DISEÑAR UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACION PARA LA EMPRESA QWERTY S.A A PARTIR DE LA NORMA ISO 27001

CRISTIAN ALBERTO GOMEZ RAVELO

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUCARAMANGA
2020

DISEÑAR UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACION PARA LA EMPRESA QWERTY S.A A PARTIR DE LA NORMA ISO 27001

CRISTIAN ALBERTO GOMEZ RAVELO

Proyecto Aplicado como requisito para optar al título de: Especialista en Seguridad Informática

Director(a)
Msc. KATERINE MÁRCELES VILLALBA

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUCARAMANGA
2020

Nota de aceptación

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Bucaramanga, Mayo de 2020

DEDICATORIA

Dedico este proyecto de grado primero que todo a Dios por darme la vida y permitirme llegar hasta este momento tan importante de mi formación profesional. A mis padres por todo su apoyo incondicional y sacrificio en todos estos años siendo un pilar fundamental en mi formación como profesional para hacer de mí una mejor persona.

RESUMEN

El trabajo final de la especialización en Seguridad Informática corresponde al Proyecto Aplicado, donde se describe los objetivos, el alcance, la expectativa del Sistema de gestión de la seguridad de la información, la metodología asociada a la definición, planeación, identificación y diseño del SGSI para la empresa **QWERTY** S.A, basado en la norma ISO 27001:2013; iniciando desde el entendimiento de la organización desde la óptica de los procesos críticos de la operación, ejecución del diagnóstico de seguridad de la información, identificación de las principales amenazas y vulnerabilidades, aplicando la metodología de Margerit para la gestión de riesgos de seguridad de la información, planeación de los planes de riesgos y generación del marco documental del sistema de gestión de seguridad de la información para **QWERTY S.A**.

El presente proyecto plantea las bases para dar inicio al diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI) bajo la norma ISO27001 en la empresa QWERTY S.A a través de unas fases estructuradas, partiendo del análisis de los activos de la empresa para identificar los riesgos y amenazas enmarcadas en las áreas de Infraestructura, Desarrollo y Soporte, siguiendo con el Análisis de gestión de riesgos a todos los procesos involucrados en el proyecto a partir de la metodología de Margerit y terminando con la definición de las políticas de seguridad acordes con los objetivos que permitan minimizar los posibles riesgos a los que está expuesta la información de la empresa en cada área.

PALABRAS CLAVE: SGSI, Activos, Análisis y Evaluación de Riesgos, Magerit, ISO/IEC 27001, Políticas de Seguridad.

ABSTRACT

The final work of the Computer Security specialization corresponds to the Applied Project, which describes the objectives, scope, expectation of and information security management system, the methodology associated with the definition, planning, identification and design of the SGSI for the company QWERTY SA, based on ISO 27001; starting from the understanding of the organization from the perspective of the critical processes of the operation, execution of the information security diagnosis, identification of the main threats and vulnerabilities, applying a Magerit methodology for the management of information security risks , planning of risk plans and generation of the documentary framework of the information security management system for QWERTY SA

This project sets the basis for starting the design of an Information Security Management System (ISMS) under the ISO27001 standard in the company QWERTY SA through structured phases, based on the analysis of the company's assets to identify the risks and threats framed in the areas of Infrastructure, Development and Support, continuing with the Risk management analysis of all the processes involved in the project based on the Magerit methodology and ending with the definition of security policies in line with the objectives that minimize the possible risks to which the company's information is exposed in each area.

KEY WORDS: ISMS, Assets, Analysis and Risk Assessment, Magerit, ISO / IEC 27001, Security Policies.

GLOSARIO

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

Confidencialidad: Es la propiedad que impide la divulgación de información a terceras personas o sistemas no autorizados. Se garantiza que el acceso a la información únicamente a aquellas personas que cuenten con la respectiva autorización.

Disponibilidad: Supone de que los usuarios autorizados tienen acceso a la información y a los activos cuando lo necesiten o lo requieran.

Integridad: Asegurar que la información almacenada y/o procesada por QWERTY S.A, no sea modificada o alterada sin autorización.

Autenticación: Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Análisis de Riesgos: Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de integridad, confidencialidad y disponibilidad de la información.

Activos de Información: Corresponde a cualquier elemento tecnológico, físico o intangible que genera, almacena o procesa información y tiene valor para la empresa, como archivos, bases de datos, manuales, programas, equipos de comunicaciones, entre otros.

Recursos Tecnológicos: Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la empresa.

Sistema de Información: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas.

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

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias que al evaluarse de manera objetiva, permiten determinar la extensión en que se cumplen los criterios definidos para la auditoría interna.

Gestión del riesgo: Proceso de actividades coordinadas para identificar, analizar, dirigir y controlar los aspectos asociados al Riesgo dentro de la empresa.

Seguridad de la información: Preservación de la integridad, la confidencialidad, y la disponibilidad de la información; además puede involucrar otras propiedades tales como autenticidad, trazabilidad, no repudio y fiabilidad.

S.G.S.I: Sistema de Gestión de Seguridad de la Información.

Valoración del riesgo: Proceso global de análisis y evaluación del riesgo.

Magerit. Es la metodología de análisis y gestión de riesgos de la información desarrollada por el Consejo Superior de Administración Electrónica.

PALABRAS CLAVES: Activo de información, Análisis y Evaluación de Riesgos, Informática, ISO/IEC 27001, Magerit, SGSI, Seguridad.

CONTENIDO

LISTADO DE TABLAS

LISTADO DE FIGURAS

INTRODUCCIÓN

La información de QWERTY S.A se constituye como uno de los activos de mayor valor para la empresa, por lo tanto esta debe ser utilizada dentro de un adecuado entorno de seguridad, cualquiera que sea el medio ya sea físico o lógico en el que se encuentre y el ambiente tecnológico en que se procese la información. A través del diseño e implementación del sistema de gestión de seguridad de la información se busca minimizar los riesgos a los que se encuentra expuesta la información de la organización.

La empresa QWERTY S.A. es una empresa del sector tecnológico que busca el desarrollo tecnológico en comunidades colombianas a través del uso de Tecnologías de Información. Este proyecto se llevara a cabo en la empresa QWERTY S.A. la cual pretende implementar políticas y controles de seguridad que permita proteger todos los activos de información de la organización, identificando las necesidades básicas de seguridad teniendo presente los requisitos, las medidas y los controles necesarios en cada uno de los procesos que permitan poder obtener confidencialidad, integridad y disponibilidad de la información.

Para la Empresa QWERTY S.A es una decisión estratégica y gerencial al implantar su Sistema de Gestión de Seguridad de la Información, el cual le permite poder brindar a sus clientes y funcionarios, niveles apropiados de protección y seguridad de la información.

El presente trabajo de grado busca diseñar un Sistema de Gestión de Seguridad de la Información de un escenario propuesto Enfoque Directivo – Administrativo sobre la empresa QWERTY S.A, teniendo en cuenta para esto el marco de referencia de la norma ISO 27001:2013 que proporciona un marco metodológico basado en buenas prácticas para la implementación del SGSI en cualquier área de la organización.

1. PLANTEAMIENTO DEL PROBLEMA

La Empresa QWERTY S.A. es una empresa del sector tecnológico que busca el desarrollo tecnológico en comunidades colombianas a través del uso de Tecnologías de información. Actualmente cuenta con 120 colaboradores entre directivos, administrativos y operativos, quienes hacen uso de forma regular de los medios de información para consulta de datos, teniendo en cuenta las diferentes gestiones que realizan con los datos surge la necesidad de diseñar un sistema para salvaguardar adecuadamente la información, dada a la problemática que se especifica a continuación.

QWERY S.A. no cuenta con un sistema de seguridad biométrico o de monitoreo que permita tener control de ingreso y egreso de los clientes internos y externos. Los servidores DHCP, HTTP y PBX se encuentran en un espacio donde no se cumplen condiciones de climatización óptimas. La configuración de la red de comunicaciones se encuentra en el mismo Segmento Aunque los equipos de cómputo cuentan con sistemas de antivirus actualizado, no se hace un seguimiento a sus actualizaciones o estado.

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

Aunque existe un Cortafuegos Cisco ASA 5505, este no cuenta con reglas implementadas para la autorización o denegación de conexiones o transmisión de datos, por lo anterior puede conllevar a fuga de información o alterar la integridad y disponibilidad de los diferentes activos de información de la empresa.

1.1 FORMULACIÓN DEL PROBLEMA

¿Es posible diseñar un sistema de gestión de seguridad de la información que permita establecer un control interno de la información desde la dependencia de sistemas de la empresa *QWERTY S.A* bajo la norma ISO/IEC 27001?

2. JUSTIFICACIÓN

El diseñar un SGSI para una empresa es muy importante, ya que la información se ha denominado como uno de los activos más valiosos que depende en gran parte el funcionamiento de una organización, a su vez el Sistema de Gestión de Seguridad de la Información garantiza el tratamiento de los problemas de seguridad que se puedan presentar. Las organizaciones y sus sistemas de información están expuestos a todo tipo de amenazas que pueden poner en peligro la inestabilidad económica y financiera; hay diversas formas entre las que se encuentra el fraude, espionaje, sabotaje, vandalismo, robos de identidad, robos de información, spam, virus informáticos, el hacking o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, que pueden afectar la imagen, la confianza de los clientes y de la empresa.

El diseño de un SGSI permitirá a la empresa QWERTY S.A identificar, gestionar y disminuir los riesgos reales y potenciales de la seguridad de la información en la entidad, de una forma organizada, documentada, sistematizada, eficiente y acondicionada a los cambios que se puedan generar en los riesgos. El diseño del sistema bajo la norma ISO 27001 tiene como objetivo asegurar que la empresa pueda mantener su integridad, confidencialidad y disponibilidad de la información teniendo en cuenta que es un modelo efectivo para administrar la seguridad de la información.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un Sistema de Gestión de la Seguridad de la información, bajo la norma ISO/IEC 27001 en la Empresa QWERTY S.A para establecer un control interno de la información en cada una de las áreas que la conforman.

3.2 OBJETIVOS ESPECIFICOS

- Analizar los activos de la empresa para identificar los riesgos y amenazas.
- Identificar riesgos y amenazas que se puedan presentar en la dependencia de sistemas.
- Realizar un análisis de gestión de riesgos a todos los procesos involucrados en el proyecto a partir de la metodología de Magerit.
- Establecer las políticas de seguridad que permitan minimizar los posibles riesgos a los que está expuesta la información de la empresa en la dependencia de sistemas.

4. MARCO REFERENCIAL

Es aquí donde se definen los conceptos importantes que se encuentran en el marco del trabajo, así como los referentes que aportaron en el desarrollo del mismo.

4.1 ANTECEDENTES

En este espacio se relacionan los trabajos que han sido importantes para el desarrollo del mismo, a continuación se mencionan:

Proyecto ***"Diseño de un SGSI basado en la norma ISO 27001 para la empresa Peñalosa cía. S.A.S. sede principal Cúcuta"*** presentado por Johanna Carolina Ararat Muñoz a la Universidad Nacional Abierta y a Distancia en el año 2018 para optar al título de Especialista en Seguridad Informática[1]. Este proyecto presenta la importancia que tiene un sistema de gestión de seguridad de la información, para la organización donde la seguridad de la información es considerada como una prioridad. Además evalúa la situación actual de seguridad de la información y se presenta una propuesta que permitirá ser apoyo a la organización para la implementación de un Sistema de Gestión de Seguridad de la Información. Este trabajo sirve como referente, dado que emplea la metodología Magerit para el análisis de riesgos a los que están expuestos los activos de información.

"Análisis de los riesgos de seguridad de la información de un aplicativo de gestión documental líder en el mercado colombiano." Esta tesis de grado se desarrolló en la ciudad de Bogotá, en donde se realizó un análisis de los riesgos de seguridad de la información de un aplicativo de gestión documental líder en el mercado Colombiano, determinando cuales son los riesgos de seguridad a los que se encuentra expuesta la información dentro del proceso y aplicativo de gestión documental, así como establecer el plan de tratamiento adecuado de dichos riesgos para controlarlos y reducirlos a niveles aceptables y asumibles para la

[1] ARARAT MUÑOZ, Johanna Carolina. Diseño de un sgsi basado en la norma iso 27001 para la empresa ma Peñalosa Cía. S.A.S. sede principal Cúcuta. Tesis de grado. Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas, Tecnología e Ingeniería, Programa de Especialización de Seguridad Informática. [en línea] [citado el 12 de septiembre 2018]. Disponible en https://repository.unad.edu.co/handle/10596/21259

entidad propietaria del software así como sus respectivos clientes. El presente proyecto se tiene como referencia para identificar, valorar, clasificar y tratar los activos de información utilizando la metodología Magerit. [2]

"Análisis y diseño de un Sistema de Gestión de Seguridad Informática en la Empresa Aseguradora Suárez Padilla & Cía. Ltda. Esta tesis de grado se desarrolló en la ciudad de Bogotá, en la Empresa Aseguradora Suárez Padilla & Cía. Ltda[3], en donde se realizó un diagnóstico de los riesgos críticos de la organización con base en la norma ISO 27001:2013. Los resultados obtenidos en el desarrollo del proyecto, fueron un compendio de Políticas asociadas con la seguridad de la información aplicados a la totalidad de los procesos internos y externos de la empresa. El presente proyecto referencia cómo se diseña un SGSI para una empresa y como se establecen las políticas de seguridad a implementar.

"Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor del Cauca". Esta tesis de grado se llevó a cabo en la Institución Universitaria Colegio Mayor del Cauca en la ciudad de Popayán Cauca[4], que cuenta con una infraestructura tecnológica en crecimiento y el desarrollo del proyecto se plantea realizar un análisis de riesgos con el fin de proponer controles de seguridad de la información. Como resultados obtenidos, se aplicó la metodología MAGERIT logrando desarrollarse todos los objetivos planteados, y se plantearon controles y políticas de seguridad de la información, como base para la implementación de un Sistema de Gestión de Seguridad de la Información. El presente proyecto se tiene como referente en cuanto a la identificación y clasificación de los activos de información, como se aplica la metodología Magerit, y las políticas de seguridad de información a implementar.

