DISEÑO DE UN PLAN DE GESTIÓN DE RIESGOS Y VULNERABILIDADES DEL CASO DE ESTUDIO DE LA EMPRESA QWERTY S.A., BASADOS EN LOS ESTÁNDAR NTC-ISO/IEC 27001 Y NTC-ISO/IEC 27032.

JORGE EMILIO SAAVEDRA AGUDELO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA-ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

TUNJA-BOYACA

2020

DISEÑO DE UN PLAN DE GESTIÓN DE RIESGOS Y VULNERABILIDADES DEL CASO DE ESTUDIO DE LA EMPRESA QWERTY S.A., BASADOS EN LOS ESTÁNDAR NTC-ISO/IEC 27001 Y NTC-ISO/IEC 27032.

JORGE EMILIO SAAVEDRA AGUDELO

Proyecto de grado para optar al título de especialista en seguridad informática

Director de proyecto:

Esp. Mariano Esteban Romero Torres

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA-ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

TUNJA-BOYACA

2020

DEDICATORIA

El presente proyecto aplicado que va enfocado al caso de estudio de la empresa QWERTY S.A., Como primera Instancia se lo dedicamos a Papito Dios y mamita maría, en segunda instancia a mi señora madre por apoyarme en cada instante durante el proceso de formación y finalmente a los ingenieros **Hernando José Peña Hidalgo, Fernando Zambrano Hernández y Mariano Esteban Romero Torres** por su asesoramiento y compartir sus conocimientos durante el desarrollo del presente proyecto.

AGRADECIMIENTOS

En primer lugar le damos gracias a Papito Dios y mamita maría por permitirnos diseñar el plan de gestión de riesgos y vulnerabilidades del caso de estudio de la empresa QWERTY S.A., y brindarnos toda la sabiduría y tiempo para el desarrollo del mismo; en segunda instancia a mi señora madre por apoyarme en cada instante durante mi formación profesional y finalmente a los ingenieros **Hernando José Peña Hidalgo, Fernando Zambrano Hernández y Mariano Esteban Romero Torres** por su asesoramiento y enseñanza durante el proceso de formación del presente proyecto Aplicado.

RESUMEN

Para el diseño y construcción del presente proyecto aplicado, se plantea utilizar procedimientos, técnicas y métodos en donde se implemente un Sistema de Gestión de Seguridad de la Información (SGSI), como así mismo la administración y gestión de la ciberseguridad y todo esto con el fin de llevar a cabo su implantación, monitoreo, procedimiento, operación, verificación, mantenimiento, sostenimiento y mejora del sistema mencionado, fortaleciendo el sistema de seguridad, identificando y gestionando los riesgos posibles en el sistema de información, basándonos en la información propuesta en el caso de estudio de la empresa QWERTY S.A, utilizando como referencia las normas internacionales ISO/IEC 27001 y ISO/IEC 27032.

PALABRAS CLAVE: Ciberseguridad, Dato, Activo, Amenaza, Confidencialidad, Salvaguarda.

ABSTRACT.

For the design and construction of this applied project, it is proposed to use procedures, techniques and methods in which an Information Security Management System (ISMS) is implemented, as well as the administration and management of cybersecurity and all this with the In order to carry out its implementation, monitoring, procedure, operation, verification, maintenance, maintenance and improvement of the mentioned system, strengthening the security system, identifying and managing the possible risks in the information system, based on the information proposed in the Case study of the company QWERTY SA, using as reference the international standards ISO / IEC 27001 and ISO / IEC 27032.

KEYWORDS: Cybersecurity, Data, Asset, Threat, Confidentiality, Safeguard.

CONTENIDO

pág.

INTRODUCCIÓN 16
1. DEFINICION DEL PROBLEMA 17
1.1. PRESENTACION 17
1.2. PLANTEAMIENTO DE PROBLEMA 18
2. JUSTIFICACIÓN 19
3. ALCANCE 20
4. OBJETIVOS 21
4.1. OBJETIVO GENERAL 21
4.2. OBJETIVOS ESPECÍFICOS 21
5. MARCO REFERENCIAL 22
5.1. MARCO TEÓRICO. 22
5.2. MARCO CONCEPTUAL. 23
5.3. ANTECEDENTES 27
5.3.1. Plan de implementación del SGSI basado en la norma ISO 27001:2013. 27
5.3.2. Elaboración de plan de implementación de la ISO/IEC 27001:2013 ..27
5.3.3. Guía para la implementación de la norma ISO 27032 28
5.3.4. Aplicación de la metodología magerit para el análisis de riesgos de los sistemas de control en la estación tenay del oleoducto. 28

5.3.5. 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. 29

5.4. MARCO LEGAL 29

5.4.1. Técnicas 30

5.4.1.1. Norma ISO 27000. 30

5.4.1.2. Norma NTC-ISO-IEC 27001:2013. 30

5.4.1.3. Normas NTC-ISO-IEC 27032. 30

5.4.2. Jurídicas (Nacional) 31

5.4.2.1. Ley 599 de 2000. 31

5.4.2.2. Ley 1266 de 2008 Habeas Data. 31

5.4.2.3. Ley 1273 de 2009. 31

5.4.2.4. Ley Estatutaria 1581 de 2012 y reglamentada parcialmente por el decreto nacional 1377 de 2013. 32

5.4.2.5. Ley 1712 del 2014. 32

5.4.2.6. Conpes 3701 julio de 2011. 32

5.4.2.7. Conpes 3854 abril de 2019: 32

5.4.2.8. Convenio de Budapest 16 de marzo de 2020 (Convenio sobre la ciberdelincuencia): 32

5.5. MARCO CONTEXTUAL 33

6. DISEÑO METODOLÓGICO. 34

7. RESULTADOS 35

7.1. IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN, RIESGOS, AMENAZAS Y VULNERABILIDADES DEL DEPARTAMENTO DE SISTEMAS DEL CASO DE ESTUDIO DE LA EMPRESA QWERTY S.A. 35

7.1.1. Identificación de los activos de información del departamento de sistemas. 35

7.1.2. Identificación de los riesgos que presentan en el caso de estudio de la empresa QWERTY S.A. 39

7.1.3. Identificación de las vulnerabilidades que se exponen los activos de información del caso de estudio de la empresa QWERTY S.A. 39

