ESQUEMA DE ASEGURAMIENTO Y GESTIÓN DE LA INFORMACIÓN PARA LA EMPRESA CASO DE ESTUDIO QWERTY S.A.

GERMAN DARIO LOPEZ RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2021

ESQUEMA DE ASEGURAMIENTO Y GESTIÓN DE LA INFORMACIÓN PARA LA EMPRESA CASO DE ESTUDIO QWERTY S.A.

GERMÁN DARÍO LÓPEZ RODRÍGUEZ

LUIS FERNANDO ZAMBRANO HERNANDEZ
Director de Trabajo de Grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2021

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá., Enero

DEDICATORIA

A Dios, que es quien siempre está a mi lado guiándome por el camino correcto de la vida, permitiéndome realizar mis proyectos y salir adelante.

A mi familia, por brindarme el apoyo y fuerza para la toma de decisiones.

A mi esposa por su apoyo incondicional.

A mis maestros, por compartir sus conocimientos, sobre los temas vistos.

A mis amigos por sus aportes y enseñanzas.

A la universidad Nacional Abierta y a Distancia - UNAD, por permitirme desarrollar mis conocimientos e ideas

AGRADECIMIENTOS

En primer lugar, quiero agradecer a todas aquellas personas, que han brindado todo su apoyo y conocimiento, para poder cumplir todas aquellas metas que me he propuesto.

A Dios por el entendimiento para la toma de buenas decisiones durante mi vida.

Por último, a la universidad UNAD por brindarme la oportunidad de llevar a cabo la especialización en seguridad informática. Al director de proyecto, por el tiempo dedicado para transmitir sus conocimientos, por la rigurosidad para lograr el desarrollo del proyecto de grado, permitiendo la claridad de las aplicaciones tanto en la práctica como en la normatividad.

CONTENIDO

pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE CUADROS

Pág.

GLOSARIO

ANÁLISIS Y GESTIÓN DE RIESGOS: Este proceso permite establecer el impacto que tendrá la materialización de un riesgo dentro de la compañía. Mediante este análisis se podrá identificar cuáles son los activos de la información a proteger según cada uno de los posibles riesgos que nos dé como resultado dicho análisis.[1]

CONTROL DE ACCESO: Este sistema es el encargado de controlar todas aquellas herramientas tecnológicas de áreas específicas. Este también permite la verificación de la identidad de las personas con permisos para los ingresos a un área específica o una cierta información. Este control de acceso cuenta con dos tipos, uno de ellos es el de acceso en donde podemos ver la parte biométrica para el control de entrada y salida en el cumplimiento de horarios y de ingreso a las áreas adecuadas dentro de la compañía, el otro tipo de acceso es el de red donde el software registra toda actividad realizada en el equipo de cómputo de la compañía.[2]

FIREWALL: Este sistema contribuye con la protección de los equipos de la compañía, de los virus y de los archivos maliciosos creando un filtro entre la red interna y la red externa, trazando permisos en el tráfico permitiendo la entrada y salida segura de la información.

LEYES DE CIBERSEGURIDAD: Dentro del diseño del SGSI, se debe tener presente el software, el hardware, los procesos, los procedimientos, las políticas y todo aquello que pueda ser para nosotros irrelevante, pero que en algún momento lleve a generar un incumplimiento a la norma, y más grave a la afectación a un individuo u organización, es por tal motivo en el que conocer algo de la normatividad es importante para la correcta implementación.[3]

---

[1] ISO, NTC-ISO/IEC 31000:2018, En Linea, 2018, disponible en: https://www.iso.org/home.html
[2] ISO, NTC-ISO/IEC 27001:2013, En Linea, 2013, disponible en: https://www.iso.org/home.html
[3] QUINTERO AGUDELO, Yolanda “La seguridad y la ciberdefensa en Colombia” En Linea, disponible en: http://polux.unipiloto.edu.co:8080/00001596.pdf

NORMA ISO 27001:2013: Esta norma se basa en la correcta administración de la información en todas aquellas áreas que deban realizar un manejo diario.[4]

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN: Es la base de la norma ISO 27001:2013, para llevar a cabo todo proceso documentado y sistematizado de la compañía. La confidencialidad, la integridad y la disponibilidad son los aspectos más importantes que debemos tener en cuenta para el levantamiento de la información dentro de la compañía, y así lograr minimizar todo riesgo a lo que se expone dicha información.[5]

SISTEMAS DE INFORMACION: Es el conjunto de recursos tangibles que tiene una compañía para brindar una correcta obtención y comunicación de la información. El sistema de información debe resultar de forma acertada y efectiva, dando a conocer que esta es veraz si se realiza el proceso con los menores recursos posibles. Estos sistemas se deben adecuar de la mejor manera a las compañías según su estructura organizacional.[6]

[4] ISO. Op. cit.
[5] ISO, NTC-ISO/IEC 27001:2013, En Linea, 2013, disponible en: https://www.iso.org/home.html
[6] Ibíd.

RESUMEN

Este trabajo académico, se basa en el desarrollo del sistema de gestión de la seguridad Información - SGSI para la empresa QWERTY S.A. la cual actualmente cuenta con la problemática de una infraestructura informática inadecuada, debido a que en el manejo de la información que se debe tratar a diario, no cuenta con las normas adecuadas tanto para los clientes internos como externos. Para poder lograr que esta se implemente de forma correcta, se establecerán objetivos de tal manera que se identifiquen las necesidades de la empresa para la aplicación del SGSI.

El proceso busca identificar de forma precisa las amenazas a las que está expuesta la información e implementar medidas para la mitigación del riesgo, con el propósito de aplicar la corrección de forma ágil en el menor tiempo posible, previniendo que los sistemas informáticos sufran pérdidas de registros información. De esta forma se podrá establecer aspectos y puntos críticos donde intervienen conceptos importantes de ciberseguridad y del entorno de la información que maneja la compañía, para así garantizar la corrección de las problemáticas identificadas durante el desarrollo de la actividad y la aplicación del SGSI basado en la norma NTC-ISO/IEC 27001:2013.

Finalmente, al establecer el sistema de seguridad de la información, se logrará identificar las debilidades actuales sobre el tratamiento de la información, implementando un proceso que cuente con una metodología de mejora continua.

Palabras Clave:

GESTION, MAGERIT, NORMA NTC-ISO/IEC 27001:2013 RIESGO, SGSI VULNERABILIDAD

ABSTRACT

This academic work is based on the development of the Information Security Management System - ISMS for the company QWERTY S.A. which currently has the problem of an IT inadequate infrastructure, because in the management of the information that must be treated on a daily basis does not have the appropriate standards for both internal and external clients. In order to ensure that it is implemented correctly, objectives will be set in such a way as to identify the needs of the company for the implementation of the ISMS.

The process seeks to accurately identify the threats to which the information is exposed and implement risk mitigation measures, with the aim of applying the correction in an agile manner in the shortest possible time, preventing computer systems from losing information log. In this way, critical aspects and points can be established where important concepts of cybersecurity and the information environment managed by the company are involved, in order to ensure the correctness of the problems identified the during development of the activity and the application of the SGSI based on the NTC-ISO / IEC 27001: 2013 standard.

Finally, by establishing the information security system, it will be possible to identify current weaknesses in the treatment of information, implementing a process that has a methodology of continuous improvement.

Keywords:

ISMS, MAGERIT, MANAGEMENT, NTC-ISO / IEC 27001: 2013.
RISK, VULNERABILITY.

INTRODUCCIÓN

En la actualidad los sistemas de información crecen de forma exponencial y son una herramienta indispensable para el desarrollo de los procesos en las organizaciones, debido a que alojan un activo indispensable como lo es la información, este concepto ha motivado a las compañías a generar estrategias que mitiguen los factores de riesgo a los que se expone la información y que pueden provocar que sufran ataques como robo, alteración y perdida bien sea parcial o total.[7]

Es importante comprender que no toda la información es esencial, por lo que para una gestión apropiada se debe clasificar de acuerdo con su valor, posteriormente evaluar las amenazas a las que se encuentra y finalmente generar los controles necesarios para su custodia. La implementación del sistema de gestión de seguridad de la información busca preservar la integridad, la disponibilidad y la confidencialidad de la información[8], al transmitirla, procesarla y guardarla.

El desarrollo del sistema de gestión de seguridad de la información, define una metodología para el levantamiento de información de los activos informáticos, su clasificación, evaluación del riesgo al que están expuestos, el análisis de los resultados obtenidos durante el proceso y la propuesta de controles adecuados para la corrección de las vulnerabilidades y las amenazas encontradas, en consecuencia el SGSI se debe realizar de forma constante, para la mejora continua en la infraestructura y la seguridad, con la finalidad del adecuado manejo de la información.[9]

[7] ANDRADE RODRIGUEZ, Yovany ” ENTENDIENDO EL SGSI” En Linea, disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2748/00002987.pdf?sequence=1
[8] ISO, NTC-ISO/IEC 27001:, En Linea, 2018, disponible en: https://www.iso.org/home.html
[9] ISOTOOLS EXCELLENCE “ISO 27001: El método MAGERIT” En Línea, marzo 2019, disponible en: https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

Mediante este proyecto académico se pretende realizar el estudio del estado actual de la Seguridad de la información en la empresa QWERTY S.A, la creación de estrategias de mitigación del riesgo asociado a un sistema de gestión de seguridad de la información, con el objeto de exponer las amenazas y riesgos, para así lograr evitar posibles acciones indeseables que puedan afectar la operación de la compañía.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La empresa QWERTY S.A es una empresa del sector tecnológico en Colombia que busca el desarrollo de las comunidades mediante el uso de tecnologías de información. Actualmente cuenta con una infraestructura dividida en áreas, para el desarrollo de las aplicaciones y del soporte técnico a los clientes internos y externos de la compañía en su diario vivir. No obstante, se identifica que no tiene las políticas claras, necesarias y adecuadas para el manejo de la información, permitiendo que esta sea un riesgo latente en los activos tecnológicos y en la información vital, permitiendo la aparición de un nuevo riesgo que actualmente no esté detectado por la compañía. QWERTY cuenta con un Firewall Cisco ASA 5505, que no tiene implementados los controles establecidos, para la protección y prevención de ataques, asegurando la información y sus equipos.

La red de las comunicaciones no tiene las secciones adecuadas, lo que indica que para poder acceder a la información, el personal simplemente debe tener la necesidad de consulta para hacerlo, ya que no cuenta con filtros necesarios para la preservación y manejo adecuado de esta, permitiendo que los datos y la información financiera que maneja cada área se convierta en un riesgo alto, ya que a esta no solamente tiene acceso el personal netamente interesado, sino cualquier persona de la compañía.

La empresa tiene un área especializada en el soporte adecuado para la parte administrativa y operativa, pero no tiene políticas establecidas para garantizar el buen uso de los recursos por cada uno de los clientes internos. Permitiendo que esto se convierta en un mal uso y un riesgo elevado por no contar con una buena política de manejo de la información.

Los servidores DHCP, HTTP y PBX, no cuentan con un ambiente adecuado para un buen funcionamiento según las especificaciones dadas por el fabricante, convirtiendo esto en otro riesgo debido a que puede generar pérdida de información y daños físicos en los equipos.

La empresa cuenta con personal bajo el contrato de aprendizaje en el área de nómina y facturación, se le delegan funciones importantes en el almacenamiento de la información, creando un riesgo debido a la falta de control, verificación y trazabilidad de esta.

Adicionalmente a esto que la empresa no tiene un sistema de seguridad biométrico y de monitoreo para el ingreso y realización de las actividades de cada uno de los clientes tanto internos como externos.

1.2 FORMULACIÓN DEL PROBLEMA

La empresa QWERTY S.A. es una empresa dedicada al desarrollo de tecnología en Colombia, cuenta con áreas de TI encargadas de dar respuesta a los requerimientos diarios tanto de clientes internos como externos, sin embargo, no cuenta con una estrategia de seguridad que garantice la protección de los activos de información de la entidad, lo que implica que se encuentran expuestos a riesgos que desconoce la organización, se evidencia que el área de TI no cuenta con procesos y procedimientos claramente definidos sobre la clasificación y administración de la información debido a que no se reconoce su importancia, por lo que esta se deja expuesta a la probabilidad de ocurrencia de un evento que genere afectación, así mismo es claro que no existen las herramientas necesarias para el control de los diferentes factores de riesgo y que no existe ninguna madurez sobre el procesos de seguridad.

¿Cómo un Sistema de Gestión de Seguridad de la Información, puede contribuir en mejorar la continuidad de negocio y la seguridad de la información en la empresa QWERTY S.A.?