---

[2] Carmen Elizabeth Fajardo Diaz. Análisis de los riesgos de seguridad de la información de un aplicativo de gestión documental líder en el mercado colombiano, 2017.

[3] Suárez Padilla Sandra Yomay. Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez Padilla & Cía. Ltda, 2015.

[4] Caicedo Cuchimba Mildred, Perafán Ruiz John Jairo. Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor del Cauca, 2014.

4.2 MARCO CONCEPTUAL

A continuación se mencionan los diferentes conceptos que son importantes para el desarrollo de este trabajo:

4.2.1. Sistema de Gestión de la Seguridad de la Información SGSI

El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

4.2.2 ¿Qué es un SGSI?

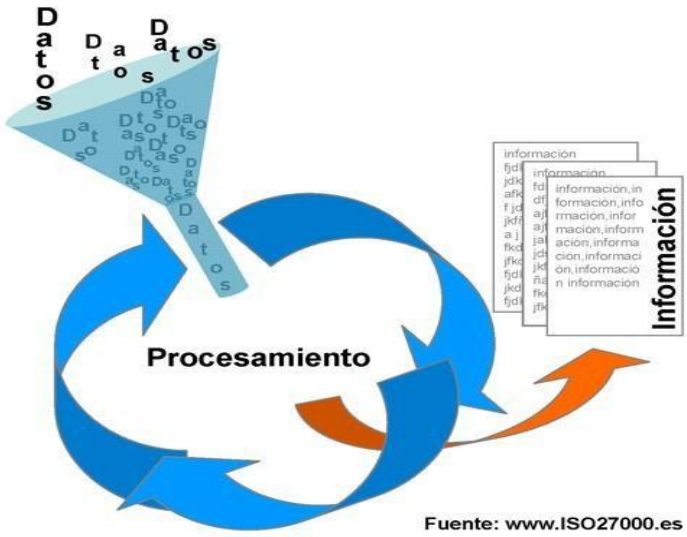
SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Según ISO 27001[5], la seguridad de la información y de los activos, consiste en la preservación de su confidencialidad, integridad y disponibilidad de los sistemas implicados en su tratamiento, dentro de una empresa, estos tres términos constituyen la base sobre la que se cimienta todo el pilar de la seguridad de la información:

[5]SGSI. Sistema de Gestión de Seguridad de la Información
ISO 27001. El portal de ISO 27001 en Español. [en línea] [citado el 12 de Octubre 2019]. Disponible en http://www.iso27000.es/iso27000.html

Figura 1. Información - SGSI[6]



- **Confidencialidad:** La información es confidencial y no se coloca a disposición ni se revela a individuos, entidades o procesos no autorizados.

- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

[6] Ibid., p. 2

Figura 2. Sistema de Gestión de Seguridad de la Información SGSI

Fuente: www.iso27000.es

4.2.3 ¿Para qué sirve un SGSI?

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas. El SGSI ayuda a establecer las políticas y procedimientos en relación a los objetivos del negocio, está orientado a garantizar la seguridad, integridad y confidencialidad de los datos de la organización. [7],

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una empresa. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

[7] Ibid., p. 2

4.2.4 ¿Qué incluye un SGSI?

En el ámbito de la gestión de la calidad según ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles. Es posible trasladar ese modelo a un Sistema de Gestión de la Seguridad de la Información basada en ISO 27001 de la siguiente forma:[8]

Figura 3. Que Incluye un SGSI

Fuente: WWW.ISO27000.ES

Documentos de Nivel 1

Manual de seguridad: Consiste en un documento el cual contiene la guía de cómo se debe implementar el sistema de gestión de seguridad de la información. En este documento se radica toda la información como alcance, responsables, objetivos, políticas, directrices, entre otras actividades.

Documentos de Nivel 2

Procedimientos: Corresponde a las actividades operativas, serán los encargados de asegurar que los procedimientos sean realizados de forma eficaz, la planificación, la operación y el control de los procesos sean los adecuados.

[8] Ibid., p. 2

Documentos de Nivel 3
Instrucciones: Documento que describe pasó a paso como se deben realizar las tareas y las actividades que se deben cumplir.

Documentos de Nivel 4
Registros: Corresponde a la evidencia documentada de la información en el cumplimiento de la gestión del SGSI. [9]

De manera específica, ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio):

- **Alcance del SGSI:** Ámbito de la organización que queda sometido al Sistema de Gestión de Seguridad de la Información donde se definirá el alcance que se lograra una vez empiece en marcha el sistema, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas para su implementación.

- **Política y objetivos de seguridad:** Documento que establece el compromiso de la alta dirección y el enfoque de la empresa en la gestión de la seguridad de la información.

- **Procedimientos y mecanismos de control:** Procedimientos de control que regulan el propio funcionamiento del SGSI.

- **Enfoque de evaluación de riesgos:** Describe la metodología a emplear para determinar cómo se evaluaran las amenazas, vulnerabilidades, probabilidades e impactos en relación a los activos de información contenidos dentro del alcance seleccionado.

- **Informe de evaluación de riesgos:** Corresponde al resultado de aplicar la metodología de evaluación seleccionada para el estudio de los activos de información de la organización.

[9] Ibid., p. 2

- **Plan de tratamiento de riesgos**: Consiste en seleccionar y aplicar las medidas más eficientes para gestionar los controles y evaluar los riesgos de seguridad de la información en la organización.

- **Procedimientos documentados**: Todo lo necesario para garantizar la planificación, operación y control de los procesos de seguridad de la información en la organización, así como la eficacia de los controles implantados.

- **Registros**: Documentos donde se evidencia la conformidad con los requisitos y el funcionamiento eficaz del Sistema de Gestión de Seguridad de la Información.

- **Declaración de aplicabilidad**: Documento que contiene los objetivos de control y los controles establecidos por el SGSI, basado en los resultados obtenidos en los procesos de evaluación y tratamiento de riesgos.

Control de la documentación

Para los documentos generados se debe establecer, documentar, implantar y mantener un procedimiento que defina las acciones de gestión necesarias para:[10]

- Aprobar documentos apropiados antes de su emisión
- Revisar y actualizar documentos cuando sea necesario y renovar su validez
- Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.
- Garantizar que las versiones relevantes de documentos vigentes están disponible en los lugares de empleo.
- Garantizar que los documentos se mantienen legibles y fácilmente identificables.
- Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su

[10] Control de documentación SGSI ISO 27001. [en línea] [citado el 12 de Octubre 2019]. Disponible http://www.iso27000.es/download/doc_sgsi_all.pdf

clasificación.

- Garantizar que los documentos procedentes del exterior están identificados.
- Garantizar que la distribución de documentos está controlada.
- Prevenir la utilización de documentos obsoletos.
- Aplicar la identificación apropiada a documentos que son retenidos con algún propósito.

4.2.5 ¿Cómo se implementa un SGSI?

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión.

Figura 4. Ciclo continuo PDCA - SGSI

Fuente: www.iso27000.es

- Planificar: Corresponde a la fase de planificación de los controles a establecer el SGSI.
- Hacer: Es la fase de implementar y utilizar el SGSI.
- Verificar: Es la fase de monitorizar y revisar el SGSI.
- Actuar: Esta fase corresponde en mantener y mejorar el SGSI.

5.2.6 Establecer el SGSI

Esta etapa comprende el definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.[11]

Además de definir una política de seguridad que: Incluya el marco general y los objetivos de seguridad de la información de la organización; considere requerimientos legales o contractuales relativos a la seguridad de la información; esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI; establezca los criterios con los que se va a evaluar el riesgo; y esté aprobada por la dirección.

Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos de la organización, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles; existen numerosas metodologías estandarizadas para la evaluación de riesgos, aunque es perfectamente aceptable definir una propia.

- **Identificar los riesgos:** Consiste en Identificar los diferentes activos que están dentro del alcance del SGSI; identificar las amenazas y vulnerabilidades en relación a los activos de igual manera los impactos en la confidencialidad, integridad y disponibilidad de los activos.

- **Analizar y evaluar los riesgos:** Consiste en analizar y evaluar los fallos de seguridad que provoquen la pérdida de confidencialidad, integridad o disponibilidad de la información; evaluar la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos de información y los controles que ya estén implementados; estimar los niveles de riesgo; determinar los criterios de aceptación del riesgo, si es aceptable o necesita ser tratado.

[11] SGSI, en base a ISO 27001: se utiliza el ciclo continuo PDCA, 2005. [en línea] Disponible en. http://www.iso27000.es/sgsi_implantar.html

Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:

- Aplicar los controles necesarios según la necesidad de la organización; aceptar el riesgo siempre y cuando se cumplan las políticas y criterios establecidos para la aceptación de los riesgos.

Figura 5. Gestión de Riesgos

Fuente: www.iso27000.es[12]

- Seleccionar los controles y los objetivos de control de la norma ISO 27001 para el tratamiento del riesgo cumpliendo con los requerimientos establecidos en el proceso de evaluación del riesgo.

- Aprobación de la alta dirección los riesgos residuales como la implantación y uso del Sistema de Gestión de Seguridad de la Información.

[12] ISO 27001. El portal de ISO 27001 en Español. 2005. [en línea] Disponible en. Obtenido de http://www.iso27000.es/iso27000.html

- Definir los lineamientos que incluya: Los objetivos de control y controles seleccionados y que actualmente ya están implantados; los objetivos de control y controles excluidos.

- EL estándar ISO 27002 proporciona una completa guía de buenas prácticas que contiene 133 controles, de los cuales 39 objetivos de control agrupados en 11 dominios. Esta norma es referenciada en ISO 27001.

5.2.7 Implementar y utilizar el SGSI

A continuación se describe los pasos a tener en cuenta al momento de implementar y utilizar el SGSI en una empresa.[13]

- Definir un plan de tratamiento de riesgos de seguridad de la información que permita identificar los recursos, acciones, responsabilidades y prioridades en la gestión de los mismos.

- Implementar el plan de tratamiento de riesgos, con el objetivo de alcanzar los controles identificados, incluyendo responsabilidades, asignación de recursos y prioridades.

- Implementación de los diferentes controles seleccionados que conlleven a los objetivos establecidos.

- Establecer y definir un sistema de gestión, que permita obtener resultados comparables y eficientes para medir la eficacia de los controles.

- Implementación de programas de capacitación y formación a todo el personal sobre la seguridad de la información.

- Gestionar las operaciones del Sistema de Gestión de Seguridad de la Información.

- Gestionar los recursos asignados al Sistema de Gestión de la Seguridad de

[13] Sistema de Gestión de la Seguridad de la Información ISO 27001. 2005. [en línea] Disponible en. Fuente: http://www.iso27000.es/download/doc_sgsi_all.pdf

la Información para garantizar la seguridad de la información.

- Implementar controles y procedimientos que garanticen una rápida respuesta a los problemas de seguridad que se puedan presentar en cada una de las partes implicadas.

- Establecer por medio de la medición la efectividad de los controles establecidos para garantizar que estos cumplan con lo establecido para garantizar la seguridad en la empresa.

- Realizar revisiones periódicas sobre las evaluaciones de riesgos y sus niveles aceptables sobre los cambios presentados en la empresa, los controles, amenazas, objetivos, procesos del negocio, entre otros.

- Realizar la planificación periódica de las auditorías internas del Sistema de Gestión de Seguridad de la Información.

- Revisar periódicamente el Sistema de Gestión de Seguridad de la Información por parte de la alta dirección con el objetivo de garantizar que el alcance definido sea el más adecuado y que las mejoras en los procesos del SGSI sean evidentes.

- Actualizar los planes de seguridad de acuerdo a los hallazgos encontrados durante las actividades de monitorización y revisión del SGSI.

- Registrar acciones y eventos que puedan haber impactado sobre el rendimiento del Sistema de Gestión de Seguridad de la Información.

- Establecer, mantener, operar, implementar, monitorizar revisar, y mejorar el SGSI. [14]
- Revisar y monitorizar el correcto funcionamiento de lo que se ha planificado en el Sistema de Gestión de Seguridad de la Información.

- Mantener y mejorar de manera continua el Sistema de Gestión de

[14] Sistema de Gestión de la Seguridad de la Información ISO 27001. 2005. [en línea] Disponible en. Fuente: http://www.iso27000.es/download/doc_sgsi_all.pdf

Seguridad de la Información, adoptando las medidas preventivas y correctivas en función de los resultados obtenidos.

5.2.8 ¿Qué tareas tiene la Gerencia en un SGSI?

La importancia de la alta dirección juega un papel muy importante para la toma de decisiones y las acciones que se puedan llevar a cabo en la implementación y puesta en marcha del SGSI en la organización.

Compromiso de la dirección

La dirección de la organización debe comprometerse con el establecimiento, operación, implementación, revisión, monitorización, mantenimiento y mejora del SGSI. Para ello, debe tomar las siguientes iniciativas:

- Establecer una política de seguridad de la información, asegurando de que se establezcan los objetivos y planes de mejora en el SGSI, Estableciendo roles y responsabilidades de seguridad de la información.

- Comunicar a la organización tanto la importancia de lograr los objetivos de seguridad de la información y de cumplir con la política de seguridad, como sus responsabilidades legales y la necesidad de mejora continua.

- Asignar suficientes recursos al SGSI en cada una de sus fases. Decidir los criterios de aceptación de riesgos y sus correspondientes niveles.

- Realizar revisiones del SGSI y asegurar que se realicen auditorías internas,

Asignación de recursos

Para el correcto desarrollo de todas las actividades relacionadas con la implementación del Sistema de Gestión de Seguridad de la Información, es Imprescindible la asignación de recursos y responsabilidad garantizar que esto sea cumplido por parte de la alta dirección.

- Establecer, monitorizar, operar, implementar y revisar el Sistema de Gestión de Seguridad de la Información.

- Mejorar y mantener la eficacia del Sistema de Gestión de Seguridad de la Información donde sea necesario.

- Se debe garantizar que los procedimientos de seguridad de la información en la organización apoyen los requerimientos del negocio.

- Identificar cada uno de los requerimientos legales y normativos, así como las obligaciones de seguridad.

- Aplicar los controles establecidos correctamente, permitiendo mantener de esa forma la seguridad de la información.