7.2. PROPUESTA DEL SGSI 41

7.2.1. Diseño del plan del SGSI 41

7.2.1.1. Contexto de la Organización. 42

A. Estudio Del Escenario....42

B. Compromiso....43

C. Conocimiento de la organización y su contexto. 44

D. Comprensión de las necesidades y expectativas de las partes interesadas. 45

7.2.1.2. Liderazgo 51

A. Alcance 51

7.2.1.3. Planificación. 51

A. Acciones para tratar riesgos y oportunidades. 51

B. Objetivos de seguridad de la información y planes para lograrlos. .65

7.3. ADMINISTRACION Y GESTIÓN DE RIESGOS DE LA CIBERSEGURIDAD DE LA EMPRESA QWERTY S.A. 73

7.3.1. Metodología para el análisis y gestión de la seguridad de la información de la empresa QWERTY S.A., basada en MARGERIT. 73

7.3.1.1. Identificación y clasificación de los activos de información del caso de estudio de la empresa QWERTY S.A. 73

7.3.1.2. Identificación de los riesgos que se exponen en el escenario 2 del caso de estudio de la empresa QWERTY S.A. 73

7.3.1.3. Identificación de la vulnerabilidades, amenazas y salvaguardas para la protección de manera eficaz y eficiente de los activos de información de la empresa QWERTY S.A. 74

7.3.1.4. Evaluación del riesgo. 85

A. Valoración de los activos de información según el impacto. 85

B. Valoración de los activos de información según el impacto y sus dimensiones de seguridad. 88

C. Análisis de riesgos y su impacto de los activos. 90

7.3.1.5. Tratamiento del riesgo..... 93

7.4. MODELO DE GESTIÓN DE LA CIBERSEGURIDAD DE LA EMPRESA QWERTY S.A., BASADOS EN LA NTC-ISO/IEC 27032. 96

7.4.1. Contextualización de la norma. 96

7.4.2. Entendimiento de la organización (Caso de estudio de la empresa QWERTY S.A.).....96

7.4.3. Pautas a tener en cuenta. 100

7.4.4. Implementación de la NTC-ISO/IEC 27032 al departamento de sistemas del caso de estudio de la empresa QWERTY S.A. 101

7.4.4.1. Alcance y campo de aplicación. 102

7.4.4.2. Aplicabilidad. 102

7.4.4.3. Referencias normativas. 103

7.4.4.4. Términos y definiciones. 103

7.4.4.5. Términos abreviados. 103

7.4.4.6. Generalidades o visión general..... 103

7.4.4.7. Partes interesadas en el ciberespacio. 103

7.4.4.8. Activos del ciberespacio. 104

7.4.4.9. Amenazas contra la seguridad y protección del ciberespacio. 107

7.4.4.10. Controles de ciberseguridad o ciberprotección. 115

8. CONCLUSIONES 118
9. RECOMENDACIONES 119
REFERENCIAS BIBLIOGRÁFICAS 120
ANEXOS.....133

LISTA DE TABLAS

pág.

Tabla 1. Activos de información a cargo del departamento de sistemas. 36

Tabla 2. Matriz de partes interesadas internas. 45

Tabla 3. Matriz de partes interesadas externas. 47

Tabla 4. Nivel de Criticidad para evaluar los activos de información para la empresa QWERTY S.A. 55

Tabla 5. Nivel de Criticidad de los activos de información a cargo de la dependencia de sistemas de la empresa QWERTY S.A. 56

Tabla 6. Declaración de aplicabilidad (SOA) la empresa QWERTY S.A 62

Tabla 7. Identificación de las amenazas, vulnerabilidades y salvaguardas que se presenta a cargo del departamento de sistemas del caso de estudio de la empresa QWERTY S.A. 77

Tabla 8. Valoración de los activos de información del departamento de sistemas del caso de estudio de la empresa QWERTY S.A., según su impacto. 86

Tabla 9. Valoración de los activos de información del departamento de sistemas del caso de estudio de la empresa QWERTY S.A., según su impacto y sus dimensiones de seguridad. 88

Tabla 10. Calificación del impacto. 90

Tabla 11.Calificación de Probabilidad. 90

Tabla 12. Hoja de Excel sobre la valoración de riesgos según el impacto y la probabilidad del riesgo existe de cada uno de los activos de información dentro del departamento de sistemas del caso de estudio de la empresa QWERTY S.A. 92

Tabla 13. Guía de estrategias para el tratamiento de los riesgos. 93

Tabla 14. Hoja de Excel con el Plan de tratamiento de riesgos, de acuerdo a la identificación, valoración y clasificación de los riesgos según las estrategias descritas dentro del departamento de sistemas del caso de estudio de la empresa QWERTY S.A. 94

Tabla 15. Conocimiento del caso de estudio de la empresa QWERTY S.A. 98

Tabla 16. Estructura norma NTC-ISO/IEC 27032. 101

Tabla 17. Reconocimiento y Categorización de los activos del ciberespacio del caso de estudio de la empresa QWERTY S.A. 108

Tabla 18. Reconocimiento de las vulnerabilidades, amenazas y salvaguardas de los activos del ciberespacio del caso de estudio de la empresa QWERTY S.A. 111

Tabla 19. Valoración de los activos del ciberespacio del caso de estudio de la empresa QWERTY S.A; según su impacto. 113

Tabla 20. Valoración de los activos del ciberespacio del departamento de sistemas del caso de estudio de la empresa QWERTY S.A; según su impacto y dimensiones de seguridad. 114

Tabla 21. Controles de ciberseguridad para los activos del ciberespacio para el departamento de sistemas del caso de estudio de la empresa QWERTY S.A. ...115

LISTA DE FIGURAS

pág.

Figura 1. Modelo PHVA aplicado a los procesos y estructura del SGSI. 42

Figura 2. Organigrama de las dependencias de sistemas de la empresa QWERTY S.A. 43

Figura 3. Estrategias para el tratamiento de riesgos en la empresa QWERTY. 53

Figura 4.Estrategias para el tratamiento de riesgos en la empresa QWERTY S.A. 54

Figura 5. Análisis y gestión de riesgos en una organización y para el caso de estudio de la empresa QWERTY. 75

Figura 6. Valoración de acuerdo al impacto. 85

Figura 7. Tablas para la valoración de riesgos según el impacto y la probabilidad del riesgo existe dentro de una organización. 91

Figura 8. Principios Básicos del COBIT 97

LISTA DE ANEXOS

Pág.