2 JUSTIFICACIÓN

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la empresa QWERTY S.A. tiene como propósito la protección de los activos de información sensible de la compañía ante cualquier amenaza que pueda generar una afectación, esto mediante la implementación de políticas, procesos y controles apropiados que permitan la gestión del riesgo, asegurando la integridad, disponibilidad y confidencialidad de la información[10], involucrando a todos los colaboradores para que adopten buenas prácticas sobre sus procesos cotidianos, enfocados en la norma NTC-ISO/IEC 27001:2013 quien precisa la metodología para la puesta en marcha de una estrategia que defina las acciones necesarias para su cumplimiento[11], dentro de la cuales se encuentra un análisis exhaustivo de la situación actual de la organización para evaluar su madurez, la identificación de los riesgos y su debido tratamiento mediante la ejecución de múltiples proyectos, con lo cual se espera lograr un nivel de riesgo aceptable, optimizando procesos internos y recursos, promoviendo la mejora continua, el cumplimiento de la legislación y garantizando la continuidad del negocio, con lo cual se obtendrán beneficios como: minimizar costos, aumentar la satisfacción del cliente, acceso a nuevos mercados y mejora competitiva que acreditan el número de organizaciones certificadas a nivel mundial de acuerdo con los resultados de la encuesta de 2018 realizada por la Organización internacional de Normalización[12].

[10] ALEMAN NOVOA, Helena, RODRIGUEZ BARRERA Claudia, “Metodologías Para el análisis de riesgos en los sgsi” En línea, Mayo 2014, disponible en: https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1754
[11] ISO, NTC-ISO/IEC 27001:2013, En Linea, 2013, disponible en: https://www.iso.org/home.html
[12] ISO, ISO SURVEY 2018. En Línea. Disponible en https://www.iso.org/the-iso-survey.html

Basados en la norma NTC-ISO/IEC 27001:2013, el sistema de gestión de la información no solo brinda elementos necesarios sobre los correctivos que se deben tomar en cuanto a la infraestructura informática[13], sino también indica que se requiere establecer políticas claras para que todo el personal de la compañía se enfoque en el adecuado uso de los recursos informáticos, de tal forma que toda persona esté en la capacidad de detectar una posible falla de seguridad y así mismo reportarla a su superior para poder aplicar el correctivo necesario en el menor tiempo posible, evitando la perdida de la información o daño material de algún equipo.

[13] MINTIC.“Seguridad y privacidad de la información. Guía, 6” En Línea, marzo 2019, disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G6_Gestion_Documental.pdf

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Establecer una estrategia de seguridad de la información que permita crear un entorno confiable mediante la protección de los activos de información en la empresa QWERTY S.A.

3.2 OBJETIVOS ESPECÍFICOS

- Clasificar los activos de información de la organización de acuerdo con su criticidad.
- Analizar el escenario actual de la compañía evaluando la madurez en el que se encuentra respecto al Sistema de Gestión de Seguridad de la Información.
- Estructurar de forma apropiadas los roles y responsabilidades a tener presente en la implementación del Sistema de Gestión de Seguridad de la Información.
- Establecer los controles necesarios de manera interna para la correcta gestión de la seguridad de la información.

4 MARCO REFERENCIAL

4.1 MARCO CONTEXTUAL

La información es un elemento importante que ha abastecido al hombre de conocimientos desde su inicio, debido al creciente caudal de conocimiento, es un recurso en constante desarrollo, de acuerdo a la necesidad en la sociedad este instrumento ha experimentado una evolución en el transcurso del tiempo asociado a la influencia de múltiples factores. El surgimiento de nuevas tecnologías de información determino el inicio de una nueva era para la administración del conocimiento donde el procesamiento de datos es un componente importante para las compañías, la información es un activo critico el cual contiene datos sensibles que se encuentran expuestos a riesgos constantes, de donde nace la necesidad de gestión y protección que garantice su seguridad de forma apropiada.

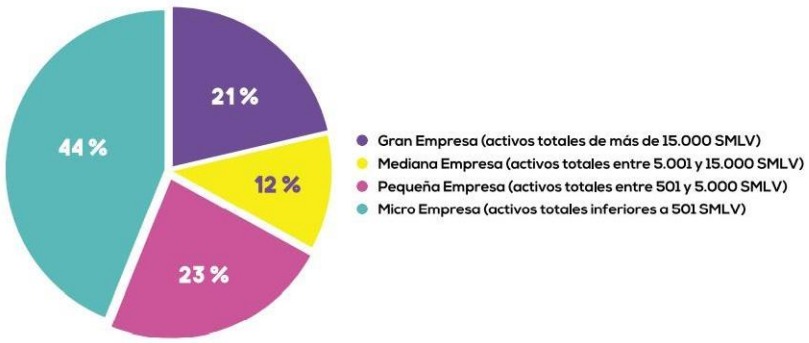
Para mantener a salvo los datos y asegurar en gran medida su protección, surge el concepto denominando “seguridad de la información” quien tiene como propósito definir controles mediante el uso de buenas prácticas, enfocándose en la preservación de su integridad, disponibilidad y confidencialidad[14].

El concepto de información ha estado vinculado de forma directa con la humanidad y al integrarse con las tecnologías actuales las cuales han tenido un crecimiento exponencial, ha expuesto a la información a riesgos que no se tenían contemplados, lo que en consecuencia nos brinda la idea que entre más servicios se generen mediante estos medios tecnológicos, mayor será la superficie de ataque a la que estará expuesta.

[14] ISO, NTC-ISO/IEC 27001:2013, En Linea, 2013, disponible en: https://www.iso.org/home.html

El estudio colaborativo “Impacto de los incidentes de seguridad digital en Colombia” realizado en 2017 por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia - MINTIC, la Organización de los Estados Americanos -OEA y el Banco Interamericano de Desarrollo - BID a sectores privados y públicos, revela que las organizaciones consideran estar preparadas para enfrentarse a incidentes digitales, no obstante la realidad es otra, ya que en términos generales disponen de una asignación de presupuesto bajo, no cuentan con un área dedicada a la seguridad digital, sin mencionar la falta de conciencia de los empleados, por lo que transfieren los incidentes al área de TI, lo que conlleva al incremento en el número de incidentes de seguridad digital.[15]

Figura 1. Tamaño de las empresas privadas en Colombia que hacen parte del estudio



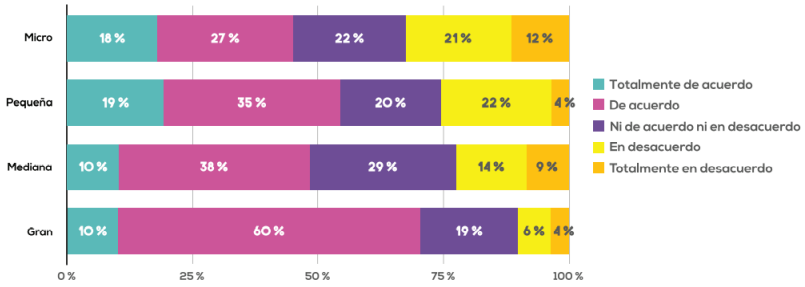
Fuente: https://revistaempresarial.com/wp-content/uploads/2017/10/Estudio-Seguridad-Digital-Colombia.pdf

El informe muestra que las entidades públicas y privadas no tienen implementado una metodología para la evaluación del riesgo, se evidencia una clara necesidad de aumento de recursos asignados a la gestión de la seguridad y que en gran porcentaje las entidades no cuentan con un área específica, a pesar de que Colombia muestra un compromiso frente a la seguridad digital se requiere contar

[15] MINTIC, OEA, BID, Impacto de incidentes de seguridad digital en Colombia” En Linea, 2017, disponible en: https://revistaempresarial.com/wp-content/uploads/2017/10/Estudio-Seguridad-Digital-Colombia.pdf

con una visión más clara sobre los costos asociados a la materialización de un riesgo, teniendo en cuenta estos datos se presenta la siguiente grafica que hace alusión a la pregunta ¿la empresa está preparada para afrontar los incidentes de seguridad?[16]:

Figura 2. Nivel de preparación para hacer frente a un incidente de seguridad.

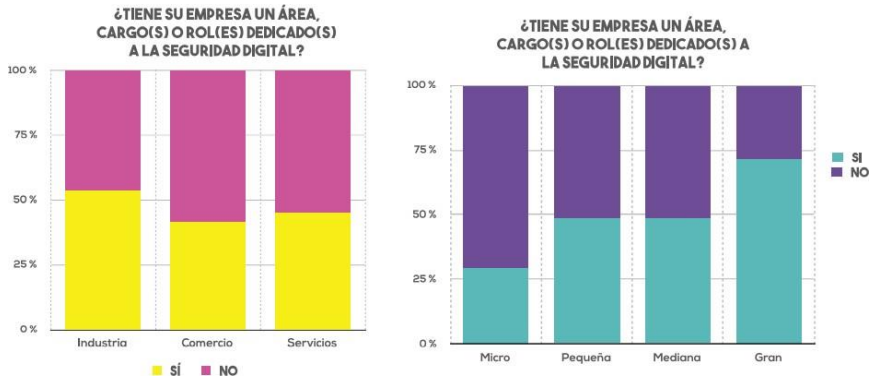


Fuente: https://revistaempresarial.com/wp-content/uploads/2017/10/Estudio-Seguridad-Digital-Colombia.pdf

El comportamiento presentado mediante las diferentes graficas demuestra que las organizaciones entienden el valor de afrontar los incidentes digitales, pero no invierten en lo necesario para detectar, gestionar y dar respuesta a estos eventos.

[16] MINTIC, OEA, BID, Impacto de incidentes de seguridad digital en Colombia" En Linea, 2017, disponible en: https://revistaempresarial.com/wp-content/uploads/2017/10/Estudio-Seguridad-Digital-Colombia.pdf

Figura 3. Cargo o rol dedicado en la organización (Tamaño y sector económico de las empresas



Fuente: https://revistaempresarial.com/wp-content/uploads/2017/10/Estudio-Seguridad-Digital-Colombia.pdf

La gestión del riesgo para cualquier entidad es un factor esencial para la prevención de incidencias que generen impactos económicos para la organización, teniendo en cuenta el informe es posible evaluar los efectos mediante la estimación del costo derivado de eventos de seguridad como en el caso de daño a los activos de la compañía, sanciones legales, afectación de la reputación, perdida de propiedad intelectual en incluso eventos presentados que afectan la continuidad del negocio, en consecuencia el estudio muestra que el costo relativo asociado a la materialización de un incidente de seguridad en las empresas colombianas disminuye en proporción al aumento de su tamaño ya que cuenta con variables como el uso de políticas, implementación de estándares, medidas de seguridad técnicas y su inversión a la seguridad digital es mayor.

La empresa QWERTY S.A. tiene como actividad principal el desarrollo de las comunidades en Colombia basándose en la tecnología de la información que se encuentra en la actualidad.

El departamento de informática de la compañía se encuentra estructurado de tal forma que permite dar el soporte a cada una de las dependencias y actividades más relevantes, como la gestión, creación de usuarios y contraseñas, el apoyo y

administración del correo usado por cada uno de los trabajadores de la compañía, brindar soporte en procesos críticos dentro del área de nómina y facturación, en cuanto se refiere a los sistemas de información.

Como parte fundamental dentro de la norma NTC-ISO/IEC 27001:2013, están definidas las especificaciones referentes a la creación, funcionamiento, mantenimiento y constante mejora del SGSI definiendo las pautas para que toda la documentación de la compañía sea parametrizada bajo una política adecuada y se le dé un manejo correcto dentro de la organización.

Todos los procedimientos y políticas que se establezcan dentro de la organización deben asegurar la protección tanto de la información como de los equipos informáticos, ya que deben estar basadas en la normatividad internacional.

Implementar un SGSI es fundamental para gestionar la información en un entorno de trabajo que requiere el uso constante de Internet, un importante número de empleados utilizan Internet para el desarrollo de sus actividades diarias, lo que expone a la información a todo tipo de peligros que no necesariamente son evidentes o fáciles de identificar, generar una estrategia de detección, análisis y gestión de riesgos,[17] crea una visión clara de los retos a los que se enfrenta la compañía e incentiva el uso de buenas prácticas basándose en la experiencia de modelos y estándares internacionales, que contribuyen a la construcción de directrices y políticas con el propósito de salvaguardar los datos, determinando los eslabones más débiles de la cadena generando controles para fortalecer los procesos de seguridad de la información. La aplicación de nuevas metodologías para el manejo de la información plantea retos a la operación que requerirán esfuerzo y tiempo, ya que la implementación del proceso requiere un cambio importante en la mentalidad y cultura de la organización, una contribución

[17] ISOTOOLS EXCELLENCE “ISO 27001: El método MAGERIT” En Línea, marzo 2019, disponible en: https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

importante de liderazgo por parte de la gerencia, sin mencionar el costo que implica la puesta en marcha de un entorno seguro.[18]

A continuación, se relaciona los aspectos a considerar para establecer una estrategia de seguridad de la información en una organización

4.1.1 SISTEMAS DE INFORMACION: Es el conjunto de recursos tangibles que tiene una compañía para brindar una correcta obtención y comunicación de la información. El sistema de información debe resultar de forma acertada y efectiva, dando a conocer que esta es veraz si se realiza el proceso con los menores recursos posibles. Estos sistemas se deben adecuar de la mejor manera a las compañías según su estructura organizacional. Basándonos en el levantamiento de la información de la compañía para la implementación de este.
Los elementos con los cuales se debe contar para poder realizar dicha implementación son servidores con una alta capacidad de funcionamiento debido a que debe permitir ejecutar varias tareas al mismo tiempo. Asegurando que cada uno de los empleados de la compañía puedan acceder a sus archivos como lo son las bases de datos, las páginas web y el manejo adecuado de la información.[19]

Actualmente todas las aplicaciones web están dirigidas a grandes bases de datos en donde la compañía puede realizar diferentes consultas según el área o tarea a gestionar de forma eficiente, esto se basa en que la productividad de la empresa está el manejo de esta.