- Realizar las respectivas revisiones cuando sea necesario y actuar adecuadamente según los resultados de las mismas.

Importancia de una Metodología de análisis de riesgo dentro de un SGSI

La importancia de implementar una metodología de análisis del riesgo es crucial para el desarrollo y operación de un Sistema de Gestión de la Seguridad de la Información en una empresa, la utilización de una metodología ayuda en forma estructurada a evaluar, identificar, controlar y valorar posibles problemas que podrían surgir en la organización, también conocidos como riesgos.

Es la forma apropiada para identificar riesgos y tomar decisiones sobre cómo gestionarlos o eliminarlos.

El propósito de una metodología para el análisis de riesgos según la norma internacional ISO 3001. Corresponde al proceso de identificar, analizar, y evaluar la efectividad de los criterios del riesgo que puedan surgir durante la ejecución de un proceso específico en una organización; este nuevo estándar utiliza cuatro pasos básicos para su análisis como son la Identificación de riesgos, análisis de riesgos, valoración de riesgos y tratamiento de riesgos llevando a cabo un proceso de evaluación de riesgos exitoso.

5.3 MARCO CONTEXTUAL

5.3.1 Nombre de la Empresa

QWERTY S.A.

5.3.2 Reseña Histórica

La Empresa QWERTY S.A. es una empresa del sector tecnológico que busca el Desarrollo tecnológico en comunidades colombianas a través del uso de tecnologías de información. Adicionalmente QWERTY S.A. ofrece soluciones concretas para lograr la mayor productividad informativa con los costos más pequeños, optimizando el presupuesto disponible.

Gracias a la experiencia de varios años de los miembros del personal en la gestión de pequeñas y medianas empresas y a un profundo conocimiento de las últimas TIC (Tecnologías de la información y comunicación), Qwerty SA puede analizar procesos de negocios, sugerir soluciones y desarrollar estrategias.

Actualmente cuenta con 120 colaboradores entre directivos, administrativos y operativos.

5.3.3 MISION

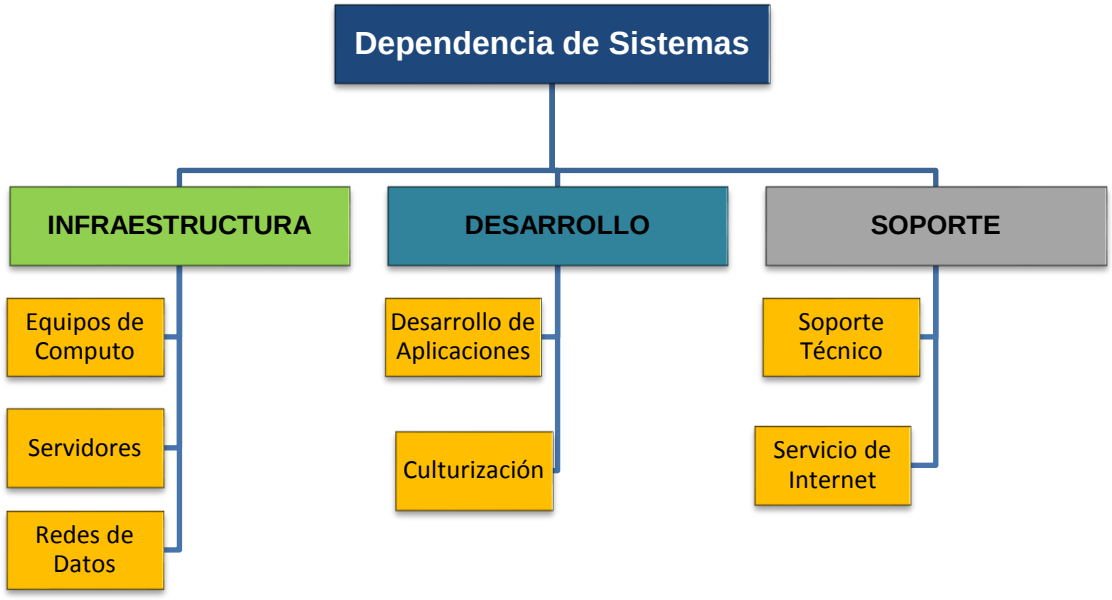
Mantener con eficiencia, efectividad y calidad total el liderazgo como la mejor Compañía de Servicios tecnológicos en Colombia; con el fin de satisfacer las necesidades de cada uno de los clientes ofreciéndoles soluciones seguras, confiables y con los más altos estándares de calidad.

5.3.4 VISION

Para el año 2025 seremos una empresa líder en el sector tecnológico, caracterizándose por ser un referente en el mercado por la calidad en la prestación de servicios, enfocándose en la satisfacción de los clientes a través de la adopción de tecnologías con los más altos estándares de calidad internacional, pero sin olvidar el componente humano, pieza fundamental para el crecimiento de la organización.

Por lo anterior, se muestra la estructura organizativa del centro de estudios, el cual cuenta con una dependencia de sistemas que brinda soporte a la infraestructura tecnológica 24/7, como se muestra en la figura 7.

Figura 6. Infraestructura Tecnológica QWERTY S.A



Fuente: Propia del Autor

En la **Figura 7.** Se presenta la estructura organizacional de la empresa, la cual consta de un centro de apoyo denominado Dependencia de Sistemas de Información que provee la infraestructura y procesos para brindar los servicios tecnológicos necesarios para cumplir las tareas académicas y administrativas de la empresa como son el desarrollo y soporte.

Las Funciones de las áreas son las que se enuncian a continuación en la tabla 1.

Tabla 1. Departamento de sistemas QWERTY S.A

AREAS	FUNCIONES
Área de Infraestructura	• Soporte al acceso a la red interna y a internet. • Revisión de diseños de cableado estructurado
Área de desarrollo	• Apoyo técnico a las dependencias de la organización del centro en desarrollo de medios eficientes para lograr actividades basadas en usos de tecnologías de la informática y las telecomunicaciones.
Área de Soporte	• Mantenimiento de computadores (sólo equipos propiedad del Centro). • Generación de conceptos técnicos para tramitar baja de equipos. • Realizar copias de seguridad de los sistemas de información y servidores virtuales que se encuentran en las dependencias de la empresa QWERTY S.A.

Fuente. Autoría

A continuación se realiza la descripción de las funciones de cada cargo relacionado con el departamento en mención:

Jefe de Sistemas: planear, coordinar, evaluar y controlar los procesos al interior

de la oficina de tecnología liderando el direccionamiento tecnológico con relación a los requerimientos de la institución y frente a los avances tecnológicos.

Ingenieros de Soporte: brindar soporte a los usuarios con equipos de cómputo de la institución.

Coordinador de Infraestructura: realizar propuestas e investigaciones en materia de infraestructura tecnológica y sistematización que garanticen la prestación de los servicios tecnológicos de la institución.

Administrador de Bases de Datos (DBA):

- Administrar la estructura de la Base de Datos
- Administrar la actividad de los datos
- Administrar el Sistema Manejador de Base de Datos
- Establecer el Diccionario de Datos
- Asegurar la confiabilidad de la Base de Datos
- Confirmar la seguridad de la Base de Datos

Administrador de Servidores:

- Controles de los sistemas y programas informáticos.
- Realizar copias de seguridad de datos.
- Aplicar actualizaciones del sistema operativo, y los cambios de configuración.
- Instalación y configuración de nuevo hardware / software.
- Añadir / borrar / modificar información de cuenta de usuario, restablecer contraseñas, etc.
- Respuesta a consultas de carácter técnico.
- Responsable de la seguridad.
- Documentar la configuración del sistema.
- Afinar el rendimiento de los sistemas.
- Mantener la red funcionando.

Administrador de redes:

- Diseño y planificación
- Configuración
- Mantenimiento
- Expansión de la red.

Coordinador de Desarrollo: se encarga de elaborar los planes de desarrollo involucrando a los implementadores y sus actividades, de tal manera que se puedan ejecutar los planes de los proyectos y con sus objetivos planteados para cada una de las fases del mismo.

Desarrolladores de Aplicaciones: llevar a cabo los mantenimientos, actualización, atención a nuevos requerimientos de los sistemas de información. Desarrollar software propuestos por la institución de acuerdo con los requerimientos expuestos en los casos de uso.

Coordinador Soporte: encargado de planear, organizar y mantener la operación arriba de todos los sistemas de información y equipamiento de cómputo de todas las áreas de la institución permitiendo el uso adecuado de toda la red computacional de la institución.

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

Asistencia para directivos, administrativos y operativos:

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

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

Apoyo en la gestión y mantenimiento de activos informáticos: servicio que cumple la función de mantener en optimo desempeño servicios tecnológicos como:

- Equipos de cómputo de escritorio, móviles y servidores,

televisores, video proyectores.

- Software operativo y aplicativo.
- Servicio de Internet.
- Todo el equipamiento que se requiera para ayudar a dar cumplimiento al objeto social.

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

- Correo electrónico.
- Sistema de gestión de calidad.

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

- Generación de nómina de trabajadores
- Generación de recibos de pago
- Creación, alimentación y custodia de Hojas de vida
- Control del seguimiento al talento humano
- Generación certificados laborales y relacionados con el modelo de negocio

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

5.4 MARCO LEGAL

Protección de la Información. En Colombia la ley 1273 de 2009 *"por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"*.[15]
El cual penaliza los delitos de tipos informáticos, debido a la necesidad de legislar y garantizar medidas frente a las nuevas tecnologías de la información que están relacionadas con cada ámbito de la actualidad, desde empresas hasta personas naturales, se destacan algunos de los artículos que comprende:

Artículo 269A. Acceso abusivo a un sistema informático: Sin importar el tipo de seguridad presente en un sistema de información, cualquier ingreso sin autorización o permanencia en contra de la voluntad de quien tenga el derecho legítimo a excluirlo es considerado un delito.

Artículo 269D. Daño informático: Llevar a cabo cualquier tipo de acción que incida de forma negativa en un sistema informático, bien sea a los datos que transitan o se almacenan atentando contra la integridad de la información disponibles, es considerado un delito.

Artículo 269E. Uso de software malicioso: El uso, implementación y distribución de cualquier software que pueda generar daños en sistemas de información, atentando contra la disponibilidad, integridad y confidencialidad de la información es considerado un delito.

[15] COLOMBIA. SENADO DE LA REPÚBLICA. Ley 1273. SENADO DE LA REPUBLICA. Ley 1273 de 2009. [en línea] [citado el 10 de Abril 2019]. Disponible en internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.htm

Artículo 269F. **Datos personales**: sin importar el medio de obtención, la sustracción de cualquier tipo de datos personales de un sistema informático sin la autorización pertinente de sus propietarios es considerada un delito.

Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data que se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Esta ley se refiere al que todo individuo puede conocer, actualizar y rectificar toda información que se relacione con él, la cual se encuentra almacenada en centrales de información.

Ley 1341 de 2009. La presente ley determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información.

A continuación se darán a conocer los siguientes modelos y estándares a tener en cuenta por la empresa QWERTY S.A para su proceso de análisis y gestión de riesgos.

ISO/IEC 27000 series: La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

ISO 27000: Contiene términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido. [16]

ISO 27001 Es la norma principal de la serie y contiene los requisitos del Sistema de Gestión de Seguridad de la Información. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI.

ISO 27002: Desde el 1 de Julio de 2007. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a Seguridad de la Información. No es certificable.

ISO 27003: Consiste en una guía de implementación de SGSI e información acerca del uso del modelo PDCA (Plan, Do, Check, Act) y de los requerimientos de sus diferentes fases.

ISO 3001. Es una norma internacional para gestionar el riesgo de las organizaciones; esta norma fue publicada en el año 2009 por la Organización Internacional de Normalización (ISO) en colaboración con la Comisión Electrotécnica Internacional (IEC) tiene por objetivo que organizaciones de todos los tamaños y tipos puedan gestionar los riesgos en la empresa de forma efectiva.

Ley 1581 de 2012. Ley estatutaria para la protección de datos personales busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones por parte de entidades de naturaleza pública y privada.

---

16 Ibid., p. 2

6. METODOLOGIA

Para desarrollar los objetivos propuestos en el proyecto aplicado, la metodología a implementar enmarca las fases de análisis y diseño, donde cada etapa corresponde a una serie de actividades encaminadas a lograr el alcance y los resultados del proyecto, las cuales se describen a continuación.

Fase 1: Análisis de los activos de la empresa QWERTY S.A para identificar los riesgos y amenazas enmarcadas en las áreas de Infraestructura, Desarrollo y Soporte.

Fase 2: Análisis de gestión de riesgos a los procesos involucrados en el proyecto a partir de la metodología de Margerit.

Fase 3: Definir las políticas de seguridad que permitan minimizar los posibles riesgos a los que está expuesta la información de la empresa en cada área.

6.1 Marco Metodológico

El desarrollo del proyecto aplicado comprende una serie de fases y actividades definidas que permiten cumplir con el objetivo del proyecto.

El proyecto está encaminado al diseño de un SGSI a la empresa QWERTY S.A bajo la norma ISO/IEC 27001 que permita definir políticas de seguridad orientadas a la disminución de riesgos para la información en cada una de las áreas que la conforman.

El objetivo de aplicar una metodología para el análisis de gestión de riesgos a todos los procesos involucrados es poder identificar y contrarrestar los riesgos a los cuales están expuestos los activos de información de la empresa QWERTY S.A, para llevar a cabo este tipo de análisis se va a realizar un estudio de las diferentes metodologías para poder seleccionar la más adecuada.

6.2 Tipo de Investigación

El desarrollo del proyecto aplicado realizado a la empresa QWERTY S.A se realizó bajo la metodología de tipo cuantitativa y descriptiva, ya que se pretende hacer la medición de los activos, vulnerabilidades, amenazas, impactos y probabilidades, y a su vez definir el nivel de aceptación del riesgo en cuanto a la confidencialidad, integridad y disponibilidad de la información.

Desarrollo metodológico de las fases correspondientes a los objetivos:

Para lograr el desarrollo de los objetivos del proyecto se realizaron las siguientes acciones, el cual se especificarán de manera detallada en el desarrollo de las fases:

- Identificación, clasificación y valoración de los activos de la empresa QWERTY S.A asociados al análisis de riesgos, empleando el modelo de clasificación descrito en la metodología MAGERIT versión 3.0 Libro II – Catalogo de elementos.