ANEXO A.....133

ANEXO B.....136

ANEXO C.....138

ANEXO D.....140

INTRODUCCIÓN

Hoy en día cuando hablamos de datos e información en las empresas, organizaciones y otras entidades, tanto del sector privado como público, inmediatamente se hace referencia a que es un activo de información y se infiere que este es un pilar fundamental para el preciso desempeño y función de una empresa u organización como tal. Partiendo de esta idea y del caso de estudio propuesto para el Diseño del plan de gestión de riesgos y vulnerabilidades de la empresa QWERTY S.A., se basará en el uso e implementación de los estándares de calidad NTC-ISO/IEC 27001 y NTC-ISO/IEC 27032.

De acuerdo a lo anterior, se dice que los activos de información tanto físicos como lógicos deben ser protegidos adecuadamente mediante la implementación de estos procesos, procedimientos y políticas de seguridad, ya sea para la administración y gestión de riesgos de la ciberseguridad o para los SGSI en las mismas entidades.

1. DEFINICION DEL PROBLEMA

1.1. PRESENTACION

Hoy en día la seguridad de los datos está en un crecimiento exponencial, dado a que los ataques informáticos se presentan de cualquier forma y en cualquier lugar, ya sea desde el quebramiento de la seguridad y protección de las cuentas personales hasta el hurto de información entre las entidades organizacionales.

De acuerdo a lo anterior, la empresa QWERTY S.A, es una organización del sector tecnológico que busca el crecimiento y desarrollo tecnológico en las comunidades colombianas a través del empleo de las TI. Hoy en día cuenta con 120 trabajadores entre directivos, administrativos y operativos, quienes hacen uso de forma regular de los medios de información para consultar datos; cuenta con unas dependencias del área de sistemas que son infraestructura, desarrollo y soporte, las cuales brindan apoyo a cualquier requerimiento a su infraestructura tecnológica de un tiempo de 24/7.

Cada una de las dependencias del área de sistemas posee sus funciones y asistencias en la entidad, con el fin de mantener un óptimo desempeño en los servicios tecnológicos, como así mismo contar con sistemas, procedimientos, técnicas y estándares que ofrezcan y salvaguarden los activos de información en donde les brinde integridad, confidencialidad y disponibilidad en sus soluciones.

Además, cabe mencionar que la empresa posee un canal de internet de 25 megas en ancho de banda dedicado para poder dar desarrollo a sus actividades rutinarias.

Dado a lo anteriormente descrito, la empresa QWERTY S.A presenta las siguientes falencias:

- No cuenta con un sistema de seguridad biométrico o de monitoreo que le proporcione 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[1].

1.2. PLANTEAMIENTO DE PROBLEMA

¿Cómo proteger de manera eficaz y eficiente los activos de información de la empresa QWERTY S.A., a partir de la implementación el estándar NTC-ISO/IEC 27001 y NTC-ISO/IEC 27032?

[1] Universidad Nacional Abierta y a Distancia Escuela de Ciencias Básicas de Tecnología e Ingeniera. (2019). *Escenario Dos (Enfoque Directivo - Administrativo)- Propuesta para el desarrollo de la alternativa de grado como Proyecto Aplicado* [Ebook] (1st ed., p. 6).

2. JUSTIFICACIÓN

El presente proyecto va a radicar en colocar un nivel superior de seguridad a los activos de la información que dependen del departamento de sistemas del sector tecnológico de la empresa QWERTY S.A., es decir que se pretende implementar mecanismos de seguridad adecuados a las diferentes dependencias que se procuran proteger, tanto en su proceso de identificación, al acceso y medios de acceso a los objetos y finalmente en la identificación de las entidades y al personal.

El resguardar la información en una organización es de gran importancia, dado que son denominados como unos de los activos más valiosos en una entidad, por lo tanto, es de suma relevancia determinar las políticas de seguridad para el uso y utilización de los datos, como así mismo la utilización de las herramientas tecnológicas, porque nos permite prevenir dificultades y acontecimientos que afecten la buena articulación o marcha de dicha organización.

De acuerdo a lo anterior se pretende identificar las vulnerabilidades concernientes a los activos de la información concernientes a la entidad de estudio, con el fin de tener control de cada uno de los requerimientos y exigencias de los prospectos o anuncios de la empresa; en pocas palabras lo que se busca es aplicar y obtener las certificaciones en seguridad de la información basados en el estándar de calidad NTC-ISO/IEC 27001 y 27032.

Desde otra perspectiva, lo que se pretende realizar con el proyecto aplicado es aprender a adquirir habilidades y destrezas de una manera inovativa con el fin de dar solución a los problemas focalizados en nuestra día a día, las cuales se presentan en las diferentes compañías u organizaciones tanto privadas como del sector público.

Además, con el desarrollo, aplicación e implementación del presente proyecto, se pretende que, con el SGSI, se proteja cada uno de los activos de la información de la entidad de estudio, como así mismo se garantice la confidencialidad, integridad y disponibilidad de los datos mediante el empleo de este estándar y se logre asegurar los beneficios económicos y los objetivos de la organización, dando cumplimiento a la legalidad, adaptación y las condiciones variables del entorno.

3. ALCANCE

Para el desarrollo del caso de estudio de la empresa QWERTY S.A., se pretende proponer el diseño del plan del SGSI basado en las 2 primeras fases del modelo PHVA encontradas en el estándar NTC-ISO/IEC 27001:2013.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Diseñar un plan de gestión de riesgos y vulnerabilidades para el caso de estudio de la empresa QWERTY S.A., basados en los estándar NTC-ISO/IEC 27001 y NTC-ISO/IEC 27032.

4.2. OBJETIVOS ESPECÍFICOS

- Identificar los activos de información, los riesgos, las amenazas y las vulnerabilidades asociadas en la dependencia de sistemas del caso de estudio de la empresa QWERTY S.A.

