechos de acceso	CNI
	A.9.3	RESPONSABILIDAD DE LOS USUARIOS	
	A.9.3.1	Uso de información de autenticación secreta	CNI
	A.9.4	CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	
	A.9.4.1	Restricción de acceso a la Información	CNI
	A.9.4.2	Procedimiento de Ingreso Seguro	CNI
	A.9.4.3	Sistema de Gestión de Contraseñas	RD
	A.9.4.4	Uso de programas utilitarios privilegiados	ND
	A.9.4.5	Control de Acceso a Códigos Fuente de Programas	CNI
	A.11.1	ÁREAS SEGURAS	
	A.11.1.1	Perímetro de seguridad física	RD
	A.11.1.2	Controles de acceso físico	RD
	A.11.1.3	Seguridad de oficinas, recintos e instalaciones	C
	A.11.1.4	Protección contra amenazas externas y ambientales	C
	A.11.1.5	Trabajo en áreas seguras	ND
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO	A.11.1.6	Áreas de despacho y cargas	ND
	A.11.2	EQUIPOS	
	A.11.2.1	Ubicación y protección de los equipos	CNI
	A.11.2.2	Servicio de suministro	C
	A.11.2.3	Seguridad del cableado	ND
	A.11.2.4	Mantenimiento de los equipos.	C
	A.11.2.5	Retiro de activos	C
	A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	CNI
	A.11.2.7	Disposición Segura o Reutilización de equipos	CNI

Clausula	Sección	Objetivos de Control	CRITERIO DE APLICABILIDAD
A.12. SEGURIDAD DE LAS OPERACIONES	A.11.2.8	Equipos de Usuario Desatendidos.	ND
	A.11.2.9	Política de Escritorio Limpio y pantalla Limpia	ND
	A. 12.1	PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	
	A.12.1.1	Procedimiento de Operación de Documentos	ND
	A.12.1.2	Gestión de Cambios	RD
	A.12.1.3	Gestión de Capacidad	RD
	A.12.1.4	Separación de las instalaciones de desarrollo, ensayo y operación.	CNI
	A.12.2	PROTECCIÓN CONTRA CÓDIGO MALICIOSO	
	A.12.2.1	Controles contra códigos maliciosos	ND
	A.12.3	COPIAS DE RESPALDO	
	A.12.3.1	Respaldo de Información	CNI
	A.12.4	REGISTRO Y SEGUIMIENTO	
	A.12.4.1	Registro de Eventos	CNI
	A.12.4.2	Protección de la Información del registro	CNI
	A.12.4.3	Registros del administrador y del operador	CNI
	A.12.4.4	Sincronización de Relojes	ND
	A.12.5	CONTROL DE SOFTWARE OPERACIONAL	
	A.12.5.1	Instalación de Software en Sistemas Operativos	ND
	A.12.6	GESTIÓN DE LA VULNERABILIDAD TÉCNICA	
	A.12.6.1	Gestión de las Vulnerabilidades Técnicas	CNI
	A.12.6.2	Restricciones sobre la instalación de Software	CNI
	A.12.7	CONSIDERACIONES DSOBRE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	
	A.12.7.1	Controles de auditorías de sistemas de información	ND
A.13 SEGURIDAD EN LAS COMUNICACIONES	A.13.1	GESTIÓN DE LA SEGURIDAD DE LAS REDES	
	A.13.1.1	Controles de Redes	RD
	A.13.1.2	Seguridad en los servicios de red	RD
	A.13.1.3	Separación en las Redes	RD
	A.13.2	TRANSFERENCIA DE INFORMACIÓN	
	A.13.2.1	Políticas y procedimientos de transferencia de información	RD
	A.13.2.2	Acuerdos sobre trasferencia de Información	RD
	A.13.2.3	Mensajería Electrónica	C
	A.13.2.4	Acuerdos de Confidencialidad o de no divulgación.	RD

Clausula	Sección	Objetivos de Control	CRITERIO DE APLICABILIDAD
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	A.14.1	REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	
	A.14.1.1	Análisis y especificación de requisitos de Seguridad de la Información	RD
	A.14.1.2	Seguridad en los servicios de las aplicaciones en redes públicas	ND
	A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	CNI
	A.14.2	SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	
	A.14.2.1	Política de Desarrollo Seguro	RD
	A.14.2.2	Procedimiento de Control de Cambios en Sistemas	RD
	A.14.2.3	Revisión Técnicas de las Aplicaciones después de los cambios en la plataforma de operación	CNI
	A.14.2.4	Restricciones en los cambios a los paquetes de software	CNI
	A.14.2.5	Principios de construcción de sistemas seguros	ND
	A.14.2.6	Ambiente de desarrollo seguro	CNI
	A.14.2.7	Desarrollo contratado externamente	ND
	A.14.2.8	Pruebas de seguridad de sistemas	ND
	A.14.2.9	Pruebas de aceptación de sistemas	C
	14.3	DATOS DE PRUEBA	
	A.14.3.1	Protección de datos de prueba	C
A.15 RELACIONES CON LOS PROVEEDORES	A.15.1	SEGURIDAD E LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES	
	A.15.1.1	Política de Seguridad de la Información para las relaciones con proveedores	C
	A.15.1.2	Tratamiento de la Seguridad dentro de los acuerdos con proveedores	C
	A.15.1.3	Cadena de Suministros de Tecnología de Información y Comunicación	C
	A.15.2	GESTIÓN DE LA PRESTACIÓN DE LOS SERVICIOS DE PROVEEDORES	
	A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	RD

Clausula	Sección	Objetivos de Control	CRITERIO DE APLICABILIDAD
	A.15.2.2	Gestión de Cambios en los Servicios de los Proveedores	RD
	A.16.1	GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	
A.16 GESTIÓN DE INCIDENTES DE SEGURIDA DE LA INFORMACIÓN	A.16.1.1	Gestión de Incidentes / Responsabilidades y Procedimientos	C
	A.16.1.2	Reporte de Eventos de Seguridad de la Información	RD
	A.16.1.3	Reporte de debilidades de seguridad de la información	RD
	A.16.1.4	Evaluación de Eventos de Seguridad de la Información y decisiones sobre ellos	C
	A.16.1.5	Respuesta a incidentes de Seguridad de la Información	C
	A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	C
	A.16.1.7	Recolección de la Evidencia	RD
	A.17.1	CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN	
A.17 ASPECTOS DE SEGURIDA D DE LA INFORMACIÓN PARA LA GESETIÓN DE LA CONTINUIDAD DE NEGOCIO	A.17.1.1	Planificación de la continuidad de la Seguridad de la Información	CNI
	A.17.1.2	Implementación de la continuidad de la Seguridad de la Información	CNI
	A.17.1.3	Verificación, revisión y evaluación de la continuidad de la Seguridad de la Información	CNI
	A.17.2	IMPLEMENTAR LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	
	A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	CNI
	A.18.1	CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES	
A.18 CUMPLIMIENTO	A.18.1.1	Identificación de la legislación aplicable y los requisitos contractuales	RD
	A.18.1.2	Derechos de Propiedad Intelectual (DPI)	RD
	A.18.1.3	Protección de Registros	RD
	A.18.1.4	Privacidad y Protección de Información de datos personales.	RD
	A.18.2	REVISIONES DE SEGURIDAD DE LA INFORMACIÓN	

Clausula	Sección	Objetivos de Control	CRITERIO DE APLICABILIDAD
	A.18.2.1	Revisión Independiente de la Seguridad de la Información	CNI
	A.18.2.2	Cumplimiento con las políticas y normas de seguridad	CNI
	A.18.2.3	Revisión del cumplimiento técnico.	CNI

Fuente: propia

Tabla 22 Resumen estado de adopción de objetivos y controles

Cantidad	Códigos	Nombre	Significado	Contribución %
15	C	Completo	El control se documentó e implemento completamente	13,76 %
22	ND	No Documentado	El control se lleva a cabo, pero el proceso debe ser documentado a fin de garantizar que se pueda volver a replicar y mantener el riesgo reducido	20,18 %
32	RD	Rediseñar	El control no cumple con las normas y es necesario diseñarlo nuevamente para cumplir con estas.	29,36 %
40	CNI	Control No Implementado	El control no está implementado, se requiere diseñarlo y documentarlo	36,70 %
0	NA	Control No Aplicable	El control no es aplicable para la entidad.	0,00 %
109	TOTALES			100,00%

Fuente: propia

10.4. DECLARACIÓN DE APLICABILIDAD

Tabla 23 Formato de la declaración de aplicabilidad de QWERTY Versión Inicial

<table>
<tr><td colspan="3">FORMATO
DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN</td><td rowspan="2">LOGO</td></tr>
<tr><td>CODIGO
FTI-01</td><td>PROCESO
GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN</td><td>VERSIÓN
1</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">Esta declaración de aplicabilidad de controles para el Sistema Integrado de Gestión de Seguridad de la Información - SIGSI, en función al comité de seguridad de la empresa QWERTY S.A. su Dirección General, como responsable de implementar, operar, mantener y mejorar el SIGSI, para determinar los resultados de la identificación, y valoración de riesgos de seguridad de la información, así como la formulación de actividades de tratamiento de riesgos, que cada líder operativo de proceso ha estimado convenientes, para mitigarlos y operar de forma segura y conforme los requisitos de los servicios ofrecidos por la empresa.

Los controles aplicables para la operación del Sistema Integrado de Gestión de Seguridad de la Información, son los numerales que se relacionan a continuación en el “Detalle de la Declaración de Aplicabilidad”, tramitado con base en las recomendaciones de la norma NTC/ISO 27001:2013.

La presente declaración de aplicabilidad será revisada conjuntamente con los resultados de cada nuevo proceso de valoración de riesgos y/o ante cambios significativos de los elementos de la plataforma tecnológica y/o de personal.

Esta información, será material de comparación en los procesos de revisión por la dirección del SIGSI, en los periodos convenidos para su actualización.
Se firma la presente Declaración de Aplicabilidad</td></tr>
<tr><td colspan="4"><table><tr><td></td><td></td><td></td></tr><tr><td>Xxxxxxx
Xxxxxxx</td><td>Xxxxxxx
Xxxxxxx</td><td>Xxxxxxx
Xxxxxxx</td></tr><tr><td>Director General de QWERTY S.A.</td><td>Director de la Dependencia de Sistemas</td><td>Jefe de la Oficina Asesora de Planeación</td></tr></table></td></tr>
</table>

A continuación, se presenta el detalle de la Declaración de Aplicabilidad de los controles necesarios para gestionar los riesgos que afectan a la Seguridad de la Información, que fueron identificados y valorados en QWERTY S.A. Desarrollo Urbano - IDU

Tabla 24 Objetivos de Control adoptados a la empresa a la luz de SIGSI

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						**LOGO**
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
A5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	A.5.1. ORIENTACION DE LA DIRECCION PARA LA GESTION DE LA SEGURIDAD DE LA INFORMACION	A 5.1.1.	Políticas de seguridad de la información	SI	Se toma este control, ya que es pertinente definir las políticas para la seguridad de la información de la empresa, aprobadas por la dirección, publicadas y comunicadas a usuarios internos y externos	Publicación de las políticas de seguridad de la información del SIGSI en QWERTY S.A.
		A 5.1.2.	Revisión de las políticas para la seguridad de la información	SI	Se adopta este control porque las políticas deben ser revisadas a intervalos específicos de tiempo, o si se presentan cambios significativos, para asegurar su eficacia continua.	Acta de reunión del comité SIGSI, donde se evidencie la revisión de dichas políticas y su alineación a la realidad.

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						**LOGO**
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
A6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	A.6.1. ORGANIZACIÓN INTERNA	A.6.1.1	Roles y responsabilidades para la Seguridad de la Información	SI	Se acoge este control toda vez que se definirán los roles y responsabilidades del equipo de SIGSI en QWERTY S.A.	Numeral 10.7 de este documento
		A.6.1.2	Separación de Deberes	SI	Se aplica este control en concordancia a que los deberes en conflicto en las dependencias de la empresa se deben separar, para reducir posibilidades de modificación no autorizada, o no intencional.	Numeral 10.7 de este documento
		A.6.1.3	Contacto con las Autoridades	SI	Se adopta este control toda vez que es imperativo mantener los contactos apropiados con las autoridades a las que haya lugar	Documento “Guía de Autoridades y grupos de interés QWERTY S.A.”

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						LOGO
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.6.1.4	Contacto con los grupos de interés especial	SI	Se adhiere el control, ya que es necesario mantener contactos con los grupos de interés especial para la empresa, foros o asociaciones profesionales especializadas en seguridad y terceros.	Documento “Guía de Autoridades y grupos de interés QWERTY S.A.”
		A.6.1.5	Seguridad de la Información en la Gestión de Proyectos	SI	Aplica este control puesto que la SI se debe mantener en la gestión de proyectos independientemente del tipo de proyecto.	Formato de lista de Chequeo “SIGSI en los proyectos”
A.7. SEGURIDAD DE LOS RECURSOS HUMANOS	A.7.1 ANTES DE ASUMIR EL EMPLEO	A.7.1.1	Seguridad de los recursos humanos / Selección	SI	Se toma este control porque se debe verificar los antecedentes de todos los candidatos a un empleo de acuerdo a las leyes, reglamentaciones y ética pertinentes, proporcionales a los requisitos de la empresa	Requisitos para contratación de prestación de servicios profesionales.

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						LOGO
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.7.1.2	Términos y Condiciones del empleo	SI	Se toma este control puesto que los acuerdos contractuales con los empleados y contratistas deben establecer sus responsabilidades y las de la organización	Solicitud da Gestión del Talento Humano, para la inclusión de obligaciones y responsabilidades frente a la Seguridad de la Información
	A.7.2 DURANTE LA EJECUCIÓN DEL EMPLEO	A.7.2.1	Responsabilidades de la Dirección	SI	Este control se toma porque la dirección de la empresa tiene que exigir a todos los usuarios internos y externos el cumplimiento de las políticas de seguridad y procedimientos establecidos por la empresa.	Numeral 10.7 de este documento
		A.7.2.2	Concienciación, educación y formación en la seguridad de la información	SI	Se adopta este control, ya que se deben dar transferencias de conocimiento y sensibilización de usuarios internos y externos de la empresa, cuando sea pertinente.	Inducciones, Transferencias de conocimiento, boletines, campañas de sensibilización.

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						**LOGO**
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.7.2.3	Proceso Disciplinario	SI	Se toma este control, ya que se debe tener un proceso formal de acciones a los empleados que hayan cometido violaciones a las políticas de Seguridad de la Información	Procedimiento para gestión de incidentes. Numeral 10.14 de este documento
	A.7.3 TERMINACIÓN Y CAMBIO DE EMPLEO	A.7.3.1	Terminación o cambio de responsabilidades de empleo	SI	Este control se adhiere puesto que las responsabilidades que son válidas después de una terminación de contrato se deben comunicar al nuevo empleado o contratista y se deben hacer cumplir.	Suscripción de cláusulas de confidencialidad y no divulgación de la información y su seguridad por un periodo de un (1) año posterior a la desvinculación o terminación del contrato.

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN			**LOGO**
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	**VERSIÓN** 1	

Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
A.8. GESTIÓN DE ACTIVOS	A.8.1 RESPONSABILIDAD POR LOS ACTIVOS	A.8.1.1	Inventario de Activos	SI	Este control se adopta porque es necesario identificar los activos asociados con información e instalaciones de procesamiento información y elaborar el inventario.	Inventario de activos numeral 10.8 de este documento
		A.8.1.2	Propiedad de los activos	SI	Se adopta este control ya que todo activo de la empresa en el inventario debe ser asignado a un usuario que se responsabilice de él.	Inventario de activos numeral 10.8 de este documento
		A.8.1.3	Uso aceptable de los activos	SI	Se toma este control, puesto que se debe identificar, documentar e implementar reglas para el uso aceptable de la información y los activos asociados al procesamiento de la información.	Uso aceptable de los activos numeral 10.9 de este documento

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						LOGO
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.8.1.4	Devolución de los Activos	SI	Se adopta el control, teniendo en cuenta el uso aceptable de los activos, todos los usuarios internos y externos de la empresa DEBEN devolver todos los activos que tengan asignados a su cargo al terminar su vínculo laboral con la empresa.	Uso aceptable de los activos numeral 10.9 de este documento
	A.8.2. CLASIFICACIÓN DE LA INFORMACIÓN	A.8.2.1	Clasificación de la Información	SI	Se adhiere este control, porque la información ha de clasificarse de acuerdo a su valor, legalidad, importancia y privacidad.	Acta del comité, archivo para presentación y aprobación de documentación clasificada como privada y pública.
		A.8.2.2	Etiquetado y manejo de información	SI	Este control aplica para la empresa ya que se debe implementar un conjunto adecuado de procedimientos para el rotulado de la información, de acuerdo con el esquema de clasificación de la empresa.	Clasificación de la información, etiquetado de los activos de información respecto a su accesibilidad y criticidad aprobados en el comité de seguridad.

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						LOGO
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.8.2.3	Manejo de Activos	SI	Este control aplica, ya que es necesario implementar procedimientos para el manejo de activos, en concordancia con el esquema de clasificación adoptado por la empresa	Uso aceptable de los activos numeral 10.9 de este documento
	A.8.3 MANEJO DE MEDIOS	A.8.3.1	Gestión de Medios Removibles	SI	Se adopta este control toda vez que es necesario adoptar procedimientos para la gestión de medios removibles, de acuerdo con la clasificación de la empresa	Uso aceptable de los activos numeral 10.9 de este documento
		A.8.3.2.	Disposición de los Medios	SI	Se toma este control, ya que es necesario conocer la forma segura en que dispone de medios cuando ya no sean requeridos.	Instructivo de borrado seguro de datos y formateo final de equipos (en construcción).

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						**LOGO**
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.8.3.3	Transferencia de Medios Físicos	SI	Se adopta este control, puesto que Los medios que contienen información, se deben proteger contra acceso no autorizado, uso indebido o daño.	Uso aceptable de los activos numeral 10.9 de este documento
A.9 CONTROL DE ACCESO	A.9.1 REQUISITOS DEL NEGOCIO	A.9.1.1	Política de control de Acceso	SI	Establecer, documentar y revisar política de control de acceso con base en los requisitos del negocio y de seguridad de información de la empresa	Política de Control de Acceso, numeral 10.10 de este documento
		A.9.1.2	Acceso a redes y servicios de red	SI	Se toma este control, ya que se debe permitir que los usuarios accedan a la red, previa autorización de sitios y file servers	Política de Control de Acceso, numeral 10.10 de este documento

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						**LOGO**
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
	A.9.2 GESTIÓN DE ACCESO A USUARIOS	A.9.2.1	Registro y cancelación del registro de usuarios	SI	Aplica este control, ya que se debe implementar un proceso formal de registro y de cancelación de registro de usuario para conceder los derechos de acceso	Procedimiento Gestionar usuarios Tecnológicos (En construcción)
		A.9.2.2	Suministro de acceso a usuarios	SI	Si aplica este control, porque es necesario implementar un usuario y clave unipersonal e intransferible a cada usuario para el acceso o denegación a los sistemas y servicios de la empresa	Procedimiento Gestionar usuarios Tecnológicos (En construcción)

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						LOGO
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.9.2.3	Gestión de derechos de acceso privilegiado	SI	Si aplica este control, toda vez que se debe controlar, restringir y conceder acceso segregado a los sistemas y servicios de la empresa en virtud de un privilegio de trabajo.	Instructiva revisión de los derechos de acceso de los usuarios (En construcción). Busca que los jefes de dependencia revisen los derechos de acceso a los recursos del personal a su cargo.
		A.9.2.4	Gestión de información de autenticación secreta de usuarios	SI	Se adopta este control, porque es necesario buscar un canal de información que entregue de manera unipersonal la autenticación secreta.	Procedimiento Gestionar usuarios Tecnológicos (En construcción)

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						**LOGO**
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.9.2.5	Revisión de los derechos de Acceso de Usuarios	SI	Se adopta este control, ya que los jefes de dependencia deben revisar los permisos de acceso de los usuarios a intervalos regulares.	Instructiva revisión de los derechos de acceso de los usuarios (En construcción). Busca que los jefes de dependencia revisen los derechos de acceso a los recursos del personal a su cargo.
		A.9.2.6	Retiro o ajuste de derechos de acceso	SI	Se aplica este control, puesto que los derechos de acceso concedidos a los usuarios de la empresa o externos se deben retirar una vez termine su vínculo laboral	Procedimiento Gestionar usuarios Tecnológicos (En construcción)
	A.9.3 RESPONSABILIDAD DE LOS USUARIOS	A.9.3.1	Uso de información de autenticación secreta	SI	Los usuarios deben cumplir con la complejidad de su autenticación secreta y entender que esta es personal e intransferible.	Procedimiento Gestionar usuarios Tecnológicos (En construcción)