4.1.3. CONTROL DE ACCESO: Este sistema es el encargado de controlar todas aquellas herramientas tecnológicas de áreas específicas. Este también permite la verificación de la identidad de las personas con permisos para los ingresos a un

[18] ANDRADE RODRIGUEZ, Yovany ” ENTENDIENDO EL SGSI” En Linea, disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2748/00002987.pdf?sequence=1
[19] EMPRENDEPYME.” ¿Qué es un sistema de información?” En Línea, marzo 2019, disponible en: https://www.emprendepyme.net/que-es-un-sistema-de-informacion.html

área específica o una cierta información. [20]Este control de acceso cuenta con dos tipos, uno de ellos es el de acceso en donde podemos ver la parte biométrica para el control de entrada y salida en el cumplimiento de horarios y de ingreso a las áreas adecuadas dentro de la compañía, el otro tipo de acceso es el de red donde el software registra toda actividad realizada en el equipo de cómputo de la compañía.

Dentro de la clasificación de la seguridad electrónica, encontramos el acceso autónomo que es donde se permite el ingreso a diferentes áreas de la compañía, sin contar con un equipo de cómputo físico, debido a que es un sistema independiente. Otra clasificación de este es el control de acceso en la red el cual se encuentra integrado por un pc, donde se encuentra un software que permitirá la verificación y la trazabilidad de los diferentes registros de las actividades según el área.[21]

La biometría se encuentra ligada al reconocimiento genético de cada ser humano, con el fin de prevenir la suplantación de cada persona, Realizando la captación de las huellas dactilares, almacenándolas en una base de datos para encontrar la similitud de lo guardado con el momento del registro.

El modelo en que se basa la norma ISO 270010, nos indica que debemos tener en cuenta todos los escenarios posibles para el cuidado necesario de la información para la prevención de ataques informáticos.

4.1.4. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN: Es la base de la norma ISO 27001, para llevar a cabo todo proceso documentado y sistematizado de la compañía.[22]

[20] TECNOSEGURO.”¿Qué es un Sistema de Control de Acceso?” En Línea, marzo 2019, disponible en: https://www.tecnoseguro.com/faqs/control-de-acceso/que-es-un-control-de-acceso
[21] Ibíd.
[22] ICONTEC.” Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos: ICONTEC 2013 (NTC-ISO 27001)

La confidencialidad, la integridad y la disponibilidad son los aspectos más importantes que debemos tener en cuenta para el levantamiento de la información dentro de la compañía, y así lograr minimizar todo riesgo a lo que se expone dicha información.[23]

El modelo de la norma nos indica que se deben crear los controles de forma precisa para el manejo y cuidado de la información, dado que la organización no está excepta de un ataque cibernético. Por lo tanto, se deben crear medidas de seguridad para la preservación de esta.

4.1.5. NORMA ISO 27001:2013: Esta norma se basa en la correcta administración de la información en todas aquellas áreas que deban realizar un manejo diario.[24]

La organización dentro del área tecnológica lograra de forma adecuada el almacenamiento y trato de la información según la importancia dentro de la compañía, objetivo por el cual la norma deja establecer parámetros para asegurar la transparencia de la ejecución de los procesos.

Los dominios de la norma ISO 27001 permitirán a la compañía realizar los controles y las gestiones necesarias para la seguridad de la información, razón por la cual se han venido enfocando en el aprendizaje de las respuestas y los correctivos que se deben tomar en el momento de la materialización de un incidente cibernético.

4.1.6. ANÁLISIS Y GESTIÓN DE RIESGOS: Este proceso nos permitirá establecer el impacto que tendrá un riesgo dentro de la compañía. Mediante este análisis se podrá identificar cuáles son los activos de la información a proteger según cada uno de los posibles riesgos que nos dé como resultado dicho análisis.

[23] ISO, NTC-ISO/IEC 27001:2013, En Linea, 2013, disponible en: https://www.iso.org/home.html
[24] NORMAISO27001.ES, ISO 27001.En Línea. Disponible en https://normaiso27001.es/

Este análisis es la gestión que nos permitirá realizar de forma correcta los controles sobre las vulnerabilidades y amenazas, según el grado de impacto que tendrán en el momento de hacerse realidad.

La metodología que se usara para el análisis de los riesgos se llama **MAGERIT** ya que es la herramienta más certera para permitirnos ver la probabilidad del riesgo o amenaza dentro de la organización, para ver el adecuado cumplimiento dentro de la norma.[25]

4.2 MARCO CONCEPTUAL

Amenaza: Aquello que de una u otra manera puede afectar la seguridad de la información del sistema informático. Las amenazas son la posibilidad de la explotación de las vulnerabilidades.

Confidencialidad: Es un servicio que ofrece la capacidad de tener el control de la información y restringir o permitir los accesos de las personas o entes autorizados.[26]

Disponibilidad: El manejo de los datos del sistema informático de una compañía, siempre debe garantizar la información cada vez que sea requerida, lo cual da a entender que no debe existir inconveniente alguno para quien la deba usar y tener a su alcance.[27]

Integridad: Toda información que se administre o maneje en el SI debe ser conservada de tal manera que no sufra ninguna alteración sin permiso previo. El adulterio de la integridad de la información se identifica cuando existe alguna

[25] ISOTOOLS EXCELLENCE “ISO 27001: El método MAGERIT” En Línea, marzo 2019, disponible en: https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/
[26] ISO, NTC-ISO/IEC 27001:2013, En Linea, 2013, disponible en: https://www.iso.org/home.html
[27] Ibíd.

modificación de esta bien sea por una persona o un dispositivo electrónico; sufriendo alteración en el contenido de esta, sin autorización alguna.[28]

Riesgo: Cualquier impedimento, amenaza o problema que afecte el SI impidiendo que los usuarios manejen la información para el cumplimiento de los objetivos.

Vulnerabilidades: Están identificadas como todas las debilidades que existen en el SI y que comprometen la seguridad de los datos. Este es un riesgo interno, que permite que los activos y el sistema en general sean afectados.

[28] ISO, NTC-ISO/IEC 27001:2013, En Linea, 2013, disponible en: https://www.iso.org/home.html

4.3 MARCO LEGAL Y NORMATIVO

Este trabajo está basado en las diferentes normas que ha establecido el estado, en cuanto refiere a la seguridad informática, ya que estas son las que reglamentan la protección de la información y el uso de los datos personales de cada una de las compañías colombianas.

Cuando se habla de un sistema de gestión en la seguridad informática, se debe tener en cuenta el diseño, para que se lleve a cabo el cumplimiento de las leyes y normas que se deban aplicar para el desarrollo de la implementación, logrando establecer la protección tanto de la compañía como de sus activos, sus colaboradores y en general las personas de cualquier delito, proceso o infracción que permita poner en riesgo los activos o bienes que le pertenezcan.

En el diseño del SGSI se debe tener en cuenta que el hardware, software, los sistemas, las metodologías, las políticas, los procedimientos, entre otros son necesarios e indispensables para la implementación, teniendo presente que estos son sensibles a generar algún incumplimiento a la norma y así permitir la aparición de consecuencias negativas bien sea a la compañía o a alguna persona especifica. Motivo por el cual se debe tener claridad en el conocimiento de las leyes, normas y decretos que buscan la protección sobre el bien personal y colectivo.

LEYES DE CIBERSEGURIDAD: Dentro del diseño del SGSI, se debe tener presente el software, el hardware, los procesos, los procedimientos, las políticas y todo aquello que pueda ser para nosotros irrelevante, pero que en algún momento nos lleve a generar un incumplimiento a la norma, y más grave a un a la afectación a un individuo u organización, es por tal motivo en el que conocer algo de la normatividad es importante para la correcta implementación.

- Ley 527 de 1999: Esta reglamenta y controla todo acceso a las firmas digitales, ventas o mensajes electrónicos, que contengan datos personales. [29]
- Decreto 1360 de 1989: Este decreto reglamenta el uso del derecho de autor, estableciendo a el software como dominio de cada compañía.
- Ley 1273 de 2009: Esta surge cuando se hace modificación del código penal, en donde se preserva el derecho de la protección de la información y los datos, dentro de cada organización en el uso de la tecnología de la comunicación.[30]
- Ley estatutaria 1581 de 2012: Regula la vigencia sobre la autorización de la difusión y actualización de los datos personales almacenados en las bases de datos de cada una de las organizaciones, con las que ha manejado algún tipo de producto o relación comercial.

CONPES 3856

Debido al hallazgo de considerables debilidades en la creación de proyectos y en la búsqueda de corregir las deficiencias en la inversión pública mejorando su calidad, se ha creado una estrategia con el propósito de estandarizar la estructura de los proyectos de Colombia, la estrategia permite construir proyectos de una forma más eficiente reduciendo tiempo y costos mediante la normalización para la prestación de servicios, estableciendo modelos creados en conjunto por los ministerios y dependencias bajo un estándar sectorial, donde se identifican oportunidades de mejora que optimicen el tiempo y los recursos de los proyectos, el resultado de este ejercicio crea estándares de calidad mínimos que pueden ser replicados y usados

[29] BUITRAGO BOTERO, Diego “Aspectos Jurídicos de Internet y el Comercio Electrónico” En Línea, marzo 2019, disponible en: http://www.informatica-juridica.com/trabajos/aspectos-juridicos-de-internet-y-el-comercio-electronico/
[30] QUINTERO AGUDELO, Yolanda “La seguridad y la ciberdefensa en Colombia” En Linea, disponible en: http://polux.unipiloto.edu.co:8080/00001596.pdf

como base para la implementación de futuros planes.[31] El uso de estrategias de estandarización contribuye a mejorar la ejecución de proyectos, basados no solo en las experiencias del país, muestra el éxito del uso de los mismos en prototipos internacionales como Reino Unido, Australia, Estados Unidos o Canadá[32], al implementar estos lineamientos se reducen los riesgos que se encuentran asociados al desarrollo de las actividades de un proyecto, mejorando de forma sustancial los resultados esperados y generando procesos de mejora para futuros planteamientos.

Estándares y Metodologías

Debido al creciente desarrollo y uso de tecnologías, uno de los propósitos principales de las organizaciones es asegurar que su información sensible sea gestionada de forma adecuada y se encuentre protegida de factores que puedan materializar los riesgos a los que se encuentra expuesta, para lo cual se ha evidenciado que se requieren una serie de procesos que garanticen el flujo apropiado basado en buenas prácticas que minimicen los constantes fallos asociados al uso inadecuado de este recurso.

La gestión de las tecnologías de la información debe contar con elementos que contribuyan a la gestión adecuada de la información para lo cual se hace necesario el uso de metodologías y estándares que permitan demostrar con resultados evidentes la protección de los datos dentro de los cuales se destacan los siguientes:

MAGERIT: Metodología utilizada para el análisis y gestión de los riesgos derivados del uso de las tecnologías de información que define una serie de controles

[31] CONPES, “ESTRATEGIA DE ESTANDARIZACIÓN DE PROYECTOS 2016-2018”, abril 2016, En línea, disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3856.pdf
[32] Ibíd, p. 10.

asociado al impacto que puede tener un riesgo frente a la materialización de una amenaza.