- Aplicar el estándar de seguridad y privacidad de los datos, con el fin de asegurar la confidencialidad, integridad, disponibilidad y no repudio de la información de la empresa QWERTY S.A, basados en las 2 primeras fases del PHVA de la norma NTC-ISO/IEC 27001:2013.

- Establecer un modelo de gestión de ciberseguridad de la empresa QWERTY S.A., haciendo uso de las metodologías y estándares basados en la NTC-ISO/IEC 27032 para la buena gestión de la seguridad de la información.

- Proponer una metodología para la gestión de seguridad de la información, para el análisis de los riesgos y vulnerabilidades a las cuales están expuestas los activos de la empresa; proyectadas desde el punto de vista cibernético.

5. MARCO REFERENCIAL

5.1. MARCO TEÓRICO.

Se ha observado que durante el paso de los últimos años, el progreso tecnológico a nivel global ha alcanzado grades avances en la comercialización, en las comunicaciones, especialmente con su innovación, estructura y robustez, la cual ha alcanzado un nivel muy alto en cuanto al procesamiento de sus datos, como así mismo en su almacenamiento y todo los anteriormente descrito con el fin de establecer grades oportunidades de negocio, pero también estas oportunidades poseen una latencia muy alta ante los riesgos de seguridad, es decir, que con cada día que pasa, la predisposición de nuestros datos de cualquier índole se encuentran más comprometidos a sufrir algún tipo de incidente de seguridad, es por eso que a través de la implementación del plan de gestión de riesgos y vulnerabilidades del caso de estudio de la empresa QWERTY S.A, se pretende aplicar y establecer todas las regulaciones que mitiguen estas amenazas tanto físicas como lógicas y para ello se basara en los estándares de calidad NTC-ISO/IEC 27001 y NTC-ISO/IEC 27032.

Dado lo anterior, un SGSI, debe fijar e instaurar los principios y metodologías de una forma clara, concisa y concretas dentro de su ejecución y cumplimiento, como así mismo debe encontrarse en óptimas condiciones y evolutivas de las contingencias que se presenten; lo cuales permiten determinar y describir lo siguiente:

1. El gobierno da cumplimiento a la disposición de estándares y políticas actuales de la seguridad de la información.
2. Reconocimiento y cuantificación de las amenazas que comprometen los activos de información en cuanto a su seguridad.
3. Determinación de las medidas, controles y mecanismos que posibilitaran la mitigación del impacto de los probables ataques informáticos en donde se vean involucrados los datos en cuanto a la Disponibilidad, Integridad, Confidencialidad y No Repudio de la información de la organización.

De igual manera con la implementación de las diferentes técnicas de seguridad de la información, especialmente en el SGSI del caso de estudio propuesto, se pretende promover la adopción del enfoque o planteamiento basado en procesos

con el fin de implementar, ejecutar, mejorar, constituir, mantener y hacer seguimiento de la operación tanto física como lógica de los diferentes activos de la información de la organización en estudio. Pero también se pretende aplicar métodos y directrices para la ciberprotección basados en la NTC-ISO/IEC 27032, en donde se prepara a las empresas y a las organizaciones en el tema de ciberseguridad con el fin de controlar, detectar y responder a los ciberataques, como así mismo brindando las mejores prácticas para la seguridad y cuidado de los activos del ciberespacio los cuales son primordiales para el desarrollo operacional dentro de la organización y así mismo se debe tener en cuenta las distintas apariencias o aspectos a los cuales se deben confrontar cuando se divulgan, se transmiten o se trasladan los datos sensibles en el ciberespacio, de tal forma que se reconozcan, se analicen y se gestionen los peligros y riesgos, precisando las tareas más significativas y/o críticas, reconociendo los activos de información y del ciberespacio, como así mismo las partes interesadas, los roles que desempeñan en la red y en el ciberespacio de tal forma que se implanten directrices y/o controles que brinden seguridad en este aspecto a toda la entidad u organización.

5.2. MARCO CONCEPTUAL.

Activo: Cualquier cosa que posee valor para un individuo, compañía, entidad u organización.

Activo de Información: Conocimiento o información que posee o tiene valor para un individuo u organización.

activo virtual: representación de un activo en el Ciberespacio.

Análisis de Riesgos: Empleo sistemático o metódico de los datos para determinar las fuentes y evaluar los riesgos.

Amenaza: Es la causa latente de un daño o destrucción de un activo de información.

Ataque: Intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo.

Causa: Motivo por la cual la contingencia sucede.

Cibercrimen: Es la acción criminal, la cual envuelve a los servicios o aplicaciones que sean objetivo en el ciberespacio.

Ciberespacio: entorno complejo que resulta de la interacción de personas, softwares y servicios en Internet por medio de dispositivos y redes de tecnología conectados a éste, los que no existen en forma física.

Ciberseguridad: Acción de proteger en contra de consecuencias, físicas, sociales financieras, ocupacionales, educacionales o de otro tipo que resultan del daño, error, accidente, perjuicio o cualquier otro evento que se pueda considerar no deseable en el ciberespacio.

Ciberprotección: Actividad de protección del ciberespacio con el objeto de custodiar la confidencialidad, integridad y disponibilidad de los datos en el Ciberespacio**.**[2]

Confidencialidad de los datos: Resguardar y certificar que los datos no se difundan, ni se pongan a disposición de personas, organizaciones o procedimientos no autorizados (Recomendaciones UIT X.805 y X.814). (Revisión del marco regulatorio para la gestión de riesgos de seguridad digital, 2017)[3]

control, contramedida: medios para manejar riesgos, incluyendo políticas, directrices, directrices, prácticas o estructuras organizacionales, las que pueden ser de naturaleza administrativa, técnica, de gestión o legales.

Controles: Son aquellos órganos de control usados para inspeccionar y controlar actividades que son juzgadas como sospechosas y que pueden perjudicar de algún modo los activos de información.

---

[2] Instituto Nacional de normalización (INN). NCh iso-27032:2015. 1st ed., Santiago de chile. (2015). pp. 3-8.

[3] Comisión de regulación de comunicaciones de la república de Colombia. (2017). *Revisión del marco regulatorio para la gestión de riesgos de seguridad digital* [Ebook] (p. 82). Bogotá D.C. Recuperado de: https://www.crcom.gov.co/recursos_user/2017/actividades_regulatorias/ciberseguridad/Documento_CRC_Seguridad_Digital_Vpublicar.pdf

Declaración de aplicabilidad: Archivo o documento que explica los propósitos de los controles concernientes a los SGSI de la organización.