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						LOGO
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
	A.9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	A.9.4.1	Restricción de acceso a la Información	SI	Se aplica este control, porque se debe restringir el acceso a la información y a las funciones de los sistemas, de acuerdo a la política de control de acceso.	Instructivo de uso adecuado de las carpetas compartidas (En construcción).
		A.9.4.2	Procedimiento de Ingreso Seguro	SI	Este control aplica, ya que el acceso a los sistemas de información debe tener un proceso de ingreso seguro.	Procedimiento Gestionar usuarios Tecnológicos (En construcción)
		A.9.4.3	Sistema de Gestión de Contraseñas	SI	Este control aplica, ya que los sistemas de información deben poseer contraseñas seguras.	Procedimiento Gestionar usuarios Tecnológicos (En construcción) Instructivo de gestión del directorio activo (En construcción)

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						**LOGO**
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.9.4.4	Uso de programas utilitarios privilegiados	SI	Este control aplica, ya que los usuarios deben usar programas establecidos y cuya utilidad no represente riesgo para los sistemas de la empresa	Instructivo de uso de herramientas de mesa de servicio (En construcción)
		A.9.4.5	Control de Acceso a Códigos Fuente de Programas	SI	Aplica este control, ya que se debe restringir el acceso a los códigos fuentes de los programas a usuarios no autorizados.	Manual de Gestión de Configuración de proyectos de tecnologías de información (En Construcción)
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO	A.11.1 ÁREAS SEGURAS	A.11.1.1	Perímetro de seguridad física	SI	Aplica el control, ya que se deben definir e implementar perímetros de seguridad para proteger los edificios, oficinas y áreas de la empresa	Recursos Físicos respecto al SIGSI

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						LOGO
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.11.1.2	Controles de acceso físico	SI	Se deben implementar controles de acceso apropiados, para asegurar que solo se permite el acceso a personal autorizado.	Recursos Físicos respecto al SIGSI Manual de seguridad y vigilancia (Manual del Outsourcing de vigilancia de la empresa)
		A.11.1.3	Seguridad de oficinas, recintos e instalaciones	SI	Se deben aplicar los controles de perímetro de seguridad física a oficinas, recintos e instalaciones.	Recursos Físicos respecto al SIGSI
		A.11.1.4	Protección contra amenazas externas y ambientales	SI	Se debe tener control de protección contra amenazas externas o ambientales, ataques maliciosos o accidentes.	Recursos Físicos respecto al SIGSI
		A.11.1.5	Trabajo en áreas seguras	SI	Se adopta este control, ya que se debe diseñar y aplicar procedimiento de seguridad para trabajar en áreas seguras.	Recursos Físicos respecto al SIGSI

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						LOGO
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.11.1.6	Áreas de despacho y cargas	SI	Se aplica este control, toda vez que se deben controlar los puntos de acceso a la empresa, áreas de entrada y salida de mercancías o donde pueden ingresar personas no autorizadas (parqueaderos) y de ser posible aislarlos de las instalaciones donde se procesar la información para evitar el acceso no autorizado	Recursos Físicos respecto al SIGSI
	A. 11.2 EQUIPOS	A.11.2.1	Ubicación y protección de los equipos	SI	Este control aplica, ya que los equipos deben estar ubicados donde se encuentren protegidos y se reduzcan los riesgos y amenazas del entorno, y las posibilidades de acceso no autorizado.	Uso aceptable de los activos numeral 10.9 de este documento

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						LOGO
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.11.2.2	Servicio de suministro	SI	Se adopta este control, toda vez que los equipos deben estar protegidos contra fallas de energía y otras posibles interrupciones.	Recursos Físicos respecto al SIGSI
		A.11.2.3	Seguridad del cableado	SI	Si aplica este control, porque los cableados de suministro eléctrico y telecomunicaciones deben estar protegidos contra interceptación, interferencia o daño.	Documento de gestión de telecomunicaciones de la empresa (En Construcción)
		A.11.2.4	Mantenimiento de los equipos.	SI	Se adopta este control, porque a los equipos se les debe dar mantenimiento con regularidad de tiempo para asegurar su funcionamiento.	Mantenimiento preventivo y correctivo.

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						**LOGO**
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.11.2.5	Retiro de activos	SI	Si aplica este control, porque los equipos y software activos no se deben retirar de su sitio de inventario sin previo aviso.	Recursos Físicos respecto al SIGSI
		A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	SI	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la empresa, teniendo presente los riesgos adicionales que incurren al estar fuera de las instalaciones	Uso adecuado de los dispositivos de almacenamiento de información (En Construcción)
		A.11.2.7	Disposición Segura o Reutilización de equipos	SI	Este control aplica, ya que todos los equipos no activos, deben ser tratados de forma segura y su información completamente borrada antes de darlos de bajo o reutilizarlos.	Instructivo de borrado seguro de datos y formateo final de equipos (en construcción).

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						LOGO
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.11.2.8	Equipos de Usuario Desatendidos.	SI	Se adopta este control, ya que los equipos desatendidos deben tener atención de seguridad también.	Instructivo de gestión del directorio activo (En construcción)
		A.11.2.9	Política de Escritorio Limpio y pantalla Limpia	SI	Se debe adoptar una política de escritorio limpio.	Instructivo de gestión del directorio activo (En construcción)
A.12. SEGURIDAD DE LAS OPERACIONES	A. 12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	A.12.1.1	Procedimiento de Operación de Documentos	SI	Aplica este control porque todo procedimiento debe ser documentado y dejar a disposición de quien lo necesite	Documentación SIGSI
		A.12.1.2	Gestión de Cambios	SI	Todos los cambios de la organización, procesos de negocios, en las instalaciones y sistemas de información que afecten la seguridad informática deben ser controlados	Procedimiento de Gestión de Cambios (En revisión)

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						LOGO
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.12.1.3	Gestión de Capacidad	SI	Este control se aplica porque es necesario el conocer los recursos disponibles de la entidad y los que ya están en uso para hacer nuevas proyecciones, asegurando el desempeño de los sistemas.	Procedimiento de Gestión de Capacidad Disponible (En revisión)
		A.12.1.4	Separación de las instalaciones de desarrollo, ensayo y operación.	SI	Se aplica este control como buena práctica, ya que los ambientes de desarrollo, operación y ensayo deben estar independizados para reducir riesgos de acceso o cambios no autorizados en el ambiente de producción.	Instructivo de definición y uso de los ambientes de trabajo para el software (En Construcción)

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						**LOGO**
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
	A.12.2 PROTECCIÓN CONTRA CÓDIGO MALICIOSO	A.12.2.1	Controles contra códigos maliciosos	SI	Se adopta este control, ya que se deben tener herramientas, para la detección, prevención y recuperación de códigos malicioso, combinados con la toma de conciencia apropiada para su uso y evasión de los códigos maliciosos.	Software de Antivirus empresarial. Instructivo del uso de Antivirus y antimalware (En Construcción)

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						LOGO
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
	A.12.3 COPIAS DE RESPALDO	A.12.3.1	Respaldo de Información	SI	Se aplica este control, puesto que es necesario realizar copias de respaldo de información, software e imágenes de sistema y ponerlas a prueba regularmente de acuerdo a una política de copias de respaldo acordadas.	Procedimiento Generación de copias de seguridad (En Construcción) Procedimiento Restauración de copias de seguridad (En Construcción) Formato Solicitud de restauración de backup (En Construcción) Formato Solicitud realización de backup (En Construcción) Formato Bitácora de control de restauraciones de copias de seguridad (En Construcción)

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						LOGO
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
	A.12.4 REGISTRO Y SEGUIMIENTO	A.12.4.1	Registro de Eventos	SI	Se adopta este control, porque es necesario elaborar, conservar y revisar regularmente los registros de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	Instructivo de revisión de registros de TI (En construcción)
		A.12.4.2	Protección de la Información del registro	SI	Es necesario este control, ya que el registro de eventos debe estar protegido contra accidentes, alteraciones y accesos no autorizados.	Instructivo de revisión de registros de TI (En construcción)
		A.12.4.3	Registros del administrador y del operador	SI	Se adopta este control, porque los registros del administrador y del operador se deben registrar, proteger y revisar con regularidad.	Instructivo de revisión de registros de TI (En construcción)

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						**LOGO**
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.12.4.4	Sincronización de Relojes	SI	Si aplica, todos los relojes de todos los sistemas de información deben estar sincronizados.	Instructivo de sincronización de relojes (En Construcción)
	A.12.5 CONTROL DE SOFTWARE OPERACIONAL	A.12.5.1	Instalación de Software en Sistemas Operativos	SI	Se aplica este control, ya que se debe implementar procedimientos para controlar la instalación de software en sistemas operativos.	Instructivo de gestión del directorio activo (En construcción)
	A.12.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA	A.12.6.1	Gestión de las Vulnerabilidades Técnicas	SI	Se adopta este control, es necesario conocer las vulnerabilidades técnicas de la infraestructura de la empresa, evaluarlas y darles solución	Procedimiento Revisión a la plataforma de tecnología de información (En Construcción) Revisión externa de las condiciones de la plataforma (Contrato de Ethical Hacking)
		A.12.6.2	Restricciones sobre la instalación de Software	SI	Se hace necesario establecer reglas sobre la instalación del software en la entidad para evitar software malicioso o no legal.	Instructivo de gestión del directorio activo (En construcción

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						**LOGO**
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
	A.12.7 CONSIDERACIONES DSOBRE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	A.12.7.1	Controles de auditorías de sistemas de información	SI	Se adopta este control, puesto que los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos de negocio	Auditorias regulares de OCI Auditorías externas
A.13 SEGURIDAD EN LAS COMUNICACIONES	A.13.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES	A.13.1.1	Controles de Redes	SI	Gestionar, controlar y proteger la información en sistemas y aplicaciones mediante el acceso autorizado en los medios de comunicación.	Documento de gestión de telecomunicaciones de la empresa (En Construcción)
		A.13.1.2	Seguridad en los servicios de red	SI	Es necesario identificar los mecanismos de seguridad, ANS y los requisitos de gestión de los servicios de red,	Documento de gestión de telecomunicaciones de la empresa (En Construcción)

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						**LOGO**
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.13.1.3	Separación en las Redes	SI	Se adopta este control, ya que la separación de redes permite mejor control sobre el acceso a diferentes sistemas de información y mitiga el riesgo.	Documento de gestión de telecomunicaciones de la empresa (En Construcción)
	A.13.2 TRANSFERENCIA DE INFORMACIÓN	A.13.2.1	Políticas y procedimientos de transferencia de información	SI	Este control se hace necesario, ya que se debe contar con las políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información.	Documento de gestión de telecomunicaciones de la empresa (En Construcción)
		A.13.2.2	Acuerdos sobre trasferencia de Información	SI	Este control es necesario, porque los acuerdos de transferencia segura de información entre la empresa y las partes externas.	Documento de gestión de telecomunicaciones de la empresa (En Construcción)
		A.13.2.3	Mensajería Electrónica	SI	Es necesario establecer la protección de la información incluida en la mensajería electrónica.	Instructivo de servicio de correo electrónico institucional.

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						LOGO
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.13.2.4	Acuerdos de Confidencialidad o de no divulgación.	SI	Se adopta este acuerdo, ya que es necesario identificar y documentar los requisitos de la confidencialidad de la información y no divulgación que prevengan el uso inadecuado de la información de la empresa.	Formato de acuerdo de confidencialidad de terceros (En revisión)
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	A.14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	A.14.1.1	Análisis y especificación de requisitos de Seguridad de la Información	SI	Se aplica este control, toda vez que siempre deben existir los requisitos de seguridad de información para nuevos como para sistemas existentes.	Procedimiento de Gestión de TI (En Construcción) Procedimiento de Gestión de Sistemas de Información (En revisión)
		A.14.1.2	Seguridad en los servicios de las aplicaciones en redes públicas	SI	La información que se divulga a través de las redes públicas debe ser salvaguardada de actividades de fraude, divulgación y modificación no autorizada	Procedimiento de Gestión de TI (En Construcción)

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						LOGO
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	SI	Se adopta este control, ya que la información involucrada en las redes y servicios públicos se debe proteger de evitar transmisión incompleta, enrutamiento equivocado, y duplicación o divulgación de mensajes no autorizados.	Procedimiento de Gestión de TI (En Construcción) Documento de gestión de telecomunicaciones de la empresa (En Construcción)
	A.14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	A.14.2.1	Política de Desarrollo Seguro	SI	Es necesario tener y aplicar reglas para el desarrollo de software dentro de la empresa (SI APLICA)	Procedimiento de Gestión de TI (En Construcción)
		A.14.2.2	Procedimiento de Control de Cambios en Sistemas	SI	Se debe definir el ciclo de vida de un software y controlar los cambios que se realizan a él de manera formal	Procedimiento de Gestión de TI (En Construcción) Procedimiento de Gestión de Cambios (En revisión)

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						**LOGO**
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.14.2.3	Revisión Técnicas de las Aplicaciones después de los cambios en la plataforma de operación	SI	Se adopta este control, ya que se debe contar con un plan de pruebas para verificar los sistemas y aplicaciones de la empresa posterior a un cambio realizado	Procedimiento de Gestión de TI (En Construcción)
		A.14.2.4	Restricciones en los cambios a los paquetes de software	SI	Se aplica este control, toda vez que se deben regular los cambios que se hace al software y permitir solo los necesarios.	Procedimiento de Gestión de TI (En Construcción)
		A.14.2.5	Principios de construcción de sistemas seguros	SI	Es necesario mantener, establecer y documentar la construcción de sistemas seguros y aplicarlos a cualquier actividad de desarrollo de sistemas de información.	Procedimiento de Gestión de TI (En Construcción)

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						LOGO
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.14.2.6	Ambiente de desarrollo seguro	SI	Se adopta este control, ya que la empresa debe garantizar el sistema de desarrollo de software con las garantías de seguridad.	Procedimiento de Gestión de TI (En Construcción)
		A.14.2.7	Desarrollo contratado externamente	SI	Si aplica este control, ya que la empresa debe supervisar y vigilar el desarrollo de software externo.	Procedimiento de Gestión de TI (En Construcción)
		A.14.2.8	Pruebas de seguridad de sistemas	SI	Si aplica este control, puesto que durante el desarrollo propio o externo de software se deben llevar a cabo las pruebas de funcionalidad.	Procedimiento de Gestión de TI (En Construcción)
		A.14.2.9	Pruebas de aceptación de sistemas	SI	Las pruebas de aceptación deben ser realizadas por los usuarios finales antes del paso a producción de una aplicación o sistemas de información.	Formato de aceptación de aplicaciones desarrolladas

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						**LOGO**
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
	14.3 DATOS DE PRUEBA	A.14.3.1	Protección de datos de prueba	SI	Se acepta este control, ya que los datos que se prestan para pruebas deben ser protegidos y controlados	Formato de aceptación de aplicaciones desarrolladas
A.15 RELACIONES CON LOS PROVEEDORES	A.15.1 SEGURIDAD E LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES	A.15.1.1	Política de Seguridad de la Información para las relaciones con proveedores	SI	Este control aplica, ya que los requisitos de seguridad de la información para las relaciones con proveedores se deben acordar y documentar	Relación con proveedores
		A.15.1.2	Tratamiento de la Seguridad dentro de los acuerdos con proveedores	SI	Este control aplica, toda vez que se deben establecer responsabilidades y acuerdos de confidencialidad de la información que manejarán los proveedores	Relación con proveedores

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						LOGO
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.15.1.3	Cadena de Suministros de Tecnología de Información y Comunicación	SI	Se adopta este control, toda vez que el acuerdo con proveedores debe tener los requisitos de seguridad de la información relativos al acceso, proceso y almacenamiento de la infraestructura TI y de los sistemas de información	Relación con proveedores
	A.15.2 GESTIÓN DE LA PRESTACIÓN DE LOS SERVICIOS DE PROVEEDORES	A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	SI	Se adopta este control, toda vez que los convenios con los proveedores deben tener un seguimiento para monitorear sus actividades y ser auditados.	Relación con proveedores

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						LOGO
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.15.2.2	Gestión de Cambios en los Servicios de los Proveedores	SI	Aplica este control, porque se deben gestionar los cambios en el suministro de servicios con proveedores, incluido el mantenimiento y la mejora de políticas procedimientos y controles de la seguridad informática	Relación con proveedores Procedimiento de Gestión de Cambios (En revisión)
A.16 GESTIÓN DE INCIDENTES DE SEGURIDA DE LA INFORMACIÓN	A.16.1 GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	A.16.1.1	Gestión de Incidentes / Responsabilidades y Procedimientos	SI	Se adopta este control, toda vez que se deben establecer las responsabilidades y procedimientos de gestión de incidentes para dar respuesta eficaz a aquellos sucesos que interfieran en el funcionamiento normal de los SI	Procedimiento de Gestión de Incidentes de Seguridad de la Información (En publicación)

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						LOGO
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.16.1.2	Reporte de Eventos de Seguridad de la Información	SI	Se adhiere este control puesto que incidentes de seguridad de la información deben quedar reportados y registrados a través de los canales de gestión apropiados.	Procedimiento de Gestión de Incidentes de Seguridad de la Información (En publicación)
		A.16.1.3	Reporte de debilidades de seguridad de la información	SI	Se toma este control porque todos los usuarios internos y externos de la empresa que usan los servicios de información, deben reportar las debilidades o falencias de seguridad que sean encuentren en dichos sistemas	Procedimiento de Gestión de Incidentes de Seguridad de la Información (En publicación)
		A.16.1.4	Evaluación de Eventos de Seguridad de la Información y decisiones sobre ellos	SI	Se toma este control, puesto que los incidentes de seguridad se deben evaluar para revisar si son incidentes conocidos	Procedimiento de Gestión de Incidentes de Seguridad de la Información (En publicación)

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						**LOGO**
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.16.1.5	Respuesta a incidentes de Seguridad de la Información	SI	Este control se toma ya que todo incidente de seguridad debe tener respuesta casi inmediata de acuerdo con los procedimientos documentados	Procedimiento de Gestión de Incidentes de Seguridad de la Información (En publicación)
		A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	SI	Se adopta este control puesto que el conocimiento adquirido al analizar y resolver los incidentes, debe quedar en una base de conocimiento para reducir la posibilidad de los problemas futuros.	Procedimiento de Gestión de Incidentes de Seguridad de la Información (En publicación)
		A.16.1.7	Recolección de la Evidencia	SI	Se adopta este control, toda vez que debe quedar la base de conocimiento de los incidentes conocidos, para la identificación de ellos como evidencia.	Procedimiento de Gestión de Incidentes de Seguridad de la Información (En publicación)

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						**LOGO**
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
A.17 ASPECTOS DE SEGURIDA D DE LA INFORMACIÓN PARA LA GESETIÓN DE LA CONTINUIDAD DE NEGOCIO	A.17.1 CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN	A.17.1.1	Planificación de la continuidad de la Seguridad de la Información	SI	Se adopta este control, toda vez que la empresa debe determinar los requisitos para la continuidad de la seguridad de la información	Documento Plan de continuidad de negocios para los servicios de TI (En construcción)
		A.17.1.2	Implementación de la continuidad de la Seguridad de la Información	SI	Se adopta este control, porque la empresa debe establecer, documentar e implementar los procesos, procedimientos y controles para asegurar la continuidad de negocio.	Documento Plan de continuidad de negocios para los servicios de TI (En construcción)
		A.17.1.3	Verificación, revisión y evaluación de la continuidad de la Seguridad de la Información	SI	Se toma este control, porque la empresa debe revisar, evaluar y corregir la continuidad del negocio para mantener los servicios de los sistemas de seguridad de la información.	Documento Plan de continuidad de negocios para los servicios de TI (En construcción)

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						**LOGO**
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
	A.17.2 IMPLEMENTAR LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	SI	Se toma este control, porque la empresa debe velar por mantener redundancia en las instalaciones para mantener en funcionamiento los sistemas de información de QWERTY S.A.	Documento Plan de continuidad de negocios para los servicios de TI (En construcción)
A.18 CUMPLIMIENTO	A.18.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES	A.18.1.1	Identificación de la legislación aplicable y los requisitos contractuales	SI	Se adopta este control, puesto que todos los requisitos estatutarios, reglamentarios y contractuales pertinentes deben cumplirse se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información.	Formato de actualización y normalización de la empresa

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						LOGO
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.18.1.2	Derechos de Propiedad Intelectual (DPI)	SI	Se toma este control porque es necesario cumplir con los requisitos estatutarios, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de software.	Procedimiento de gestión de licenciamiento de SW
		A.18.1.3	Protección de Registros	SI	Se adhiere este control puesto que los registros de los requisitos reglamentarios y contractuales deben protegerse contra perdida, falsificación y destrucción o acceso no autorizado.	Procedimiento de gestión de licenciamiento de SW