- La metodología a emplear para realizar el respectivo análisis de gestión de riesgos a los procesos involucrados en la empresa QWERTY S.A, es la Metodología de Análisis y Gestión de Riesgos de los sistemas de información MAGERIT versión 3.0 descrita en el libro I – Método.

- Análisis de gestión de riesgos de seguridad de la información aplicando la metodología seleccionada a los procesos involucrados.

- Valoración y evaluación de los riesgos de seguridad de la información en la empresa QWERTY S.A en términos de probabilidad de ocurrencia e impacto.

- Diseño del plan de tratamiento de riesgos orientado a salvaguardar la integridad, disponibilidad y seguridad de la información de los activos de la empresa.

- Diseño de la política de seguridad de la información para la organización.

No obstante, cada uno de los objetivos propuestos se desarrolló mediante la ejecución de las siguientes fases:

Fase 1

Análisis de los activos de la empresa para identificar los riesgos y amenazas enmarcadas en las áreas de Infraestructura, Desarrollo y Soporte.

6.3.1 IDENTIFICACION, CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS SEGÚN LA METODOLOGIA SELECIONADA

Los Activos son los recursos del sistema de información, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por la dirección.[17]

Para realizar el análisis de riesgos de seguridad de la información se hizo una revisión de algunas de las metodologías existentes, para poder seleccionar aquella que mejor se adapte a los requerimientos de la empresa.

Una metodología de análisis de riesgos en Seguridad de la Información es una guía paso a paso que permite la aplicación de técnicas, obtener resultados para la toma de decisiones en el momento de implementar controles que minimicen el riesgo al que están expuestos los activos de información para una empresa.

Las metodologías que se analizaron fueron las siguientes:

1. MAGERIT
2. OCTAVE
3. ISO/IEC 27005
4. MEHARI
5. CORAS
6. NIST SP 800-30

[17] MAP - Metodología MAGERIT Versión 1.0
Fuente: http://dis.um.es/~barzana/Curso03_04/MAGERIT.pdf

Tabla 2. Ventajas y desventajas de metodologías de análisis de riesgos

Metodologías de gestión de Riesgos	Ventajas	Desventajas
MAGERIT	Es una de las metodologías más completas, tanto en el análisis como en la gestión de riesgos, es de carácter público, permite un análisis completo en lo referente a Recursos de Información, Amenazas y tipo de Activos.	No involucra a los procesos, recursos ni vulnerabilidades como elementos del modelo a seguir. No posee un inventario completo en lo referente a Políticas.
OCTAVE	Es una metodología auto dirigida, Comprende los procesos de análisis y gestión de riesgos, involucra a todo el personal de la entidad. Se considera de las más completas, ya que involucra elementos de análisis: procesos, activos y dependencias, recursos, vulnerabilidades, amenazas y salvaguardas.	Usa muchos documentos anexos para llevar a cabo el proceso de análisis de riesgos, lo que la hace complicada de entender. No explica en forma clara la definición y determinación de los activos de información.
ISO/IEC 27005	Es un Estándar Internacional, está orientada a la monitorización y revisión de riesgos, se la considera con un alcance completo, tanto en el análisis como en la gestión de Riesgos.	No posee herramientas, técnicas, ni comparativas de ayuda para su implementación, No detalla la forma de valorar las amenazas.
MEHARI	Usa un modelo de análisis de riesgos cualitativo y cuantitativo. Por medio de esta metodología	Integra los principios de confidencialidad, integridad y disponibilidad de la información como objetivos de seguridad, dejando a un lado el no repudio.

	se detectan vulnerabilidades mediante el uso de auditorías y se analizan los riesgos.	
CORAS	Provee un repositorio de paquetes de experiencias reutilizables. Provee un reporte de las vulnerabilidades encontradas. Útil en el desarrollo y mantenimiento de nuevos sistemas. Basada en modelos de riesgos de sistemas de seguridad críticos.	No realiza análisis de riesgos cuantitativos. En su modelo no tiene contemplados elementos como los procesos y las dependencias.
NIST SP 800 – 30	Tiene un bajo costo, comparado el riesgo mitigado y la aplicación de esta. Se destaca por la gestión de riesgos en Proyectos TI, basándose en la confidencialidad, integridad y disponibilidad de la información.	Al igual que CORAS, No es totalmente completa al dejar de lado elementos importantes como los procesos, las dependencias y los activos. Al ser tan robusta, resulta tediosa la aplicación de esta metodología para pequeñas empresas.

Fuente: M. C. Duarte Monografía: Diseño de políticas de Seguridad de la Información para la Unidad de Tecnología de la Cámara de Comercio de Cúcuta. Publicaciones e investigaciones, p. 41 – 43 2019

Basados en las ventajas y desventajas reflejadas en la tabla anterior se seleccionan las siguientes características descriptivas comunes que permiten analizar y comparar la aplicación de cada metodología a este caso en específico.[18]

18

- **Ámbito de aplicación:** Corresponde al tipo de organización a la cual está especialmente dirigida la metodología a emplear.

- **Costo de Implementación:** Se considera si la metodología implica altos costos a la empresa para su implementación y ejecución.

- **Disponibilidad de profesionales entrenados**: Hace referencia a la facilidad para conseguir documentación específica, profesionales entrenados en cada área y proyectos similares en Colombia.

- **Licenciamiento:** Se determina si la metodología implementada implica la adquisición de una licencia para su utilización.

- **Incluye recomendaciones para los controles de seguridad:** La metodología establecida incluye recomendaciones de controles o salvaguardas de los activos de información de la empresa.

- **Incluye análisis cuantitativo**: La metodología permite un análisis tanto cuantitativo como cualitativo para su respectivo análisis.

Para la evaluación se asignó un peso a estas características, siendo 3 la ponderación más alta, y 1 la más baja. Analizando estas características para las metodologías seleccionadas, se obtiene el siguiente cuadro:

Fuente: M. C. Duarte Monografía: Diseño de políticas de Seguridad de la Información para la Unidad de Tecnología de la Cámara de Comercio de Cúcuta. Publicaciones e investigaciones, p. 41 – 43 2019

Tabla 3. Evaluación de metodologías de análisis de riesgos

Metodología (de 1 a 3 / 3 es mejor)							
Característica	Importancia (1 a 3 / 3 es mayor peso)	**Octave**	**Magerit**	**Mehari**	**NISP 800-30**	**ISO/IEC 27005**	**CORAS**
Ámbito de aplicación	3 x	3	3	3	2	3	3
Costo de implementación	3 x	2	3	3	3	3	3
Simplicidad en la documentación	2 x	1	2	2	2	2	1
Disponibilidad de profesionales entrenados	3 x	1	3	2	2	2	1
Licenciamiento	3 x	1	3	3	3	3	2
Incluye recomendaciones para los controles	2 x	3	3	1	3	2	2
Incluye análisis cuantitativo	2 x	3	3	3	3	3	3
Total:		**14**	**20**	**17**	**18**	**18**	**15**

Fuente: Propia

La puntuación más alta, que se obtiene de la sumatoria del puntaje de cada característica multiplicado por la importancia de la misma, la obtiene la metodología Magerit, y se selecciona ésta como la metodología para hacer el análisis de riesgos a la empresa QWERTY S.A, el cual permitirá desarrollar la clasificación de los activos identificados en la empresa QWERTY S.A empleando la metodología MAGERIT, la cual propone el siguiente modelo de clasificación.

Tabla 4. Clasificación de los activos definida en la metodología MAGERIT. (Gobierno de España, 2012, p8)

CATEGORÍA DEL ACTIVO	DESCRIPCIÓN DE LOS POSIBLES ACTIVOS
[D] Datos e información	La información se caracteriza por ser el activo más importante que le permite a la organización prestar sus servicios. Su forma de almacenamiento puede ser digital o físico y se puede ver representada en ficheros, copias de respaldo, datos de gestión interna, credenciales, datos de validación de credenciales, datos de control de acceso, registro de actividad, códigos fuente, código ejecutable, etc.
[K] Claves criptográficas	Es empleada para proteger o autenticar el secreto de los datos. Las claves criptográficas, son indispensables para garantizar el funcionamiento de los mecanismos criptográficos.
[S] Servicios	Contempla los servicios prestados por el sistema que satisfacen la necesidad de los usuarios. Dentro de los cuales se pueden encontrar correo electrónico, almacenamiento de ficheros, gestión de identidades, gestión de privilegios, acceso remoto, etc.
[SW] Software - Aplicaciones Informáticas	Se caracterizan porque gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios. Dentro de la clasificación se puede relacionar desarrollo propio, desarrollo a medida, aplicaciones ofimáticas, sistemas operativos, antivirus, etc.
[HW] Equipamiento Informático	Brindan soporte directo o indirectamente a los servicios que presta la organización, siendo repositorios temporales o permanentes de datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesamiento o transmisión de datos. Dentro de esta clasificación se relaciona todo el hardware de la red como dispositivos de red, servidores, host y periféricos.

[COM] Redes de comunicaciones	Se centran en los medios de transporte que llevan datos de un sitio a otro. Las redes pueden ser propias o contratadas a terceros. Se relacionan las redes LAN, Internet, redes inalámbricas, etc.
[Media] Soportes de información	Se consideran dispositivos físicos que permiten almacenar información de forma permanente o durante periodos de tiempo como discos físicos y virtuales, memorias USB, CD-DVD, etc.
[AUX] Equipamiento auxiliar	Infraestructura que sirve de soporte a los sistemas de información, sin estar directamente relacionados con los datos como fuentes de alimentación, UPS, equipos de climatización, cableado, mobiliario, equipos de destrucción de soportes de información, suministros esenciales, etc.
[L] Instalaciones	Relaciona los lugares donde se hospedan los sistemas de información y comunicaciones. Ej. Edificios, oficinas, instalaciones de respaldo.
[P] Personal	Involucra el personal relacionado con los sistemas de información como pueden ser los usuarios internos, externos, operadores, administradores del sistema, desarrolladores, etc.

Fuente: Magerit 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos

ANÁLISIS DE ACTIVOS

Estas 10 categorías de Activos se articulan como las 10 capas principales en el diseño de la seguridad, desde el punto de vista de las repercusiones en 'cadena' de los problemas de seguridad de unos Activos sobre otros.[19] Entre ellos están:

Tabla 5. Tipo de Activos Metodología Margerit

ACTIVOS	DESCRIPCIÓN
[D] **DATOS**	Copias de Respaldo, datos de control de acceso, código fuente.
[K] **CLAVES CRIPTOGRAFICAS**	Claves privadas de firmas.
[S] **SERVICIOS**	Página Web, Correo electrónico.
[SW] **SOFTWARE**	Sistemas operativos, Sistemas aplicativos, Antivirus.
[HW] **EQUIPAMENTO INFORMÁTICO**	Equipos de escritorio, Equipos móviles, Enrutadores.
[COM] **REDES DE COMUNICACIONES**	Red telefónica, Alámbrica, Inalámbrica, Telefonía, Internet.
[Media] **SOPORTE DE INFORMACIÓN**	Discos de almacenamiento de información.
[AUX] **EQUIPAMENTO AUXILIAR**	Fuentes de alimentación, Equipos de climatización, de destrucción.
[L] **INSTALACIONES**	Oficinas, Edificios, Vehículos.
[P] **PERSONAL**	Usuarios internos, Externo, Administradores Todos los trabajadores de la empresa.

Fuente: libro II-MAGERIT- catálogo de elementos

[19] MAP - Metodología MAGERIT Versión 1.0 [en línea] Disponible en. http://dis.um.es/~barzana/Curso03_04/MAGERIT.pdf

A partir de lo anterior, se realiza un inventario e identificación, ubicación y responsable de cada activo a partir del alcance determinado para el departamento de sistemas, alineando a la metodología Magerit, como se observa en la siguiente tabla:

Tabla 6. Identificación de Activos

CATEGORÍA DEL ACTIVO	NOMBRE DEL ACTIVO	Cantidad	Descripción del Activo	Ubicación	Área	Responsable
Tipo: [D] Datos	Base de datos	1	Datos almacenados sistemáticamente para su posterior uso.	Data center	Departamento de Sistemas	Ingeniero de Sistemas
	Backups de Respaldo	1				
	Backups de bases de datos	1				
Tipo: [S] Servicios	Página Web	1	Servicio contratado con la empresa Godaddy.com.	Empresa Godaddy	Área de Desarrollo	Jefe de sistemas
	Correo Electrónico	1	Servicio de mensajería que permite a los usuarios enviar y recibir mensajes.	Empresa QWERTY S.A	Área de Desarrollo	Jefe de sistemas
Tipo: [SW] Software	Windows 10 Pro	18	Sistema Operativo que proporciona los programas a las computadoras de la empresa	Oficina de Registro y Control - Sala de Internet	Departamento de Sistemas	Jefe de sistemas
	Antivirus	18	Programa que permite detectar y eliminar virus informáticos.	Equipos de Computo	Departamento de Sistemas	Jefe de sistemas

Tabla 6. (Continuación)

CATEGORÍA DEL ACTIVO	NOMBRE DEL ACTIVO	Cant	Descripción del Activo	Ubicación	Área	Responsable
Tipo: [HW] Equipamiento Informático	Servidor de Impresión	1	Impresora HP LaserJet Enterprise serie 600, Permite la concurrencia de hasta 25 usuarios y el volumen mensual de impresión es de 200 a 25000 páginas	Oficina de nómina y facturación Dependencia directiva y administrativa	Área de Infraestructura y Desarrollo	Jefe de sistemas
	Servidor de Archivos FTP	1	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.	Oficina antigua de sistemas	Área de Infraestructura y Desarrollo	Jefe de sistemas
	Servidor DHCP	1	Servidor que asigna y administra de forma dinámica el direccionamiento dentro de la organización.	Data center	Departamento de Sistemas	Administrador de Redes
	Servidor de Nomina y Facturación	1	Plataforma de desarrollo propio. Tiene como función el almacenamiento y la administración de la nómina y facturación de la empresa QWERTY S.A.	Empresa QWERTY S.A	Nómina y Facturación	Jefe de sistemas
	Equipos de Computo	18	Dispositivo electrónico para uso laboral	Sala de Computo	Departamento de Sistemas	Ingeniero de Sistemas
	Cortafuegos - Firewall	1	Sistema de seguridad que está protegiendo a la red de datos, de intrusiones que se puedan presentar en la red	Data center	Departamento de Sistemas	Ingeniero de Redes
	Teléfonos IP	6	Sistema de comunicación a través de teléfonos Voz IP, que comunica las oficinas y departamentos del centro.	Dependencias del centro	Departamento de Sistemas	Coordinador de Infraestructura

Tabla 6. (Continuación)

CATEGORÍA DEL ACTIVO	NOMBRE DEL ACTIVO	Cant	Descripción del Activo	Ubicación	Área	Responsable
Tipo: [COM] Redes de Comunicaciones	Puntos de acceso alámbricos (hub)	4	Dispositivos de red encargados de la interconexión de la red de datos.	Red de datos del centro QWERTY S.A	Departamento de Sistemas	Ingeniero de Redes
	Switches	6				
	Router	1				
	Internet	1				
Tipo: [L] Instalaciones	Data Center	1	Centro de procesamiento de datos	Departamento de Sistemas	Sistemas	Jefe de sistemas
	Oficinas	1	Salón destinado al trabajo está distribuido por áreas	Empresa QWERTY S.A	Registro y Control Académico	Auxiliares Administrativos
Tipo: [P] Personal	Técnicos de mantenimiento	2	Personal técnico encargado de realizar el mantenimiento preventivo a los equipos de cómputo.	Departamento o de Sistemas	Área de Soporte	Coordinador de Soporte
	Trabajadores	1	Personal de la empresa	Empresa QWERTY S.A	Registro y Control Académico	Jede Administrativo

Fuente: Elaboración propia

Dado a lo anterior, se realiza la clasificación de los activos a partir de los lineamientos de Margerit, estableciendo las vulnerabilidades, amenazas y riesgos.