Magerit, es una estrategia de trabajo de uso libre, cuenta con un proceso sistematizado, con un alcance completo sobre la identificación, análisis y gestión del riesgo, cuenta con documentación completa, contemplando aspectos prácticos para su aplicación, además de contar con análisis cualitativos y cuantitativos, lo que la convierte en una herramienta muy útil dentro del proceso.[33]

OCTAVE: Es un marco que permite la identificación y gestión de riesgos de seguridad me diente la definición de un método que realiza una valoración integral, usando esta estructura es posible determinar los activos críticos de la organización que se encuentran alineados con la misión de la compañía, a partir de esta información es posible diseñar una estrategia que permita reducir el riesgo asociado a las amenazas a las que se expone la información.[34]

NIST SP 800 – 30: Esta publicación tiene como objetivo proporcionar una guía para la evaluación del riego utilizando una jerarquía segmentada en tres niveles, orienta a las organizaciones en la identificación del riesgo permitiendo que las entidades puedan evidenciar si cuenta con un nivel aceptable o en caso contrario definir la estrategia y planes de acción que se deben implementar para generar un nivel de tolerancia del riesgo.[35]

---

[33] ALEMAN NOVOA, Helena, RODRIGUEZ BARRERA Claudia, “Metodologías Para el análisis de riesgos en los sgsi” En línea, Mayo 2014, disponible en: https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1754

[34] 1. Christopher J. AlbertsSandra G. BehrensRichard D. PethiaWilliam R. Wilson, “Operationally Critical Threat,Asset, and VulnerabilityEvaluation SM(OCTAVESM) Framework,Version 1.0” En Linea, Junio 1999, disponible en:https://kilthub.cmu.edu/articles/Operationally_Critical_Threat_Asset_and_Vulnerability_Evaluation_OCTAVE_Framework_Version_1_0/6575906/1

[35] 1. NIST, “Guide for Conducting Risk Assesment”, En Línea, septiembre 2012, disponible en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

ISO/IEC 27001: Estándar internacional de seguridad de la información mediante el cual se busca garantizar la confidencialidad, disponibilidad e integridad de la información mediante la evaluación del riesgo y la implementación de controles, mejorando la competitividad e imagen de las organizaciones que la implementan.[36]

La ISO, International Organization for Standardization, 'Organización Internacional de Estandarización'. Es la organización encargada del sistema de la normalización internacional para varios productos de todas las áreas.

Entre todas aquellas normas que manejan encontramos la norma ISO/IEC 27001:2013, que establece los parámetros de la implementación, la mejora y el mantener de SGSI. El cual fue publicado en octubre del 2005, y que hoy en día es el único estándar reconocido internacionalmente para la gestión de la seguridad de la información. Esta norma se basa en anteriores estándares de seguridad de la información como lo son:

- 1901 – Norma “BS”: La British Standards Institution, esta se usaba en las normas que tenían el prefijo “BS” de carácter internacional, donde se crean las normas ISO: 9001, ISO 14001 Y OSHSAS 18001.

- 1995- BS 7799-1:1995: Ayuda a las empresas británicas a realizar la administración de la seguridad de la información.

- 1998- bs 7799-2:1999: Establecía las condiciones para la implementación de los sistemas de gestión de seguridad de la información de manera certificable.

[36] ISO, NTC-ISO/IEC 27001:2013, En Linea, 2013, disponible en: https://www.iso.org/home.html

- 1999- BS 7799-1:1999: Se dedica revisar toda la norma permitiendo la corrección de los errores.

- 2000 – ISO 17799:2000: La ISO, adquirido la norma británica bs 7799-1 dando nombre a la norma ISO 17799, sin presentar cambios.

- 2002 – BS 7799-2:2002: Se realiza la publicación de la versión que permitía la aprobación de acreditación de las empresas por parte de Reino Unido y diferentes Países.

- 2005 – ISO 27001:2005 e ISO17799:2005: Surge el estándar ISO 27001 como única norma internacional con certificación y se verifica la ISO 17799 permitiendo la aparición de la ISO 27001:2005.

- 2007 – ISO 17799: Se empieza a llamar a ISO 27002:2005

- 2007 – ISO 27001:2007: Aparece nueva versión.

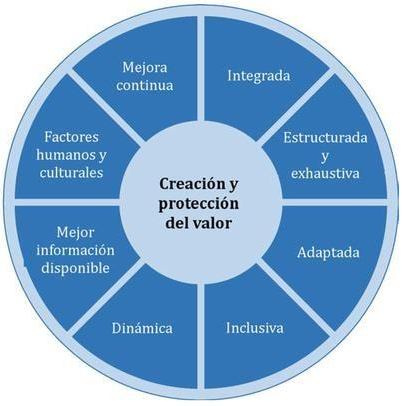
- 2009 – Se publican las modificaciones recibiendo el nombre ISO 27001:2007/1M:2009

2013: Este año se publica una versión nueva de la ISO 27001, que trae varios cambios relacionados con la estructuración, la evaluación y el manejo de los riesgos.

ISO/IEC 27002: Es una Guía que contiene las mejores prácticas para la implementación del SGSI, tiene como objetivo establecer los principios y normas para la implementación, mantenimiento y mejora del SGSI, donde se incluye además la implementación y gestión de controles asociados a los riesgos evidenciados en la organización, políticas de seguridad en la información, la identificación y clasificación de activos, protección contra amenazas ambientales y físicas, responsabilidades sobre la administración de la operación, planes de continuidad, garantizando el cumplimiento de regulaciones y obligaciones contractuales.

ISO/IEC 31000: Guía que contiene los lineamientos necesarios para la gestión del riesgo los cuales se pueden adaptar a cualquier tipo de organización, este marco se fundamenta en principios para gestión del riesgo de forma eficaz. La gestión del Riesgo es un proceso integral que implica el uso de buenas prácticas, políticas y procedimientos, esta se puede aplicar en deferentes niveles de la organización tanto operacional como estratégico con el propósito de que la entidad tenga comprensión y conciencia del riesgo.[37]

Figura 4. Principios ISO/IEC 31000



Fuente: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

[37] ISO, NTC-ISO/IEC 31000:2018, En Linea, 2018, disponible en: https://www.iso.org/home.html

5 DISEÑO METODOLOGICO

Dentro del proceso se realizó una comparativa entre los estándares de análisis y gestión del riesgo como lo son OCTAVE, NIST SP 800 – 30 MAGERIT e ISO/IEC 31000 con el propósito de identificar cual es más acorde a las necesidades actuales de QWERTY S.A, dentro de los cuales se evidencia que MAGERIT cuenta con los lineamientos necesarios para el cumplimiento de los objetivos propuestos en la entidad de acuerdo con los siguiente:

- Determinar los activos de la organización.
- Determinar las Amenazas
- Determinar las salvaguardas
- Identificar el impacto residual
- Identificar el riesgo residual
- Establecer el proceso de gestión del riesgo.

5.1.1 ETAPAS DEL PROYECTO.

- **Identificación de Activos.**

  En conjunto con la Organización QWERTY S.A. se debe realizar el proceso de identificación y clasificación de los activos que hacen parte del estudio dentro del proyecto de grado.

- **Identificación de vulnerabilidades y amenazas.**

  Es necesario realizar la identificación de las vulnerabilidades que puedan afectar los activos de información de la Organización, posteriormente es necesario determinar las amenazas que pueden explotar las debilidades identificadas, estas serán consignadas en una Matriz de Riesgos siguiendo la metodología MAGERIT[38].

[38] ISOTOOLS EXCELLENCE “ISO 27001: El método MAGERIT” En Línea, marzo 2019, disponible en: https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

- **Valoración de Activos.**

  Se debe priorizar los activos de acuerdo con su criticidad, definir una valoración de los activos de acuerdo con el impacto que pueda generar sobre los procesos de QWERTY S.A. al presentarse la materialización de un riesgo.

- **Análisis del escenario actual de la Organización.**

  Se analizará el estado actual de la organización en términos de seguridad de la información con el objetivo de entender su contexto y evaluar opciones de mejora, en esta etapa se utilizará el documento de declaración de aplicabilidad SOA NTC-ISO/IEC 27001:2013[39].

- **Estructura Organizacional roles y responsabilidades.**

  De acuerdo con los análisis realizados en las etapas anteriores se establecerá los roles necesarios para llevar a cabo las actividades y gestionar los procesos del riesgo.

- **Creación de controles y plan de tratamiento.**

  La identificación de las vulnerabilidades se utilizará para crear controles de seguridad que mitiguen los riesgos encontrados y generar planes de acción para llegar a un nivel de riesgo aceptable los cuales se consignará en la matriz de riesgo.

Garantizar que la información tenga su integridad disponibilidad y confidencialidad mediante el uso adecuado de políticas y estándares de seguridad definidos en la norma ISO 27001 definidos a partir de una evaluación de los riesgos que se encuentran actualmente en la compañía y de aquellos que posiblemente pueden aparecer, debido a que los ciberdelincuentes siempre tienen como objetivo adueñarse de la información, dentro de esta se encuentra incluido el manejo de las herramientas y los métodos para defenderse de dichos ataques bien sea de forma externa o interna actualmente en la empresa.

[39] ISO, NTC-ISO/IEC 27001:2013, En Linea, 2013, disponible en: https://www.iso.org/home.html

En esta siguiente etapa basándonos en los resultados de la evaluación de los riesgos, se establecerán controles necesarios para la mitigación de los hallazgos y se iniciará la presentación de un avance sobre el diseño del SGSI basado en las necesidades, permitiéndonos determinar la probabilidad y la cantidad de veces en que se puede presentar dicho evento, para así proceder a realizar una clasificación del riesgo según su impacto (leve, moderado y alto) permitiéndonos la identificación de procesos a realizar.

5.1.2 TIPO DE ESTUDIO

Para el proyecto aplicado se realizan evaluaciones de manera cualitativa y cuantitativa, ya que se realizará la medición de los riesgos, vulnerabilidades y amenazas basado en la escala de medición de la metodología MAGERIT para lo cual se utilizará la matriz de riesgos como una herramienta que permite la identificación de los riesgos y su estimación, la cual se relaciona a continuación:

Figura 5. Matriz de Riesgo

		Consecuencias				
Probabilidad		Insignificante 1	Menor 2	Moderada 3	Mayor 4	Catastrófica 5
Raro	1	Bajo	Bajo	Moderado	Alto	Alto
Improbable	2	Bajo	Bajo	Moderado	Alto	Extremo
Posible	3	Bajo	Moderado	Alto	Extremo	Extremo
Probable	4	Moderado	Alto	Alto	Extremo	Extremo
Casi seguro	5	Alto	Alto	Extremo	Extremo	Extremo

Extremo: Los riesgos extremos deben ponerse en conocimiento de los Directores y ser objeto de seguimiento permanente.
Alto: Los riesgos altos requieren la atención del Presidente / Director General / Director Ejecutivo.
Moderado: Los riesgos moderados deben ser objeto de seguimiento adecuado por parte de los niveles medios de Dirección.
Bajo: Los riesgos bajos deben ser objeto de seguimiento por parte de los supervisores.

Fuente: Riesgo y administración del riesgo. ¿Qué es una Matriz de Riesgo?. en línea, Articulo Web: https://swescom.wordpress.com/riesgo-y-administraciondel-riesgo/

5.1.3 TIPOS DE INFORMACIÓN

La información será de fuente primaria, es fiable y entregada por los responsables de cada proceso, esta información es un recurso esencial debido a que será utilizado como objeto para el análisis de los riesgos y las vulnerabilidades de los activos dentro de la empresa QWERTY

5.1.4 TÉCNICAS DE RECOLECCIÓN Y ANÁLISIS DE LA INFORMACIÓN

Para la implementación de SGSI, se realizó el uso de la fuente bibliográfica, manuales, ponencias de expertos, textos, y demás elementos documentales que permitan la recopilación de la información.

También se utilizarán varios instrumentos de recolección de la información para poder completar los análisis de la evaluación realizadas, como lo son:

- **Check-list:** Se implementa dentro del proyecto como técnica de verificación en las no conformidades y las conformidades dentro de la empresa QWERTY S.A
- **Observación Directa:** Se hará uso de este observando las características, condiciones y conductas dentro de la compañía. Esta técnica se implementará en los sistemas informáticos existentes, y con las personas directamente implicadas en el manejo de la información.

5.1.5 POBLACIÓN ESTUDIADA (UNIVERSO – MUESTRA)

La población que servirá dentro del objetivo dentro del proyecto aplicado será identificada por medio de los equipos de cómputo, procedimientos, procesos y personas, lo que nos permitirá llevar a cabo las entrevistas y las auditorías a el personal encargado del área informática, directivos, procedimientos y procesos

ejecutados e implementados y a su vez a las herramientas tanto externas como internas en los equipos involucrados.

Dentro de este proyecto aplicado la población objeto es el personal de la compañía QWERTY S.A.S, la cual se llevará a cabo sobre el 100 % del personal vinculado en el área de sistemas.

5.1.6 VALORACIÓN DEL RIESGO

Posterior al levantamiento de información se procederá entonces con una valoración cualitativa y cuantitativa sobre los activos de la compañía y se planteará una clasificación teniendo en cuenta su criticidad, los riesgos asociados y la probabilidad de materialización de dichos riesgos.

5.1.7 DIMENSIONES DE SEGURIDAD.

Se utiliza las siguientes dimensiones para evaluar lo valioso que es un activo, para este caso se utilizaron las siguientes:

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de la Información
- A] Autenticidad
- [T] trazabilidad

5.1.8 CRITERIOS DE VALORACION

Cuadro 1. Criterios de Valoración

Nivel		Criterio
10 (Extremo)	E	Daño extremadamente grave
9 (Muy alto)	MA	Daño muy grave
6 - 8 (Alto)	A	Daño grave
3 - 5 (Medio)	M	Daño importante
1 - 2 (Bajo)	B	Daño Menor
0 (Despreciable)	D	Irrelevante a efectos prácticos

Fuente: MAGERIT versión 3 (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. en línea, Articulo Web: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Cuadro 2. Criterios de Valoración.