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						LOGO
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.18.1.4	Privacidad y Protección de Información de datos personales.	SI	Se adopta este control, ya que la empresa de garantizar la privacidad y protección de los datos personales de los usuarios internos y externos de la empresa de acuerdo a la legislación y reglamentación pertinente.	Política de protección de datos personales.
	A.18.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN	A.18.2.1	Revisión Independiente de la Seguridad de la Información	SI	Se adopta este control, toda vez que los procesos, procedimientos, objetivos de control, controles, políticas y gestión de la seguridad de la información se deben revisar periódicamente.	Procedimiento Revisión a la plataforma de tecnología de información (En Construcción) Procedimiento Evaluación independiente y auditorías internas (En construcción)

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						**LOGO**
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**
		A.18.2.2	Cumplimiento con las políticas y normas de seguridad	SI	Se toma este control, ya que se debe revisar periódicamente el cumplimiento de los procesos, procedimientos, objetivos de control, políticas y gestión relacionados con las normas de seguridad de los sistemas de información.	Procedimiento de Seguimiento a la Gestión de TI (En construcción)
		A.18.2.3	Revisión del cumplimiento técnico.	SI	Se toma este control, puesto que los Sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información	Procedimiento de Seguimiento a la Gestión de TI (En construcción)

Total, controles implementados	
Total, controles SIN implementar	

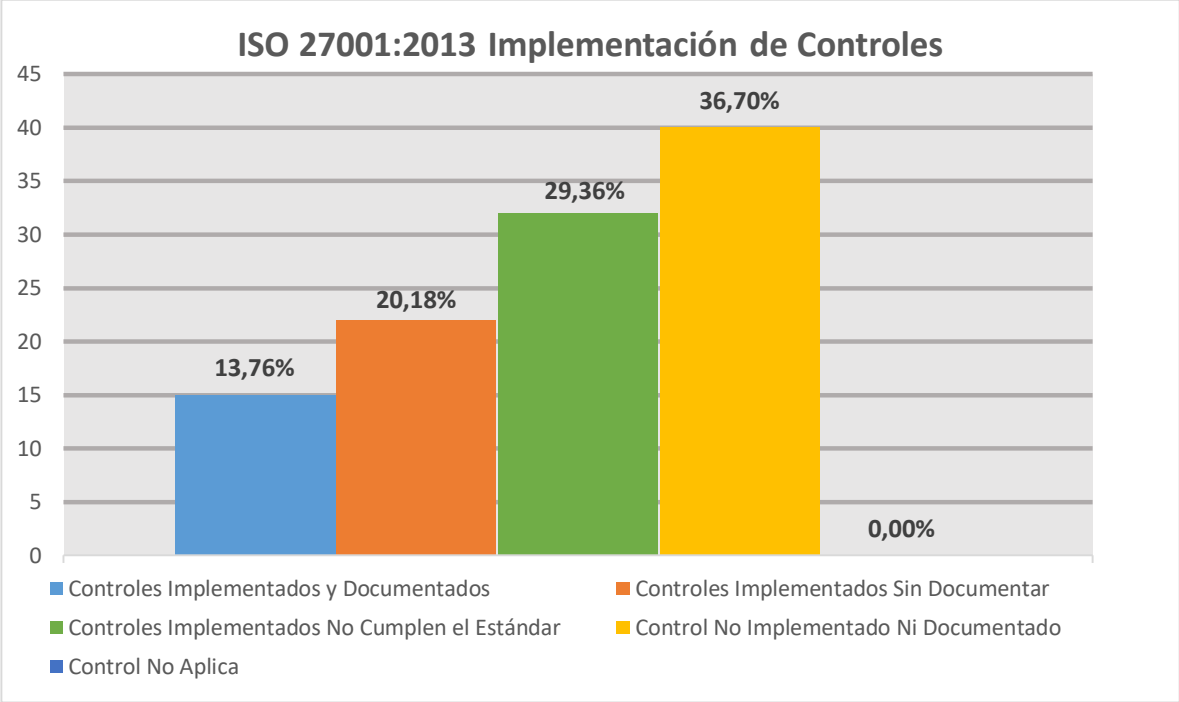
Revisado por: _____ Fecha de Revisión: _____

Profesional delegado del SIGSI

FORMATO DECLARACIÓN DE APLICABILIDAD (DA- SIGSI) PARA SEGURIDAD DE LA INFORMACIÓN						**LOGO**
CODIGO FTI-01	**PROCESO** GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN				**VERSIÓN** 1	
Dominio	**Subdominio**	**Control Actual**	**Objetivos de Control**	**Aplica**	**Justificación**	**Declaración de Aplicabilidad**

Fuente: propia

Ilustración 12. Análisis del Estado de Implementación



fuente propia

Se puede ver que solamente el 13,76% de los controles que se pueden encontrar en el estándar ISO 27001:2013 se están cumpliendo, lo cual es bastante bajo para la empresa dado la cantidad de activos imprescindibles que tiene la empresa y que al contrario de esto el 86,24% son controles no implementados, mal implementados (no cumplen con el estándar) o implementados sin documentar. Lo cual es un riesgo de seguridad de la información ya que no se deja una trazabilidad del conocimiento adquirido para mitigar el riesgo sobre el activo y puede ser costando lo mismo durante los años venideros sin validar la depreciación del activo.

Esto genera una alerta que debe ser atendida con la disposición de los elementos necesarios para bajar el riesgo, razón por la cual es preciso rediseñar los controles, documentar algunos o construir aquellos que no están para mejorar la protección de los bienes de la empresa y evitar las grandes pérdidas de la información y las vulnerabilidades.

De acuerdo con lo analizado, es posible evidenciar que QWERTY S.A. presenta falencias en cuanto a la aplicación de controles a la luz de la norma, por lo cual se hace necesario crear un plan de tratamiento de gestión de riesgos donde se definan los controles a través de procesos transversales y globales a la empresa en el estándar de la ISO 27001:2013, para evitar que las amenazas se conviertan en hechos a través de la explotación de las vulnerabilidades de los activos de información por no poseer dichos controles. Es por esto que se propone el diseño de un Sistema Integrado de Gestión de Seguridad Informática que contengan declarados y definidos los puntos que se exponen a continuación, con base en los hallazgos obtenidos.

10.5. ALCANCE DEL SISTEMA DE GESTIÓN INTEGRADO DE SEGURIDAD DE LA INFORMACIÓN

El sistema integrado de gestión de seguridad de la información quiere desde su inicio crear una base del estado de seguridad de la dependencia de informática de QWERTY S.A. facilitando la identificación de la fisura entre el estado actual y la implementación del modelo. Debe entenderse como punto de partida la primera medición de la percepción de seguridad que se tiene en la dependencia de la empresa y la manifestación de la necesidad de la implementación del sistema de seguridad de la información.

La seguridad de la información debe entenderse como un entorno envolvente que posee diferentes principios básicos que son relevantes a la hora de realizar las pruebas. La evaluación de seguridad ha de ser útil como la etapa inicial, pero no es efectiva para realizar evaluaciones más complejas que se vayan dando al mejorar los niveles de seguridad. Es por esto que la seguridad de la información es un proceso que muta con el tiempo y no debe entenderse como un producto final para entregar.

Es por esto que el SIGSI propuesto tendrá un alcance inicial, y será desarrollado como un primer eslabón en la gran empresa de construir los procesos, los procedimientos, la normatividad y las políticas que empezarán a aplicarse en la dependencia de sistemas y luego irán expandiéndose para permear toda la empresa, desarrollándose de manera estratégica, tener un ciclo de vida, y ser revaluado con cierta periodicidad de tiempo.

10.6. USO ACEPTABLE DE LOS ACTIVOS

10.6.1. Propiedad y uso general

- La información propiedad de la QWERTY S.A, independiente del dispositivo de almacenamiento, electrónico o informático, en calidad de propio o arrendado, de un empleado, contratista, proveedor o tercero sigue siendo propiedad exclusiva de la empresa. Todo usuario ha de asegurar a través de los medios legales y/o técnicos que la información se encuentra protegida conforme a la política de Protección de Datos Estándar.

- Todo usuario (interno o externo) que tenga un vínculo laboral, de participación o de confidencialidad con la empresa está en la completa obligación de reportar de forma inmediata sobre robo, alteración, daño, perdida o divulgación no autorizada de información propia de la empresa.

- Todo usuario (interno o externo) puede acceder, usar o compartir información propiedad de QWERTY S.A. en la medida que sea autorizado y sea necesario con sus funciones o actividades asignadas.

- Los empleados son responsables a su idiosincrasia de hacer un uso correcto de las aplicaciones de interés personal, las dependencias de forma propia, son

responsables de la creación de guías, instructivos o manuales referentes al uso de los sistemas de la entidad (Intranet, Extranet, Internet). Si dichas guías no existen, lo empleados deben ser cobijados por las políticas de seguridad de la información consultadas a su supervisor o gerente.

- El comportamiento dentro de la red de la empresa, en concordancia con las políticas de seguridad de la información ha de ser individualizado, monitoreado y documentado de acuerdo a las políticas de auditoria.

- QWERTY S.A. se reserva el derecho de auditar las redes y sistemas de manera periódica para asegurar el cumplimiento de la política de uso aceptable de los activos.

10.6.2. Seguridad de Información Propietaria

- Cada uno de los dispositivos móviles y de cómputo que se conectan a la red interna de la empresa, deben cumplir la Política de Acceso Mínimo como el uso de usuario y contraseña.

- Todas las contraseñas a nivel de sistemas y/o usuario deben cumplir con la Política de Contraseñas seguras que se tiene en la empresa. Entendiéndose que se encuentra prohibido facilitar el acceso a otros usuarios, sin vínculo laboral con la empresa o haber pasado por diligenciar y aprobar el acuerdo de confidencialidad, ya sea de forma intencional, omisión o por error.

- Cada uno de los dispositivos informáticos han de estar asegurados con un protector de pantalla, protegido por contraseña con la función de activación automática a los 600 segundos. Si el usuario va a dejar su estación de trabajo

o activo desatendido, retirándose del sitio, se aplicará la política de bloqueo de pantalla implementado en el directorio activo.

- Cada una de las publicaciones de información realizada por los usuarios internos de la empresa por medio de un correo electrónico institucional a grupos de noticias, foros, redes sociales entre otros, deben contener una advertencia que indique que las opiniones expresadas son estrictamente del usuario y no necesariamente involucran las opiniones de la empresa a menos que las publicaciones formen parte de las obligaciones, actividades y labores en la empresa.

- Los usuarios deben extremar precauciones al abrir archivos adjuntos de correo electrónico recibidos de remitentes desconocidos, a fin de evitar spam, malware o contenido malicioso.

10.6.3. Uso Inaceptable

Las actividades enunciadas a continuación se encuentran prohibidas, exceptuando aquellas circunstancias en que los usuarios por sus funciones o desempeño legítimo o autorizado de sus funciones tengan que realizarlas.

En ninguna circunstancia, un usuario interno o externo está autorizado a participar en actividades que sean consideradas ilegales bajo las leyes del país, locales o de índole internacional, utilizando recursos de la empresa y que pongan en tela de juicio su buen nombre.

Las siguientes actividades no son exhaustivas, solo proporcionan un marco para aquellas actividades iniciales que se consideran de uso inaceptable.

10.6.3.1. Actividades de red y sistemas

- Violación a los derechos de autor de cualquier persona o empresa, patentes o propiedad intelectual, leyes o reglamentos, incluyendo, pero no limitando a la instalación de software “no licenciado” u otros productos que no contenga licencia apropiada para la empresa.

- La violación a los derechos de copia de materiales como revistas, fotografías, libros y cualquier otra fuente escrita, musical o audiovisual, sin previa autorización por parte de su(s) autor(es).

- El uso de cuentas de usuario, servidores o acceso a datos que no sea para actividades de la empresa, incluso si cuenta con acceso autorizado está prohibido.

- La exportación de software, información técnica o tecnología de cifrado en actividades que violen las leyes internacionales, regionales o locales. Debe ser consultado el manejo adecuado antes de realizar dicha exportación.

- El uso de programas maliciosos como virus, gusanos, caballos de Troya, ransomware entre otros en la red o en servidores.

- Compartir la contraseña de acceso a servicios de la empresa a familiares, amigos o conocidos.

- Usar un activo de cómputo para participar, reclutar o transmitir material que incumpla las leyes de acoso sexual, acoso laboral u hostilidad en la empresa o lugar de trabajo.

- Usar un activo de cómputo para realizar ofertas fraudulentas de productos, artículos o servicios procedentes de cualquier cuenta propiedad de la empresa.

- Realizar actividades que ocasiones problemas de seguridad o interrupción en la comunicación de la red. Dichas violaciones incluyen, pero no están limitadas al acceso indebido de datos para los que no es destinatario o conectarse a un servidor o cuenta de usuario sin autorización previa. Para los propósitos de esta sección, "interrupción" incluye, pero no se limita al espionaje en la red, inundaciones de ping, suplantación de paquetes, denegación de servicios, etc., con fines maliciosos

- Realizar actividades de barrido de puertos, escaneos de seguridad o cualquier otra que no esté debidamente diligenciada como actividad de mejora por la dependencia de sistemas y seguridad de la información de la empresa.

- Ejecutar cualquier análisis en la red que intercepte datos destinados a servidores o activos de cómputo de usuario final, a menos que esta labor esté debidamente diligenciada como actividad de mejora por la dependencia de sistemas y seguridad de la información de la empresa.

- No realizar la autenticación de usuarios y la seguridad de cualquier activo de red, de cómputo o cuenta de usuario interno o externo.

- Introducir Honeypots, Honeynets o tecnología similar en la red empresarial.

- Realizar actividades de denegación de servicio o cualquier similar que niegue parcial o completamente los servicios de la empresa.

- Realizar actividades que conlleven a ejecutar /scripts /comandos o envío de mensajes con la intención de dañar, pausar o interferir en las sesiones normales

de usuario final, por cualquier medio, de forma local o a través de la red /Internet /Extranet /Intranet.

- Proporcionar información confidencial y personal sobre usuarios internos y/o externos a la empresa.

- El ingreso de dispositivos de almacenamiento extraíble (memorias, pendrive, discos duros portátiles entre otros), su uso y autorización debe estar dado por la dependencia de sistemas.

- La extracción de información propiedad de la empresa utilizando cualquier medio que no esté relacionada con sus labores normales de trabajo.

- El acceso a sitios Web de dudosa reputación o potencialmente peligrosos, tales como de Pornografía, Malware, Piratería, Proxy, etc.

10.6.3.2. Actividades de comunicación de información y correo electrónico

- Envió de correo electrónico que no tenga que ver con actividades de la empresa, incluyendo el envío de “correo malintencionado”, “publicidad”, “correo basura” u otro material que no haya sido especificado.

- Cualquier forma de acoso de índole laboral, sexual entre otro, teléfono u otro medio con lenguaje soez y mal intencionado.

- El uso no autorizado o la alteración del contenido de encabezados de correo electrónico.

- Solicitar datos personales a cualquier usuario interno o externo, con vinculo o no con la empresa a fin de recolectar respuestas con uso malintencionado o propio ajeno a las actividades propias de la empresa.

- El uso de correo electrónico de forma indebida por parte de los usuarios internos y externos o por sus proveedores de servicio dentro y fuera de la empresa para hacer publicidad.

- La publicación repetida de los mismos mensajes o similares, no relacionados con el negocio a un gran número de grupos de noticias, Foros, Blogs, Redes Sociales, entre otros.

10.5.3.3 Blogs y Medios Sociales

- Solo las personas de la dependencia de comunicaciones están autorizados a realizar publicaciones a Blogs o Redes Sociales desde las cuentas empresariales, para el resto de usuario está prohibido. Los blogs de los sistemas internos de la empresa son objeto de seguimiento.

- La información descrita como propietaria de la empresa no debe ser revelada, publicada o transmitida a través de Blogs o Redes Sociales.

- Los usuarios no podrán participar en ningún Blog o Red Social que pueda dañar o ensuciar la imagen, reputación y/o buena voluntad de la empresa y/o cualquiera de sus empleados.

- Los usuarios tienen prohibido hacer comentario discriminatorio, palabras despectivas, difamatorias o de acoso cuando participen en Blogs, Redes Sociales u otros medios.

- Los usuarios tampoco pueden atribuir las declaraciones personales, opiniones o creencias a la empresa cuando participan en los blogs y redes sociales. Si un usuario está expresando sus creencias y / u opiniones en Blogs o Red Social, el usuario no puede, expresa o Implícitamente, representarse a sí mismos como empleado o representante de la empresa. Los empleados asumen cualquier y todos los riesgos asociados con estas publicaciones.

10.7. MÉTODO DE GESTIÓN DE LOS RIESGOS QWERTY

10.7.1. INDICADORES DE GESTIÓN

Los indicadores de gestión y cumplimiento de seguridad de la información están relacionados con las razones que contribuyen a la administración del proceso, activo o sistema de información, así como el grado de consecución de las actividades propuestas para reducción, mitigación o aceptación del riesgo.

En QWERTY S.A. se establecen los siguientes indicadores de gestión de seguridad de la información haciendo uso de fórmulas que miden el porcentaje de los controles implementados y de esta manera validar si el control implementado es lo suficientemente efectivo para mitigar el riesgo o se debe mejorar o cambiar:

Tabla 25 Indicador de Gestión - Organización de la Información

INDICADOR 01- ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN					
IDENTIFICADOR	SIGSI-IN-01				
DEFINICIÓN	Determina y hace seguimiento al compromiso de los altos niveles de personal de la empresa en lo referente a la asignación de personal y responsabilidades relacionadas a la seguridad de la información al interior de QWERTY S.A.				
OBJETIVO	Informar sobre las acciones de los altos mandos en la asignación de recursos en la gestión de seguridad de la información.				
TIPO DE INDICADOR	Indicador de Gestión				
DESCRIPCIÓN DE VARIABLES		**FORMULA**		**FUENTE DE INFORMACIÓN**	
IN01-V01: Número de personas con su rol definido		$\left(\frac{IN01 - V01}{IN01 - V02}\right) X\ 100$		Contratación y asignación de roles al personal de la empresa.	
IN01-V02: Número de personas con su respectivo rol definido después de un año de gestión				Actas de asignación de personal	
METAS					
MÍNIMA	75% - 80%	**SATISFACTORIA**	80% - 90%	**SOBRESALIENTE**	100%
OBSERVACIONES					
La creación de nuevos cargos y asignación de responsabilidades a estos, por lo cual el indicador no está solamente orientado a la contratación de nuevas personas sino a la asignación de responsabilidades a las que ya se encuentran laborando.					

Fuente: propia basada en el guía 9 de mintic

Tabla 26 Indicador de Gestión – Cubrimiento SIGSI

INDICADOR 02- CUBRIMIENTO DE SIGSI EN LOS ACTIVOS DE QWERTY S.A.					
IDENTIFICADOR	SIGSI-IN-02				
DEFINICIÓN	Se busca identificar y hacer seguimiento al comportamiento de los activos críticos de información que tiene la empresa y los controles que se pueden aplicar sobre ellos.				
OBJETIVO	Hacer el seguimiento al inventario e inclusión de activos de la empresa y su control, dentro del marco de referencia para el sistema integrado de gestión de seguridad de información adoptado por QWERTY S.A.				
TIPO DE INDICADOR	Indicador de Gestión				
DESCRIPCIÓN DE VARIABLES		**FORMULA**		**FUENTE DE INFORMACIÓN**	
IN02-V04: Número de activos incluidos en el SIGSI en la zona de riesgo inaceptable y la implementación del control no requiere compra de elementos de hardware o software.		$\left(\frac{IN02 - V03}{IN02 - V04}\right) X\ 100$		Alcance del SIGSI, activos de información, plan de tratamiento de riesgos y matriz de riesgos.	
IN02-V04: Número de activos incluidos en el SIGSI en la zona de riesgo inaceptable				Inventario de activos de información, nuevos	
METAS					
MÍNIMA	75% - 80%	**SATISFACTORIA**	80% - 90%	**SOBRESALIENTE**	100%
OBSERVACIONES					
Incluir un activo, es una correcta clasificación del activo, su tratamiento en la evaluación de riesgos y los controles que se pueden aplicar a dicho activo para minimizar el riesgo calculado.					

Fuente: propia basada en el guía 9 de mintic

Tabla 27 Indicador de Gestión Plan SIGSI de conocimiento

INDICADOR 03- PLAN DE CONOCIMIENTO DE SIGSI					
IDENTIFICADOR	SIGSI-IN-03				
DEFINICIÓN	Este indicador permite medir el conocimiento de los usuarios finales sobre los temas de seguridad informática y su aplicación en los activos de la entidad bajo su asignación. Se pueden realizar por medio de auditorías y por los porcentajes de la participación en transferencias de conocimientos sobre seguridad informática en QWERTY S.A.				
OBJETIVO	Evidenciar la efectividad de los planes de comunicación, sensibilización y aprendizaje de los temas relacionados a la seguridad informática de la empresa.				
TIPO DE INDICADOR	Indicador de Gestión				
DESCRIPCIÓN DE VARIABLES		**FORMULA**		**FUENTE DE INFORMACIÓN**	
IN03-V05: Número de fallas o incumplimientos en los programas de sensibilización o evaluación de los eventos realizados para dar a conocer la temática		$\left(\frac{IN03 - V05}{IN03 - V06}\right) X\ 100$		Auditorías internas, atención al ciudadano, lista de asistencia a eventos de sensibilización	
IN03-V06: Total de personas a sensibilizar sobre la seguridad informática				Total de empleados y usuarios de QWERTY S.A.	
METAS					
MÍNIMA	75% - 80%	**SATISFACTORIA**	80% - 90%	**SOBRESALIENTE**	100%
OBSERVACIONES					
Se debe tener todos los insumos que puedan probar la entrada, participación y asistencia a las actividades periódicas que permitan medir al personal capacitado.					