Tabla. Clasificación de vulnerabilidades, amenazas y riesgos por activo

CATEGORÍA DEL ACTIVO	NOMBRE DEL ACTIVO	VULNERABILIDAD	AMENAZA	RIESGOS	SALVAGUARDAS
Tipo: [D] Datos	Base de datos	Cuentas de usuarios mal configuradas	[E1] Errores de los usuarios	-No existe seguimiento sobre el estado del software antivirus	Software Antivirus
	Backups de Respaldo	Ausencia de copias de Seguridad	[E15] Alteración accidental de la información	Perdida de Datos	Establecer Backup diario
	Backups de bases de datos	Configuración inadecuada de los Backups	[E.18] Destrucción de información	Pérdida de la disponibilidad, debido a pérdida accidental de información.	Planificación de las copias. (backup)
Tipo: [S] Servicios	Página Web	Administración inadecuada de roles y privilegios	[A.22] Manipulación de programas.	Pérdida de la confidencialidad, integridad, disponibilidad debido a la alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	SW Protección de las Aplicaciones Informáticas
	Correo Electrónico	Se encuentra alojado en un solo hosting.	[A6] Abuso de privilegios de acceso	En caso de falla del hosting, no se cuenta con respaldo, por lo cual el servidor de correo quedaría inaccesible.	Backup de Respaldos, controles de privacidad
Tipo: [SW] Software	Windows 10 Pro	Falta de control de actualización de antivirus y su estado	Errores de mantenimiento/actualización de equipos	No se cuenta con software Antivirus Actualizado.	Establecer mantenimientos preventivos

	Antivirus	Errores de mantenimiento / actualización de programas (software)	[E8] Difusión de software dañino	No se cuenta con software Antivirus Actualizado.	Implementación de actualización automática de las firmas de virus del endpoint en los equipos clientes, mediante la instalación de un servidor de antivirus que diariamente realice las descargas de actualizaciones y las mantenga disponibles para los equipos cliente.
Tipo: [HW] Equipamiento Informático	Servidor de Impresión	Mantenimiento insuficiente	Manipulación de equipos	Daños, por mal uso inadecuado de las impresoras.	Establecer mantenimientos y actualizaciones
	Servidor de Archivos FTP	Deficientes actualizaciones de programas ya reparados por el fabricante.	[E.21] Errores de mantenimiento / actualización de programas (software)	Pérdida de la disponibilidad, integridad y confidencialidad de la información debido a equivocaciones de personas con responsabilidades de instalación y operación	Establecer actualizaciones
	Servidor DHCP	Software y parches y seguridad desactualizados	[A.9] Reencaminamiento de mensajes	Pérdida de la integridad debido a envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.	SW Protección de las Aplicaciones Informáticas Como: programas, aplicativos, desarrollos, etc.

	Equipos de Computo	Defectos de origen o fallas presentadas durante el funcionamiento del activo	[I.5] Avería de origen físico o lógico	Pérdida de la disponibilidad debido a fallos en los equipos y/o fallos en los programas. Puede ser debido a un defecto de origen funcionamiento del sistema.	HW Protección de los Equipos Informáticos (antivirus actualizado y habilitado, antimalware)
	Servidor de Nomina y Facturación	Personal no calificado que accede al sistema	[E.1] Errores de los usuarios	Pérdida de la integridad de la información debido a equivocaciones de las personas cuando usan los servicios, datos, etc.	Formación y concienciación (capacitaciones y transferencia de conocimiento al personal que atiende la contingencia).
	Cortafuegos - Firewall	Faltas de reglas de autorización y denegación de transmisión de y comunicación	[E8] Difusión de software dañino	Debido a que el firewall no cuenta con las debidas reglas de autorización y denegación de comunicaciones entrante y salientes, un atacante puede ingresar en la red interna y difundir un software dañino desde el servidor DHCP	Establecer actualizaciones y establecer reglas de Firewall
	Teléfonos IP	Todos los teléfonos tienen la misma contraseña para acceder a la consola admin de éste. Requerimientos mínimos de energía para su funcionamiento	[A.14] Interceptación de información (escucha)	Pérdida en la confidencialidad debido a que el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.	Establecer actualizaciones y mantenimientos preventivos
Tipo: [COM] Redes de Comunicaciones	Puntos de acceso alámbricos (hub)	Puntos expuestos a desconexiones, Ubicación del activo sin protección	[A.23] Manipulación de los equipos	Pérdida de la disponibilidad del activo debido alteración intencionada de su funcionamiento, persiguiendo un beneficio indirecto.	Protección de los Equipos Informáticos Como: dispositivos de red, servidores, host y periféricos, Impresoras. Switches, Router.

	Switches	Configuraciones insuficientes o inadecuadas	[E.2] Errores del administrador	Pérdida de la disponibilidad, integridad y confidencialidad del activo debido a equivocaciones de personas con responsabilidades de instalación y operación	HW Protección de los Equipos Informáticos (Configuraciones adecuadas)
	Router	Puntos expuestos a desconexiones	[I.8] Fallas servicios de comunicaciones	Pérdida de la disponibilidad debido al cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.	Protección de las comunicaciones (disposición de cableada en canaletas)
	Internet	Falta de comunicación con los servicios accedidos a través de internet.	[A6] Abuso de privilegios de acceso	No se cuenta con redundancia de equipos o de proveedor ISP, por tal motivo en caso de falla, el centro quedaría incomunicado con las plataformas que se acceden a través de internet.	Instalar sistema de seguridad biométrico o de monitoreo.
Tipo: [L] Instalaciones	Data Center	Insuficientes o inadecuados sistemas de identificación y autorización.	[A.11] Acceso no autorizado	Pérdida de la integridad y confidencialidad de la información debido a accesos a recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y	Control de los accesos físicos (dispositivos de control de acceso, CCTV)

				autorización.	
	Oficinas	Personal de otras dependencias tiene acceso a las oficinas	[I7] Condiciones inadecuadas de temperatura o humedad	Perdida de activos	Establecer política de control de acceso.
Tipo: [P] Personal	Técnicos de mantenimiento	Falta de control de perfiles y permisos de usuarios.	[A6] Abuso de privilegios de acceso	Avería de origen físico o lógico	Se deben establecer políticas de control de acceso y se debe implementar la separación de perfiles y niveles de acceso a la información
	Trabajadores	Personal desactualizado en el uso de herramientas y con falta de compromiso	[E.2] Errores del administrador	Pérdida de la disponibilidad debido a equivocaciones de personas con responsabilidades de instalación y operación	Formación, capacitaciones y transferencia de conocimiento.

Fuente: Elaboración propia

- Valoración de las tres dimensiones de la seguridad para cada activo.

Para cada uno de los activos de información de la empresa QWERTY S.A se establecieron la disponibilidad, la confidencialidad y la integridad como las dimensiones a valorar. Estas dimensiones son aquellas características de la información que pueden verse disminuidas en su valor en el caso de la materialización de una amenaza.

Para el caso de los activos de información de la empresa QWERTY S.A se definieron las siguientes tablas de valoración para cada una de las dimensiones de seguridad establecidas.

- **Confidencialidad:** Es aquella característica de la información que hace referencia a que el activo sólo es accesible para las personas o sistemas que están autorizados. Se tiene en cuenta la clasificación de la información en pública, clasificada o reservada.

- **Integridad:** Es aquella característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

- **Disponibilidad:** Es aquella característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

A continuación se realizará la evaluación de los activos en cada uno de los parámetros de seguridad de acuerdo a la Confidencialidad, Integridad y Disponibilidad junto con la valoración realizada bajo la escala de criterios definida de cada activo de información de la empresa QWERTY S.A.

Tabla 7. Dimensiones de Valoración

NOMBRE DE DIMENSION		
NOMBRE	**CODIGO**	**CRITERIO DE EVALUACIÓN**
Disponibilidad	[D]	¿Qué importancia tendría que el activo no estuviera disponible?
Integridad	[I]	¿Qué importancia tendría que los datos fueran modificados fuera de control?
Confidencialidad	[C]	¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?
Autenticidad de los usuarios de servicio	[A_S]	¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree?
Autenticidad de los datos de origen	[A_S]	¿Qué importancia tendría que los datos no fueran realmente imputables a quien se cree?
Trazabilidad del servicio	[T_S]	¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio?
Trazabilidad de los datos	[T_D]	¿Qué importancia tendría que no quedara constancia del acceso a los datos?

Fuente. Margerit – Vesion3, Libro II-Método

El criterio de evaluación tomado, corresponde a cada una de las preguntas descritas en la **Tabla 7. Dimensiones de Valoración**, adicionalmente la respuesta se calificó con un valor en puntos dependiendo de la importancia que tiene el activo para el proceso analizado según la escala de valoración que se muestra a continuación. El nivel de seguridad requerido en los aspectos de la autenticidad, trazabilidad, confidencialidad, integridad y disponibilidad estarán basados en los siguientes criterios.

Tabla 8. Impacto perdida de confidencialidad

Tipo de Función	Confidencialidad
Personas	Uso inadecuado de la información propia del cargo
Servicios	Uso no autorizado del activo
Información	Acceso no autorizado al activo por personal no autorizado
Hardware	Acceso a la configuración del activo sin autorización
Software	Conocimiento de la parametrización del activo

Fuente: Elaboración propia

- **Confidencialidad:** se establecerá en función de las consecuencias que tendría su revelación a personas no autorizadas o que no necesitan conocer la información.

Tabla 9. Valoración Confidencialidad

	CONFIDENCIALIDAD			
	Criterio	**Categoría**	**Valoración**	**Explicación**
Dimensión	MA	Muy Alto	**5**	El acceso no autorizado o divulgación de la información gestionada por este activo impacta de forma muy alta a la empresa.
	A	Alto	**4**	El acceso no autorizado o divulgación de la información gestionada por este activo impacta de forma alta a la empresa.
	M	Medio	**3**	El acceso no autorizado o divulgación de la información gestionada por este activo impacta de forma negativa no solo el proceso evaluado sino otros procesos de la empresa.
	B	Bajo	**2**	El acceso no autorizado o divulgación de la información gestionada por este activo impacta levemente de forma negativa a la empresa.
	MB	Muy Bajo	**1**	El acceso no autorizado o divulgación de la información gestionada por este activo NO impacta de forma negativa a la empresa.

Fuente: Elaboración propia

Tabla 10. Impacto perdida de Integridad

Tipo de Función	Integridad
Personas	Generación de datos incorrectos
Servicios	Se valora la exactitud en la prestación del servicio
Información	Errores en el procesamiento del sistema
Hardware	Configuración alterada indebidamente
Software	Modificación en la parametrización del software

Fuente: Elaboración propia

- **Integridad** se establecerá en función de las consecuencias que tendría su modificación por alguien que no está autorizado a modificar la información.

Tabla 11. Valoración Integridad

	INTEGRIDAD			
	Criterio	**Categoría**	**Valoración**	**Explicación**
Dimensión	MA	Muy Alto	**5**	La pérdida del estado completo del activo impacta de forma Muy alta a la empresa.
	A	Alto	**4**	La pérdida del estado completo del activo impacta de forma alta a la empresa.
	M	Medio	**3**	La pérdida del estado completo del activo impacta de forma negativa no solo el proceso evaluado sino otros procesos de la empresa.
	B	Bajo	**2**	La pérdida del estado completo del activo impacta levemente de forma negativa a la empresa.
	MB	Muy Bajo	**1**	La pérdida del estado completo del activo NO impacta de forma negativa a la empresa.

Fuente: Elaboración propia

Tabla 12. Impacto perdida Disponibilidad

Tipo de Función	Disponibilidad
Personas	En el proceso no se encuentra disponible la persona
Servicios	No se puede tener acceso al activo o no está disponible
Información	No se puede acceder o utilizar el activo de información
Hardware	No se puede acceder o utilizar el activo
Software	No se puede acceder o utilizar el activo

Fuente: Elaboración propia

- **Disponibilidad** se establecerá en función de las consecuencias que tendría el que una persona autorizada no pudiera acceder a la información cuando la necesita.