Valor			Criterio
4	Muy frecuente	MF	A diario
3	Frecuente	F	Mensualmente
2	Normal	N	Una vez al año
1	Poco frecuente	PF	Cada varios años

Fuente: MAGERIT versión 3 (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. en línea, disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Cuadro 3. Criterios de Valoración.

Valor		Criterio
100%	MA	Degradación MUY ALTA del activo
80%	A	Degradación ALTA considerable del activo
50%	M	Degradación MEDIANA del activo
10%	B	Degradación BAJA del activo
1%	MB	Degradación MUY BAJA del activo

Fuente: MAGERIT versión 3 (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. en línea, Articulo Web: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

6 RESULTADOS DE LOS OBJETIVOS

Mediante las medidas planteadas se implementó una estrategia de seguridad de la información generando un entorno confiable mediante la protección de los activos de información en la empresa QWERTY, a través de la identificación, análisis y gestión de los riesgos encontrados.

6.1 DESARROLLO DE OBJETIVO 1

- Clasificar los activos de información de la organización de acuerdo con su criticidad.

Para el desarrollo del proyecto se establece canales de comunicación con las diferentes áreas de la organización que permitieron contar con la información necesaria para la ejecución de las diferentes actividades requeridas durante todas las etapas del proyecto.

6.1.1 IDENTIFICACÓN DE LOS ACTIVOS

En la fase inicial se identifican los activos tecnológicos de la compañía para su posterior clasificación e identificación de riesgos, los cuales son entregados por el área de infraestructura bajo la siguiente estructura:

Tabla 1 Inventario Activos.

Activo	Descripción	Ubicación	Cant.
Servidor de Impresión: Servidor marca dell en torre PowerEdge T440 Ver ficha técnica	Equipo de cómputo que conecta dos impresoras: Destinadas a: Una (1) Impresora HP LaserJet Enterprise serie 600, activo que brinda el servicio para la dependencia de nómina y facturación. Permite la concurrencia de hasta 25 usuarios y el volumen mensual de impresión es de 200 a 25000 páginas Una (1) Impresora SMART MultiXpress M4370LX, impresora que ofrece el servicio de escáner e impresión con un ciclo de trabajo de hasta 300000 páginas mensuales con capacidades de red alámbrica e inalámbrica. Impresora destinada para el servicio de directivos y administrativos y docentes	Oficina de nómina y facturación. Dependencia directiva y administrativa	1 1
Servidor de archivos FTP:	Equipo de cómputo que tiene como función el almacenamiento y la administración de los archivos que se están generando en el interior de la	Oficina antigua de sistemas	1

Servidor marca dell en torre PowerEdge T130 Ver ficha técnica	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 Servicio contratado con la empresa Godaddy.com		
Página web Plan Máximo Ver ficha del proveedor	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. El hospedaje web la infraestructura del servidor es Apache, PHP, MySQL.	Empresa Godaddy	1
Servidor de nómina y facturación Servidor marca dell en torre PowerEdge T440 Características de servidor Apache 2.4.25 PHP 5.6.30 - 7.1.1 MySQL 5.7.17 phpMyAdmin 4.6.6	Plataforma de desarrollo propio. Tiene como función el almacenamiento y la administración de la nómina y facturación de la empresa QWERTY S.A.		2

Servidor DHCP Servidor marca dell en torre PowerEdge T440	Servidor que asigna y administra de forma dinámica el direccionamiento dentro de la organización		1
Equipos de cómputo para gestión de Sistema de contable Plan Cloud Plus <u>Más Información del proveedor</u>	Equipos de cómputo donde se gestiona información online relacionada con el desarrollo del objeto social Presupuesto • Proveedores • Órdenes de compra • Inventarios	Dependencia de desarrollo tecnológico	3
Cortafuegos Cisco ASA 5505 <u>Ver ficha técnica</u>	Sistema de protección	Sistema de seguridad que está protegiendo a la red de datos, de intrusiones que se puedan presentar en la red	1
Equipos de Computo Sistemas operativos win 10 Pro	Equipos destinados para el desarrollo del objeto social	Dependencia de infraestructura	3
Equipos de Computo Sistemas operativos win 10 Pro	Equipos destinados para el desarrollo del objeto social	Dependencia de control y seguimiento	10
Equipos de Computo	Equipos destinados para el desarrollo del objeto social	Dependencia de prueba de software	5
Puntos de acceso alámbricos (hub)	Dispositivos de red encargados de la interconexión de la red de datos	Red de datos del centro	4

Switches cisco catalyst 2960	Dispositivos de red encargados de la interconexión de la red de datos	Red de datos del Centro	6
Técnicos de mantenimiento	Personal técnico encargado de realizar el mantenimiento preventivo a los equipos de computo	Departamento de Sistemas	2
Teléfonos IP	Sistema de comunicación a través de teléfonos Voz IP, que comunica las oficinas y departamentos del centro	Dependencias del centro	6
Puntos de acceso	Puntos de acceso al servicio de internet en el campus universitario	Departamento de sistemas	2

Fuente: Escenario2_EnfoqueDirectivoAdministrativo.pdf

Posterior a la entrega del inventario de activos informáticos mediante el formato definido en el punto anterior, se realizó un desglose y tipificación de los activos, con lo cual se procede a la evaluación de los activos teniendo en cuenta una escala de valores estándar definidos por la metodología MAGERIT, el propósito de esta etapa fue identificar los activos y entender su importancia dentro de la ejecución de los procesos de la QWERTY S.A, evaluando su exposición a vulnerabilidades y amenazas.

6.1.2 CARACTERIZACION DE LOS ACTIVOS DE LA ORGANIZACIÓN

Se elaboro una matriz inicial de acuerdo con la metodología MAGERIT contenido en el documento “ANEXO 1” en la cual se procede con:

- Identificación de activos.
- Identificación de Vulnerabilidades.
- Identificación de amenazas.

En el documento matriz inicial se identifican los elementos que componen los sistemas, se evidencia la segmentación de acuerdo con el tipo de activo además se da una breve descripción que permite su fácil identificación, evaluando la información que se gestiona en el activo y los servicios que presta el activo, se procedió entonces con la siguiente tipificación conforme a la arquitectura del sistema[40]:

- S- SERVICIOS
  - S int SOPORTE TECNICO
  - S ftp TRANSFERENCIA DE ARCHIVOS
  - S www PAGINA WEB
  - S file ALMACENAMIENTO DE ARCHIVOS
- D- DATOS / INFORMACION
  - D files NOMINA DE TRABAJADORES
  - D files RECIBOS DE PAGO
  - D files HOJAS DE VIDA
  - D files SEGUIMIENTO TALENTO HUMANO
  - D files CERTIFICADOS - LABORALES - MODELO DE NEGOCIO
- SW - APLICACIONES SOFTWARE
  - SW app Apache 2.4.25
  - SW app PHP 5.6.30 - 7.1.1
  - SW bd MySQL 5.7.17
  - SW app phpMyAdmin 4.6.6
  - SW av Antivirus
- HW HARDWARE
  - HW host Servidor de Impresión
  - HW host Servidor de archivos FTP
  - HW host Servidor PBX
  - HW host Servidor de Nómina y Facturación
  - HW host Servidor DHCP
  - HW pc Equipos de Computo
  - HW pc Equipos de Computo
  - HW pc Equipos de Computo
  - HW pc Equipos de Computo
  - HW host Puntos de acceso alámbricos (hub)

40 MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS, MAGERIT versión 3 (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, En Linea, octubre 2012, disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

    - HW ipphone Teléfonos IP
    - HW host Puntos de acceso
    - HW print Impresora HP LaserJet Enterprise serie 600
    - HW print Impresora SMART MultiXpress M4370LX
- COM – COMUNICACIONES
    - HW firewall Cortafuegos Cisco ASA 5505
    - HW switch Switches cisco catalyst 2960
- L – INSTALACIONES
    - L site Dependencia Nómina y Facturación
    - L site Sala de Sistemas
    - L site Campus Universitario
- P – PERSONAL
    - P adm Funcionarios
    - P prov Proveedores

6.1.3 VALORACION DE LOS ACTIVOS.

Con el propósito de evaluar las consecuencias que puede generar una amenaza se realizó una valoración de los activos teniendo en cuenta las propiedades que lo hacen importante, en esta etapa se asigna un valor a las dimensiones del activo, es decir a los cinco aspectos definidos dentro de la metodología MAGERIT[41].

Teniendo en cuenta los resultados generados en el análisis de la valoración se evidencia que los servidores y servicios son activos que la indisponibilidad es un factor que genera un impacto muy grave sobre la operación, por otro lado, se observa que los documentos cuentan con una medida similar en cuando a la integridad de los datos, mientras que el software un muestra un daño importante en temas de autenticidad y trazabilidad, estos datos se encuentran consignados en el documento “MATRIZ INICIAL” de la siguiente forma:

[41] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS, MAGERIT versión 3 (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, En Linea, octubre 2012, disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Cuadro 4. Valoración de Activos.

Fuente: “elaboración propia”

Cuadro 5. Valoración de Activos

HW HARDWARE						DIMESIONES DE SEGURIDAD				
MAGERIT		ACTIVO	DESCRIPCION			A	T	C	I	D
HW	host	Servidor de Impresión: Servidor marca dell en torre PowerEdge T440	Equipo de cómputo que conecta dos impresoras: Destinadas a: Una (1) Impresora HP LaserJet Enterprise serie 600, activo que brinda el servicio para el a rea de registro y control académico. Permite la concurrencia de hasta 25 usuarios y el volumen mensual de impresión es de 200 a 25000 páginas Una (1) Impresora SMART MultiXpress M4370LX, impresora que ofrece el servicio de escáner e impresión con un ciclo de trabajo de hasta 300000 paginas mensuales con capacidades de red alámbrica e inalámbrica. Impresora destinada para el servicio de funcionarios y docentes	De origen industrial	IT15	B	MA	B	MA	MA
HW	host	Servidor de archivos FTP: Servidor marca dell en torre PowerEdge T130	Equipo de cómputo que tiene como función el almacenamiento y la administración de los archivos que se están generando en el interior de la organización como son: Digitalización de documento de entrada y de salida, audios generados en reuniones, asambleas y otro tipo de encuentros, video, generados por docentes y funcionarios. Dentro de las políticas de uso, para este servidor solo pueden tener acceso las personas autorizadas para los fines correspondientes	De origen industrial	IT16	MA	MA	B	M	MA
HW	host	Servidor PBX		De origen industrial	IT17	M	B	B	B	B
HW	host	Servidor de Nómina y Facturación Servidor marca dell en torre PowerEdge T440 Características de servidor Apache 2.4.25 PHP 5.6.30 - 7.1.1 MySQL 5.7.17 phpMyAdmin 4.6.6	Plataforma de desarrollo propio. Tiene como función el almacenamiento y la administración de las notas y evaluación académica, de este se generan: • Matriculas • Hojas de vida de los estudiantes • Evaluación de Materias • Certificados académicos • Generación de sabanas de notas	De origen industrial	IT18	MA	MA	M	M	MA
HW	host	Servidor DHCP Servidor marca dell en torre PowerEdge T440	Servidor que asigna y administra de forma dinámica el direccionamiento dentro de la organización	De origen industrial	IT19	B	MB	B	MA	A
HW	pc	Equipos de Computo Sistemas operativos win 10 Pro	Equipos destinados para el sistema de registro y control académico del centro	Errores y fallos no intencionados	IT20	MA	MA	B	M	A
HW	pc	Equipos de Computo Sistemas operativos win 10 Pro	Equipos destinados a las tareas de orden académico	Errores y fallos no intencionados	IT21	MA	MA	B	M	A
HW	pc	Equipos de Computo	Equipos destinados gestión del desarrollo tecnológico	Errores y fallos no intencionados	IT22	MA	MA	B	M	A
HW	pc	Equipos de Computo	Equipos destinados para desarrollo del objeto social	Errores y fallos no intencionados	IT23	MA	MA	B	M	A
HW	host	Puntos de acceso alámbricos (hub)	Dispositivos de red encargados de la interconexión de la red de datos	De origen industrial	IT24	A	M	A	M	M
HW	ipphone	Teléfonos IP	Sistema de comunicación a través de teléfonos Voz IP, que comunica las oficinas y departamentos del centro	Errores y fallos no intencionados	IT25	M	A	A	M	M
HW	host	Puntos de acceso	Puntos de acceso al servicio de internet en el campus universitario	De origen industrial	IT26	B	B	MB	A	A
HW	print	Impresora HP LaserJet Enterprise serie 600	Brinda el servicio para el a rea de registro y control académico	Errores y fallos no intencionados	IT27	A	A	MA	M	M
HW	print	Impresora SMART MultiXpress M4370LX	Impresora destinada para el servicio de funcionarios y docentes	Errores y fallos no intencionados	IT28	A	A	MA	M	M
COM - COMUNICACIONES						DIMESIONES DE SEGURIDAD				
MAGERIT		ACTIVO	DESCRIPCION	AMENAZAS		A	T	C	I	D
HW	firewall	Cortafuegos Cisco ASA 5505	Sistema de protección	Errores y fallos no intencionados	IT29	A	MA	MA	MA	A
HW	switch	Switches cisco catalyst 2960	Dispositivos de red encargados de la interconexión de la red de datos	Errores y fallos no intencionados	IT30	MB	B	MA	M	A
L - INSTALACIONES						DIMESIONES DE SEGURIDAD				
MAGERIT		ACTIVO	DESCRIPCION	AMENAZAS		A	T	C	I	D
L	site	Dependencia Nómina y Facturación	Oficina Contabilidad	Ataques intencionados	IT31	A	M	A	MA	MA
L	site	Sala de Sistemas	Oficina Sistemas	Ataques intencionados	IT33	M	M	M	M	M
L	site	Campus Universitario		Desastres naturales	IT34	M	M	M	M	M
P - PERSONAL						DIMESIONES DE SEGURIDAD				
MAGERIT		ACTIVO	DESCRIPCION	AMENAZAS		A	T	C	I	D
P	adm	Funcionarios	Usuarios que cuentan con acceso a la infraestructura de TI	Errores y fallos no intencionados	IT35	M	A	M	MA	MA
P	prov	Proveedores	Compañías que aprovisionan Software, Hardware y Servicios a la Compañía	Errores y fallos no intencionados	IT36	M	A	M	M	MA

Fuente: “elaboración propia”

6.1.4 AMENAZAS Y VULNERABILIDADES.

Esta etapa comprende el proceso de identificación realizado sobre las amenazas y vulnerabilidades que pueden generar una afectación sobre los activos, estas amenazas son eventos que pueden ocurrir sobre los activos generando daños.