Disponibilidad: Es la característica de que los datos sean asequibles y utilizables por aprobación de la organización que la posea.

Evaluación del riesgo: procedimiento de relacionar el riesgo estimado versus los criterios de riesgo dados, para señalar la trascendencia del riesgo.

Evento de seguridad de la información: Asistencia identificada de un requisito de un procedimiento, prestación o un sistema de red, el cual señala los posibles quebramientos de las políticas de seguridad de la información o las deficiencias de las salvaguardas, o de una postura desentendida anticipadamente la cual pueden ser concernientes a la seguridad y su solidez.

Gestión del Riesgo: Son aquellas labores coordinadas para administrar e inspeccionar una entidad en correlación con el riesgo.

Incidente de seguridad de la información: es una circunstancia o un encadenamiento de acontecimientos que vulneran la seguridad de la información que son inesperados y que poseen una posibilidad relevante de involucrar las operaciones la organización y finalmente poner en riesgo la seguridad de la información.

Integridad: Garantiza la precisión y la autenticidad de la información, salvaguardando los datos contra actividades no autorizadas de su reformación, eliminación, invención o re-actuación y cabe indicar que estas acciones no son aprobadas, es decir que estas actividades de protección de la información son de exactitud y disposición completa de los activos.

No repudio: Prestación que tiene como finalidad de asegurar la disponibilidad de evidencias que puedan exponerse a intermediarios y emplearse para demostrar que un especifico suceso o acción haya tenido lugar, con la intensión de eludir una entidad u organización refute haber efectuado una operación de tratamiento de

datos, suministrando argumentos de dichas actividades en la red. (Guerra de la Espriella & Lizcano Ortiz, 2018)[4]

Parte interesada: (gestión de riesgos) persona u organización que puede afectar, verse afectado por o percibirse como afectados por una decisión o actividad. [Guía ISO 73:2009].

Política de seguridad: Conjunto de prácticas, reglas o leyes cuyos fines son decretar procedimientos para resguardar los activos de información como así mismo los bienes de la entidad u organización con el objeto de llevar a cabo sus propósitos de protección.

Riesgo: Es la mezcla de probabilidades o posibilidades de que ocurra algún acontecimiento y las consecuencias es estas sean perjudiciales.

Seguridad de la información: protección de la confidencialidad, la integridad y la disponibilidad de la información. Igualmente, la seguridad de la compromete otras características tales como: legitimidad, fiabilidad, trazabilidad y no repudio de los datos.

SGSI: Un sistema de gestión de la seguridad de la información, que cita a un conjunto de políticas de seguridad en cuanto a la administración de la información.

software engañoso: software que realiza actividades en el computador de un usuario sin antes notificar al usuario de lo que va a hacer exactamente en el computador o sin pedir el consentimiento del usuario para llevar a cabo estas acciones.

Tratamiento del riesgo: proceso de recopilación e implementación de técnicas para enmendar el riesgo.

Vulnerabilidad. Cualquier fragilidad que pudiera emplearse con el fin de quebrantar la información que contiene un sistema de una organización.

---

[4] Guerra de la Espriella, M., & Lizcano Ortiz, C. (2018). Compilación Jurídica MINTIC-RESOLUCIÓN 2258 DE 2009 [Ebook] (p. 4). Recuperado de: https://normograma.mintic.gov.co/mintic/docs/pdf/resolucion_crc_2258_2009.pdf

5.3. ANTECEDENTES

5.3.1. Plan de implementación del SGSI basado en la norma ISO 27001:2013.

Autores: Maya Arango, Paula Andrea

Año de Publicación: 2016.

Descripción: En este trabajo de grado se detalla los objetivos, la importancia, la expectativa del sistema de gestión de la seguridad de la información y la metodología relacionada con la planeación, descripción, concepto e identificación y creación del modelo de seguridad de la información para la empresa textilera S.A., basado en la norma ISO 27001:2013. El principal objetivo es sentar las bases del proceso de mejora continua y plantear las acciones necesarias para minimizar el impacto de los riesgos potenciales. El proyecto plantea el establecimiento de las bases para la implementación de un SGSI (sistema de gestión de la seguridad de la información). (Maya Arango, 2016)[5]

5.3.2. Elaboración de plan de implementación de la ISO/IEC 27001:2013

Autores: Garrido Camargo, Cristóbal

Año de Publicación: 2018.

Descripción: En este trabajo se muestra el proceso realizado para elaboración del Plan de Implementación de la ISO/IEC 27001:2013 en una multinacional dedicada al reciclaje de residuos industriales que, aunque concienciada con la necesidad de asegurar adecuadamente sus sistemas de información, no contaba hasta el momento con un SGSI. El proyecto recoge las tareas realizadas para sentar las bases para la implantación del SGSI, y genera una serie de entregables que formarán parte del sistema de gestión documental del SGSI. Además, muestra la

---

[5] Maya Arango, P. (2016). Plan de implementación del SGSI basado en la norma ISO 27001:2013. Eds.a.ebscohost.com.bibliotecavirtual.unad.edu.co. Recuperado de: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/53466/8/pmayaaTFM0616memoria.pdf.

evolución y mejora de la seguridad de la información conseguida con la puesta en marcha del SGSI. (Garrido Camargo, 2018)[6]

5.3.3. Guía para la implementación de la norma ISO 27032

Autores: Guzmán Solano, Sandra Liliana

Año de Publicación: 2019

Descripción: En este trabajo contiene el análisis del estado de Ciberseguridad en Colombia y una guía para que las compañías implementen controles bajo las buenas prácticas determinadas en la norma ISO 27032 (GUZMÁN SOLANO, 2019)[7].

5.3.4. Aplicación de la metodología magerit para el análisis de riesgos de los sistemas de control en la estación tenay del oleoducto.

Autores: Hernán Mauricio Rojas Peña.

Año de Publicación: 2019.