Tabla 13. Valoración Disponibilidad

	DISPONIBILIDAD			
	Criterio	**Categoría**	**Valoración**	**Explicación**
Dimensión	MA	Muy Alto	**5**	La no disponibilidad o ausencia del activo impacta de forma Muy alta a la empresa.
	A	Alto	**4**	La no disponibilidad o ausencia del activo impacta de forma alta a la empresa.
	M	Medio	**3**	La no disponibilidad o ausencia del activo impacta de forma negativa no solo el proceso evaluado sino otros procesos de la empresa.
	B	Bajo	**2**	La no disponibilidad o ausencia del activo impacta levemente de forma negativa a la empresa.
	MB	Muy Bajo	**1**	La no disponibilidad o ausencia del activo NO impacta de forma negativa a la empresa.

Fuente: Elaboración propia

Tabla 9. Valoración de dimensiones de los activos de información.

Nombre del Activo	Valoración de Dimensiones			Valor Cuantitativo (Criticidad)	Valor Cualitativo (Criticidad)
	D	I	C		
Tipo: [D] Datos					
Base de datos	4	4	4	4	Alto
Backups de Respaldo	3	3	3	3	Medio
Backups de bases de datos	3	3	3	3	Medio
Tipo: [S] Servicios					
Página Web	5	5	5	5	Muy Alto
Correo Electrónico	4	4	4	4	Alto
Tipo: [SW] Software					
Windows 10 Pro	3	3	3	3	Medio
Antivirus	3	3	3	3	Medio
Tipo: [HW] Equipamiento Informático					
Servidor de Impresión	4	4	4	4	Alto
Servidor de Archivos FTP	3	3	3	3	Medio
Servidor DHCP	3	3	3	3	Medio
Equipos de Computo	3	3	3	3	Medio
Servidor de Nomina y Facturación	4	4	4	4	Alto
Cortafuegos - Firewall	3	3	3	3	Medio
Teléfonos IP	2	1	1	1	Bajo
Tipo: [COM] Redes de Comunicaciones					
Puntos de acceso alámbricos (hub)	3	3	3	3	Medio
Switches	3	3	3	3	Medio
Router	3	3	3	3	Medio
Internet	5	5	5	5	Alto
Tipo: [L] Instalaciones					
Data Center	2	2	2	2	Bajo
Oficinas	2	2	2	2	Bajo
Tipo: [P] Personal					
Técnicos de mantenimiento	3	3	3	3	Medio
Trabajadores	3	3	3	3	Medio

Fuente: Elaboración propia

Fase 2

Análisis de gestión de riesgos a todos los procesos involucrados en el proyecto a partir de la metodología de Margerit.

7. ANÁLISIS Y GESTION DE LOS RIESGOS

Se analizar los activos de la empresa QWERTY S.A para identificar los riesgos y amenazas enmarcadas en las áreas de Infraestructura, Desarrollo y Soporte. La metodología de gestión de riesgos es utilizada ampliamente para identificar y tratar los riesgos potenciales de la empresa QWERTY S.A.

MAGERIT Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, cumple a cabalidad la función de analizar los riesgos a los procesos involucrados en el proyecto aplicado. Siguiendo el método, se podrán identificar los activos que posee la empresa QWERTY S.A, se establecerá las amenazas a las que están expuestos estos activos, y permitirá determinar las salvaguardas apropiadas para los activos involucrados y así poder estimar el nivel de impacto en caso de que se materializa alguna amenaza.

7.1 Método de Análisis de Riesgos

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.

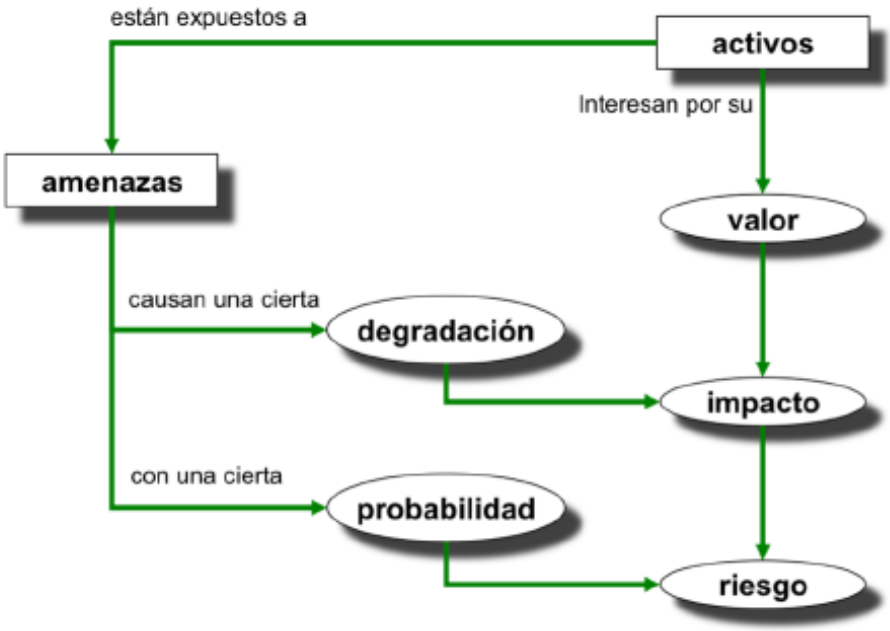
2. Determinar a qué amenazas están expuestos aquellos activos

3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.

4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Figura 7. Elementos del análisis de riesgos potenciales



Fuente: MAGERIT – Versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Los objetivos que persigue MAGERIT son:

Objetivos directos:

1. Concienciar de la existencia de riesgos derivados del uso de las TICS y de la necesidad de gestionarlos a toda la organización y sus responsables.
2. Ofrecer un método sistemático para gestionar estos riesgos.
3. Ayudar a descubrir y planificar el tratamiento pertinente para su control.

Objetivos indirectos:

1. Preparar a la Organización para los siguientes procesos, según corresponda:

- Evaluación
- Auditoría
- Certificación o
- Acreditación

7.2 ALCANCE DE LA GESTIÓN DE RIESGOS

La gestión de riesgos se aplica sobre los activos de información de la empresa QWERTY S.A relacionados en las áreas de Infraestructura, desarrollo y soporte con el fin de aplicar las normas y correctivos correspondientes con el fin de garantizar la integridad, confiabilidad y disponibilidad de la información al igual que la protección de los recursos informáticos y sus instalaciones.

METODOLOGÍA PARA LA VALORACIÓN DEL RIESGO EN LOS ACTIVOS DE INFORMACIÓN MAGERIT

Se tendrá en cuenta la frecuencia de ocurrencia del riesgo en la empresa QWERTY S.A, la probabilidad y el impacto generado en la organización estará basado en los siguientes criterios.

- **Valoración del Impacto:** es directamente relacionado con el activo y se puede medir en una escala numérica en donde 1 es un impacto muy bajo y 5 es muy frecuente.
- **Valoración de la Probabilidad:** hace referencia a la probabilidad de ocurrencia de un evento de riesgo y se puede calcular por medio de una escala numérica, en donde 1 es nula/rara vez ocurre y 5 es muy frecuente.

Tabla 14. Probabilidad del Riesgo

	Nomenclatura	Categoría	Valoración
Probabilidad	MF	Muy Frecuente	**5**
	F	Frecuente	**4**
	MA	Posible	**3**
	B	Poco probable	**2**
	MB	Muy raro	**1**

Esta valoración se realiza de acuerdo a la probabilidad de ocurrencia de los riesgos identificados. Número de veces por periodo de tiempo y el impacto las consecuencias de llegar a concretarse el riesgo.

Tabla 15. Impacto del Riesgo

	Nomenclatura	Categoría	Valoración
Impacto	MF	Muy Frecuente	**5**
	A	Alto	**4**
	MA	Medio	**3**
	B	Bajo	**2**
	MB	Muy Bajo	**1**

Finalmente se toman las dos métricas anteriores y se procede a estimar el riesgo, dando como resultado un mapa de calor y sus respectivas zonas de riesgo.

Tabla 16. Matriz de probabilidad e impacto.

IMPACTO						
	MA					
	A					
	M					
	B					
	MB					
RIESGO		**MB**	**B**	**M**	**A**	**MA**
		PROBABILIDAD				

7.3 ESTIMACIÓN DEL RIEGO

La gestión de riesgos se aplica sobre los activos de información de la empresa QWERTY S.A, se tendrá en cuenta la frecuencia de ocurrencia del riesgo en cada área. La probabilidad y el impacto generado en la organización estarán basados en los siguientes criterios.

La matriz cuantitativa que determina el valor final del riesgo se observa en la siguiente tabla: **Riesgo = Impacto x Probabilidad**

Tabla 17. VALORACIÓN DEL RIESGO

CATEGORÍA	NOMENCLATURA	VALORACION CUALITATIA	VALORACION CUANTITATIVA
Critico	(MA)	Muy Alto	16 a 25
Importante	(A)	Alto	10a 15
Moderado	(M)	Medio	5 a 9
Bajo	(B)	Bajo	3 a 4
Despreciable	(MB)	Muy Bajo	1 a 2

Fuente: Elaboración Propia

A continuación se detalla la matriz de valoración de riesgo por cada activo estimando la probabilidad de ocurrencia e impacto generado en la organización QWERTY S.A.

Tabla 18. Matriz de valoración de Riesgo

Nombre del Activo	Amenaza	Impacto en cada Dimensión			Valoración del Riesgo			
		D	I	C	Probabilidad	Impacto	Calificación	Nivel del Riesgo
Tipo: [D] Datos								
Base de datos Página Web	[A11] Acceso no autorizado	4	4	4	3	5	15	**Alto**
Backups de Respaldo	[E4] Errores de configuración	4	3	3	3	3	9	**Medio**
Backups de bases de datos	[E15] Alteración accidental de la información	3	3	3	3	3	9	**Medio**
Tipo: [S] Servicios								
Página Web	[A11] Acceso no autorizado	5	5	5	5	5	25	**Muy Alto**
Correo Electrónico	[A11] Acceso no autorizado	4	4	4	3	5	15	**Alto**
Tipo: [SW] Software								
Windows 10 Pro	[E20] Vulnerabilidades de los programas (software)	3	3	3	3	3	9	**Medio**
Antivirus	[E21] Errores de mantenimiento / actualización de programas (software)	3	3	3	3	3	9	**Medio**
Tipo: [HW] Equipamiento Informático								
Servidor de Impresión	[E1] Errores de los usuarios	4	4	4	3	5	15	**Alto**
Servidor de Archivos FTP	[E2] Errores del administrador	3	3	3	3	3	9	**MEDIO**
Servidor DHCP	[E21] Errores de mantenimiento / actualización de programas (software)	3	3	3	3	3	9	**Medio**
Equipos de Computo	[A5] Suplantación de la identidad del usuario	3	3	3	3	3	9	**Medio**
Servidor de Nomina y Facturación	[E1] Errores de los usuarios	4	4	4	3	5	15	**Alto**
Cortafuegos Firewall	[A11] Acceso no autorizado	3	3	3	3	3	9	**Medio**
Teléfonos IP	[I8] Fallo de servicios de comunicaciones	3	1	1	3	1	3	**BAJO**
Tipo: [COM] Redes de Comunicaciones								
Puntos de acceso alámbricos (hub)	[A4] Manipulación de la configuración	3	3	3	3	3	9	**Medio**
Switches	[I8] Fallo de servicios de comunicaciones	3	3	3	3	3	9	**Medio**

Router	[I8] Fallo de servicios de comunicaciones	3	3	3	3	3	9	**Medio**
Internet	[I8] Fallo de servicios de comunicaciones	4	4	4	3	5	15	**Alto**
Tipo: [L] Instalaciones								
Data Center	[E1] Errores de los usuarios	2	2	2	2	2	4	**BAJO**
Oficinas	[N*] Desastres naturales	2	2	2	2	2	4	**BAJO**
Tipo: [P] Personal								
Técnicos de mantenimiento	[A23] Manipulación de los equipos	3	3	3	3	3	9	**MEDIO**
Trabajadores	[A6] Abuso de privilegios de acceso	3	3	3	3	3	9	**MEDIO**

Fuente: Elaboración Propia

La valoración de los activos de información a partir de su criticidad se realizó de manera personal, realizando un análisis objetivo y dando valor de importancia según el criterio y riesgo que puedan llegar a ocurrir en cada uno de los activos analizados en la empresa QWERTY S.A.

Se hizo la respectiva valoración a los 22 activos dando como resultado lo siguiente:

Tabla 19. Valoración de activos a partir de su criticidad

RIESGO	CANTIDAD ACTIVOS	CATEGORIA
MUY ALTO	1	CRITICO
ALTO	5	IMPORTANTE
MEDIO	13	MODERADO
BAJO	3	BAJO
MUY BAJO	0	DESPRECIABLE

Fuente: Propia

A continuación se describe el análisis realizado correspondiente a la valoración de aquellos riesgos de tipo Critico, Importante, medio y bajo.

Nivel crítico:

Dentro del nivel crítico se encuentra el servicio de página web donde se puede determinar que es uno de los activos con mayor riesgo, debido a la Administración inadecuada de roles y privilegios por parte de los usuarios que la utilizan.

Otro punto a tener en cuenta es que por falta de mantenimientos y de actualizaciones en los sistemas, se puede aprovechar este tipo de vulnerabilidad para realizar ataques como denegación del servicio, a través de la explotación de vulnerabilidades; se están utilizando protocolos como HTTP que no son seguros, ya que se necesitan la creación de certificados de autenticación de igual manera es importante que estos servicios incluyan procesos de auditoría.

Nivel Importante:

Dentro de esta categoría se encuentran los datos, servicios, equipamiento informático y las redes de comunicaciones.

Las bases de datos de la página web no cuentan con un sistema de respaldo permanente ni con un sistema de seguridad ante una eventual pérdida de información, el acceso no autorizado y errores de usuarios se puede evitar con la implementación de capacitaciones por grupos de expertos en el manejo de aplicativos utilizados por la organización esto con el fin de que el personal a cargo asuma la responsabilidad de su manejo y de esta forma se puedan evitar incidentes a futuro.

Se evidencia fallas en el servicio de Internet por lentitud en el servicio, la red no cuenta con fibra óptica, esto presenta demora en los procesos y en el rendimiento de las operaciones que se realizan sistemáticamente; se recomienda aumentar el ancho de banda e implementar servicio de fibra óptica que garantice un mayor rendimiento y conectividad.