Fuente: propia basada en el guía 9 de mintic

Tabla 28 Indicador de Gestión Cumplimiento de Políticas

INDICADOR 04- CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN QWERTY S.A.			
IDENTIFICADOR	SIGSI-IN-04		
DEFINICIÓN	Medir el cumplimiento de las políticas definidas para la seguridad de información en QWERTY S.A.		
OBJETIVO	Identificar el nivel de madurez de los procesos de QWERTY S.A. orientados a SIGSI		
TIPO DE INDICADOR	Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
IN04-V07: ¿La empresa ha definido una política general de seguridad de la información?		IN04-V0X = 1 (si hay evidencia) IN04-V0X = 0 (NO hay evidencia)	Sistema Integrado de Gestión de la Seguridad Informática
IN04-V08: ¿La empresa definió una organización en termino de personal, roles y responsabilidades para cumplir con las políticas?			Sistema Integrado de Gestión de la Seguridad Informática
IN04-V09: ¿La empresa cumple los requisitos legales, reglamentarios y contractuales?			Sistema Integrado de Gestión de la Seguridad Informática
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

Tabla 29 Indicador de Gestión Lineamientos de Seguridad

INDICADOR 05- IDENTIFICACIÓN DE LOS LINEAMIENTOS DE SEGURIDAD DE QWERTY S.A.			
IDENTIFICADOR	SIGSI-IN-05		
DEFINICIÓN	Se quiere medir el grado de seguridad en los equipos de cómputo.		
OBJETIVO	Medir el nivel de preparación del recurso humano en cuanto aplicar seguridad informática en los equipos de computo		
TIPO DE INDICADOR	Indicador de Gestión		
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
IN05-V10: ¿La empresa posee lineamientos de trabajo de los responsables de seguridad informática y vigila el cumplimiento de sus políticas periódicamente?		IN05-VX = 1 (si hay evidencia) IN05-VX = 0 (NO hay evidencia)	Usuarios Internos
IN02-V11: ¿La empresa posee lineamientos de protección de las instalaciones físicas, los equipos de cómputo y su entorno para evitar accesos no autorizados mitigando el riesgo de la información de la entidad y vigila el cumplimiento de estos con regularidad?			Usuarios internos
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

Fuente: propia basada en el guía 9 de mintic

Tabla 30 Indicador de Gestión - Control de acceso

INDICADOR 06- VERIFICACIÓN DEL CONTROL DE ACCESO			
IDENTIFICADOR	SIGSI-IN-06		
DEFINICIÓN	Revisa los procedimientos, actividades, normativas y estándares en cuanto al control de acceso a la empresa		
OBJETIVO	Identificar la existencia de políticas de control de acceso.		
TIPO DE INDICADOR	Indicador de cumplimiento		
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
IN06-V12: ¿La empresa tiene normas para controlar el acceso de los usuarios, empleados, terceros, contratistas, proveedores entre otros, a las instalaciones de la misma y sus oficinas?		IN06-VX = 1 (si hay evidencia) IN06-VX = 0 (NO hay evidencia)	Usuarios internos y externos.
IN06-V13: ¿La empresa tiene normas para controlar el acceso de los usuarios, empleados, terceros, contratistas, proveedores entre otros, a sus servicios y redes de comunicación?			Usuarios internos y externos.
IN06-V14: ¿La empresa tiene normas para controlar el acceso de los usuarios, empleados, terceros, contratistas, entre otros, a los sistemas de información?			Usuarios internos
IN06-V15: ¿La empresa tiene normas para controlar el acceso de los usuarios, empleados, terceros, contratistas, entre otros, terminales móviles y accesos remotos a los recursos de QWERTY S.A.?			Usuarios Internos
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

Fuente: propia basada en el guía 9 de mintic

Tabla 31 Indicador de Gestión - Mantenimiento de Software

INDICADOR 07- ADQUISICIÓN Y MANTENIMIENTO DE SOFTWARE			
IDENTIFICADOR	SIGSI-IN-07		
DEFINICIÓN	Este indicador quiere medir las políticas que se tienen presente en la empresa para la adquisición de software, la ejecución de software libre, y el desarrollo de software en la empresa (si se presenta el caso)		
OBJETIVO	Identificar las políticas, normas o lineamientos en cuanto al software que posee la empresa y/o desarrollo de software in-house		
TIPO DE INDICADOR	Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
IN07-V16: ¿Se poseen políticas, lineamientos, normas y/o estándares para la adquisición de software y/o aplicaciones licenciado de terceros en la empresa?		IN07-VX = 1 (si hay evidencia) IN07-VX = 0 (NO hay evidencia)	Usuarios internos
IN07-V17: ¿Se poseen políticas, lineamientos, normas y/o estándares para la adquisición de software y/o aplicaciones libre en la empresa?			Usuarios internos
IN07-V18: ¿Se poseen políticas, lineamientos, normas y/o estándares para la adquisición de software desarrollado en la empresa?			Usuarios del grupo de desarrollo (si aplica en QWERTY S.A.)
IN07-V19: ¿Se poseen políticas, lineamientos, normas y/o estándares para la gestión de cambios de software que posee la empresa (adquirido o desarrollado)?			Usuarios internos
IN07-V20: ¿Se poseen políticas, lineamientos, normas y/o estándares para la gestión de incidentes de software que posee la empresa (adquirido o desarrollado)?			Usuarios internos
IN07-V21: ¿Se poseen políticas, lineamientos, normas y/o estándares para la gestión de requerimientos de software que posee la empresa (adquirido o desarrollado)?			Usuarios internos
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

Fuente: propia basada en el guía 9 de mintic

Tabla 32 Indicador de Gestión – Confidencialidad de la Información

INDICADOR 08- DIMENSIÓN DE CONFIDENCIALIDAD DE LA INFORMACIÓN			
IDENTIFICADOR	SIGSI-IN-08		
DEFINICIÓN	Se quiere reflejar una métrica de clasificación de la información confidencial en la empresa.		
OBJETIVO	Identificar el nivel de políticas y/o procedimientos para clasificar la información de la empresa como confidencial		
TIPO DE INDICADOR	Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
IN08-V22: ¿Se han implementado lineamientos, normas y/o estándares para clasificar la información como confidencial (personal y privada) de los diferentes sistemas de información de QWERTY S.A.?		IN08-VX = 1 (si hay evidencia) IN08-VX = 0 (NO hay evidencia)	Usuarios internos
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

Fuente: propia basada en el guía 9 de mintic

Tabla 33 Indicador de Gestión Integridad de la Información

INDICADOR 09- DIMENSIÓN DE INTEGRIDAD DE LA INFORMACIÓN			
IDENTIFICADOR	SIGSI-IN-09		
DEFINICIÓN	Se quiere reflejar una métrica de clasificación de la integridad de la información en la empresa.		
OBJETIVO	Identificar el nivel de políticas y/o procedimientos para evitar el deterioro o modificación no autorizada de la información de la empresa		
TIPO DE INDICADOR	Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
IN09-V23: ¿Se han implementado lineamientos, normas y/o estándares contra la modificación o perdida a priori o accidental de información.?		IN09-VX = 1 (si hay evidencia) IN09-VX = 0 (NO hay evidencia)	Usuarios internos y externos
IN09-V24: ¿Se han implementado lineamientos, normas y/o estándares para recuperar la información en caso de presentarse modificación o perdida no autorizada a priori o accidental de información.?			Usuarios internos
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

Fuente: propia basada en el guía 9 de mintic

Tabla 34 Indicador de Gestión - Disponibilidad de la Información

INDICADOR 10- DIMENSIÓN DE DISPONIBILIDAD DE LA INFORMACIÓN			
IDENTIFICADOR	SIGSI-IN-10		
DEFINICIÓN	Se quiere reflejar una métrica de clasificación de la disponibilidad de la información en la empresa.		
OBJETIVO	Identificar el nivel de políticas y/o procedimientos para mantener disponible la información de la empresa.		
TIPO DE INDICADOR	Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
IN10-V25: ¿Se han implementado lineamientos, normas y/o estándares orientados a la continuidad de los servicios a fin de mantener la información disponible?		IN10-VX = 1 (si hay evidencia) IN10-VX = 0 (NO hay evidencia)	Usuarios internos
IN10-V26: ¿Se han implementado mecanismos para que los servicios de QWERTY S.A. tengan altos índices de disponibilidad?			Alcance del SIGSI, activos de información, plan de tratamiento de riesgos y matriz de riesgos.
IN10-V27: ¿Se han clasificado lo servicios de QWERTY S.A. en grado de tiempo que pueden permanecer indisponibles sin afectar el negocio?			Alcance del SIGSI, activos de información, plan de tratamiento de riesgos y matriz de riesgos.
IN10-V28: ¿Se han creado o discutido los planes de DRP para conocer los RTO y RPO que puede soportar la empresa?			Alcance del SIGSI, activos de información, plan de tratamiento de riesgos y matriz de riesgos.
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

Fuente: propia basada en el guía 9 de mintic

Tabla 35 Indicador de Gestión - Ataques a la Empresa

INDICADOR 11- ATAQUES INFORMÁTICOS A LA EMPRESA					
IDENTIFICADOR	SIGSI-IN-11				
DEFINICIÓN	Este indicador quiere medir las veces que se han realizado intentos de aprovechamiento de vulnerabilidades de los servicios informáticos de la empresa, exitosos o fallidos identificando el tipo de ataque, modo de operación y operación realizada proactiva o reactiva sobre el ataque.				
OBJETIVO	Identificar la cantidad de ataques informático que recibe la empresa en un periodo de tiempo definido.				
TIPO DE INDICADOR	Indicador de Cumplimiento				
DESCRIPCIÓN DE VARIABLES		**FORMULA**		**FUENTE DE INFORMACIÓN**	
IN11-V29: Número de ataques recibidos en los últimos 6 meses		$\left(\frac{IN11-V30}{IN11-V29}\right) X\ 100$		Herramienta de monitoreo /Usuarios internos	
IN11-V30: Número de ataques recibidos en los últimos 6 meses impidieron la prestación de algún o todos los servicios de la empresa a sus usuarios internos o externos				Herramienta de monitoreo / Usuarios internos	
METAS					
MÍNIMA	75% - 80%	**SATISFACTORIA**	80% - 90%	**SOBRESALIENTE**	100%
OBSERVACIONES					
Este indicador nos ayudará a mejorar herramientas para la mitigación o prevención de ataques en la empresa.					

Fuente: propia basada en el guía 9 de mintic

Tabla 36 Indicador de Gestión - Implementación de Controles

INDICADOR 12- PORCENTAJE DE IMPLEMENTACIÓN DE CONTROLES					
IDENTIFICADOR	SIGSI-IN-12				
DEFINICIÓN	Se quiere identificar el nivel de madurez del SIGSI en relación a la empresa				
OBJETIVO	Identificar el grado de avance de la implementación de los controles				
TIPO DE INDICADOR	Indicador de Gestión				
DESCRIPCIÓN DE VARIABLES		**FORMULA**		**FUENTE DE INFORMACIÓN**	
IN12-V31: Número de controles implementados		$\left(\frac{IN12-V31}{IN12-V32}\right) X\ 100$		Plan de tratamiento de riesgos	
IN12-V32: Número de controles del plan de tratamiento de riesgos que se quieren implementar.				Plan de tratamiento de riesgos	
METAS					
MÍNIMA	75% - 80%	**SATISFACTORIA**	80% - 90%	**SOBRESALIENTE**	100%
OBSERVACIONES					
La creación de nuevos cargos y asignación de responsabilidades a estos, por lo cual el indicador no está solamente orientado a la contratación d nuevas personas sino a la asignación de responsabilidades a las que ya se encuentran laborando.					

Fuente: propia basada en el guía 9 de mintic

10.8. POLÍTICA GENERAL DE SIGSI-QWERTY

La Política General del Sistema Integral de la Gestión de la Seguridad de la Información de su privacidad es una aclaración global que personifica la posición de la administración de la dependencia de sistemas en relación a la seguridad de los activos de información (los empleados, contratistas, terceros, aprendices, practicantes, proveedores y clientes, las tecnologías de la información incluido procesos y procedimientos, hardware y software.), que soportan los procesos de la dependencia y apoyan la implementación del Sistema Integral de Gestión de Seguridad de la Información, mediante la creación, modificación y publicación de sus políticas, procedimientos, procesos, manuales e instructivos, así como de la adjudicación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

QWERTY S.A., quiere asegurar la dirección estratégica de la empresa, instaura la relación de la política de seguridad de la información y los objetivos de la misma, correspondiente a los siguientes objetivos:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

- Fortalecer la cultura de seguridad de la información en los empleados, contratistas, terceros, aprendices, practicantes, proveedores y clientes de QWERTY S.A.
- Garantizar la continuidad del negocio frente a incidentes.

Alcance/Aplicabilidad

- Esta política aplica a toda la entidad, sus empleados, contratistas, terceros, aprendices, practicantes, proveedores y clientes de QWERTY S.A.

Nivel de cumplimiento

- Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

A continuación, se establecen las 12 políticas de seguridad que soportan el SIGSI de QWERTY S.A.:

- QWERTY S.A. quiere definir, ejecutar y operar de forma continua para lograr una mejora acreciente en su Sistema Integrado de Gestión de Seguridad de la Información, respaldado en directrices precisas forjadas con base a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas, terceros, aprendices, practicantes, proveedores y clientes.
- QWERTY S.A. protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.

- QWERTY S.A. protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- QWERTY S.A. protegerá su información de las amenazas originadas por parte del personal.
- QWERTY S.A. protegerá las infraestructuras de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- QWERTY S.A. controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- QWERTY S.A. implementará control de acceso a la información, sistemas y recursos de red.
- QWERTY S.A. garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- QWERTY S.A. responderá a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- QWERTY S.A. afianzará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- QWERTY S.A. vigilará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

10.9. ACLARACIÓN DE REPRESENTANTES Y FUNCIONES

SIGSI es un sistema que debe ser manejado por un equipo en los que cada miembro debe tener un rol establecido y unas tareas designadas de manera muy específica para que no haya lugar a imprecisiones en las responsabilidades que tiene cada uno de los responsables de este nuevo equipo.

En consecuencia, de esta definición, QWERTY S.A. asegura que cada una de las actividades establecidas para este sistema tenga un responsable claro y que cada miembro responsable entienda claramente sus representaciones y funciones.

10.9.1. Identificación de los Representantes

Se hace necesario contar con la participación (así sea solo informado) de manera muy efectiva al personal de más alto nivel de la empresa para que se involucre con el desarrollo del SIGSI. Este apoyo garantiza desde el comienzo, la consecución del proyecto tiene un inicio exitoso con la implementación del sistema integrado de gestión de seguridad de la información para la empresa. Los representantes del más alto nivel deben conocer el equipo de grupo de trabajo de implementar SIGSI en QWERTY S.A. conociendo y entendiendo cada atribución y obligaciones de acuerdo a lo establecido en el documento de política de la empresa.

10.9.2. Perfiles y Responsabilidades

Conjunto de integrantes al interior de la empresa QWERTY S.A. determinados de forma general.

Responsable de Seguridad de la Información para la entidad

Dado que no se conoce con cuanto personal cuenta la empresa, se debe definir por lo menos una persona con el rol de responsable de la seguridad de la información, el cual también podrá cumplir el papel de líder de proyecto y quien tendrá las siguientes responsabilidades:

- Usar su experticia, herramientas y técnicas para ayudar al desarrollo de las habilidades del proyecto a fin de cumplir con las expectativas del mismo.
- Reconocer el estado actual de la empresa y lo que se quiere lograr con el Sistema Integrado de Gestión de Seguridad de la Información.
- Generar el cronograma de SIGSI.
- Establecer la planeación, implementación y monitorear las actividades, tiempos, costos y plan de trabajo de la planeación (cronograma) establecida.
- Liderar el equipo del proyecto SIGSI en la empresa, definiendo responsabilidades, roles y tiempos de entrega de las actividades para cada uno de los miembros.
- Coordinar las tareas comunes del equipo y brindar ayuda al administrativo.
- Llevar el proyecto al cumplimento de la implementación de SIGSI en la empresa.
- Permanecer alerta en la ejecución de los planes de trabajo, las pruebas y el resultado de los riesgos para hacer llegar al comité de seguridad en caso de ser necesario.
- Monitorear y asegurar el estado del SIGSI en términos de calidad de los productos, fechas y los costos.
- Vigilar por el mantenimiento de la documentación del proyecto, su custodia y protección.

- Ayudar a crear la Base de Conocimiento sobre el SIGSI en relación a las lecciones aprendidas.
- Prever las reuniones de seguimiento y la vigilar la actualización de los indicadores de gestión del proyecto.

Después de definido el rol y responsable principal del proyecto se pueden establecer responsabilidades por los dominios de seguridad que se tienen en una arquitectura empresarial estándar:

Tabla 37 Roles y responsabilidades en dominios de seguridad informática

DOMINIO	RESPONSABILIDADES
SERVICIOS TECNÓLOGICOS	• Liderar la gestión de riegos de seguridad sobre gestión de TI y de información. • Gestionar la implementación de políticas, normas y procedimientos de seguridad de información. • Crear los mecanismos de control para medir el nivel de cumplimiento de las medidas de seguridad. • Supervisar las respuestas a incidentes de violación de seguridad, ayudando – si hay lugar - a los asuntos disciplinarios y legales. • ayudar a la dirección y los administradores de los procesos misionales en la empresa. • Avance de los planes de BIA y DRP. • Realizar o supervisar las actividades de prueba para mitigar e implementar controles sobre las vulnerabilidades de los activos y servicios de tecnología de la información.
ESTRATEGIA TI	• Ayudar la a definir la estrategia informática para alcanzar los objetivos y minimizar los riesgos de QWERTY S.A. Guiando la prestación del servicio y la adquisición de nuevos activos para garantizar la seguridad de la información.
SISTEMA DE INFORMACIÓN	• Dictaminar los requisitos mínimos de seguridad que tendrán que cumplir los diferentes sistemas de información a desarrollar, actualizar o adquirir dentro de QWERTY S.A.

DOMINIO	RESPONSABILIDADES
	• Apoyar la ejecución de los controles en los sistemas de seguridad de la información de acuerdo a las leyes que regulen la empresa. • Ejecutar las pruebas periódicas a los activos y procesos de la empresa para verificar las vulnerabilidades, riesgos y amenazas y las oportunidades de mejora. • Velar el proceso de gestión de incidentes, su investigación y determinación de las causas, adjudicando posibles responsables y recomendaciones de mejora a los sistemas, activos y/o procesos afectados. • Apoyar el desarrollo de los planes de DRP y BIA en la empresa.
DE INFORMACIÓN	• Supervisar que se garanticen las dimensiones de seguridad de la información en los componentes, activos y procesos de la empresa. • Observar el cumplimiento de las obligaciones legales y regulatorias que apliquen a la empresa, relacionadas con la seguridad de la información.

Fuente: propia basada en el guía 4 de mintic

Equipo del Proyecto

Ilustración 13. Equipo de SIGSI en QWERTY S.A.

Fuente propia

Responsabilidades y funciones de los miembros del equipo del SIGSI:

- Apoyo al líder del proyecto.
- Consultores de primer nivel a dudas técnicas y procedimientos del proyecto.
- Ayudar en el cometido de proveedores de tecnología e infraestructura.
- Participar en reuniones de seguimiento o en las que sean agendados por el líder del proyecto.
- Asistir a las reuniones de seguimiento o de cualquier otra naturaleza planeadas por el líder de proyecto.

se pueden dar otras obligaciones impartidas por el líder del proyecto o el comité de seguridad de la empresa, se deben destacar que, si no existe un rol fundamental en la creación y ejecución de SIGSI, *Responsable de Tratamiento de datos personales* de acuerdo a la ley de protección de Datos Personales (Ley 1581 de 2012), las responsabilidades del tratamiento de datos personales son:

- Mantener informado a los titulares de la información sobre los derechos que tienen a la hora de permitir a la empresa el manejo de sus datos personales.
- Gestionar las PQR (peticiones, quejas y reclamos).
- No utilizar datos sin previa autorización de acuerdo a la política de la empresa, exceptuando casos extremos donde sean requeridos.
- Asegurar y mantener en absoluta reserva la información del titular que no deba ser gestionada o divulgada.
- Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente.