Descripción: En este trabajo se realiza el análisis y gestión de los riesgos de cada uno de los sistemas de control de la estación de Tenay, la cual se encuentra ubicada en la ciudad de Neiva Huila y cuenta con un sistema de supervisión y adquisición

---

[6] Garrido Camargo, C. (2018). Elaboración de plan de implementación de la ISO/IEC 27001:2013 [Ebook] (1st ed., pp. 7-12). Universitat Oberta de Catalunya (UOC). Recuper http://openaccess.uoc.edu/webapps/o2/bitstream/10609/88265/10/cgarridocaTFM0119memoria.pdf .

[7] GUZMÁN SOLANO, S. (2019). GUÍA PARA LA IMPLEMENTACION DE LA NORMA ISO 27032. [Ebook] (1st ed., pp. 7-17). Universidad católica de Colombia. Retrieved 27 April 2020, from https://repository.ucatolica.edu.co/bitstream/10983/23385/1/Proyecto%20Guia%20ISO%2027032.pdf.

de datos desde el cual puede operar de manera remota y controlada el transporte de hidrocarburos.[8]

5.3.5. 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.

Autor: Juan David Camargo Ramírez.

Año de Publicación: 2017

Descripción: En este trabajo se muestra la planeación o diseño de un SGSI, en donde se identifica, se gestiona y disminuye los riesgos reales y potenciales de la seguridad de la información de CNSC (Comisión nacional del servicio civil), en donde se pretende ejecutar de una manera organizada, documentada, sistematizada, eficiente y adecuada a los cambios que se puedan generar atraves de las amenazas, riesgos y vulnerabilidades en el sistema de información del CNSC.[9]

5.4. MARCO LEGAL

El marco de normatividad que regula la seguridad de la información en Colombia, se encuentra regido por las siguientes normas técnicas y legislaciones jurídicas que se dan de la siguiente manera:

---

[8] APLICACION DE LA METODOLOGÍA MAGERIT PARA EL ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE CONTROL EN LA ESTACIÓN TENAY DEL OLEODUCTO. (2019). [Ebook] (1st ed., pp. 10-14). Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/27758/1/1075211684.pdf.

[9] Camargo Ramirez, J. (2017). DISEÑO DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) EN EL ÁREA TECNOLOGICA DE LA COMISIÓN NACIONAL DEL SERVICIO CIVIL - CNSC BASADO EN LA NORMA ISO27000 E ISO27001 [Ebook] (1st ed., pp. 9-12). Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/11992/1/75104100.pdf.

5.4.1. Técnicas

5.4.1.1. Norma ISO 27000.

Esta norma internacional nos da una visión general de cada uno de los estándares y series que la componen, indicando su alcance de actuación y su propósito de publicación. De igual manera recoge todos los conceptos para la familia ISO 27000, como así mismo presenta los fundamentos para la implementación de los SGSI en cuanto a su establecimiento, monitorización y mejora del mismo.[10]

5.4.1.2. Norma NTC-ISO-IEC 27001:2013.

En la república de Colombia existen unos lineamientos para la implementación de los sistemas de gestión de la seguridad de la información (SGSI), los cuales están estipulados en la norma NTC-ISO-IEC 27001:2013 y regulados por ICONTEC. Dado a lo anterior este estándar de calidad está dirigida especialmente cualquier tipo de empresa u organización sin importar si es privada, pública o sin ánimo de lucro. Además, con esta norma se especifica los requisitos que requieren las organizaciones para el diseño e implementación de controles de seguridad de los 33, cuales se derivan las acciones que deben tomar para evitar la materialización de riesgos. De igual manera este estándar se determinan las actividades que deben aplicar cada una de la entidades u organizaciones para la perfecta aplicación del SGSI en su empresa. Finalmente, con el anexo A, se relacionan 14 dominios y 113 controles con el fin de reducir los riesgos, vulnerabilidades y amenazas que coloquen en riesgo cada uno de los activos información y su funcionalidad.[11]

5.4.1.3. Normas NTC-ISO-IEC 27032.

En la república de Colombia existen unos lineamientos o directrices que están enfocados a las tecnologías de la información, orientadas exactamente a la ciberseguridad de las empresas u organizaciones en nuestro país, es este estándar de calidad ha sido creado con el fin de avalar y garantizarla protección de los datos

---

[10] López, A. (2020). Serie 27k. Iso27000.es. Recuperado de: http://www.iso27000.es/iso27000.html.

[11] DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI BASADO EN LA NORMA ISO27001 PARA EL COLEGIO PROCOLOMBIANO DE LA CIUDAD DE BOGOTÁ, QUE INCLUYE: ASESORIA, PLANEACIÓN. (2016). [Ebook] (1st ed., pp. 32-33). Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/11950/1/17348959.pdf.

en el momento de intercambio de información en la red, como así mismo para mejorar la seguridad de los datos en el ciberespacio de la internet.

5.4.2. Jurídicas (Nacional).

5.4.2.1. Ley 599 de 2000.

La descrita es de tipo penal y trata sobre la violación ilícita de las comunicaciones relacionadas indirectamente con los delitos informáticos, en cuanto a los siguientes artículos:

- **Artículo 192.** Violación ilícita de las comunicaciones.
- **Artículo 193.** Ofrecimiento, venta o compra de instrumentos aptos para interceptar la comunicación privada entre personas.
- **Artículo 194.** Divulgación y empleo de documentos reservados.
- **Artículo 195.** Acceso abusivo a un sistema informático; derogado por el artículo 4 de la ley 1273 del 2009.
- **Artículo 196.** Violación ilícita de comunicaciones o correspondencia de carácter oficial.

5.4.2.2. Ley 1266 de 2008 Habeas Data.

La cual se dictan las disposiciones generales del hábeas data y 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.

5.4.2.3. 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.

- **Artículo 269A:** Acceso abusivo a un sistema informático.
- **Artículo 269B:** Obstaculización ilegitima de un sistema informático o red de telecomunicación.
- **Artículo 269C:** Intercepción de datos informáticos.

- **Artículo 269D:** Daño informático.
- **Artículo 269E:** Uso de software malicioso.
- **Artículo 269F:** Violación de datos personales.
- **Artículo 269G:** Suplantación de sitios web para capturar datos personales.
- **Artículo 269H:** Circunstancias de agravación punitiva.