Nivel Moderado:

A pesar de que la empresa QWERTY S.A cuenta con un software de antivirus, no existe un seguimiento adecuado en cuanto a mantenimiento y actualizaciones, lo que puede conllevar a pérdida de información a causa de virus, spiware, ransomware, etc. Otro punto a tener en cuenta es que por falta de mantenimientos y de actualizaciones en los sistemas, se puede aprovechar este tipo de vulnerabilidades para realizar ataques como denegación del servicio, a través de la explotación de vulnerabilidades; se están utilizando protocolos como HTTP que no son seguros ya que se necesitan la creación de certificados de autenticación

Existen errores de los usuarios para el manejo de los sistemas, en este caso se proponen controles como el realizar jornadas de capacitación a los usuarios finales sobre el correcto uso de los aplicativos, y de las impresoras; así como la implementación de políticas orientadas a las buenas practicas del manejo y uso de la información y de los activos informáticos.

Los servidores DHCP y FTP no están ubicados en un espacio donde cuente con un sistema de ventilación en óptimas condiciones, teniendo en cuenta que esto puede generar un riesgo al recalentarse los equipos y producir un corto circuito generando incendios, perdida de equipos u otro tipo de eventos que puedan dañar los medios donde se almacena la información.

Teniendo en cuenta que la empresa no posee ningún tipo de segmentación en su redes, se puede llevar a cabo análisis de tráfico a través de programas fáciles de adquirir y gratuitos como wireshark; los computadores no cuenta con un programa que impida la instalación de este tipo de programas. Se recomienda implementar políticas de acceso a la información de acuerdo a su clasificación. También se pueden implementar medidas de cifrado de las comunicaciones y políticas de backup.

Los equipos de redes switches, router, hub se encuentran obsoletos y no cuentan con soporte de mantenimiento esto conduce a presentar fallas en el servicio de comunicaciones.

Modificación de la información

Para la mitigación de este riesgo se propone la solución de implantar controles, verificaciones y copias de seguridad que permitan verificar que la información no ha sido modificada ni manipulada; también implementar controles criptográficos con el fin de garantizar que información sensible para la organización no puede ser vulnerada. Se debe reducir la cantidad de usuarios autorizados que tengan acceso a lugares privados como las bases de datos, el servidor de aplicaciones, los repositorios de información entre otros.

Se deben implementar un control de usuarios y asignación de claves; por lo que se recomienda fijar políticas de creación de contraseñas y cambio de las mismas como la asignación de privilegios en los perfiles de cada usuario para evitar este tipo de riesgos por suplantación de identidad o acceso no autorizado por parte de los trabajadores y técnicos de mantenimiento.

Se recomienda implantar políticas que fijen la ejecución de auditorías internas semestrales o anules con el fin de verificar que los procesos y manejo de activos e

información se estén realizando de manera adecuada de lo contrario poder mejorar y aplicar correctivos de mejora.

Nivel Bajo:

Dentro de esta categoría se encuentran, Equipamiento informático, e Instalaciones donde se evidencia que los servicios de telefonía IP presentan fallas de comunicaciones por ancho de banda y por errores en las configuraciones del Router de igual manera no existe un plan de mantenimiento que garantice su óptimo funcionamiento.

El acceso no autorizado a las instalaciones son Insuficientes, no existe sistemas de identificación y autorización lo que conduce a la pérdida de integridad y confidencialidad de la información, debido a accesos a recursos del sistema sin tener autorización para ello, la empresa no cuenta con un sistema de seguridad biométrico o cámaras de monitoreo que permita tener control sobre cada una de las áreas de la empresa.

7.4 PLAN DE TRATAMIENTO DE RIESGO

El plan determinado para el tratamiento de riesgos contempla las medidas que se tomaran las cuales serán evaluadas y tendrán un seguimiento constante, donde se actualice la valorización de las vulnerabilidades, el impacto y los riesgos.

Las siguientes son las medidas a tener en cuenta en cada riesgo identificado:

Tabla 24. Tratamiento de Riesgos

MEDIDA	DESCRIPCION
Evitar el riesgo	Se utiliza cuando se aplican mejoras en el proceso para evitar el riesgo.
Reducir el riesgo	Se logra optimizando los procedimientos
Dispensar el riesgo	Para implementar esta medida se distribuye el riesgo en varios lugares.
Transferir el riesgo	Se identifica en pasar el riesgo de un lugar a otro o entre procesos
Asumir el riesgo	Cuando el riesgo es asumido es necesario identificar el responsable que realizara la mitigación.

Fuente: Elaboración Propia

Existen algunos factores de vital importancia a la hora de implementar los controles y que deben tenerse en cuenta, como son:

- La efectividad de las opciones recomendadas
- La adecuación a leyes y normas existentes
- El impacto operacional de las modificaciones
- La confiabilidad de tales controles

7.5 DESCRIPCIÓN DEL PLAN DE ACCIÓN

De acuerdo con la estrategia de tratamiento seleccionada en cada riesgo, se plantean los siguientes controles enfocados a reducir, mitigar y controlar los riesgos inherentes que se encuentran presentes en la herramienta de gestión documental objeto del presente trabajo de grado.

DOCUMENTO DE APLICABILIDAD

Nombre del Activo	Control	Actividad	Descripción de la aplicación del control	Responsable
Tipo: [D] Datos				
Base de datos Página Web	A.14.3.1 Protección de datos de prueba	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	Solo los administradores tienen acceso a los datos de prueba, están custodiados en un servidor virtual del área de sistemas.	Administrador de Bases de Datos (DBA)
Backups de Respaldo Backups de bases de datos	A12.3.1 Respaldo de la información	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	El área de sistemas se encarga del respaldo de la información de los servidores virtuales y de los sistemas de información.	
Tipo: [S] Servicios				
Página Web	A13.1.2 Seguridad de los servicios	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	Establecer la tecnología aplicada a la seguridad de servicios de red, (autenticación, encriptación y controles de conexión de red).	Jefe de sistemas

Correo Electrónico	A.14.1.3 Protección de transacciones de los servicios de las aplicaciones.	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	El ingreso a los sistemas de información y correo electrónico se realiza mediante contraseñas	
Tipo: [SW] Software				
Windows 10 Pro	A12.5.1 Instalación de software en sistemas operativos	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	Se tienen separadas sesiones en los computadores, solo puede instalar software el personal de sistemas con clave de administrador.	Ingeniero de sistemas
Antivirus	A12.2.1 Controles contra códigos maliciosos	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Establecer un indicador para el seguimiento de la gestión de incidentes de seguridad asociados a códigos maliciosos y generar las acciones de mejora requeridas.	
Tipo: [HW] Equipamiento Informático				
Servidor de Impresión	A.12.3.1 Respaldo de la información A.11.2.4 Mantenimiento de los equipos.	Se requiere realizar un plan de mantenimiento y actualización de los servidores de Impresión y FTP de la Organización	Se solicita aplicar configuración, actualización y mantenimiento del servidor de impresión, FTP, así como realizar una actualización a los usuarios que tienen acceso al servidor para verificar cuales están en uso y cuales es necesario desactivar	Administrador de Servidores
Servidor de Archivos FTP				
Servidor DHCP	A11.1.4 Protección contra amenazas externas y ambientales.	Elaborar el procedimiento para el mantenimiento de los servidores HTTP, DHCP y PBX de la Organización	Los servidores DHCP, HTTP y PBX se encuentran en un espacio donde no se cumplen condiciones de climatización óptimas. Se deben implementar mecanismos como sensores de humedad y de calor, sistemas de refrigeración certificados, entre otros.	

	A11.2.1 Ubicación y protección de los equipos		Se deben implementar controles físicos como cámaras de seguridad, controles de acceso biométrico, CCTV, etc.	
Equipos de Computo	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información. A11.2.1 Ubicación y protección de los equipos	Establecer política de control de acceso.	Se solicita aplicar configuración, actualización y mantenimiento a los equipos de cómputo, así como realizar una actualización a los usuarios que tienen acceso al servidor para verificar cuales están en uso y cuales es necesario desactivar. Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	
Servidor de Nomina y Facturación	A14.2.2 Procedimientos de control de cambios en sistemas	Actualización de las licencias de software		
Cortafuegos Firewall	A13.1.1 Controles de redes	Se requiere elaborar una política para la implementación de políticas y gestión del firewall de la entidad	Establecer los procedimientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red, cuando sea necesario.	
Teléfonos IP	A12.1.3 Gestión de capacidad	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Se requiere re inducción y capacitación del personal de la mesa de servicio en temas de instalación y configuración de equipos tecnológicos, además concientizar al personal con relación al uso adecuado que se les debe dar a las herramientas tecnológicas asignadas para su labor	
Tipo: [COM] Redes de Comunicaciones				

Puntos de acceso alámbricos (hub)	A11.2.3 Seguridad en el cableado.	Realizar una campaña de mantenimiento de la red cableada en la organización con el fin de mitigar el riesgo de pérdida de la disponibilidad del activo	Todo el cableado del Centro se encuentra protegido y con las medidas de acuerdo a la legislación vigente.	Administrador de redes
Switches	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información. A11.2.1 Ubicación y protección de los equipos	Solicitar al proveedor horas de capacitación a los administradores de los Swiches	Definir los parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad y de red.	
Router	A13.1.3 Separación en las redes A11.2.1 Ubicación y protección de los equipos	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	Implementar la segregación de la red en función de los grupos de servicios, usuarios y sistemas de información.	
Internet	A9.1.2 Acceso a redes y a servicios en red	Garantizar la seguridad del funcionamiento y de la calidad del servicio de internet en la empresa	Establecer acuerdos de servicios que incluyan estos mecanismos de seguridad a aplicar, niveles de servicios y requisitos de administración de todos los servicios de redes, sean internos o contratados. Es importante que estos servicios incluyan procesos de auditoría	
Tipo: [L] Instalaciones				
Data Center	A9.1.1 Política de control de acceso	Realizar una campaña de mantenimiento de la red cableada en la organización con el fin de mitigar el riesgo de pérdida de la disponibilidad del activo	Se realiza la identificación de activos y se documenta	Ingenieros de Soporte

Oficinas	A11.1.2 Controles de acceso físicos	Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	Establecer un procedimiento formal donde se implementen los lineamientos en términos de acceso físico establecidos por la Organización, apoyados en mecanismos de seguridad (lector de huella o carné, vigilancia privada, circuito cerrado de televisión, manejo de visitantes, manejo de personal de limpieza y soporte), que incluya registros de ingreso (bitácora y/o rastros de auditoría).	
Tipo: [P] Personal				
Técnicos de mantenimiento	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	Se requiere re inducción y capacitación del personal de la mesa de servicio en temas de instalación y configuración de equipos tecnológicos, además concientizar al personal con relación al uso adecuado que se les debe dar a las herramientas tecnológicas asignadas para su labor	Coordinador de Infraestructura
Trabajadores	A16.1.3 Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	Procedimiento de reporte de incidentes y vulnerabilidades de seguridad.	

Fuente: Elaboración propia

Fase 3

Definir las políticas de seguridad que permitan minimizar los posibles riesgos a los que está expuesta la información de la empresa **QWERTY S.A** en cada área.

Introducción

Debido a la importancia de la información que maneja la empresa QWERTY S.A Se hace necesario implementar las siguientes políticas para la protección de la información y seguridad en las dependencias de sistemas.

Alcance

Esta política es aplicable a todos los departamentos (áreas) de la Empresa QWERTY S.A. Colaboradores y ejecutivos estos con el fin de garantizar la protección de la información.

A continuación se establecen las políticas de seguridad que soportan el SGSI de la empresa QWERTY S.A

8. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Se establecen políticas que garanticen que tanto los colaboradores y ejecutivos estén comprometidos con la seguridad de la información de la empresa QWERTY S.A por lo que se les asignaran funciones y responsabilidades frente a la manejo de la información y de los activos; el Área de Tecnología y Sistemas de Información será quien habilite los accesos y permiso de la información para quienes la necesiten pero estos deberán asumir la responsabilidad de la misma y acatar las normas a las que está sujeta el manejo de la información así como las consecuencias al mal manejo de la misma.

Política de Gestión de Activos

- La identificación y actualización del inventario de Activos de Información de la dependencia de sistemas en la empresa QWERTY S.A se realizara de manera anual o cada vez que sea necesario. Se llevara a cabo por medio de una matriz de valoración de activos y análisis de riesgos con el objetivo de poder determinar su clasificación y valoración frente a los criterios de confidencialidad, integridad y disponibilidad de la información, el jefe de sistemas será el responsable de realizar esta actividad.

- Los activos de información deben estar etiquetados y clasificados según la norma ISO 27001, teniendo en cuenta la normatividad vigente establecida en la ley 1712 de 2014.

Política de dispositivos móviles.

El departamento de TI define las siguientes políticas con respecto a los dispositivos móviles (Smart phones, portátiles, tabletas, entre otros) estos son una herramienta de trabajo que se utilizaran únicamente para facilitar las comunicaciones de los usuarios permitidos dentro de la empresa QWERTY S.A.

- Todo dispositivo móvil, equipo portátil y/o de escritorio deberá estar inventariado y registrados en el sistema para su conexión.

- La información almacenada en los dispositivos móviles deberá estar encriptada para asegurar la información en el caso de pérdida o robo.

- Todo dispositivo móvil y equipos portátiles estarán configurados para ser usado con credenciales de dominio de la empresa QWERTY S.A.

- Los dispositivos móviles deben tener contraseñas de ingreso de manera automática y manual.

- En caso extravío o hurto del equipo, deberá informar de manera inmediata al departamento de TI.

Política de devolución de los Activos

- Los funcionarios activos deberán realizar la devolución de los activos físicos o electrónicos asignados por la empresa por medio del formato devolución de activos una vez finalizado el empleo.

- El área de TI será el responsable de llevar a cabo este proceso para garantizar que la devolución del activo se realizó de manera correcta cumpliendo con todos los lineamientos establecidos por la empresa.

Política de Gestión de medios removibles

- La copia de archivos en medios de almacenamiento está restringida, por lo cual se deshabilita la opción de escritura en dispositivos USB en todos los equipos de cómputo de la empresa.