10.10. POLÍTCA DE CONTROL DE ACCESO

1. La primera vez que un usuario se autentique en el dominio, se le solicitará que cambie la contraseña de acceso a los servicios de red y sistemas de información. Posteriormente, el sistema o aplicación obligará al usuario a cambiar las contraseñas cada 30 días.

2. Las contraseñas son de uso personal e intransferible y es responsabilidad del usuario dar buen uso a ellas, evitando escribirlas o dejarlas a la vista.

3. El área de sistemas estará a cargo de la creación, modificación e inactivación de usuarios en los sistemas de información, de acuerdo con las necesidades de los procesos, además, realizará una verificación anual para fortalecer dicha gestión.

4. Para el acceso a las aplicaciones que requieran usuario y contraseña, las contraseñas deben contener mayúsculas, minúsculas, caracteres especiales y números, con una longitud mínima de 8 caracteres, además, se mantiene un

registro de las últimas 5 contraseñas utilizadas por el usuario, con el fin de evitar la reutilización de estas.

5. El acceso a los equipos desde una red externa debe establecerse por medio de métodos de autenticación con protocolos seguros de comunicación (VPN).

6. No prestar, divulgar o difundir la contraseña de acceso a los servicios de red y sistemas de información a compañeros, jefes u otras personas externas a QWERTY S.A. en llegado momento que la soliciten.

7. Todos los usuarios deben dar cumplimiento a los lineamientos dados en esta política, por lo tanto, son responsables de cualquier acción que se realice utilizando el usuario y contraseña asignados.

8. El acceso a bases de datos, servidores y demás componentes tecnológicos de administración de la plataforma y sistemas de información de QWERTY S.A., debe estar autorizado únicamente por el área de informática, de acuerdo a los lineamientos establecidos por esta oficina.

9. Los derechos de acceso de los usuarios a la información y a la Plataforma Tecnológica de QWERTY S.A. deben ser revisados mínimo cada 6 meses y cada vez que se realicen cambios de personal en los procesos o grupos de trabajo.

10.11. PROCEDIMIENTOS DE OPERACIÓN PARA GESTIÓN DE TI

10.11.1. PROCEDIMIENTOS PARA EL RECURSO HUMANO

Todo lo concerniente al personal que labora en QWERTY, se puede concretar los sucesivos procedimientos:

- TRANSFERENCIA DE CONOCIMIENTO AL PERSONAL E IDENTIFICACIÓN EMPRESARIAL: Estima la metodología que se tiene por la empresa para realizar la transferencia de conocimientos sobre los procedimientos y procesos que tiene la empresa acerca de la seguridad, además de identificar los riesgos y amenazas que se pueden presentar en temas de seguridad de la información con base a sus identificaciones y funciones dentro de la misma. Dichas transferencias de conocimiento y sensibilizaciones se deben llevar de manera periódica o a menos de seis meses de un personal nuevo en la empresa.

- INGRESO Y RETIRO DEL PERSONAL (VINCULACIÓN Y DESVINCULACIÓN) Este procedimiento encamina la forma como la empresa gestiona de manera eficiente y segura el ingreso y desvinculación del personal, con base en los datos y fechas de contratación de cada usuario y/o persona y con los respectivos documentos debidamente diligenciados.

10.11.2. PROCEDIMIENTO PARA LA ADMINISTRACIÓN Y GESTION DE ACTIVOS

Los activos de la empresa deben tener una clasificación aceptada y fácil de reconocer por el personal adyacente a la empresa, su identificación y clasificación debe estar enmarcada de acuerdo a su valoración de criticidad e importancia para la empresa, así como el nivel de confidencialidad que pueda manejar. Este procedimiento de identificación tiene que estar encaminado al cumplimiento de requisitos en las dimensiones de la seguridad de la información, el proceso de entrega y recepción al momento de llegar a la empresa con asignación de placa de inventario. Y en el proceso de desvinculación a la hora de dar de baja el activo con un procedimiento de borrado seguro para no permitir la fuga de información.

10.11.3. PROCEDIMIENTO DE CONTROL DE ACCESO

El acceso a la información dentro y fuera de las instalaciones de la empresa deben estar enmarcados por los siguientes procedimientos.

- ISSI (Ingreso seguro a los sistemas de información): es necesario y primordial por parte de la empresa emplear métodos preventivos a ataques de fuerza bruta que puedan vulnerar los sistemas de información y comprometer los datos. De igual manera validar diferentes métodos de identificación y autorización del personal para ingresar a los sistemas de información. Y los métodos de cifrado de información para que, sobrepasando las barreras anteriores, la información sustraída no sea de utilidad para el atacante.

- ADMINISTRACIÓN DE USUARIOS Y CONTRASEÑAS: La empresa debe encaminar de forma precisa y exacta la creación de usuarios y la asignación de claves (con un nivel de seguridad previamente definido) asegurando en mayor medida que esta sea personal e intransferible y que cumple con su política de seguridad de contraseñas. Al igual que vigilar el cambio de forma periódica, llevando un registro de la misma y determinando un número de contraseñas para que no sea nuevamente repetida con facilidad. Una contraseña es el mínimo requisito de seguridad que todo sistema de información, como bases de datos, repositorios, sistemas operativos y aplicaciones debe tener. Definiendo el rol de cada usuario y con permiso exclusivo a los sistemas que requiera con los privilegios correspondientes.

- ISI (Ingreso Seguro a las Instalaciones): se deben suministrar formas de identificación al personal que labora en la empresa, tales como credenciales, escarapelas o carnés donde se contengan datos básicos y una fotografía. Además de la fecha de vencimiento de contrato. Esto con la finalidad de regular el ingreso a las instalaciones y evitar el acceso a personal ajeno a la empresa,

cuando una persona extraña a las instalaciones quiera ingresar, debe ser informado, debe tener un registro y debe ser acompañado por un miembro de la empresa.

10.11.4. PROCEDIMIENTO DE SEGURIDAD FÍSICA

Restricción de acceso a áreas específicas de la empresa por no contar con la autorización respectiva, para evitar el daño a la infraestructura, las instalaciones o la información.

- CONTROL DE ACCESO FÍSICO: Es necesario definir los pasos que deben tener en cuenta las personas que quieran lograr acceso a sitios seguros de la empresa. Este procedimiento debe tener bitácoras donde se registre las fechas y horas de ingreso, llenar permiso para ingresar a estas áreas restringidas y su respectiva justificación.

- PROTECCIÓN DE ACTIVOS: Se deben definir los pasos que conlleva los equipos para asegurar su protección. Este procedimiento debe indicar la ubicación del equipo, el tipo de información que procesa, la confidencialidad de la información y los controles que se aplicaran para evitar las amenazas de índole, físicas, naturales, industriales, de suministro de energía o robo.

- RETIRO DE ACTIVOS: en este procedimiento debe quedar de forma clara por qué y cómo serán retirados los activos degradados o inoperativos de la empresa. Se debe indicar el conducto regular de solicitudes, autorizaciones, avisos y sobre avisos a todas las personas involucradas en el proceso, desde la alta gerencia hasta los operativos. Así mismo como definir los controles de seguridad aplicados al equipo cuando se vaya a retirar de la empresa para su disposición final (controles criptográficos, cifrado de disco y/o borrado seguro)

- MANTENIMIENTO DE EQUIPOS: se debe dejar claro en este procedimiento la periodicidad con la que se realizarán los mantenimientos preventivos a los activos, los mantenimientos correctivos donde se reporte la falla, la solución y el nuevo costo del activo. Se debe aclarar la preparación del personal que ejecutará dicho mantenimiento y un registro apropiado.

10.11.5. PROCEDIMIENTO DE OPERACIONES ASEGURADAS

Se solicita asegurar las operaciones para que se lleven a cabo de forma correcta dentro de las instalaciones o locaciones de la empresa anunciando los siguientes procedimientos.

- GESTIÓN DE CAMBIOS: debe estar definido el personal que participará en el comité de cambios, el líder del comité de cambios y la periodicidad con la que se realiza este comité de cambios. Se debe definir dentro del comité de cambios un representante por proceso de negocio o sistema de información. Se debe establecer un RFC (solicitud para cambio), el registro del comité, los cambios significativos midiendo el impacto y la indisponibilidad del servicio producido, y también el proceso de comunicación y divulgación.

- GESTION DE LA CAPACIDAD: este procedimiento debe ser claro para verificar y mantener actualizado la forma en que la empresa realiza una administración favorable de los sistemas de información y activos de la misma. Previendo mantener siempre recursos de estos ítems de configuración. También las actividades que se deban realizar para propender estos estados, tales como depuración de datos que no se usen, sustituir o reemplazar aplicaciones obsoletas, reorganizar la infraestructura y adquisición y compra de nuevos elementos de configuración.

- AMBIENTES SEPARADOS: Es importante definir y mantener separado de forma física y lógica ambientes de producción, pruebas y desarrollo, para no propender a problemas operacionales que ocasionen indisponibilidad en las aplicaciones (sobre todo en el ambiente de producción). Este procedimiento puede verse limitado por la gestión de capacidad.

- PROTECCIÓN CONTRA SOFTWARE MALICIOSO: Se debe definir los controles físicos e intangibles que tiene contra software malicioso como virus, malware, bots y ransomware. Identificando licencias, actualizaciones, manual de instalación, de cuarentena, de purga y de recuperación de información. También monitoreo y reportes de ataques evitados y no evitados.

10.11.6. PROCEDIMIENTO DE SEGURIDAD DE LAS COMUNICACIONES

Con este procedimiento se quiere blindar los servicios de comunicaciones la empresa y mantener su seguridad alta:

- PROTECCIÓN DE SERVICIOS DE RED: se debe dejar definido el cómo se protege la información, indicando los controles de seguridad para que la información se transfiera a través de los dispositivos de comunicación de manera segura, codificada y confiable, protegiéndola de intrusiones o robo de la misma por interceptación o envío hacía direcciones o dispositivos fraudulentas.

- TRASPASO DE INFORMACIÓN: Debe aclararse los procesos que conllevan el flujo de información de forma segura dentro y fuera de la empresa. Aplicando los métodos más estrictos para proteger la información de actividades como interceptación, copiado sin autorización, modificación y/o destrucción. Es necesario definir que las personas que tengan acceso a los dispositivos de

comunicación sustenten acuerdos de confidencialidad y no divulgación. Dichos acuerdos deben ser actualizados y revisados de forma regular, y en ellos debe quedar consignado las condiciones sobre la información a proteger, la duración del acuerdo, las obligaciones, funciones y responsabilidades, quien es propietario de la información, el tipo de información y las acciones en caso de incumplimiento que se puedan acarrear o presentar.

10.11.7. PROCEDIMIENTO VINCULO CON LOS PROVEEDORES

En este apartado debe quedar claro los derechos y deberes que tienen las personas y/o usuarios externos a la empresa con relación a los activos de la misma por medio del cumplimiento de los siguientes procedimientos:

- TASIAP (Tratamiento de la Seguridad de la Información en los Acuerdos con Proveedores): se deben definir los acuerdos de confidencialidad y no divulgación que la empresa pueda establecer, acordar, aprobar y divulgar con personas externas a la empresa que tengan o tramiten cierto vínculo laboral o de servicios con la misma. Los requerimientos y obligaciones relacionados con dicha seguridad de la información deben contemplar características tales como: aspectos legales, descripción de la información, tipo de acceso, reglas de uso aceptable, informes, reuniones de seguimiento, auditorias de servicio y acciones en caso de incumplimiento.

10.11.8. PROCEDIMIENTO DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE APLICACIONES Y SOFTWARE

Este procedimiento debe enunciar y establecer los diferentes procesos de seguridad que se llevaran a cabo con base en mantener y resguardar la seguridad de la información del software que pueda ser comprado, desarrollado o suministrado por

un tercero a la empresa. Validando que cada uno mantenga y preserve las dimensiones de la seguridad como lo son la confidencialidad, integridad y disponibilidad. Es necesario llevar un control de software, donde se pueda evidenciar su cambio de versión, los manuales de instalación, configuración y ***troubleshooting*** que pueda tener el software. El personal autorizado para su instalación y el ciclo de vida de dicho software a fin de determinar si debe ser reemplazado o dado de baja por obsolescencia tecnológica.

10.11.9. PROCEDIMIENTO GESTIÓN DE INCIDENTES

La empresa está en la capacidad de definir las acciones que se deben llevar a cabo antes, durante y después de la ocurrencia de un incidente que afecte una o varias de las dimensiones de la información. Especificando las personas involucradas en su solución temporal y su solución definitiva. Se deben definir roles, responsabilidades y acciones a tomar. Medir el riesgo y las acciones a realizar para mitigar, reducir, transferir o aceptar la consecuencia del evento. Se debe documentar, recolectar y clasificar las evidencias del incidente para que este no se convierta en problema y mejorar la respuesta cuando este pase a ser incidente conocido.

10.11.10. PROCEDIMIENTO BCP (PLAN DE CONTINUIDAD DE NEGOCIO)

Se debe definir las actividades previas, durante y posterior a un incidente o evento que amenace la continuidad de la operación de la empresa. Se deben indicar todos los procesos misionales, estratégicos, de apoyo y de tecnologías de información que posea la empresa y evaluar su nivel de criticidad. Se establecerá los RTO y los RPO que deben cumplirse para mantener activo la empresa sin verse afectada ni en su imagen ni económicamente. Se debe evaluar un DRP.

10.12. POLÍTICA DE SEGURIDAD PARA PROVEEDORES

1. Los proveedores o contratistas que tengan relaciones comerciales con QWERTY S.A. deberán firmar el “Acuerdo de Confidencialidad y Reserva de Manejo de la Información”, para cualquier contrato o acuerdos con terceras partes, que implique un intercambio, uso o procesamiento de información de la entidad. Estos acuerdos harán parte integral de los contratos o documentos que legalicen la relación del negocio.

2. Para el ingreso a las áreas seguras definidas por QWERTY S.A. los proveedores o contratistas, deben estar permanentemente identificados y cumplir con los controles establecidos por la QWERTY S.A.

3. Dentro del contrato o acuerdo entre QWERTY S.A. y el proveedor se debe definir claramente el tipo de información que se va a manejar o intercambiar por las partes.

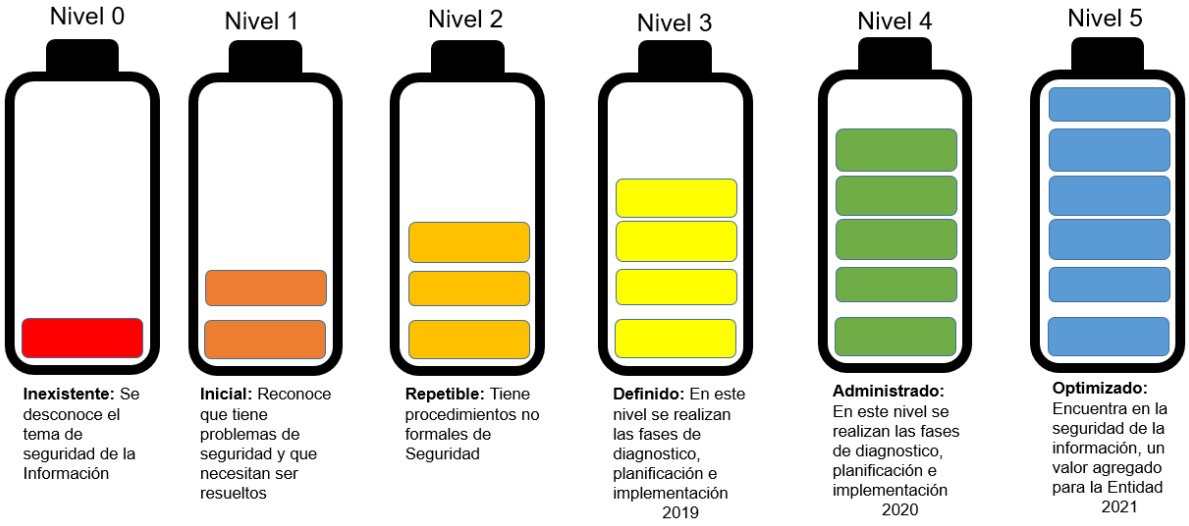
4. El área de informática, o a quien esta delegue, debe verificar las condiciones de comunicación segura, cifrado y transmisión de información, desde y hacia los terceros o proveedores de servicios.

5. El supervisor de contrato debe administrar los cambios en el suministro de servicios, por parte de los proveedores o terceros, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos con ellos y monitoreando la aparición de nuevos riesgos.

11. RECOMENDACIÓN

La implementación del sistema de gestión de seguridad de la información es importante para la empresa QWERTY SA, por lo que, se hace necesario la aprobación por parte de comité directivo, socializarlo con toda la empresa y hacer campañas de concienciación y sensibilidad a los usuarios para el entendimiento y aplicación en sus labores diarias, de esta manera se logra reducir los riesgos y las amenazas a la que están expuestos los activos de información.

Ilustración 14. Etapas de implementación de SIGSI en QWERTY S.A.



Fuente modelo de nivel de madurez Framework COBIT

Después de realizado el levantamiento de información y la valoración de los activos, se establece que para el año 2019 se tiene **definido** el SIGSI en QWERTY ya que se han realizado las diferentes fases de diagnóstico, planificación e implementación, sin embargo, esto es solo el comienzo del plan, y se proyecta que para los años venideros el sistema empiece a ser administrado y optimizado a fin de permitir mejores resultados y el cambio o mantenimiento de los controles a fin de brindar las

prácticas más recomendadas en cuanto al tema de seguridad de la información se trata.

Estas etapas deben hacerse a través de los procesos de planificación, implementación, evaluación del desempeño y la mejora continua, que son muy semejantes al ciclo PHVA.

Ilustración 15. Ciclo de Mejora continua SIGSI en QWERTY S.A.

Fuente http://www.uniajc.edu.co/documentos/planes/2019/PLAN_SEGURIDAD_PRIVACIDAD_INFORMACION_UNIAJC.pdf

Realizada la etapa de diagnóstico, se debe seguir con la fase de planeación, donde es necesario entender la empresa, las necesidades y expectativas de la misma, los involucrados en el comité del SIGSI, las diferentes políticas, las acciones para abordar, mitigar, reducir, transferir o aceptar los riesgos y los objetivos y planes para lograr estas acciones sobre los riesgos. También contemplar los recursos, la comunicación de este sistema a toda la empresa y la documentación y donde se encuentra.

Durante la etapa de implementación, se debe validar los controles y su eficiencia en relación a evitar que los riesgos se materialicen, evidenciar el plan de tratamiento

de riesgos y poner en práctica los indicadores de gestión definidos para verificar su eficiencia y eficacia.

Esto se logra por medio del monitoreo, la medición, el análisis tanto de los controles como de los nuevos riesgos que se pueden dar por la depreciación de los activos, la evaluación sobre los resultados favorables o desfavorables de los controles e indicadores de gestión aplicados. Todo esto se puede ayudar a través de auditorías internas y externas que muestren el avance o el estancamiento del sistema aplicado y la presentación de un informe ejecutivo que evaluará la alta dirección de QWERTY S.A. para determinar o enrutar el camino del sistema integrado de gestión de seguridad de la información.

La migración del servicio FTP a un servicio en nube es lo más recomendable para asegurar la confidencialidad, integridad y disponibilidad de la información de QWERTY.

Dentro de los activos que tiene QWERTY es importante reemplazar los 4 hub de acceso alámbrico a switches.

Por último, la etapa de mejora continua permitirá llevar a cabo mejoras continuas, con el cual se partirá a partir de lo aprendido, recomenzando nuevamente el ciclo y dando acciones correctivas que permitan mantener la mejora continua a fin de que esto se convierta en un ciclo que conlleve a alcanzar la madurez del sistema.

12. RESULTADOS Y DISCUSIÓN

Inicialmente se realizó un proceso de recolección de información, mediante encuestas y entrevistas de tal forma que se pudiera capturar la mayor cantidad de información de la compañía e identificando la percepción y la realidad del estado de la seguridad informática.

También se realiza una valoración de los riesgos que tiene cada uno de los activos de la compañía con el fin de realizar un trabajo de remediación y mitigación por medio de un sistema de gestión de la seguridad.

Una vez obtenida la información y proponer los controles adecuados para mitigar cada uno de los riesgos, se define un plan de mejora continua y revisión para mantenerse a la vanguardia de nuevas amenazas o de controles poco eficientes.

12. CONCLUSIONES

- Se elaboró un sistema integrado de gestión de seguridad informática, que hasta ahora empieza a madurar de acuerdo a los diferentes pasos que se tuvieron en cuenta para medir el estrado inicial de la empresa QWERTY S.A. partiendo en el nivel de crecimiento de la empresa en la cual la seguridad de la información e informática tiene una importancia significativa. Por lo cual se establece como punto inicial en la empresa el nivel de ***definido*** en el cual se deben llevar a cabo las diferentes fases de diseño, implementación y diagnóstico del sistema.