5.4.2.4. Ley Estatutaria 1581 de 2012 y reglamentada parcialmente por el decreto nacional 1377 de 2013.

Por la cual se dictan disposiciones generales para la protección de datos personales.

5.4.2.5. Ley 1712 del 2014.

En donde se reglamenta el acceso a la información pública y la privacidad de los datos personales y la información que debe tratar las entidades públicas.

5.4.2.6. Conpes 3701 julio de 2011.

Trata sobre los lineamientos de política para ciberseguridad y ciberdefensa, es decir que fortalece las capacidades del estado para enfrentar amenazas que atentan contra su seguridad y defensa en el ámbito cibernético, creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio.

5.4.2.7. Conpes 3854 abril de 2019:

Trata sobre la política nacional de la seguridad digital, es decir que fortalece las capacidades múltiples de las partes interesadas con el fin de identificar, gestionar, tratar y mitigar los riesgos de la seguridad digital.

5.4.2.8. Convenio de Budapest 16 de marzo de 2020 (Convenio sobre la ciberdelincuencia):

trata del primer tratado internacional, creado con el objetivo de proteger a la sociedad frente a los delitos informáticos y los delitos de internet, mediante la

elaboración de leyes adecuadas y la mejora de las técnicas de investigación y el aumento de la cooperación internacional.[12]

5.5. MARCO CONTEXTUAL

La empresa QWERTY S.A., es una entidad del sector tecnológico que busca el crecimiento tecnológico en las comunidades colombianas atraves del uso de las TI. Cuenta con 3 dependencias en el área de sistemas, como son infraestructura, desarrollo y soporte la cual busca brindar apoyo, asistencia y mantenimiento a cada una de las dependencias que conforman la organización. De igual manera, la dependencia de sistemas ofrece servicios de asistencia para directivos, administrativos y operativos, dándole así un apoyo en cada uno de los servicios que posea la descrita. Ya para finalizar, la empresa QWERTY S.A. cuenta con una alta prestación de servicios con el fin de mantener un óptimo desempeño en cada una de áreas y funciones especialmente en el sector tecnológico y así mismo contar con las mejores medidas de seguridad y protección, manteniendo la integridad, confidencialidad y disponibilidad de los datos.

[12] Mercado, Y. (2020). Tercera web conferencia del curso de Aspectos Eticos Y legales de la seguridad informatica.. Lecture, Adobe Connect recuperado de: http://conferencia2.unad.edu.co/pgepdmgxi3u0/?proto=true

6. DISEÑO METODOLÓGICO.

Para el desarrollo del diseño metodológico del presente caso de estudio de la empresa QWERTY S.A., se efectúa mediante la implementación de las primeras 2 fases del ciclo PHVA de un SGSI y con esto se pretende adoptar una orientación apoyados en cada uno de los procedimientos los cuales permitan implementar, fijar operar, mantener, mejorar y hacer seguimiento del SGSI adoptado por la empresa. Dado lo anterior, en su primera fase, denominada **Planear**, se llevó acabo la contextualización de la organización, el estudio del escenario, es decir su análisis, como así mismo el establecimiento de políticas, objetivos, procesos y procedimientos de seguridad que permitan gestionar el riesgo y mejorar la seguridad de la información dentro de la empresa. En cuanto a la segunda fase del PHVA, denominada **Hacer**, se implementó cada una de las políticas, controles, procesos y procedimientos que posee el Sistema de gestión de la seguridad de la información de la empresa QWERTY S.A., los cuales se encuentran desarrollados en el capítulo 7 sobre la propuesta del SGSI.

Por otro lado, también se implementó el modelo de gestión de la ciberseguridad basados en la norma NTC-ISO/IEC 27032 en donde se definen los métodos y principios que se van aplicar en cada uno de los ítems planteados y dispuestos en el caso de estudio propuesto, como así mismo la aplicación de las prácticas de la ciberseguridad al departamento de sistemas de la empresa QWERTY S.A.

Ya para finalizar, se implementó la metodología para el análisis y gestión de la seguridad de la información basada en MARGERIT, en donde se identificaron las amenazas, vulnerabilidades, y salvaguardas, como así mismo se efectúa la evaluación, valoración y tratamiento del riesgo según el impacto y su probabilidad de acuerdo cada uno de los activos de información hallados en la empresa QWERTY S.A.

7. RESULTADOS

7.1. IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN, RIESGOS, AMENAZAS Y VULNERABILIDADES DEL DEPARTAMENTO DE SISTEMAS DEL CASO DE ESTUDIO DE LA EMPRESA QWERTY S.A.

7.1.1. Identificación de los activos de información del departamento de sistemas.

Partiendo que los activos de información son los recursos o bienes de un SGSI y que son indispensables para que una empresa u organización se desempeñe y cumpla sus objetivos que se han propuesto, a continuación, se reconocerá los activos de información del departamento de sistemas del caso de estudio de la empresa QWERTY S.A.

Tabla 1. Activos de información a cargo del departamento de sistemas.

Activo	Descripción	Ubicación	Categorización[.] Cantidad(.)
Servidor de Impresión: **Servidor marca Dell en torre PowerEdge T440** **Ver ficha técnica**	Equipo de cómputo que conecta dos impresoras: Destinadas a: Una (1) Impresora HP LaserJet Enterprise serie 600, activo que brinda el servicio para la dependencia de nómina y facturación. Permite la concurrencia de hasta 25 usuarios y el volumen mensual de impresión es de 200 a 25000 páginas	Oficina de nómina y facturación	[HW] Equipamento Informático - (1)
	Una (1) Impresora SMART MultiXpress M4370LX, impresora que ofrece el servicio de escáner e impresión con un ciclo de trabajo de hasta 300000 páginas mensuales con capacidades de red alámbrica e inalámbrica. Impresora destinada para el servicio de directivos y administrativos y docentes.	Dependencia directiva y administrativa	[HW] Equipamento Informático - (1)
Servidor de archivos FTP: **Servidor marca Dell en torre PowerEdge T130** **Ver ficha técnica**	Equipo de cómputo que tiene como función el almacenamiento y la administración de los archivos que se están generando en el interior de la organización como son: Digitalización de documento de entrada y de salida, audios generados en reuniones, asambleas y otro tipo de encuentros, video, generados por docentes y funcionarios. Dentro de las políticas de uso, para este servidor solo pueden tener acceso las personas autorizadas para los fines correspondientes.	Oficina antigua de sistemas	[D] Datos - (1)
Página web del Plan Máximo	Servicio contratado con la empresa Godaddy.com	Empresa Godaddy	