- El área de TI serán los encargados de habilitar y deshabilitar la opción de escritura en dispositivos USB en todos los equipos de la empresa.

- La autorización de uso de los medios removibles debe ser tramitada a través del área de TI por el jefe de área y será objeto de auditorías de seguridad.
.
- El uso de medios removibles que almacenan información y pueden ser extraídos de los computadores como USB o Discos Duros (HDD) debe estar autorizado por el área de TI con aprobación del jefe de área para su respectiva autorización.

Política de control y administración de acceso

- Cada empleado de QWERTY S.A es responsable del mecanismo de control de acceso que le sea proporcionado por el departamento de Sistemas, esto corresponde al usuario y password asignado.

- Por cada funcionario o contratista debe tener un usuario y una contraseña para el acceso a los equipos asignados para el desarrollo de las funciones.

- Los usuarios y contraseñas son personales e intransferibles y no deben compartirse ni prestarse.

- La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.

- Solo los funcionarios pertenecientes al Área de TI, están autorizados para la creación, modificación y desactivación de las cuentas de usuarios cuando la solicitud este aprobada por el jefe de área.

Política de gestión de contraseñas

- El Área de Tecnologías y Sistemas de la Información serán los encargados de suministrar a los usuarios autorizados las claves para el acceso a los equipos de cómputo y servicios de red.

- Las claves o contraseñas para el acceso a los sistemas de información son de uso personal e intransferible, es responsabilidad de cada usuario el buen uso de la misma.

- Las claves o contraseñas deberán tener mínimo ocho (8) caracteres alfanuméricos, puede utilizar combinación de letras, números y símbolos.

- Por políticas de seguridad los sistemas estarán programados periódicamente para el cambio de contraseña de accesos a los sistemas de información.

Política de control de acceso a redes e internet

- La red inalámbrica podrá ser permitida a los funcionarios, contratistas o terceros bajo la autorización y control del ingeniero de sistemas.

- La red inalámbrica permitida para las conexiones tiene sistema de seguridad WAP2 (Acceso Wi-Fi protegido 2)

- El Jefe del área de sistemas será el encargado de garantizar la conectividad y acceso a redes e internet.

- El departamento de TI establece los controles necesarios para evitar las descargas de software no autorizados en los equipos de cómputo además de controlar el acceso a la información almacenada en los portales de almacenamiento con el objetivo de evitar la pérdida de información.

- Los usuarios tendrán restringido el acceso a redes sociales y a páginas no autorizadas.

Política sobre controles criptográficos

- QWERTY S.A por medio del área de TI implementa el uso de herramientas y técnicas criptográficas para garantizar la integridad y seguridad de la información de la empresa.

- El área de TI serán los encargados de proveer las herramientas de encriptación de datos a los usuarios por solicitud previa del jefe de área.

- Las claves de encriptación se debe almacenar en lugares externos con sistema de acceso para garantizar la seguridad.

- El área de TI establece el estándar de encriptación utilizando el algoritmo de cifrado 256 bits, para las herramientas criptográficas administradas por la empresa.

Política sobre seguridad física y del entorno

- Se debe implementar un programa de seguridad física para el ingreso a las oficinas, dependencias y áreas de la empresa.

- Se debe registrar o documentar los Controles de acceso para restringir la divulgación no autorizada, modificación o destrucción de la información, incluyendo controles de acceso físico y lógico.

- El área de Tecnología debe implementar un sistema de seguridad biométrico o de monitoreo que permita tener control de ingreso y egreso de los clientes al interior de la empresa.

Política de seguridad de equipos de cómputo

- El área de tecnología y sistema de información definirá e implementara los respectivos mantenimientos preventivos y correctivos de todos los equipos de cómputo.

- El Área de TI establece los procedimientos para asegurar la protección de la información en los equipos de cómputo de la empresa.

- El mantenimiento de equipos, instalación y actualización de software estará a cargo del jefe de sistemas.

- El Área de TI debe implementar sistemas de alimentación eléctrica, como por ejemplo: planta eléctrica para no parar las operaciones de los sistemas de información durante una falta de suministro de energía.

- Todos los equipos de cómputo de la empresa deben tener instalados un programa de antivirus con sistema de actualización automático.

Política de copias de seguridad y respaldo de Información

- El administrador de backup es el encargado der realizar periódicamente las copias de seguridad y de generar tareas de restauración de la información en la empresa con su respectiva documentación.

- Todas las copias de información y de respaldo estarán bajo custodia y almacenadas en un lugar adecuado con sistema de seguridad para el control de acceso.

- Toda información secreta debe estar encriptada, ya sea que se encuentre al interior o externamente en cualquier medio de almacenamiento, transporte o transmisión.

- Los medios y equipos de cómputo donde se almacenan la información debe mantenerse con las medidas de protección físicas y lógicas establecidas por la empresa.

Política de uso de los activos

- Los activos de información pertenecen a QWERTY S.A y el uso de los mismos debe emplearse exclusivamente con propósitos laborales.

- Los usuarios de QWERTY S.A no deben mantener almacenados en los discos duros de las estaciones de trabajo, archivos de música, fotos, videos y cualquier tipo de archivo que no sean de carácter laboral.

- Los usuarios autorizados serán los únicos que podrán utilizar quipos, sistemas y/o aplicativos informáticos disponibles para su uso dentro de la empresa.

- El usuario será responsable del buen uso y manejo adecuando con su cuenta de usuario.

- Los usuarios no tendrán permitido realizar ninguna de las siguientes labores sin autorización del área de TI.

    - Instalar software en cualquier equipo de la empresa
    - descargar software de Internet en cualquier equipo de la empresa
    - Copiar o distribuir cualquier software de la empresa.
    - Cambiar la configuración de hardware de la empresa.

Política de adquisición y mantenimiento de sistemas de información.

- Solo los funcionarios pertenecientes al Área de TIC, están autorizados para instalar software y/o hardware en los equipos, servidores e infraestructura tecnológica de la empresa.

- El área de TI serán los únicos encargados de realizar tareas de mantenimientos, actualizaciones, revisión de hardware y software, recuperar datos perdidos, eliminar software malicioso, entre otros.

- Todo nuevo hardware y software que se vaya a comprar o solicitar por cualquier dependencia, deberá ser gestionado por el Área de TI para su correcto funcionamiento.

Política de uso de correo electrónico.

- El personal de soporte tecnológico establecerá los procedimientos y controles que permitirán proteger el servidor de correo electrónico contra código malicioso que pudiera trasmitirse a través de los mensajes de texto.

- El uso del correo electrónico es estrictamente laboral, los usuarios y claves de los administradores de sistemas y del personal del Área de TI son de uso personal e intransferible.

Política de seguridad en las comunicaciones

- El área de TI (Tecnologías de la Información) establece las medidas de seguridad para garantizar el servicio de red de la empresa.

- El área de TI establece la configuración de red por medio de la segmentación de grupos y garantizando los servicios de conectividad.

- El área de TI define los servicios, protocolos y puertos autorizados por la empresa.

9. CONCLUSIONES

La implementación del diseño de sistema de gestión de seguridad de la información realizada a la empresa QWERTY S.A, bajo la norma ISO 27001 debe garantizar la disponibilidad, integridad y confidencialidad de la información.

El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegido se encuentra el sistema. En coordinación con los objetivos, estrategia y política de la Organización, las actividades de tratamiento de los riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos en el proyecto aplicado con el nivel de riesgo que acepta la Dirección.

Se puede decir que todo el proceso realizado para el análisis de riesgos, la definición de políticas de seguridad, la declaración de aplicabilidad y de los controles conforma el diseño del SGSI para la empresa QWERTY S.A bajo la norma ISO/IEC 27001 teniendo como objetivo realizar un análisis de gestión de riesgos a todos los procesos involucrados en el proyecto a partir de la metodología de Margerit.

Con el resultado obtenido en el Análisis y la Gestión de Riesgos estableceremos unos controles adecuados que nos permitan, establecer las políticas de seguridad para garantizar la seguridad y minimizar los posibles riesgos a los que está expuesta la información de la empresa QWERTY S.A en cada área.

10. RECOMENDACIONES

La empresa debe contar con una estructura organizativa así como de recursos necesarios, entre otras cosas, para llevar a cabo la implantación del SGSI.

La implantación de las medidas de seguridad requiere una organización gestionada y la participación informada de todo el personal que trabaja con el sistema de información. Es este personal el responsable de la operación diaria, de la reacción ante incidencias y de la monitorización en general del sistema para determinar si satisface con eficacia y eficiencia los objetivos propuestos.

Para que se pueda implementar un sistema centralizado de gestión de identidades que incluya las políticas y lineamientos contenidos en la norma ISO 27001 expuestos en el desarrollo de este documento es necesario tener en cuenta los siguientes aspectos:

La alta gerencia debe:

- Establecer y apoyar la política de seguridad de la información.
- Asegurarse de que se establecen objetivos y planes del SGSI en su entidad.
- Establecer roles y responsabilidades de seguridad de la información.
- Dar a conocer a la organización tanto la importancia de lograr los objetivos de seguridad de la información y de cumplir con la política de seguridad, como sus responsabilidades legales, contractuales y la necesidad de mejora continua.

11. BIBLIOGRAFÍA

AGUSTÍN LÓPEZ, Neira. “Sistema de Gestión de Seguridad de la Información (SGSI). De ISO 27001”. {En línea}. {16, Abril 2019}. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

ÁVAREZ RIAÑO, Jerzon. "Diseño de un sistema de gestión de seguridad de la información - SGSI basado en la norma ISO27001 para el colegio PRO-COLOMBIANO de la ciudad de Bogotá”. {En línea}. {18, Abril 2019}. Disponible en: https://repository.unad.edu.co/handle/10596/11950

CAMARGO RAMÍREZ, Juan. "Diseño de un sistema de Gestión de la Seguridad de la Información (SGSI) en el área tecnológica de la Comisión Nacional del Servicio Civil - CNSC basado en la norma ISO27000 e iso27001." {En línea}. {18, Abril 2019}. Disponible en: https://repository.unad.edu.co/handle/10596/11992

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

GONZÁLEZ GARCÍA, Ronald Alejandro. “Diseño del Sistema de Gestión de Seguridad de la Información para el área de tecnología de la empresa Baker Tilly Colombia Ltda.” Bogotá, bajo la norma ISO 27001:2013. {En línea}. {20, Marzo 2019}. Disponible en: https://repository.unad.edu.co/handle/10596/12722

GUZMAN, Carlos. “Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad financiera de segundo piso”. Trabajo de grado. Bogotá, D.C.: Institución Universitaria Politécnico Gran Colombiano. Facultad de Ingeniería y Ciencias Básicas. 2015. 173 p.

HERNÁNDEZ, Enrique. “Seguridad y Privacidad en los Sistemas Informáticos”. {En línea}. {24, Marzo 2019}. Disponible en: http://www.disca.upv.es/enheror/pdf/ACTASeguridad.PDF

ICETEX. “Manual de Políticas de Seguridad de La Información”. {En línea}. {10, Marzo 2019}. Disponible en: https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manualseguridadinformacion.pdf

INCODER. “Política de Seguridad de La Información”. {En línea}. {6, Marzo 2019}. Disponible en: http://www.incoder.gov.co/documentos/A%C3%91O_2014/Gestion_Incoder/Politicas/Agosto_15/PoliticadeSeguridaddelaInformacion.pdf

INTECO. (2010). Implantación de un SGSI en la empresa - Incibe. Recuperado el, de Instituto Nacional de Tecnologías de la Comunicación: {En línea}. {16, Marzo 2019}. Disponible en: Fuente: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/

ISO 27000.ES. “El Portal de ISO 27001 en Español”. {En línea}. {5 de mayo de 2019}. Disponible en: http://www.iso27000.es/herramientas.html

ISOTools, (s.f). “Sistemas de Gestión de Riesgos y Seguridad”. {En línea}. {5, Mayo 2019}. Disponible de: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. ”. {En línea}. {5, Mayo 2019}. Disponible de: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WQ991DDhDIU.

NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos

OIDOR GONZÁLEZ, Juan Carlos. “Diseño de un Sistema de Gestión de Seguridad de la Información - SGSI bajo la norma ISO/IEC 27001:2013 para la empresa en Línea Financiera. Cali. {En línea}. {5, Marzo 2019}. Disponible de: https://repository.unad.edu.co/handle/10596/11907.

RODRÍGUEZ CORREA, Jorge Leonardo. “Diseño de un Sistema de Gestión de Seguridad de la Información basado en ISO2700 para laboratorios servicios farmacéuticos de calidad SFC LTDA”. {En línea}. {8, Marzo 2019}. Disponible de: Obtenido de: https://repository.unad.edu.co/handle/10596/12598.

RUEDA LEÓN, Alix. & CASTILLO SARMIENTO, José. "Diseñar SGSI para el Colegio Agroindustrial de Puerto Nuevo.". *Repositorio Institucional UMNG*. Universidad Militar Nueva Granada. {En línea}. {20, Mayo 2019}. Disponible en: https://repository.unad.edu.co/handle/10596/17415

Sistema de Gestión de la Seguridad de la Información. {En línea}. {20, Mayo 2019}. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

Sistema de gestión de seguridad de la seguridad de la información, ISO 27001. . {En línea}. {20, Mayo 2019}. Disponible en: https://www.eoi.es/blogs/ciberseguridad/2016/06/11/introduccion-a-la-iso-27001-en-la-empresa/

Universidad Nacional de Córdoba (Argentina). “Políticas de Seguridad de la Información para la UNC”. Obtenido de Políticas de Seguridad de la Información para la UNC: {En línea}. {7, Marzo 2019}. Disponible en: http://www.unc.edu.ar/gestion/unidades/direccion- operativa/concursos/dgti/00003-08.pdf

UNAD. “Políticas Marco de Referencia SGSI”. Obtenido de Políticas Marco de Referencia SGSI: {En línea}. {6, Mayo 2019}. Disponible en: https://gidt.unad.edu.co/images/Documentos/20150303%20-%20Resolucin%204256%20-%20Polticas%20Marco%20de%20Referencia%20del%20SGSI.pdf