- El sistema integrado de gestión de seguridad informática que se desarrolló durante la ejecución de este proyecto para la empresa QWERTY S.A. bajo la implantación del mismo en la normativa ISO 27001:2013 abordó aquellos documentos y registros que son obligatorios y comúnmente usados por la mayoría –sino todos – los sistemas de gestión de seguridad a nivel mundial bajo la misma referencia.

- Durante la validación del estado inicial en el cual se puede encontrar QWERTY, se ha validado los activos de la empresa en las tres dimensiones primordiales de la información, dándole a cada uno de ellos un valor cualitativo y cuantitativo a fin de poder conocer su escala de vulnerabilidad, su importancia para la empresa y el riesgo que existe que se pueda hacer real una amenaza y afecte de manera menor o significativa la empresa por no prevenir, mitigar, reducir o transferir dicho riesgo.

- Se midieron cada uno de los activos que se presentaron durante el desarrollo de este proyecto de acuerdo a la metodología escogida, permitiendo así crear o clasificar grupos de activos de acuerdo a su función o representación dentro de la empresa QWERTY S.A. se realizó la valoración del riesgo, clasificando este

en catastrófico, alto, medio o bajo de acuerdo a la probabilidad de materialización de una amenaza y permitiendo escoger y documentar los controles que se puedan aplicar para soslayar dicho riesgo.

- Gracias a la metodología Magerit, se han clasificado estas amenazas y se han cruzado con cada una de las categorías de los activos para darles un valor a fin de poder medir el estado actual de los mismos en la clasificación de los grupos de la metodología. En concordancia con esto, se realizó la validación de estas vulnerabilidades a la luz de la norma ISO 27001:2013 para implementación de los controles más comunes o estándares que debe llevar un sistema integrado de gestión de la seguridad de la información.

- Para revisar los controles se han establecido en la *declaración de aplicabilidad* en la cual se toman en cuenta dichas salvaguardas del Anexo A: y se evidencia la justificación del porque es aplicable para la empresa. Al aplicar estos controles y como se ha realizado la recomendación es necesario tener un comité que gestione el sistema que se quiere crear en QWERTY S.A. y que permita la aplicación de las políticas que todo el personal de la empresa debe conocer para ayudar a construir una mejor seguridad.

- Se ha establecido unas políticas generales básicas que son lo mínimo que debe tener un sistema integrado de gestión de seguridad de la información en relación a los controles de acceso, el uso adecuado de los activos, procedimientos de gestión de tecnologías de información, la seguridad física, la seguridad de operaciones y el vínculo con los proveedores entre otros.

- Es por esto, que el Sistema Integrado de Gestión de la Seguridad de la Información de la empresa QWERTY S.A. se ha definido en una etapa **Definido** ya que la empresa es muy consciente de que tiene problemas y algunos procedimientos formales de seguridad, sin embargo, las fases de diagnóstico,

planeación e implementación hasta ahora se están empezando a construir por medio de la consolidación de los documentos que propone como obligatorios la norma y que están definidos aquí

1. Alcance del sistema de gestión de la seguridad de la información
2. Políticas y objetivos del SGSI
3. Metodología e informes de evaluación y tratamiento del riesgo
4. Declaración de aplicabilidad
5. Plan de tratamiento del riesgo
6. Funciones y responsabilidades de seguridad
7. Inventario de Activos
8. Uso aceptable de los activos
9. Política de control de acceso
10. Procedimientos operativos para gestión de TI
11. Principios de ingeniería de seguridad
12. Política de seguridad para proveedores

- De los cuales muchos ya se han comenzado a diseñar y estructurar y otros están al pendiente en las siguientes etapas mientras se madura el sistema y se autoevalúa para su regulación, administración y optimización.

13. BIBLIOGRAFÍA

1. ABRIL ESTUPIÑAN, Ana., PULIDO, Jarol y BOHADA John. Análisis de riesgo en seguridad de la información. En: Ciencia, innovación y tecnología (RCIYT), enero-diciembre 2013, vol 1, p. 39 -53. Disponible en Internet: https://www.jdc.edu.co/revistas/index.php/rciyt/article/view/121/113

2. ÁLVAREZ BASALDÚA, Luis Daniel, Seguridad Informática (Auditoria de sistemas). Tesis de maestría. Maestro en Ingeniería de sistemas empresariales. México D.F.: Universidad Iberoamericana. 2005. 117 p. Disponible en Internet: http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

3. ÁLVAREZ M. Gonzalo y PÉREZ, Pedro Pablo. Seguridad Informática para empresas y particulares. Madrid España.: McGraw-Hill, 2004, 413 p. ISBN: 84-481-4008-7

4. AUSTIN, Robert D. y DARBY, Christopher A.R. El mito de la Seguridad Informática. En: Harvard Deusto Bussines Review, enero – diciembre 2004, no. 120, p. 66-74. ISSN: 0210-900X125.

5. BARRIO A. Moisés, Delitos 2.0: Aspectos penales, procesales y de la seguridad de los ciberdelitos, España. La Ley agosto 2018, 310 p. ISBN: ISBN number:9788490207437, ISBN number:9788490207444

6. BAUTISTA, Marco Antonio. Marco de referencia para la formulación de un plan de continuidad de negocio para TI, un caso de estudio (Tesis de maestría). [En línea] Universidad de las Américas, Quito. 2014 p. 135 [Citado 10 de marzo 2019] Disponible en Internet: http://dspace.udla.edu.ec/handle/33000/3081

7. BAYONA, Sussy. CHAUCA, Wilber. LOPEZ, Milagros y MALDONADO, Carlos. [En línea] Publicado en: CISTI – Conferencia ibérica de sistemas y tecnologías de la información (10: 17 – 20 Junio de 2015) Implementación de la NTP ISO/IEC 27001 en las instituciones Públicas: Caso de Estudio. 2015, p 410 – 415.

8. BEACHY, Rob. End user information security policy template. Brainmass, 2012. 28 p. Disponible en Internet: http://bibliotecavirtual.unad.edu.co/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=529772&lang=es&site=ehost-live

9. BISOGNO, María Victoria. Metodología para el aseguramiento de entornos informatizados – MAEI. Tesis de grado [En línea]. Buenos Aires – Argentina. Universidad de Buenos Aires, Facultad de Ingeniería. 2004, 235 p. Disponible en Internet: http://materias.fi.uba.ar/7500/bisogno-tesisdegradoingenieriainformatica

10. BRICEÑO S. Francisco Javier. Implementación de un sistema de seguridad en un edificio público. (Proyecto fin de carrera) [En línea]. Leganés – Madrid España. Universidad Carlos III de Madrid, Departamento de automatización. 2010, 118 p. Disponible en Internet: https://e-archivo.uc3m.es/bitstream/handle/10016/10587/PFC_FranciscoJavier_Briceno_Sanz.pdf?sequence=1&isAllowed=y

11. BUITRAGO E. Johanna C. BONILLA P. Diego H. y MURILLO V. Carol E. Diseño de una metodología para la implementación del sistema de gestión de seguridad de la información – SGSI, en el sector de laboratorios de análisis de microbiológicos, basados en ISO 27001. Tesis de postgrado Gerencia de procesos y calidad. [En línea] Universidad EAN, Bogotá D.C.: 2012 p 142. Disponible en Internet: https://repository.ean.edu.co/bitstream/handle/10882/2692/MurilloCarol2012.pdf?sequence=1

12. CANO, Anisley. CAMPILLO, Irima y CUESTA R. Floricelda. Sistema de Gestión de Información para la Educación Superior. En: Ciencias de la Información. Mayo a Agosto 2014, vol. 46, no. 1, p 21-24. Disponible en Internet: http://cinfo.idict.cu/index.php/cinfo/article/view/635/488

13. CARDENAS S. Leidy Johanna, MARTÍNEZ A. Hugo y BECERRA A. Luis Eduardo. Gestión de seguridad de la información: Revisión Bibliográfica. En: El profesional de la información [En línea], Bucaramanga – Colombia, Universidad Industrial de Santander. 2016, vol. 25, no. 6. p. 931 – 948 eISSN: 1699-2407. Disponible en Internet: https://recyt.fecyt.es/index.php/EPI/article/view/epi.2016.nov.10/32176

14. CHOI, Kyung y TORO A. Marlon M. Cibercriminología. Guía para la investigación del cibercrimen y mejores prácticas en seguridad digital. Bogotá D.C.: Universidad Antonio Nariño. 2017, 604 p. ISBN 9789588687711.

15. CISTI – CONFERENCIA IBERICA DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN. (7: 20 - 23 junio, 2012: Madrid España) Optimización de la

economía de la seguridad de la información, Consejo General de Colegios Oficiales de Ingeniería Técnica en Informática, 2012, p. 126 – 129.

16. COLLAZOS, B. Manuel. La nueva versión ISO 27001:2013 Un cambio en la integración de los sistemas de gestión [diapositivas], PRIME Asesoría y desarrollo Integral Profesional, Lima – Perú. 27 diapositivas.

17. COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581 (18, octubre 2012) Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial Bogotá D.C., 2012 No. 48.587. p 1 – 301. Disponible en Internet: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf

18. COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (5, enero 2009) Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"-… Diario Oficial Bogotá D.C., 2009 No. 47.223. p 1 – 4. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

19. CORNEJO, S. Gloria y MANCHOLA, Sandra. Investigación sobre el Hacker y sus posibles comienzos en la Comunidad Estudiantil, Caso de Estudio (Proyecto de grado) [En línea] Universidad Piloto de Colombia, Bogotá D.C. 2015 p. 167 [Citado 11 de marzo de 2019] Disponible en Internet: http://polux.unipiloto.edu.co:8080/00002887.pdf

20. DUMAN, Ekrem, ATIYA, Amir. Use of risk analysis in computer-aided persuasion. 2011, vol. 88, p. 345 (NATO Science for Peace and Security Series. The NATO Science for peace and security programme. IOS Press.) ISBN: 978-1-60750-828-1. Disponible en Internet: http://bibliotecavirtual.unad.edu.co/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=422088&lang=es&site=ehost-live

21. ESTADOS UNIDOS, YMCA BUFALO NIAGARA DEPARTMENT. Information security End-user policy. New York, 2015. 26 p. disponible en Internet: https://www.politecnicojic.edu.co/images/downloads/biblioteca/guias/NTC5613.pdf

22. GÓMEZ, Oiner. BAUTA, C. René y ESTRADA S. Vivian. Modelo para la compartimentación de la información en las organizaciones. En: Ciencias de la Información. Enero a abril 2014, vol. 45, no. 1, p 11-17. Disponible en

Internet: https://biblat.unam.mx/hevila/Cienciasdelainformacion/2014/vol45/no1/2.pdf

23. GUIJARRO-RODRÍGUEZ, Alfonso. Defensa en profundidad aplicado a un entorno empresarial. En: Espacios. Junio 2018, vol. 39, no. 42, p 19. Disponible en Internet: http://www.revistaespacios.com/a18v39n42/a18v39n42p19.pdf

24. HURTADO, Rubén. RODRÍGUEZ, Wilson. FUENTES, Héctor y GALLEGUILLOS, Carlos. Impacto en los beneficios de la implementación de la normas de calidad ISO 9000 en las empresas. [En línea] En: Revista de la Facultada de Ingeniería. Copiapó Chile: Universidad de Atacama. 2009, p. 17-26. Disponible en Internet: http://www.revistaingenieria.uda.cl/Publicaciones/230003.pdf

25. INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN, Tecnología de la información, técnicas de seguridad. Sistemas de gestión de seguridad de la información (SGSI). Requisitos. NTC-ISO/IEC 27001. Bogotá D.C.: El instituto, 2013 45 p. Disponible en Internet: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

26. INTERNATIONAL ORGANIZATION OF STANDARIZATION and INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information technology – security techniques - information security management systems – Overview and vocabulary. ISO/IEC 27000:2016, Geneva, Switzerland: IOS, 2016, 42 p. Disponible en Internet: http://standards.iso.org/ittf/PubliclyAvailableStandards/c066435_ISO_IEC_27000_2016(E).zip

27. INTECO. SGSI. España, [En línea] 2010. [vídeos de youtube], 15 vídeos publicados por Instituto Nacional de Ciberseguridad. Disponible en Internet: https://www.youtube.com/watch?v=zV2sfyvfqik&list=PLN3XU56O7eKxo4flrxApWQG_5qc0TiGmA

28. ISO27000, Sistema de Gestión de la Seguridad de la Información, [En línea], www.iso27000.es s.f. 14 p. [Citado 18 Abril de 2019] Disponible en Internet: http://www.iso27000.es/download/doc_sgsi_all.pdf

29. ISOTOOLS EXCELLENCE, ISO 27001: Aspectos claves de su diseño e implementación, [En línea], www.isotools.org s.f. 23 p. [Citado 15 Abril de 2019] Disponible en Internet: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

30. LA ESTRELLA, Redacción Digital. Los 5 tipos de Ransomware que más afectan los usuarios. [En línea]. 2019. Artículo. [Citado el 12 de marzo 2019] Disponible en Internet: https://www.laestrella.com.pa/cafe-estrella/tecnologia/190126/5-tipos-afectan-ransomware

31. LA VANGUARDIA, Redacción Digital. El malware sofisticado y los sistemas operativos desactualizados, entre las principales amenazas móviles para 2019. [En línea]. 2019. Artículo [Citado 12 de marzo 2019] Disponible en Internet: https://www.lavanguardia.com/vida/20190212/46406846701/el-malware-sofisticado-y-los-sistemas-operativos-desactualizados-entre-las-principales-amenazas-moviles-para-2019.html

32. LÓPEZ, Purificación. Seguridad Informática, Pozuelo de Alarcón, Madrid, Editex, 2010. P 240, ISBN: 978-84-9771-657-4.

33. MARTELO, Raúl. TOVAR, Luis y MAZA, Diego. Modelo básico de seguridad lógica. Caso de Estudio. [En línea] Laboratorio de redes Universidad de Cartagena, Cartagena. 2018, En: Información tecnológica (versión en línea), vol 29, no. 1. Disponible en Internet: http://dx.doi.org/10.4067/S0718-07642018000100003

34. MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de riesgos de los Sistemas de Información. Libro I – Método. NIPO: 630-12-171-8. Madrid, España. 2012 127 p. Disponible en Internet: https://www.politecnicojic.edu.co/images/downloads/biblioteca/guias/NTC5613.pdf

35. MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de riesgos de los

Sistemas de Información. Libro II – Catalogo de Elementos. NIPO: 630-12-171-8. Madrid, España. 2012 127 p. Disponible en Internet: https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

36. MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de riesgos de los Sistemas de Información. Libro III – Guía de Técnicas. NIPO: 630-12-171-8. Madrid, España. 2012 127 p. Disponible en Internet: https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html

37. MINTIC. Guía 1 – Metodológica de Pruebas de Efectividad Bogotá D.C.: Ministerio, 2016, 28 p. Disponible en Internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf

38. MINTIC. Guía 3 – Procedimiento de Seguridad de la Información Bogotá D.C.: Ministerio, 2016, 19 p. Disponible en Internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

39. MINTIC. Guía 5 – Gestión Clasificación de Activos, Bogotá D.C.: Ministerio, 2016, 18 p. Disponible en Internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

40. MINTIC. Guía 7 – Gestión de Riesgos Bogotá D.C.: Ministerio, 2016, 39 p. Disponible en Internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

41. MINTIC. Guía 17 – Mejora continua Bogotá D.C.: Ministerio, 2015, 10 p. Disponible en Internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G17_Mejora_continua.pdf

42. NAJAR, P. José y SUÁREZ, S. Nubia. La seguridad de la información: un activo valioso de la organización. En: Vínculos. Febrero 2015, vol 12, no 1, p 89-97. Disponible en Internet: https://revistas.udistrital.edu.co/index.php/vinculos/article/view/10518/11480

43. PICÓN C. Ingrid. Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013. Trabajo de Grado Sistemas de Gestión de seguridad de la información, Master en seguridad de tecnologías de la información y de las comunicaciones (MISTIC). Colombia.: Instituto colombiano para la evaluación de la Educación – ICFES, 2016, p 29. Disponible en Internet: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/54261/5/ipiconTFM0616memoria.pdf

44. POSADA, M. Ricardo. El delito de acceso abusivo a sistema informático: a propósito del art. 269ª del CP de 2000. En: Revista de derecho, comunicaciones y nuevas tecnologías. Junio de 2013, no. 9, p 1-31 Disponible en Internet: https://derechoytics.uniandes.edu.co/components/com_revista/archivos/derechoytics/ytics129.pdf

45. SUÁREZ, Diana y ÁVILA, F. Aldeir. Una forma de interpretar la seguridad Informática. En: Innovación, ingeniería y desarrollo, Enero-diciembre 2013, vol 2, no. 2, p. 87-93. Disponible en Internet: https://docplayer.es/36805408-Una-forma-de-interpretar-la-seguridad-informatica.html

46. SUCA, Jackeline Tatiana. Propuesta metodológica para implementar la Norma Técnica Peruana ISO/IEC 27001:2008 de Seguridad de la Información en entidades públicas del Estado. Tesis de grado Ingeniería de Sistemas. Arequipa – Perú.: Universidad Católica de Santa Marta. Facultada de Ciencias e ingenierías físicas y formales programa profesional de ingeniería de sistemas. 2014, 183.

47. VARGAS, Ana Cecilia y CASTRO M. Alonso. Sistemas de gestión de seguridad de la información [diapositivas]. Costa Rica. Universidad de Costa Rica, s.f. [En línea] 32 diapositivas, color, Disponible en Internet: http://archivo.ucr.ac.cr/docum/ISOEIC27000.pdf

48. VERA, C. Romel, ¿Se puede usar una PC sin antivirus? En: 3C TIC. Septiembre 2016 vol. 5, no. 2, p. 1-12. doi:10.17993/3ctic.2016.52. ISSN: 2254 – 6529.

49. VOUTSSAS, Juan. Preservación documental digital y seguridad informática. En: Investigación Bibliotecológica: archivonomía, bibliotecología e información, 2010, vol. 24, no. 50, p 1-24 DOI: http://dx.doi.org/10.22201/iibi.0187358xp.2010.50.21416, ISSN:2448 – 8321

50. YOUNGIN, You. JUNHYOUNG, Oh. SOOHEON, Kim y KYUNGHO Lee. Advanced approach to information security management system utilizing maturity models in critical infrastructure. En: KSII Transaction on internet and information systems [En línea]. Octubre 2018, vol. 12, no. 10, p. 4995 – 5014 doi: http://doi.org/10.3837/tiis.2018.10.020 ISSN : 1976-7277

14. ANEXOS

14.1. Encuesta para el levantamiento de Información

Anexo 1 Tabulación de Encuesta

1. Con que frecuencia realiza cambio de claves de acceso al equipo.

Frecuentemente De vez en cuando Nunca

Tabla 38 Anexo Encuesta, Tabulación pregunta 1

Valor	Frecuencia	Porcentaje %
Frecuentemente	10	16,7%
De vez en cuando	30	50,0%
Nunca	20	33,3%
Total	60	100%

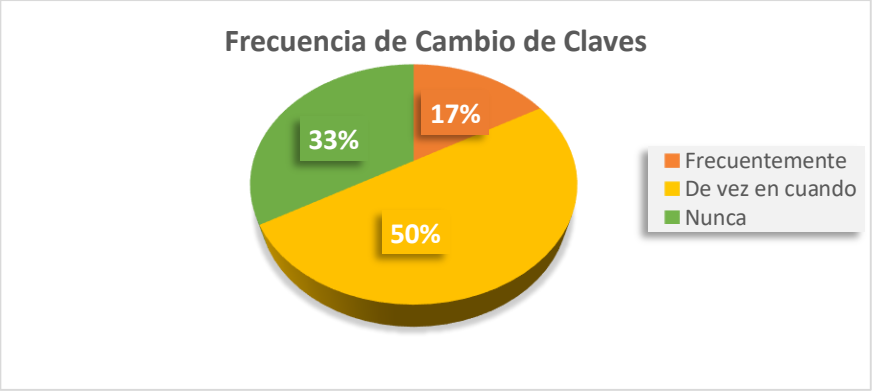


Ilustración 16. Anexo Encuesta, resultado pregunta 1

Se evidencia que más de la mitad de los trabajadores de QWERTY (67%) conocen que deben realizar cambio de contraseña, sin embargo, es menor el porcentaje de las personas que lo realizan frecuentemente, comparado con los que lo hacen de vez en cuando. Lo que nos lleva a concluir que no existe una política definida en este sentido.

2. Utiliza contraseñas seguras o fáciles.

SI NO, No sé

Tabla 39 Anexo Encuesta, Tabulación pregunta 2

Valor	Frecuencia	Porcentaje %
SI	30	50%
No	20	33,3%
No sé	10	16,7%
Total	60	100%

Ilustración 17. Anexo Encuesta, resultado pregunta 2

Es notorio igualmente, que esta parte que realiza el cambio de las contraseñas utiliza contraseñas complicadas, lo que ayuda a fortalecer el hecho de que no sea fácil obtener la contraseña, sin embargo, es preocupante que el 17% lo que se traduce en que casi 20 usuarios no conocen si usan o no contraseñas seguras, lo que se traduce en que estos usuarios no conocen que es una contraseña segura.