Los servicios muestran que existen amenazas asociadas a errores o fallos no intencionados pero que pueden generar fugas de información, sin embargo,

cuenta con una materialización de poca frecuencia, se observó vulnerabilidades sobre el software y asociadas a errores de usuario con una frecuencia estimada semanal, el cual se muestra a continuación:

Cuadro 6. Valoración de Activos

COM - COMUNICACIONES					
MAGERIT		ACTIVO	AMENAZAS	VULNERABILDIADES	FRECUENCIA
HW	firewall	Cortafuegos Cisco ASA 5505	Errores y fallos no intencionados	E2	F
HW	switch	Switches cisco catalyst 2960	Errores y fallos no intencionados	E2	F
L - INSTALACIONES					
MAGERIT		ACTIVO	AMENAZAS	VULNERABILDIADES	FRECUENCIA
L	site	Dependencia Nómina y Facturación	Ataques intencionados	A11	PF
L	site	Sala de Sistemas	Ataques intencionados	A11	PF
L	site	Campus Universitario	Desastres naturales	N1	PF
P - PERSONAL					
MAGERIT		ACTIVO	AMENAZAS	VULNERABILDIADES	FRECUENCIA
P	adm	Funcionarios	Errores y fallos no intencionados	E19	PF
P	prov	Proveedores	Errores y fallos no intencionados	E19	PF

Fuente: “elaboración propia”

Cuadro 7. Valoración de Activos

S- SERVICIOS					
MAGERIT		ACTIVO	AMENAZAS	VULNERABILDIADES	FRECUENCIA
S	int	SOPORTE TECNICO	Errores y fallos no intencionados	E19	PF
S	ftp	TRANSFERENCIA DE ARCHIVOS	Errores y fallos no intencionados	E19	PF
S	www	PAGINA WEB	Errores y fallos no intencionados	E19	PF
S	file	ALMACENAMIENTO DE ARCHIVOS	Errores y fallos no intencionados	E19	PF
D- DATOS / INFORMACION					
MAGERIT		ACTIVO	AMENAZAS	VULNERABILDIADES	FRECUENCIA
D	files	NOMINA DE TRABAJADORES	Errores y fallos no intencionados	E1	F
D	files	RECIBOS DE PAGO	Errores y fallos no intencionados	E1	F
D	files	HOJAS DE VIDA	Errores y fallos no intencionados	E1	F
D	files	SEGUIMIENTO TALENTO HUMANO	Errores y fallos no intencionados	E1	F
D	files	CERTIFICADOS - LABORALES - MODELO DE NEGOCIO	Errores y fallos no intencionados	E1	F
SW -APLICACIONES SOFTWARE					
MAGERIT		ACTIVO	AMENAZAS	VULNERABILDIADES	FRECUENCIA
SW	app	Apache 2.4.25	Errores y fallos no intencionados	E20	F
SW	app	PHP 5.6.30 - 7.1.1	Errores y fallos no intencionados	E20	F
SW	bd	MySQL 5.7.17	Errores y fallos no intencionados	E20	F
SW	app	phpMyAdmin 4.6.6	Errores y fallos no intencionados	E20	F
SW	av	Antivirus	Errores y fallos no intencionados	E2	F

Fuente: “elaboración propia”

6.2 DESARROLLO DE OBJETVO 2

- Analizar el escenario actual de la compañía evaluando la madurez en el que se encuentra respecto al Sistema de Gestión de Seguridad de la Información.

6.2.1 DECLARACIÒN DE APLICABILDIAD.

La empresa QWERTY S.A. cuenta con una serie de activos y servicios tecnológicos que cumplen con las necesidades de los diferentes procesos de la organización, sin embargo, en términos de la seguridad de la información se evaluó si cuenta con los controles necesarios para garantizar su correcta gestión, por lo cual se ejecutó un análisis de brecha basado en la declaración de aplicabilidad de acuerdo con la norma ISO/IEC 27001:2013 para el desarrollo del Sistemas de Gestión de Seguridad de la información donde se evidencio lo siguiente:

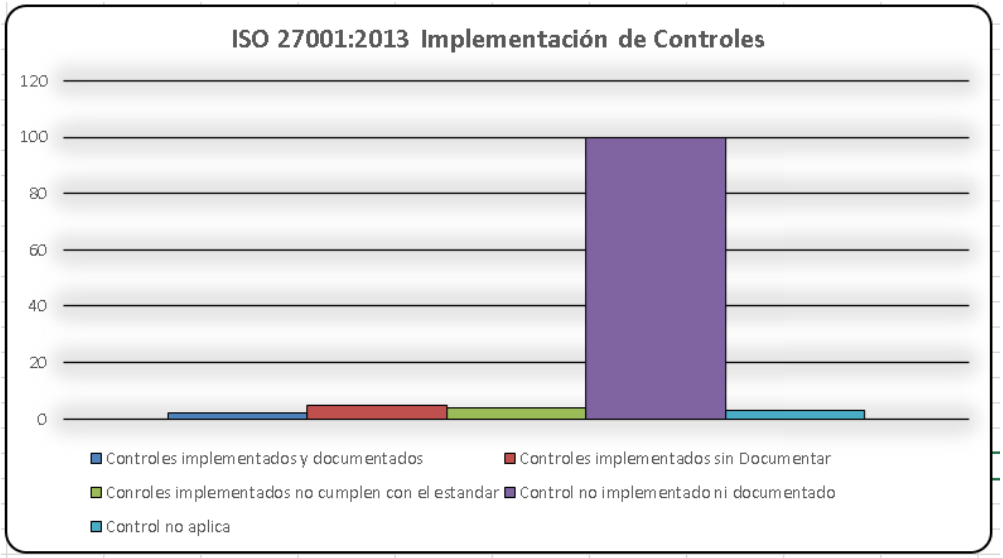
Después de realizar la respectiva validación del cumplimiento de la norma ISO/IEC 27001:2013 sobre los controles implementados del Anexo A mediante el uso del anexo ISO27k_SOA_2013, se evidencia que el cumplimiento es mínimo, algunos de los controles se encuentran sin documentar y la mayor cantidad de controles no se encuentran implementados en la organización.

Tabla 2. Estado de Implementación ISO/IEC 27001.

Estado de Implementación ISO 27001:2013 – Anexo A					
Reference	Controles implementados y documentados	Controles implementados sin Documentar	Controles implementados no cumplen con el estándar	Control no implementado ni documentado	Control no aplica
Controles	2	5	4	100	3
Porcentaje	1,8	4,4	3,5	87,7	2,6

Fuente: “ Anexo ISO27k_SOA_2013”

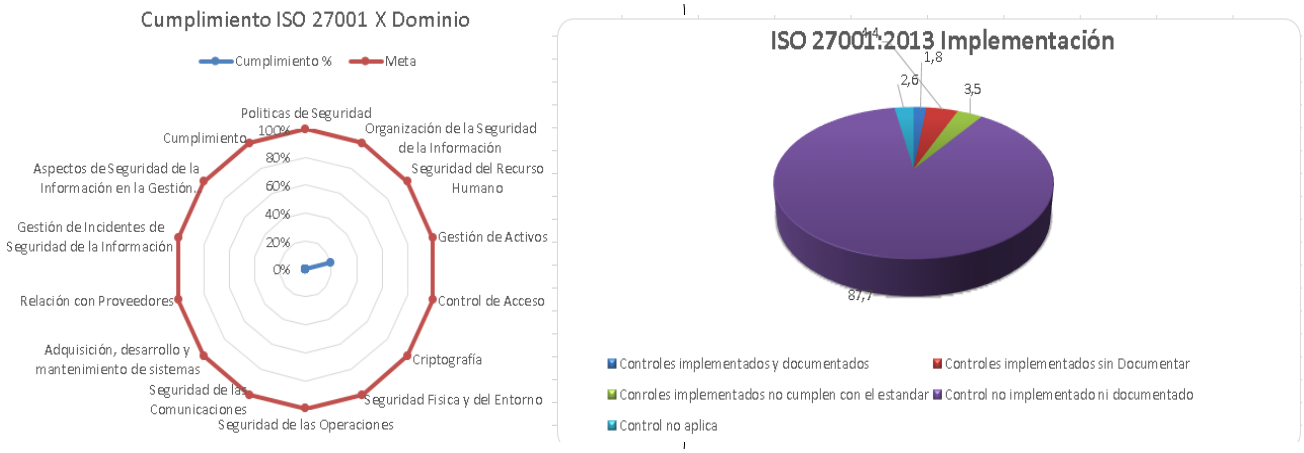
Figura 6. Implementación de Controles



Fuente: " Anexo ISO27k_SOA_2013"

De acuerdo con el análisis el cumplimiento actual de la organización se encuentra asociado a temas relacionado con la gestión de activos el cual fue necesario para el análisis de riesgos y amenazas del objetivo 1, por otro lado, se evidencia que la implementación de forma gráfica el escaso cumplimiento de la norma.

Figura 7. Cumplimiento e Implementación ISO/IEC 27001



Fuente: " Anexo ISO27k_SOA_2013"

Los resultados obtenidos en el análisis no fueron satisfactorios de acuerdo con los resultados esperados, no obstante, define el punto de partida en términos de los requerimientos que la Organización necesita para garantizar entornos más confiables para la gestión de la información, a partir del resultado es posible determinar los elementos necesarios para el cumplimiento de la norma buscando como objetivo un nivel aceptable del riesgo asociado no solo a los controles tecnológicos sino también a controles administrativos, estandarización de procedimientos, políticas y buenas prácticas.

6.3 DESARROLLO DE OBJETVO 3

- Estructurar de forma apropiada los roles y responsabilidades a tener presente en la implementación del Sistema de Gestión de Seguridad de la Información.

La situación de la Organización requirió establecer un proceso de seguridad que permitiera la apropiada gestión de la información, por consiguiente, fue necesario evaluar la implementación de un equipo de trabajo enfocado en crear, implementar y mantener controles, procedimiento y políticas para la gestión de la seguridad de la información, teniendo esto en cuenta se generó la siguiente estructura para dicho propósito:

6.3.1 CONSTITUCION DEL COMITÉ DE SEGURIDAD DE LA INFORMACION (CSI).

Se procede entonces con la creación del comité de seguridad ya que el SGSI debe contar con el apoyo de los directivos de QWERTY S.A. para lograr el cumplimiento de los objetivos propuestos, garantizando los recursos necesarios para su implementación, desarrollo y continuidad, estableciendo la estructura y

responsabilidades de los involucrados, velando por el desarrollo de directrices y políticas que garantice la protección de los activos de información.

También fue necesario contar con el apoyo de altos directivos en todas las fases del desarrollo de este esquema de aseguramiento iniciando con la planeación, donde se plantearon los objetivos que desea alcanzar la entidad y para los cuales los representantes participaron activamente en la identificación de los términos en los que se logró cumplir los compromisos de implementación, teniendo en cuenta los lineamientos del contexto de la organización, posteriormente se sugiere realizar las respectivas auditorias donde se ejecute la recolección de información para medir, analizar y evaluar la efectividad del sistema de gestión, delimitando los controles que certifiquen que cumple con los requisitos propuestos.