3. La oficina de sistemas divulga las políticas de seguridad

SI NO, No sé

Tabla 40 Anexo Encuesta, Tabulación pregunta 3

Valor	Frecuencia	Porcentaje %
SI	40	66,7%
No	5	8,3%
No sé	15	25,0%
Total	60	100%

Ilustración 18. Anexo Encuesta, resultado pregunta 3

Los usuarios tienen la percepción de que la oficina de informática de QWERTY S.A. si ha compartido las políticas de seguridad de la información y la seguridad informática, solo un 5% no conoce si estas políticas han sido impartidas, sin embargo, no se les vio muy convencidos a lo que se referían con las políticas de seguridad.

4. Acostumbra a bloquear la sesión al ausentarse del puesto de trabajo

SI NO

Tabla 41 Anexo Encuesta, Tabulación pregunta 4

Valor	Frecuencia	Porcentaje %
SI	30	50%
No	30	50%
Total	60	100%

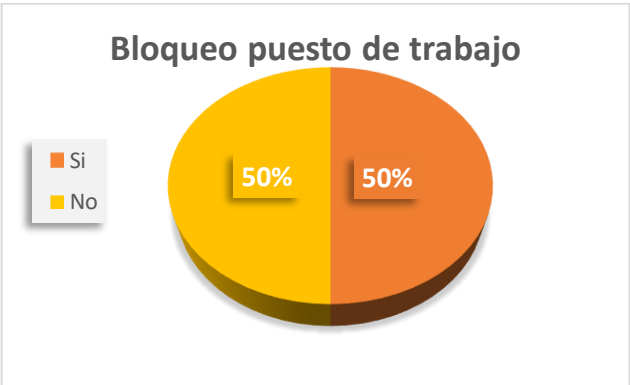


Ilustración 19. Anexo Encuesta, resultado pregunta 4

Este resultado es preocupante, ya que se encuentra un empate (50%) entre quienes bloquean sesión y se paran del puesto sin bloquearla, desconocen los riesgos que implica el que una sesión se quede abierta y alguien más pueda acceder a su información de forma inescrupulosa.

5. Tiene precaución al abrir los adjuntos de los correos electrónicos.

SI NO, No sé

Tabla 42 Anexo Encuesta, Tabulación pregunta 5

Valor	Frecuencia	Porcentaje %
SI	20	33%
No	35	58%
No sé	5	8%
Total	60	100%

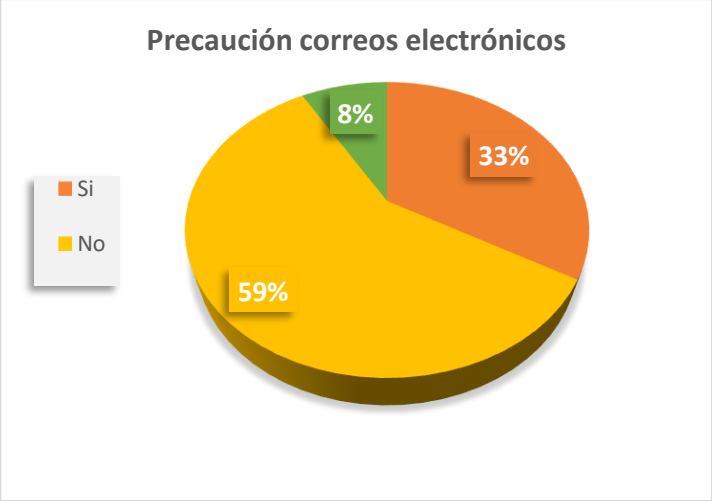


Ilustración 20. Anexo Encuesta, resultado pregunta 5

Como respuesta a este punto, muchas de las personas dijeron que ellos abrían los adjuntos a los correos electrónicos sin ser precavidos de que estos pudieran contener virus, un 64% de los empleados abren el correo sin validar los archivos que abren o sin desconfiar de la procedencia del archivo. Siendo víctimas de bots, phishing y otros tipos de ataques, colocando en riesgo las dimensiones de la seguridad informática.

6. Reporta anomalías en su equipo al equipo de soporte tecnológico

SI NO

Tabla 43 Anexo Encuesta, Tabulación pregunta 6

Valor	Frecuencia	Porcentaje %
SI	30	50%
No	30	50%
Total	60	100%

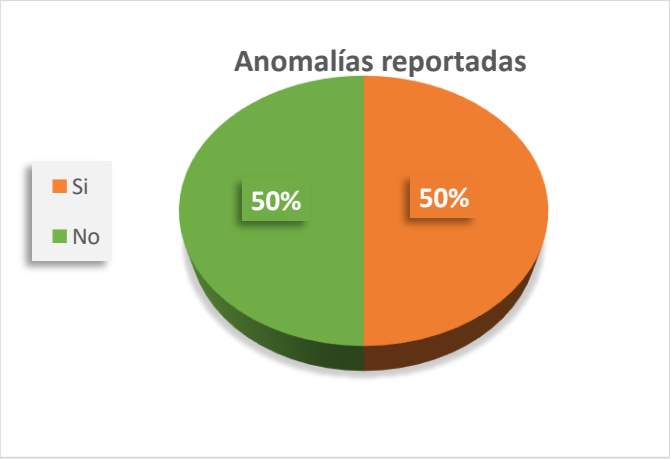


Ilustración 21. Anexo Encuesta, resultado pregunta 6

Solo la mitad de los usuarios reportan las anomalías de los equipos, indicados como un mal funcionamiento en que los equipos se quedan congelados, sin embargo, muchos otros no los hacen porque conciben que, aunque los equipos se quedan o trabajan lento es normal para ellos.

7. Reporta mensajes de antivirus al equipo de soporte tecnológico

SI NO

Tabla 44 Anexo Encuesta, Tabulación pregunta 7

Valor	Frecuencia	Porcentaje %
SI	50	83%
No	10	17%
Total	60	100%

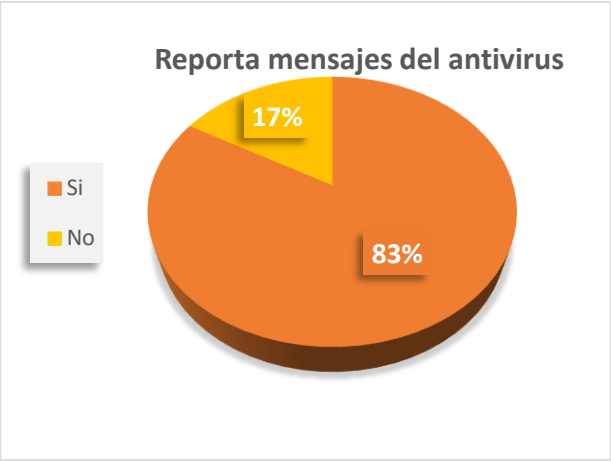


Ilustración 22. Anexo Encuesta, Tabulación pregunta 7

El 83% de los usuarios reporta los mensajes que arroja el antivirus porque consideran que cuando un mensaje de estos aparece es porque el equipo tiene un virus, está infectado y es mejor que lo revise el equipo especializado. Aunque casi todos los mensajes son de alguna amenaza detenida, los usuarios perciben el mensaje como un virus o un mal ya arraigado en el equipo y que lo puede dañar.

8. Utiliza modo incognito en su navegador de internet para no dejar rastros de páginas.

SI NO, No sé

Tabla 45 Anexo Encuesta, Tabulación pregunta 8

Valor	Frecuencia	Porcentaje %
SI	50	83,3%
No	5	8,3%
No sé	5	8,3%
Total	60	100%

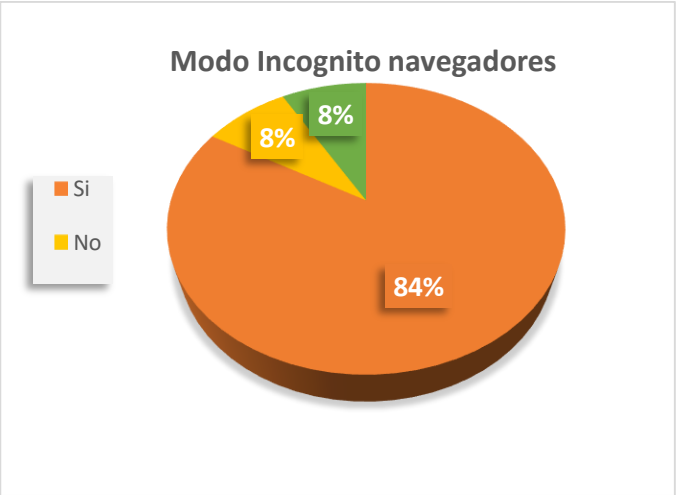


Ilustración 23. Anexo Encuesta, resultado pregunta 8

Se aprecia en este sentido, que la mayor parte de los usuarios no les gusta que estén pendientes de lo que hacen en internet, el 84% de los usuarios navega en modo incognito para esconder actividades extra-laborales que no quieren que se den cuenta de que están haciendo o porque páginas están navegando.

9. Acostumbra a apagar su equipo al terminar su jornada laboral.

SI NO

Tabla 46 Anexo Encuesta, Tabulación pregunta 9

Valor	Frecuencia	Porcentaje %
SI	40	67%
No	20	33%
Total	60	100%

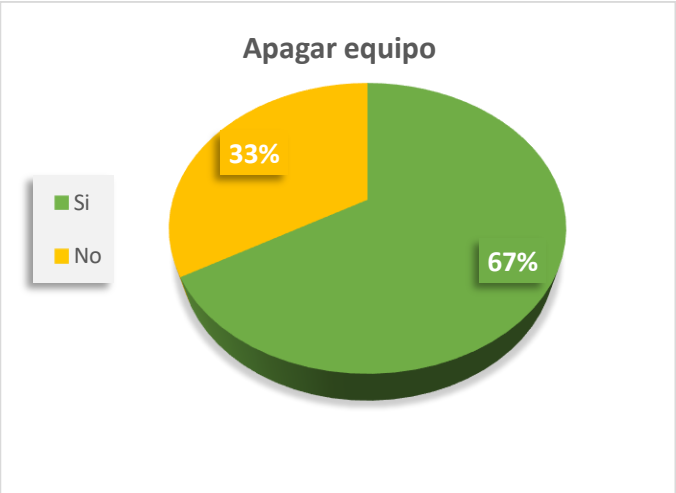


Ilustración 24. Anexo Encuesta, resultado pregunta 9

La mayor parte de los usuarios cumplen con apagar los equipos al final de la jornada, ayudando de esta manera a cumplir con las políticas de seguridad informática y ambiental. Considerando que no se dejan procesos corriendo en los equipos.

10. Comparte su sesión de usuario con sus compañeros de trabajo.

SI NO, No sé

Tabla 47 Anexo Encuesta, Tabulación pregunta 10

Valor	Frecuencia	Porcentaje %
SI	10	16,7%
No	40	66,7%
No sé	10	16,7%
Total	60	100%

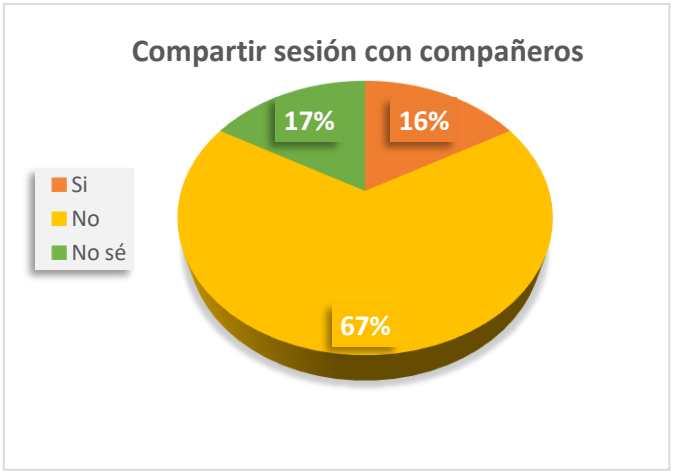
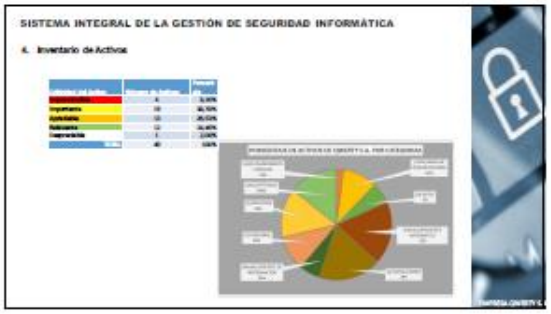


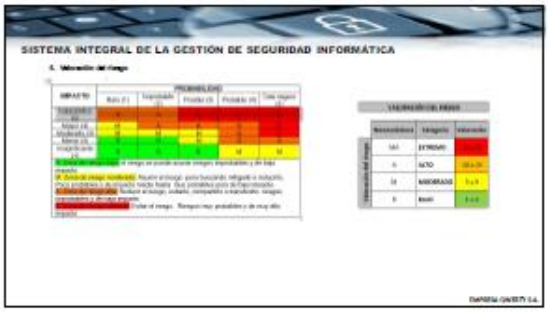
Ilustración 25. Anexo Encuesta, resultado pregunta 10

Las personas que laboran en QWERTY S.A. no comparten su sesión con sus compañeros, entienden muy bien que las sesiones son personales y son muy meticulosos y celosos con la información que respaldan. Sin embargo, es preocupante ver que un número pequeño 16% si lo hace, poniendo en riesgo el dejar que otros usuarios trabajen bajo su nombre en la empresa. Pero más preocupante aún es conocer que el 17% no sabe que es compartir una sesión.

14.2. Presentación en Power Point


SISTEMA INTEGRAL DE LA GESTIÓN DE SEGURIDAD INFORMÁTICA


SISTEMA INTEGRAL DE LA GESTIÓN DE SEGURIDAD INFORMÁTICA
4. Inventario de Activos

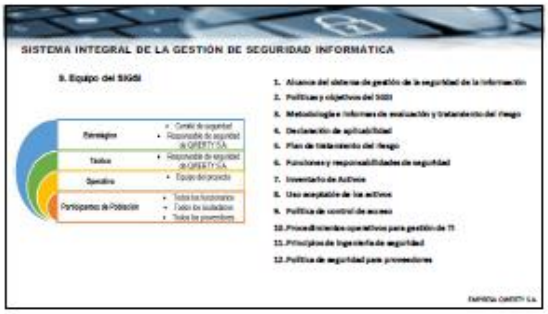

SISTEMA INTEGRAL DE LA GESTIÓN DE SEGURIDAD INFORMÁTICA
5. Valoración del riesgo


SISTEMA INTEGRAL DE LA GESTIÓN DE SEGURIDAD INFORMÁTICA
5. Valoración del riesgo


SISTEMA INTEGRAL DE LA GESTIÓN DE SEGURIDAD INFORMÁTICA
6. Implementación de Controles


SISTEMA INTEGRAL DE LA GESTIÓN DE SEGURIDAD INFORMÁTICA
Nivel 0
Nivel 1
Nivel 2
Nivel 3
Nivel 4
Nivel 5


SISTEMA INTEGRAL DE LA GESTIÓN DE SEGURIDAD INFORMÁTICA
8. Fases de SIGSI
Diagnóstico
Planificación
Implementación
Evaluación de Desempeño
Mejora Continua


SISTEMA INTEGRAL DE LA GESTIÓN DE SEGURIDAD INFORMÁTICA
9. Equipo del SIGSI
Estratégico
Táctico
Operativo
Participantes de Protección
1. Alcance del sistema de gestión de la seguridad de la información
2. Políticas y objetivos del SGSI
3. Metodología e informes de evaluación y tratamiento del riesgo
4. Declaración de aplicabilidad
5. Plan de tratamiento del riesgo
6. Funciones y responsabilidades de seguridad
7. Inventario de Activos
8. Uso aceptable de los activos
9. Política de control de acceso
10. Procedimientos operativos para gestión de TI
11. Principios de ingeniería de seguridad
12. Política de seguridad para proveedores

14.3. Resumen Académico Ejecutivo (RAE)

Tabla 48 Resumen Académico Ejecutivo (RAE)

RESUMEN ACADÉMICO EJECUTIVO (RAE)	
Título del texto	DISEÑO DE UN SISTEMA INTEGRADO DE GESTION DE SEGURIDAD DE LA INFORMACION PARA LA EMPRESA QWERTY S.A
Nombres y Apellidos del Autor	**Carlos Andrés Ubaque Mahecha** **Gilberto Alexis Montoya Téllez**
Año de la publicación	**2019**
Resumen del texto: Sin lugar a dudas el activo más importante para una empresa es la información. En los últimos tiempos esta visión se ha ampliado dando una cobertura global, no solo a la información en sí misma, sino a todos los procesos que acompañan el tratamiento de dicha información a través de los sistemas actuales que están bajo las normas vigentes. La empresa QWERTY S.A. no posee dicho sistema, siendo vulnerable a diferentes ataques que se ven a diario en el mundo informático. Por esto se quiere "diseñar" un sistema de seguridad de la información que cumpla con las expectativas y se acomode al presupuesto de la empresa, con los objetivos de control referenciados en las normativas ISO-27001, bajo el marco de referencia COBIT y la metodología MAGERIT V.3. Este sistema de seguridad se quiere diseñar e implementar para prevenir los delitos informáticos establecidos en la legislación colombiana "ley 1273-2009". Por personajes como Hackers, Crackers o Lammers. Y educar en ingeniería social a los usuarios para que no permitan la perdida de datos indiscriminadamente. Se requiere establecer una investigación cuantitativa que analice los datos de los CI (*ítems de configuración,* por sus siglas en inglés) actuales de la empresa, los procesos que se llevan a cabo sobre la información y la documentación de dichos procesos, las vulnerabilidades, las amenazas, el impacto de los riesgos a presentar, y el costo de no implementar este SIGSI para la empresa tanto monetariamente como funcionalmente. A fin de establecer el alcance del sistema, en proporción a las necesidades básicas de seguridad identificadas, los controles que se pueden aplicar y el monitoreo de dichos controles a través del ciclo PHVA propuesto por Edwards Deming.	
Palabras Claves	QWERTY S.A., SIGSI, hackers, lammers, ISO 27001, Magerit, PHVA, CI, Vulnerabilidad, amenaza, ingeniería social, riesgos, impacto,

RESUMEN ACADÉMICO EJECUTIVO (RAE)	
	Bytes, Wannacry, hetero-evaluación, controles, ciberseguridad, TI, ethical hacking, pentesting.

Problema que aborda el texto:

Objetivos del texto:

Diseñar un sistema de gestión de seguridad de la información para la empresa caso de estudio QWERTY S.A, que permita gestionar la seguridad de la información a partir de buenas prácticas de un Sistema Integrado de Gestión de Seguridad de la Información.

•Analizar los procesos existentes en la empresa para generar un análisis de riesgo y listar los activos informáticos de la empresa evidenciando sus vulnerabilidades y su probabilidad de frecuencia de ocurrencia de riesgo en ellos QWERTY S.A.
•Implementar las mejores prácticas, que permita dar cumplimiento a la legislación en la seguridad de la información.
•Establecer controles para aplicar y evaluar la ejecución de los mismos para ver oportunidades de mejora.
•Definir las políticas de seguridad que se aplicarán en la empresa QWERTY S.A.

Hipótesis planteada por el autor:

¿Cuál es el grado de seguridad de los sistemas de información de la empresa QWERTY S.A. en relación a las normativas vigentes que permitan el diseño de un sistema de gestión de seguridad de la información en el cual se implementen controlen que ayuden a mitigar los riesgos de fallo en las dimensiones claves de la información?

Tesis principal del autor:

No se realiza tesis de grado, se realizó un proyecto aplicado hacía una empresa.

Conclusiones del texto:

Durante la validación del estado inicial en el cual se puede encontrar QWERTY, se ha validado los activos de la empresa en las tres dimensiones primordiales de la información, dándole a cada uno de ellos un valor cualitativo y cuantitativo a fin de poder conocer su escala de vulnerabilidad, su importancia para la empresa y el riesgo que existe que se pueda hacer real una amenaza y afecte de manera menor o significativa la empresa por no prevenir, mitigar, reducir o transferir dicho riesgo.

Gracias a la metodología Magerit, se han clasificado estas amenazas y se han cruzado con cada una de las categorías de los activos para darles un valor a fin de poder medir el estado actual de los mismos en la clasificación de los grupos de la metodología. En concordancia con esto, se realizó la validación de estas vulnerabilidades a la luz de la norma ISO 27001:2013 para implementación de los

controles más comunes o estándares que debe llevar un sistema integrado de gestión de la seguridad de la información.