6.3.2 RESPONSABILIDADES DEL COMITÉ.

La estructura del comité dentro de su estrategia para el SGSI debe asignar las responsabilidades y funciones para el avance del proceso:

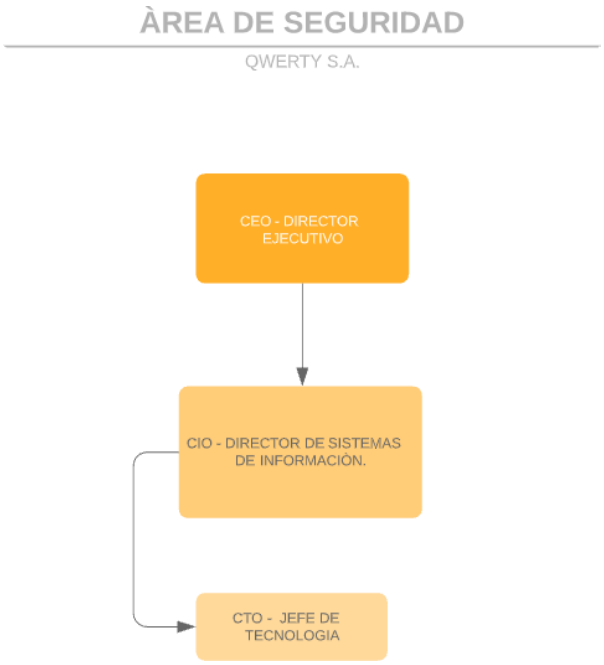
- Establecer un flujo de aprobación de políticas, procedimientos y normas para el sistema de gestión.
- Organizar al equipo de trabajo que será el responsable de la implementación del sistema de gestión.
- Definir los roles, perfiles y responsabilidades del equipo de trabajo de la implementación.
- Tomar las acciones que correspondan para planear, ejecutar y monitorear las actividades necesarias para el desarrollo del SGSI.
- Vigilar el cumplimiento de las directrices y lineamientos establecidos en el sistema de gestión.
- Administrar y soportar los objetivos propuestos en el sistema de gestión.
- Coordinar y promover la comunicación entre las áreas involucradas.

- Crear proyectos tecnológicos que apoyen los procesos del sistema de gestión.
- Analizar y cualificar los controles propuestos dentro del plan para la mitigación del riesgo.
- Fomentar en la organización la importancia del sistema de gestión de seguridad de la información en todos los procesos.

De conformidad con lo que se requiere para gestión apropiada de la información se establecieron funciones y responsabilidades definidas de la siguiente manera:

6.3.3 ORGANIGRAMA - ROLES Y RESPONSABILDADES

Figura 8. Organigrama QWERTY S.A.



Fuente: ”elaboración propia”

6.3.4 CEO - Chief Executive Officer.

Director ejecutivo, es la máxima autoridad y quien es responsable de todo lo relacionado con los servicios tecnológicos de la organización, quien supervisa que las estrategias definidas cumplan con los objetivos de la organización, delimita los principios y es responsable de los resultados del comité directivo.

- Responsable del desarrollo de estrategias y actividades que garanticen el cumplimiento de las metas propuestas por la compañía.
- Planificar y elegir los objetivos para el cumplimiento de metas.
- Rendir Cuentas a la junta directiva de los resultados obtenidos.

6.3.5 CIO - Chief Information Officer.

Director de sistemas de información, está encargado de alienar las estrategias con las tecnologías de información, mejorando la eficiencia de los procesos mediante el uso de nuevas tecnologías.

- Alinear las estrategias de la organización con las tecnologías de la información.
- Responsable de la gestión del riesgo y continuidad del negocio.
- Implementar soluciones innovadoras para la optimización de los procesos.

6.3.6 CTO - Chief Technology Officer.

Es responsable de las tecnologías de la información, pero enfocado de forma más técnica, por lo que está a cargo de la gestión operativa diaria de la organización.

- Gestión de las plataformas tecnológicas.
- Garantizar el funcionamiento de las operaciones.
- Mantener la continuidad del negocio.
- Establecer los controles necesarios de manera interna para la correcta gestión de la seguridad de la información.

6.4 DESARROLLO DE OBJETVO 4

- Establecer los controles necesarios de manera interna para la correcta gestión de la seguridad de la información.

6.4.1 PLAN DE TRATAMIENTO

Posterior al análisis sobre los activos de la organización, su situación frente a las amenazas y el riesgo al que se encuentran expuestos se procede con el diseño de un plan de tratamiento en donde se busca, trasferir, Asumir o mitigar el riesgo por medio de los controles Organizacionales y técnicos.

Controles Organizacionales: Son aquellas medidas que se basan en las políticas, procesos y procedimientos que conllevan a una buena administración, permitiendo el buen uso de la implementación de los recursos.

Controles Técnicos: Son todos los tratamientos que se aplican directamente al software y hardware de la compañía, que no cuentas con lineamientos estipulados bajo algún tipo de documentación

En el plan define el activo evaluado, su nivel de riesgo, la estrategia planteada para el tratamiento del riesgo, el control propuesto, la descripción del plan de acción y el responsable.

De acuerdo con los resultados de los hallazgos que se evidencian sobre los diferentes activos de la organización se generan los controles que se deben aplicar para la mitigación del riesgo y en el cual se encuentran los siguientes puntos:

- Se debe considerar que la página web de la organización debido a su exposición a internet cuenta con una amplia superficie de ataque, el activo puede generar un riesgo reputacional y por lo tanto se sugieren mecanismos de control de acceso y gestión del sitio, adicional se requiere el uso de buenas prácticas de desarrollo, por otro lado se debe tener en cuenta temas asociados con malware con el propósito de evitar la distribución de este tipo de amenazas a los usuarios que constantemente naveguen o utilicen recursos del sitio, cabe destacar que debido a que la pagina está contratada mediante un proveedor, QWERTY S.A. podría transferir los riesgos al tercero que deberá ser responsable de cualquier eventualidad incluso de las no detectadas durante el proceso.
- Una falla sobre el servidor de impresión puede generar una afectación importante sobre las actividades laborales diarias por lo que se sugiere realizar un monitoreo para prevenir y dar solución oportuna a cualquier irregularidad que se presente en la prestación del servicio, el cual debe ser utilizado únicamente por el personal autorizado.

Cuadro 8. Plan de Tratamiento.

ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANÁLISIS DE RIESGOS	QUE				F AN DE TRATAMIENTO DE RIESGOS			
	NIVEL DEL RIESGO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	ESTRATEGIA DE TRATAMIENTO DEL RIESGO	IDENTIFICACIÓN DEL CONTROL	DESCRIPCIÓN DEL PLAN DE ACCIÓN (CONTROLES)	RESPONSABLE
[www] Página Web	CRITICO	25	25	25	MITIGAR	A9.4.5 Control de acceso al código fuente de los programas	El área de sistemas de QWERTY S.A., como garante de la administración de los sistemas de información, aplicativos y sus códigos fuente, debe proteger contra accesos no autorizados a través de mecanismos de control de acceso lógico, de igual forma sus desarrolladores, deben implementar las buenas prácticas de desarrollo en los software generados para vigilar el acceso lógico e impedir accesos no autorizados a los sistemas administrados por la entidad educativa.	Jefe Departamento de sistemas
						A12.2.1 Controles contra el código malicioso	La entidad educativa "QWERTY S.A." debe brindar las herramientas elementales para garantizar la protección de la información y los recursos TIC adquiriendo controles para evitar la modificación, divulgación o daño causado por software malicioso, así mismo capacitar a sus funcionarios y terceros en buenas prácticas con relación a los ataques de software malicioso.	Jefe Departamento de sistemas
Servidor Impresión	IMPORTANTE	9	25	25	MITIGAR	A12.4.1 Registro de eventos	El área de sistemas de QWERTY S.A., como garante de la administración de la infraestructura tecnológica debe Inspeccionar el contenido de los archivos de registro de eventos de los servidores acorde con el tiempo definido de la criticidad del registro de eventos, a través de alarmas generadas por el sistema, eventos de acceso no autorizado, acceso a aplicaciones no autorizadas y cualquier situación anormal que se presente.	Jefe Departamento de sistemas
						A9.1.2 Acceso a las redes y a los servicios de red	El área de infraestructura del QWERTY S.A., como garante de la administración de la infraestructura tecnológica para el acceso a la red de la Entidad debe únicamente proporcionar acceso a usuarios autorizados, a través de un formato previa autorización del jefe inmediato del colaborador y verificación de roles y perfiles	Jefe de Infraestructura

Fuente: "elaboración propia"

- El servidor de nomina contiene datos sensibles, para el cual se sugiere un control de monitoreo de registros con el propósito de evaluar accesos no autorizados, cambios sobre los datos o cualquier anomalía sobre el sistema y los archivos.
- En el caso del servidor DHCP como acción preventiva se propone el monitoreo del registro de eventos con el objetivo de prevenir cualquier tipo de acceso o modificaciones de configuración no autorizadas.
- En el caso del dispositivo perimetral se sugiere la implementación de controles de acceso físicos y lógicos, definir una política que permita normalizar las reglas de control de tráfico que se crean en el dispositivo, el monitoreo constante de los logs de eventos e implementar controles mas restrictivos para la protección de la red interna.

Cuadro 9. Plan de Tratamiento.

ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANÁLISIS DE RIESGOS	NIVEL DEL RIESGO	QUE			PLAN DE TRATAMIENTO DE RIESGOS			
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	ESTRATEGIA DE TRATAMIENTO DEL RIESGO	IDENTIFICACIÓN DEL CONTROL	DESCRIPCIÓN DEL PLAN DE ACCIÓN (CONTROLES)	RESPONSABLE
Servidor de Nómina y Facturación	CRITICO	15	15	25	MITIGAR	A12.4.1 Registro de eventos	El área de sistemas de QWERTY S.A., como garante de la administración de la infraestructura tecnológica debe Inspeccionar el contenido de los archivos de registro de eventos de los servidores acorde con el tiempo definido de la criticidad del registro de eventos, a través de alarmas generadas por el sistema, eventos de acceso no autorizado, acceso a aplicaciones no autorizadas y cualquier situación anormal que se presente.	Jefe de Infraestructura
Servidor DHCP	APRECIABLE	9	25	20	MITIGAR	A12.4.1 Registro de eventos	El área de sistemas de QWERTY S.A., como garante de la administración de la infraestructura tecnológica debe Inspeccionar el contenido de los archivos de registro de eventos de los servidores acorde con el tiempo definido de la criticidad del registro de eventos, a través de alarmas generadas por el sistema, eventos de acceso no autorizado, acceso a aplicaciones no autorizadas y cualquier situación anormal que se presente.	Jefe de Infraestructura
[FIREWALL] Cortafuegos Cisco	CRITICO	25	25	20	MITIGAR		La entidad educativa "QWERTY S.A." a través de el área de infraestructura debe implementar el monitoreo y seguimiento al registro de logs para evidenciar posibles intrusiones no autorizadas.	Jefe de Infraestructura
						A13.1.2 Seguridad de los servicios de red	El área de infraestructura del QWERTY S.A., como garante de la administración de la infraestructura tecnológica debe establecer reglas para la configuración del Firewall e implementar lineamientos y políticas de seguridad para acceder a los recursos y servicios de la organización.	Jefe de Infraestructura
							El área de infraestructura del QWERTY S.A., como garante de la administración de la infraestructura tecnológica debe Implementar controles de acceso físico y lógico que restrinjan el acceso no autorizado	Jefe de Infraestructura
						A9.1.2 Acceso a las redes y a los servicios de red	El área de infraestructura del QWERTY S.A., como garante de la administración de la infraestructura tecnológica debe implementar configuraciones de seguridad que permitan salvaguardar la información e infraestructura de red de la organización	Jefe de Infraestructura

Fuente: "elaboración propia"

De acuerdo con lo planteado la dirección debe evaluar la adopción de las sugerencias planteadas dentro de plan de tratamiento, priorizando de forma inmediata aquellos riesgos que cuenten con un nivel crítico y alto, para establecer un nivel de impacto aceptable, posteriormente implementar las medidas asociadas a los niveles inferiores teniendo en cuenta la afectación que estos puedan generar sobre la organización

7 RESULTADOS ESPERADOS

Después de diseñar una estrategia de aseguramiento y gestión de la información, se desea que la empresa QWERTY S.A.S lo use para llevar a cabo la aplicación de los controles y políticas de seguridad que se han generado a partir de la identificación de la gestión diaria de los activos en el área informática, según lo establecido en la norma ISO 27001 y la metodología MAGERIT.

Destacando la valoración de las vulnerabilidades, riesgos y amenazas, la aparición de recomendaciones que permitirán el trato adecuado de los riesgos y la aplicación de la política de seguridad, entre otros.