Dichos controles se han establecido en la *declaración de aplicabilidad* en la cual se toman en cuenta dichas salvaguardas del Anexo A: y se evidencia la justificación del porque es aplicable para la empresa. Al aplicar estos controles y como se ha realizado la recomendación es necesario tener un comité que gestione el sistema que se quiere crear en QWERTY S.A. y que permita la aplicación de las políticas que todo el personal de la empresa debe conocer para ayudar a construir una mejor seguridad. Se ha establecido unas políticas generales básicas que son lo mínimo que debe tener un sistema integrado de gestión de seguridad de la información en relación a los controles de acceso, el uso adecuado de los activos, procedimientos de gestión de tecnologías de información, la seguridad física, la seguridad de operaciones y el vínculo con los proveedores entre otros.

Es por esto, que el Sistema Integrado de Gestión de la Seguridad de la Información de la empresa QWERTY S.A. se ha definido en una etapa **Definido** ya que la empresa es muy consciente de que tiene problemas y algunos procedimientos formales de seguridad, sin embargo, las fases de diagnóstico, planeación e implementación hasta ahora se están empezando a construir por medio de la consolidación de los documentos que propone como obligatorios la norma y que están definidos aquí

1. Alcance del sistema de gestión de la seguridad de la información
2. Políticas y objetivos del SGSI
3. Metodología e informes de evaluación y tratamiento del riesgo
4. Declaración de aplicabilidad
5. Plan de tratamiento del riesgo
6. Funciones y responsabilidades de seguridad
7. Inventario de Activos
8. Uso aceptable de los activos
9. Política de control de acceso
10. Procedimientos operativos para gestión de TI
11. Principios de ingeniería de seguridad
12. Política de seguridad para proveedores

De los cuales muchos ya se han comenzado a diseñar y estructurar y otros están al pendiente en las siguientes etapas mientras se madura el sistema y se autoevalúa para su regulación, administración y optimización

ABRIL ESTUPIÑAN, Ana., PULIDO, Jarol y BOHADA John. Análisis de riesgo en seguridad de la información. En: Ciencia, innovación y tecnología (RCIYT), enero-diciembre 2013, vol 1, p. 39 -53. Disponible en Internet: https://www.jdc.edu.co/revistas/index.php/rciyt/article/view/121/113

RESUMEN ACADÉMICO EJECUTIVO (RAE)

ÁLVAREZ BASALDÚA, Luis Daniel, Seguridad Informática (Auditoria de sistemas). Tesis de maestría. Maestro en Ingeniería de sistemas empresariales. México D.F.: Universidad Iberoamericana. 2005. 117 p. Disponible en Internet: http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

ÁLVAREZ M. Gonzalo y PÉREZ, Pedro Pablo. Seguridad Informática para empresas y particulares. Madrid España.: McGraw-Hill, 2004, 413 p. ISBN: 84-481-4008-7

AUSTIN, Robert D. y DARBY, Christopher A.R. El mito de la Seguridad Informática. En: Harvard Deusto Bussines Review, enero – diciembre 2004, no. 120, p. 66-74. ISSN: 0210-900X125.

BARRIO A. Moisés, Delitos 2.0: Aspectos penales, procesales y de la seguridad de los ciberdelitos, España. La Ley agosto 2018, 310 p. ISBN: ISBN number:9788490207437, ISBN number:9788490207444

BAUTISTA, Marco Antonio. Marco de referencia para la formulación de un plan de continuidad de negocio para TI, un caso de estudio (Tesis de maestría). [En línea] Universidad de las Américas, Quito. 2014 p. 135 [Citado 10 de marzo 2019] Disponible en Internet: http://dspace.udla.edu.ec/handle/33000/3081

BAYONA, Sussy. CHAUCA, Wilber. LOPEZ, Milagros y MALDONADO, Carlos. [En línea] Publicado en: CISTI – Conferencia ibérica de sistemas y tecnologías de la información (10: 17 – 20 Junio de 2015) Implementación de la NTP ISO/IEC 27001 en las instituciones Públicas: Caso de Estudio. 2015, p 410 – 415.

BEACHY, Rob. End user information security policy template. Brainmass, 2012. 28 p. Disponible en Internet: http://bibliotecavirtual.unad.edu.co/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=529772&lang=es&site=ehost-live

BISOGNO, María Victoria. Metodología para el aseguramiento de entornos informatizados – MAEI. Tesis de grado [En línea]. Buenos Aires – Argentina. Universidad de Buenos Aires, Facultad de Ingeniería. 2004, 235 p. Disponible en Internet: http://materias.fi.uba.ar/7500/bisogno-tesisdegradoingenieriainformatica

BRICEÑO S. Francisco Javier. Implementación de un sistema de seguridad en un edificio público. (Proyecto fin de carrera) [En línea]. Leganés – Madrid España. Universidad Carlos III de Madrid, Departamento de automatización. 2010, 118 p. Disponible en Internet: https://e-

archivo.uc3m.es/bitstream/handle/10016/10587/PFC_FranciscoJavier_Briceno_Sanz.pdf?sequence=1&isAllowed=y

BUITRAGO E. Johanna C. BONILLA P. Diego H. y MURILLO V. Carol E. Diseño de una metodología para la implementación del sistema de gestión de seguridad de la información – SGSI, en el sector de laboratorios de análisis de microbiológicos, basados en ISO 27001. Tesis de postgrado Gerencia de procesos y calidad. [En línea] Universidad EAN, Bogotá D.C.: 2012 p 142. Disponible en Internet: https://repository.ean.edu.co/bitstream/handle/10882/2692/MurilloCarol2012.pdf?sequence=1

CANO, Anisley. CAMPILLO, Irima y CUESTA R. Floricelda. Sistema de Gestión de Información para la Educación Superior. En: Ciencias de la Información. Mayo a Agosto 2014, vol. 46, no. 1, p 21-24. Disponible en Internet: http://cinfo.idict.cu/index.php/cinfo/article/view/635/488

CARDENAS S. Leidy Johanna, MARTÍNEZ A. Hugo y BECERRA A. Luis Eduardo. Gestión de seguridad de la información: Revisión Bibliográfica. En: El profesional de la información [En línea], Bucaramanga – Colombia, Universidad Industrial de Santander. 2016, vol. 25, no. 6. p. 931 – 948 eISSN: 1699-2407. Disponible en Internet: https://recyt.fecyt.es/index.php/EPI/article/view/epi.2016.nov.10/32176

CHOI, Kyung y TORO A. Marlon M. Cibercriminología. Guía para la investigación del cibercrimen y mejores prácticas en seguridad digital. Bogotá D.C.: Universidad Antonio Nariño. 2017, 604 p. ISBN 9789588687711.

CISTI – CONFERENCIA IBERICA DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN. (7: 20 - 23 junio, 2012: Madrid España) Optimización de la economía de la seguridad de la información, Consejo General de Colegios Oficiales de Ingeniería Técnica en Informática, 2012, p. 126 – 129.

COLLAZOS, B. Manuel. La nueva versión ISO 27001:2013 Un cambio en la integración de los sistemas de gestión [diapositivas], PRIME Asesoría y desarrollo Integral Profesional, Lima – Perú. 27 diapositivas.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581 (18, octubre 2012) Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial Bogotá D.C., 2012 No. 48.587. p 1 – 301. Disponible en Internet: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (5, enero 2009) Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"-… Diario Oficial Bogotá D.C., 2009 No. 47.223. p 1 – 4. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

CORNEJO, S. Gloria y MANCHOLA, Sandra. Investigación sobre el Hacker y sus posibles comienzos en la Comunidad Estudiantil, Caso de Estudio (Proyecto de grado) [En línea] Universidad Piloto de Colombia, Bogotá D.C. 2015 p. 167 [Citado 11 de marzo de 2019] Disponible en Internet: http://polux.unipiloto.edu.co:8080/00002887.pdf

DUMAN, Ekrem, ATIYA, Amir. Use of risk analysis in computer-aided persuasion. 2011, vol. 88, p. 345 (NATO Science for Peace and Security Series. The NATO Science for peace and security programme. IOS Press.) ISBN: 978-1-60750-828-1. Disponible en Internet: http://bibliotecavirtual.unad.edu.co/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=422088&lang=es&site=ehost-live

ESTADOS UNIDOS, YMCA BUFALO NIAGARA DEPARTMENT. Information security End-user policy. New York, 2015. 26 p. disponible en Internet: https://www.politecnicojic.edu.co/images/downloads/biblioteca/guias/NTC5613.pdf

GÓMEZ, Oiner. BAUTA, C. René y ESTRADA S. Vivian. Modelo para la compartimentación de la información en las organizaciones. En: Ciencias de la Información. Enero a abril 2014, vol. 45, no. 1, p 11-17. Disponible en Internet: https://biblat.unam.mx/hevila/Cienciasdelainformacion/2014/vol45/no1/2.pdf

GUIJARRO-RODRÍGUEZ, Alfonso. Defensa en profundidad aplicado a un entorno empresarial. En: Espacios. Junio 2018, vol. 39, no. 42, p 19. Disponible en Internet: http://www.revistaespacios.com/a18v39n42/a18v39n42p19.pdf

HURTADO, Rubén. RODRÍGUEZ, Wilson. FUENTES, Héctor y GALLEGUILLOS, Carlos. Impacto en los beneficios de la implementación de la normas de calidad ISO 9000 en las empresas. [En línea] En: Revista de la Facultada de Ingeniería. Copiapó Chile: Universidad de Atacama. 2009, p. 17-26. Disponible en Internet: http://www.revistaingenieria.uda.cl/Publicaciones/230003.pdf

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN, Tecnología de la información, técnicas de seguridad. Sistemas de gestión de seguridad de la información (SGSI). Requisitos. NTC-ISO/IEC 27001. Bogotá D.C.: El instituto, 2013 45 p. Disponible en Internet:

http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

INTERNATIONAL ORGANIZATION OF STANDARIZATION and INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information technology – security techniques - information security management systems – Overview and vocabulary. ISO/IEC 27000:2016, Geneva, Switzerland: IOS, 2016, 42 p. Disponible en Internet: http://standards.iso.org/ittf/PubliclyAvailableStandards/c066435_ISO_IEC_27000_2016(E).zip

INTECO. SGSI. España, [En línea] 2010. [vídeos de youtube], 15 vídeos publicados por Instituto Nacional de Ciberseguridad. Disponible en Internet: https://www.youtube.com/watch?v=zV2sfyvfqik&list=PLN3XU56O7eKxo4flrxApWQG_5qc0TiGmA

ISO27000, Sistema de Gestión de la Seguridad de la Información, [En línea], www.iso27000.es s.f. 14 p. [Citado 18 Abril de 2019] Disponible en Internet: http://www.iso27000.es/download/doc_sgsi_all.pdf

ISOTOOLS EXCELLENCE, ISO 27001: Aspectos claves de su diseño e implementación, [En línea], www.isotools.org s.f. 23 p. [Citado 15 Abril de 2019] Disponible en Internet: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

LA ESTRELLA, Redacción Digital. Los 5 tipos de Ransomware que más afectan los usuarios. [En línea]. 2019. Artículo. [Citado el 12 de marzo 2019] Disponible en Internet: https://www.laestrella.com.pa/cafe-estrella/tecnologia/190126/5-tipos-afectan-ransomware

LA VANGUARDIA, Redacción Digital. El malware sofisticado y los sistemas operativos desactualizados, entre las principales amenazas móviles para 2019. [En línea]. 2019. Artículo [Citado 12 de marzo 2019] Disponible en Internet: https://www.lavanguardia.com/vida/20190212/46406846701/el-malware-sofisticado-y-los-sistemas-operativos-desactualizados-entre-las-principales-amenazas-moviles-para-2019.html

LÓPEZ, Purificación. Seguridad Informática, Pozuelo de Alarcón, Madrid, Editex, 2010. P 240, ISBN: 978-84-9771-657-4.

MARTELO, Raúl. TOVAR, Luis y MAZA, Diego. Modelo básico de seguridad lógica. Caso de Estudio. [En línea] Laboratorio de redes Universidad de Cartagena, Cartagena. 2018, En: Información tecnológica (versión en línea), vol

29, no. 1. Disponible en Internet: http://dx.doi.org/10.4067/S0718-07642018000100003

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de riesgos de los Sistemas de Información. Libro I – Método. NIPO: 630-12-171-8. Madrid, España. 2012 127 p. Disponible en Internet: https://www.politecnicojic.edu.co/images/downloads/biblioteca/guias/NTC5613.pdf

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de riesgos de los Sistemas de Información. Libro II – Catalogo de Elementos. NIPO: 630-12-171-8. Madrid, España. 2012 127 p. Disponible en Internet: https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de riesgos de los Sistemas de Información. Libro III – Guía de Técnicas. NIPO: 630-12-171-8. Madrid, España. 2012 127 p. Disponible en Internet: https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html

MINTIC. Guía 1 – Metodológica de Pruebas de Efectividad Bogotá D.C.: Ministerio, 2016, 28 p. Disponible en Internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf

MINTIC. Guía 3 – Procedimiento de Seguridad de la Información Bogotá D.C.: Ministerio, 2016, 19 p. Disponible en Internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

MINTIC. Guía 5 – Gestión Clasificación de Activos, Bogotá D.C.: Ministerio, 2016, 18 p. Disponible en Internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

MINTIC. Guía 7 – Gestión de Riesgos Bogotá D.C.: Ministerio, 2016, 39 p. Disponible en Internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

MINTIC. Guía 17 – Mejora continua Bogotá D.C.: Ministerio, 2015, 10 p. Disponible en Internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G17_Mejora_continua.pdf

NAJAR, P. José y SUÁREZ, S. Nubia. La seguridad de la información: un activo valioso de la organización. En: Vínculos. Febrero 2015, vol 12, no 1, p 89-97. Disponible en Internet: https://revistas.udistrital.edu.co/index.php/vinculos/article/view/10518/11480

PICÓN C. Ingrid. Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013. Trabajo de Grado Sistemas de Gestión de seguridad de la información, Master en seguridad de tecnologías de la información y de las comunicaciones (MISTIC). Colombia.: Instituto colombiano para la evaluación de la Educación – ICFES, 2016, p 29. Disponible en Internet: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/54261/5/ipiconTFM0616memoria.pdf

POSADA, M. Ricardo. El delito de acceso abusivo a sistema informático: a propósito del art. 269ª del CP de 2000. En: Revista de derecho, comunicaciones y nuevas tecnologías. Junio de 2013, no. 9, p 1-31 Disponible en Internet: https://derechoytics.uniandes.edu.co/components/com_revista/archivos/derechoytics/ytics129.pdf

SUÁREZ, Diana y ÁVILA, F. Aldeir. Una forma de interpretar la seguridad Informática. En: Innovación, ingeniería y desarrollo, Enero-diciembre 2013, vol 2, no. 2, p. 87-93. Disponible en Internet: https://docplayer.es/36805408-Una-forma-de-interpretar-la-seguridad-informatica.html

SUCA, Jackeline Tatiana. Propuesta metodológica para implementar la Norma Técnica Peruana ISO/IEC 27001:2008 de Seguridad de la Información en entidades públicas del Estado. Tesis de grado Ingeniería de Sistemas. Arequipa – Perú.: Universidad Católica de Santa Marta. Facultada de Ciencias e ingenierías físicas y formales programa profesional de ingeniería de sistemas. 2014, 183.

VARGAS, Ana Cecilia y CASTRO M. Alonso. Sistemas de gestión de seguridad de la información [diapositivas]. Costa Rica. Universidad de Costa Rica, s.f. [En línea] 32 diapositivas, color, Disponible en Internet: http://archivo.ucr.ac.cr/docum/ISOEIC27000.pdf

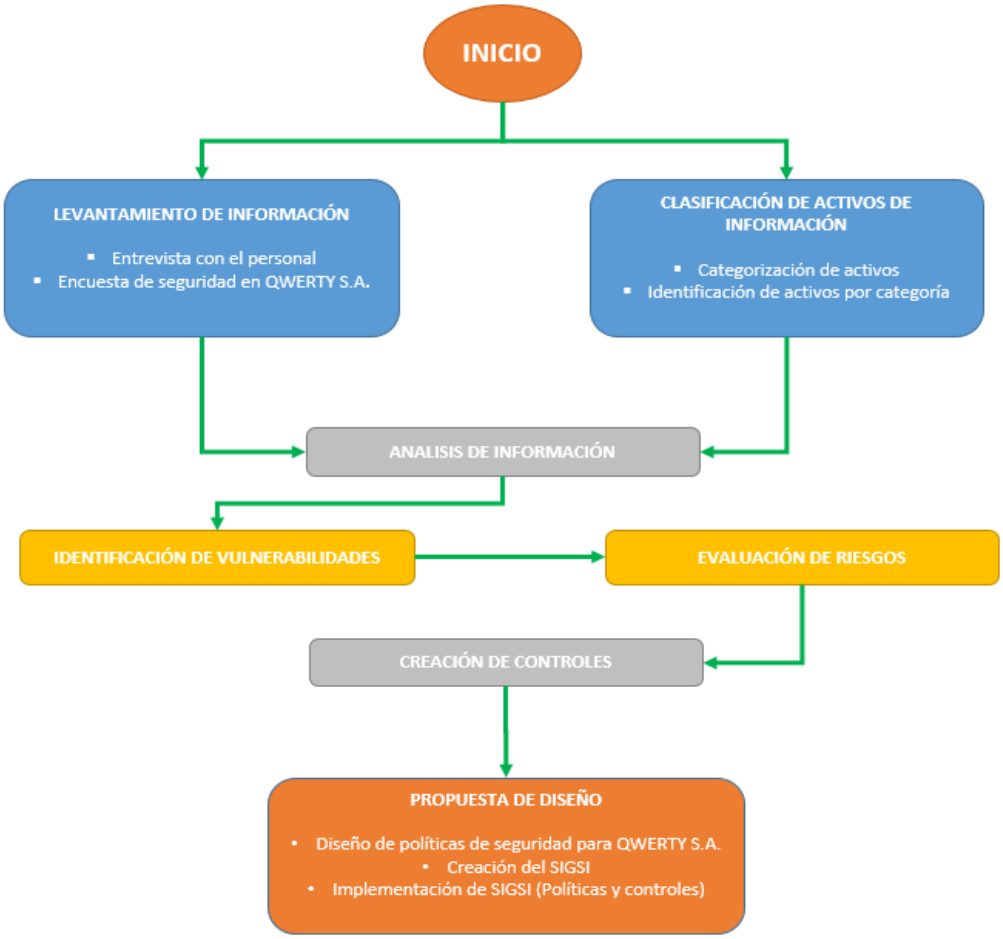
VERA, C. Romel, ¿Se puede usar una PC sin antivirus? En: 3C TIC. Septiembre 2016 vol. 5, no. 2, p. 1-12. doi:10.17993/3ctic.2016.52. ISSN: 2254 – 6529.

VOUTSSAS, Juan. Preservación documental digital y seguridad informática. En: Investigación Bibliotecológica: archivonomía, bibliotecología e información, 2010, vol. 24, no. 50, p 1-24 DOI: http://dx.doi.org/10.22201/iibi.0187358xp.2010.50.21416, ISSN:2448 – 8321

YOUNGIN, You. JUNHYOUNG, Oh. SOOHEON, Kim y KYUNGHO Lee.

RESUMEN ACADÉMICO EJECUTIVO (RAE)	
Advanced approach to information security management system utilizing maturity models in critical infrastructure. En: KSII Transaction on internet and information systems [En línea]. Octubre 2018, vol. 12, no. 10, p. 4995 – 5014 doi: http://doi.org/10.3837/tiis.2018.10.020 ISSN : 1976-7277	
Nombre y apellidos de quien elaboró este RAE	**Gilberto Alexis Montoya Téllez**
Fecha en que se elaboró este RAE	12 diciembre de 2019

Imagen (mapa conceptual) que resume e interconecta los principales conceptos encontrados en el texto:



Comentarios finales:

Se pudieron establecer los activos de información dentro de la empresa QWERTY logrando establecer la criticidad de cada uno de ellos y la importancia que cada

uno tiene en la labor de los trabajadores de la empresa, cada uno de los activos de información constituyen una parte importante en el porvenir de la empresa, hay que tener en cuenta que los procesos sufren un cambio durante el tiempo, en el cual involucran tecnología y personal capacitado para administrarlos.

El análisis de riesgos nos determinó el nivel al que están expuesto cada uno de los activos, las salvaguardas actúan en el momento que se potencialice una amenaza y que podría comprometer los activos y su funcionamiento. Sin embargo, hay que recordar que los riesgos pueden ser mitigados, transferidos, eliminados o aceptados. El pago de un seguro o trasladar el riesgo a una aseguradora son alternativas que la empresa puede hacer uso, pero para ello, es importante contar un presupuesto para el pago y sostenimiento del seguro. Trasladar el riesgo a un tercero también es viable ya que este tiene muchas más herramientas para tratar el riesgo.

El sistema de gestión de la empresa nos permite tener los procesos documentados y con los lineamientos exigidos por la norma ISO 27001:2013.