8 CONCLUSIONES

La identificación de activos de información y su clasificación es esencial para definir su criticidad para el negocio, evaluar su prioridad y generar las medidas necesarias para garantizar un entorno más seguro, es necesario contar con la visibilidad de lo que tenemos en la organización para tomar decisiones frente a las amenazas y riesgos de los diferentes ambientes a los que se encuentran expuestos.

La declaración de Aplicabilidad es una referente para conocer la situación actual de la Organización en términos de seguridad y establecer el objetivo al que deseamos llegar con la implementación de estándares y normas de seguridad.

La creación de procesos y procedimientos de seguridad dentro de la organización, así como su gestión y control, requiere establecer una estructura organizativa que defina el rol y los responsables de cada actividad, se debe contar con recurso humano idóneo para garantizar no solo el cumplimiento de lo establecido sino lograr la mejora continua mediante la creación de nuevas estrategias.

El plan de tratamiento debe estar enfocado en dar solución a las debilidades encontradas en la empresa de acuerdo con los resultados obtenidos en el análisis de riesgo, la creación de controles de seguridad y la evaluación de su efectividad es una tarea constante que requiere un trabajo continuo y periódico que proporciona un nivel de riesgo aceptable para el normal funcionamiento de los procesos críticos de la Compañía.

9 RECOMENDACIONES

Se recomienda la ejecución de auditorías de forma constante, después de haber realizado la implementación de la estrategia de aseguramiento, para así poder detectar las falencias que pongan en riesgo los activos de la compañía y así mismo la información que contienen estos.

Se recomienda llevar a cabo la implementación de las políticas, ya que a través de estas la seguridad de los activos y su información aumentara de tal manera que el riesgo se reducirá permitiendo que este no se materialice y afecte la integridad, la confidencialidad y la disponibilidad de la información.

10 BIBLIOGRAFÍA

ACEITUNO CANAL, Vicente.” Seguridad de la Información” En Línea, marzo 2019, disponible en: https://www.iberlibro.com/Seguridad-Informaci%C3%B3n-Vicente-Aceituno-Canal-Creaciones/13992357369/bd

ANDRADE RODRIGUEZ, Yovany ” ENTENDIENDO EL SGSI” En Linea, disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2748/00002987.pdf?sequence=1

ALEMAN NOVOA, Helena, RODRIGUEZ BARRERA Claudia, “Metodologías Para el análisis de riesgos en los sgsi” En línea, Mayo 2014, disponible en: https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1754

BOHÓRQUEZ MUÑOZ , ana maría “diseño de un sistema de gestión de seguridad de la información (sgsi) para la agencia de aduanas move cargo s.a. nivel 1” En Línea, marzo 2019, disponible en:.https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/25618/1/ambohorquezmu.pdf

BUITRAGO BOTERO, Diego “Aspectos Jurídicos de Internet y el Comercio Electrónico” En Línea, marzo 2019, disponible en: http://www.informatica-juridica.com/trabajos/aspectos-juridicos-de-internet-y-el-comercio-electronico/

CALDERÓN SÁNCHEZ, Álvaro. “implementación del sgsi en el área de redes de compuserver basado en la norma iso/iec27001:2013” En Línea, marzo 2019, disponible en: https://repository.unad.edu.co/handle/10596/3676

CENTRO UNIVERSITARIO DE GUANTÁNAMO CUBA. “Vía para fortalecer el aprendizaje de las Redes Informáticas” En Línea, marzo 2019, disponible en: https://www.redalyc.org/pdf/4757/475748678004.pdf

Christopher J. AlbertsSandra G. BehrensRichard D. PethiaWilliam R. Wilson, “Operationally Critical Threat,Asset, and VulnerabilityEvaluation SM(OCTAVESM) Framework,Version 1.0” En Linea, Junio 1999, disponible en:https://kilthub.cmu.edu/articles/Operationally_Critical_Threat_Asset_and_Vulnerability_Evaluation_OCTAVE_Framework_Version_1_0/6575906/1

CONPES, “ESTRATEGIA DE ESTANDARIZACIÓN DE PROYECTOS 2016-2018”, Abril 2016, En línea, disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3856.pdf

DEGERENCIA.COM “Tecnología de Información” En Línea, marzo 2019, disponible en: https://degerencia.com/tema/gerencia/tecnologia-de-informacion/

DORDOIGNE ,José. “Redes Informáticas - Nociones fundamentales (6ª edición)” En Línea, marzo 2019, disponible en:https://www.ediciones-eni.com/libro/redes-informaticas-nociones-fundamentales-6-edicion-protocolos-arquitecturas-redes-inalambricas-virtualizacion-seguridad-ipv6-9782409012792

EINCON CARDENAS, Erick. “Instrumentos Normativos de Ciberseguridad” En Línea, marzo 2019, disponible en: https://web.certicamara.com/app/webroot/media/import/normativa-colombiana-en-materia-de-ciberseguridad-y-ciberdefensa-1-marzo-2014.pdf

“el modelo OSI y los protocolos de red” En Línea, marzo 2019, disponible en: https://blyx.com/public/docs/pila_OSI.pdf

EMPRENDEPYME.” ¿Qué es un sistema de información?” En Línea, marzo 2019, disponible en: https://www.emprendepyme.net/que-es-un-sistema-de-informacion.html

FABUEL DÍAZ, Carlos Manuel . “implantación de un sistema de seguridad perimetral” En Línea, marzo 2019, disponible en: http://oa.upm.es/22228/1/PFC_CARLOS_MANUEL_FABUEL_DIAZ.pdf

GESTION.ORG.“Que es el control de gestión” En Línea, marzo 2019, disponible en: https://www.gestion.org/que-es-el-control-de-gestion/

GÓMEZ, Joel. “la seguridad y confidencialidad de la información es obligación de todos” En Línea, marzo 2019, disponible en: https://www.merca20.com/la-seguridad-y-confidencialidad-de-la-informacion-es-obligacion-de-todos/

GRUPO FUNCIONAL DE SEGURIDAD INFORMATICA DE LA UNAD “10 Mandamientos en Seguridad Informática que deberíamos seguir...” En Línea, marzo 2019, disponible en: https://noticias.unad.edu.co/index.php/gidt/1703-mandamientos

H. TOLOSA, Gabriel “Protocolos y Modelo OSI” En Línea, marzo 2019, disponible en: http://www.tyr.unlu.edu.ar/pub/02-ProtocolosOSI.pdf

ICONTEC.” Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos: ICONTEC 2013 (NTC-ISO 27001)

ISEC."Control de acceso: qué es y para qué sirve” En Línea, marzo 2019, disponible en: http://www.isec.com.co/control-de-acceso-que-es-y-para-que-sirve/

ISO, NTC-ISO/IEC 27001:2013, En Linea, 2013, disponible en: https://www.iso.org/home.html

ISO, NTC-ISO/IEC 31000:2018, En Linea, 2018, disponible en: https://www.iso.org/home.html

ISO27000.ES.”El portal de ISO 27001 en español” En Línea, marzo 2019, disponible en: http://www.iso27000.es/iso27000.html

ISO27000.ES.“Sistema de Gestión de la Seguridad de la Información” En Línea, marzo 2019, disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

ISO 27001:2013, SGSI “¿Por qué implantar un SGSI basado en la norma ISO 27001?” En Línea, marzo 2019, disponible en: https://www.pmg-ssi.com/2015/05/por-que-implantar-un-sgsi-basado-en-la-norma-iso-27001/

ISO27K IMPLEMENTERS' FORUM.“Consejos de implantación y métricas de ISO/IEC 27001 y 27002” En Línea, marzo 2019, disponible en: http://www.iso27000.es/download/ISO_27000_implementation_guidance_v1_Spanish.pdf

ISOTools. “La norma ISO 27001 Aspectos clave de su diseño e implantación” En Línea, marzo 2019, disponible en: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

ISOTOOLS EXCELLENCE “ISO 27001: El método MAGERIT” En Línea, marzo 2019, disponible en: https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

INCAP.“Sistema de Información” En Línea, marzo 2019, disponible en: http://www.incap.int/sisvan/index.php/es/acerca-de-san/conceptos/sistema-de-vigilancia

KASPERSKY LAB. “¿Qué es un firewall?” En Línea, marzo 2019, disponible en: https://latam.kaspersky.com/resource-center/definitions/firewall

KIMALDI ELECTRONICS, S.L. “¿Qué es la biometría?” En Línea, marzo 2019, disponible en: https://www.kimaldi.com/blog/biometria/que_es_la_biometria/

MARTÍNEZ DE LA CRUZ, Sergio Alejandro. “Importancia de los sistemas de información para las Pymes” En Línea, marzo 2019, disponible en: https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/

MARKUS ERB “Gestión de Riesgo en la Seguridad Informática” En Línea, marzo 2019, disponible en: https://protejete.wordpress.com/

MAYA ARANGO, Paula Andrea. “plan de implementación del sgsi basado en la norma iso 27001:2013” En Línea, marzo 2019, disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/53466/8/pmayaaTFM0616memoria.pdf

MENDOZA, Miguel Ángel. ”¿Cómo definir el alcance del SGSI?En Línea, marzo 2019, disponible en:https://www.welivesecurity.com/la-es/2018/01/09/definir-alcance-sgsi/

MIFSUD, elvira “monográfico: Introducción a la seguridad informática” En Línea, marzo 2019, disponible en: http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-%20seguridad-informatica

MINTIC, OEA, BID, Impacto de incidentes de seguridad digital en Colombia” En Linea, 2017, disponible en: https://revistaempresarial.com/wp-content/uploads/2017/10/Estudio-Seguridad-Digital-Colombia.pdf

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS, MAGERIT versión 3 (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, En Linea, octubre 2012, disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES "Ciberseguridad" En Línea, marzo 2019, disponible en: https://www.mintic.gov.co/portal/604/w3-article-6120.html

MINTIC."Guía para la Implementación de Seguridad de la Información en una MIPYME" En Línea, marzo 2019, disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

MINTIC."Seguridad y privacidad de la información. Guía, 2" En Línea, marzo 2019, disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

MINTIC."Seguridad y privacidad de la información. Guía, 6" En Línea, marzo 2019, disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G6_Gestion_Documental.pdf

MINTIC."Seguridad y privacidad de la información. Modelo" En Línea, marzo 2019, disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

NIST, “Guide for Conducting Risk Assesment”, En Linea, Septiembre 2012, disponible en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

NORMAISO27001.ES, ISO 27001 En Linea, disponible en: https://normaiso27001.es/

PMG SSI.”¿Qué es SGSI?” En Línea, marzo 2019, disponible en: https://www.pmg-ssi.com/2015/07/que-es-sgsi/

PORTAFOLIO. “Siete consejos para proteger los sistemas informáticos de su compañía” En Línea, marzo 2019, disponible en: https://www.portafolio.co/innovacion/siete-recomendaciones-para-proteger-los-sistemas-informaticos-de-su-compania-506755

QUINTERO AGUDELO, Yolanda “La seguridad y la ciberdefensa en Colombia” En Linea, disponible en: http://polux.unipiloto.edu.co:8080/00001596.pdf

REVISTA TECNOLÓGICA ESPOL “Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001” En Línea, marzo 2019, disponible en: http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

RIOS, Julio. “Seguridad Informática” En Línea, marzo 2019, disponible en: https://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml#introducca#ixzz2fCGghfuG

SECURITY IN-A-BOX. “protege tu dispositivo de malware y ataques de phishing” En Línea, marzo 2019, disponible en: https://securityinabox.org/es/guide/malware/

SIGNIFICADOS.COM. “Significado de Sistema de información” En Línea, marzo 2019, disponible en: https://www.significados.com/sistema-de-informacion/

SYMANTEC CORPORTATION.” La importancia de utilizar un firewall para la protección contra amenazas” En Línea, marzo 2019, disponible en: https://www.websecurity.symantec.com/es/es/security-topics/importance-using-firewall-threat-protection

TECNOLOGÍA- DEFINISTA “Definición de Tecnología de la Información” En Línea, marzo 2019, disponible en: https://conceptodefinicion.de/tecnologia-de-la-informacion/

TECNOLOGÍA & INFORMÁTICA. “Que es un Firewall y como funciona.” Tipos de firewall” En Línea, marzo 2019, disponible en: https://tecnologia-informatica.com/que-es-firewall-como-funciona-tipos-firewall/

TECNOSEGURO.”¿Qué es un Sistema de Control de Acceso?” En Línea, marzo 2019, disponible en: https://www.tecnoseguro.com/faqs/control-de-acceso/que-es-un-control-de-acceso

THALESGROUP.“Biometría para identificación y autenticación” En Línea, marzo 2019, disponible en: https://www.gemalto.com/latam/sector-publico/inspiracion/biometria

UNIVERSIDAD TECNOLOGICA DE PEREIRA. “políticas de seguridad de activos de información” En Línea, marzo 2019, disponible en: https://www.utp.edu.co/cms-utp/data/bin/UTP/web/uploads/media/calidad/documentos/politicas_sgsi.pdf