Ver ficha proveedor	La página web tiene como objeto la publicación de contenido relacionado con el modelo negocio. Está construida a partir del sistema gestor de contenidos dinámicos Joomla versión 2.5 El hospedaje web la infraestructura del servidor es Apache, PHP, MySQL.		Servicios [S] - (1)
Servidor de nómina y facturación. **Servidor marca Dell en torre PowerEdge T440.** **Características de servidor** **Apache 2.4.25** **PHP 5.6.30 - 7.1.1 MySQL 5.7.17** **PhpMyAdmin 4.6.6**	Plataforma de desarrollo propio. Tiene como función el almacenamiento y la administración de la nómina y facturación de la empresa QWERTY S.A.		[SW] Software - (2)
Servidor DHCP **Servidor marca Dell en torre PowerEdge T440**	Servidor que asigna y administra de forma dinámica el direccionamiento dentro de la organización.		[HW] Equipamento Informático - (1)
Equipos de cómputo para gestión del desarrollo tecnológico	Equipos de cómputo donde se gestiona información online relacionada con el desarrollo del objeto social Presupuesto. • Proveedores • Órdenes de compra • Inventarios	Dependencia de desarrollo tecnológico	[HW] Equipamento Informático - (3)
Cortafuegos Cisco ASA 5505 **Ver ficha técnica**	Sistema de protección.	Sistema de seguridad que está protegiendo a la red de datos, de intrusiones que se	[HW] Equipamento Informático - (1)

		puedan presentar en la red	
Equipos de Computo Sistemas operativos win10 Pro	Equipos destinados para el desarrollo del objeto social.	Dependencia de control y seguimiento	[HW] Equipamento Informático - (10)
Equipos de Computo	Equipos destinados para el desarrollo del objeto social.	Dependencia de prueba de software.	[HW] Equipamento Informático - (5)
Puntos de acceso alámbricos (hub)	Dispositivos de red encargados de la interconexión de la red de datos.	Red de datos del centro.	[COM] redes de comunicaciones. (4)
Switch's cisco catalyst 2960	Dispositivos de red encargados de la interconexión de la red de datos.	Red de datos del Centro.	[COM] redes de comunicaciones. (6)
Técnicos de mantenimiento	Personal técnico encargado de efectuar el mantenimiento preventivo y correctivo a los equipos PC.	Departamento de Sistemas.	[P] Personal (2)
Teléfonos IP	Sistema de comunicación a través de teléfonos Voz IP, que comunica las oficinas y departamentos del centro.	Dependencias del centro	[HW] Equipamento Informático - (6)
Puntos de acceso	Puntos de acceso al servicio de internet en el campus universitario.	Departamento de sistemas	[COM] redes de comunicaciones. (2)

7.1.2. Identificación de los riesgos que presentan en el caso de estudio de la empresa QWERTY S.A.

1. 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.

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

3. La configuración de la red de comunicaciones se encuentra en el mismo segmento.

4. Aunque los equipos de cómputo cuentan con sistemas de antivirus actualizado, no se hace un seguimiento a sus actualizaciones o estado.

5. 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.

6. Aunque existe un Cortafuegos Cisco ASA 5505, este no cuenta con reglas implementadas para la autorización o denegación de conexiones o transmisión de datos[13].

7.1.3. Identificación de las vulnerabilidades que se exponen los activos de información del caso de estudio de la empresa QWERTY S.A.

1. En el servidor de impresión de detecta daños por desgaste y defectos desde fabrica, como de igual manera carencia de mantenimientos preventivos al descrito.

2. En cuanto al Servidor FTP, se halla que existe una carencia de configuraciones de seguridad hacia el servidor, como así mismo la falta de

---

[13] Universidad Nacional Abierta y a Distancia Escuela de Ciencias Básicas de Tecnología e Ingeniera. (2019). *Escenario Dos (Enfoque Directivo - Administrativo)- Propuesta para el desarrollo de la alternativa de grado como Proyecto Aplicado* [Ebook] (1st ed.,Ibid., p. 3,4-6).

actualizaciones del antivirus y finalmente la administración y configuración del servidor no se encuentra centralizada.

3. La página Web contiene errores en la gestión de recursos y configuraciones. De igual manera se ven fallos en la depuración es decir en la misma programación del sitio web y se detecta la ejecución de códigos malintencionados por factor humano.

4. En los servidores de nómina y facturación se detectan vulnerabilidades en cuanto al control de accesos no autorizados, falta de políticas, procedimientos y normas sobre el uso no controlado del sistema.

5. En cuanto al servidor DHCP, se denota la ausencia de un control ambiental que permitan controlar las variables de temperatura y humedad relativa. De igual modo se detecta inseguridades basadas en las políticas de seguridad tanto físicas como lógicas especialmente en el uso de las credenciales y en el cifrado de la información.

6. En los equipos de cómputo de las diferentes dependencias de la empresa QWERTY S.A., se detecta vulnerabilidades como: mala configuraciones de los equipos PC, Daños por variaciones de voltajes e idas de energía eléctrica, falta de mantenimientos preventivos y correctivos de los descritos, falta de cuidados a las políticas de credenciales y finalmente flaquezas por factor humano.

7. En los equipos de servicio y comunicación de la red de la empresa QWERTY S.A., se localizan debilidades en cuanto a deficiencia e inseguridades en la configuración de algunos de los equipos de red tales como: puntos de acceso switch’s y Router’s. De igual manera, falta mecanismos de monitoreo, controles de acceso, aplicación y empleo de políticas de seguridad dentro de la red y finalmente la aplicación de cifrados de protección de datos.

8. En firewall se encuentran inseguridades tales como: controles de acceso no autorizados, usos incorrectos del software y del hardware, conexiones de equipos no permitidos, configuraciones inadecuadas y finalmente la degradación del servicio.

9. En el proveedor de servicio de internet (ISP), se hallan vulnerabilidades como: fugas de información, accesos no autorizados al servicio y gran número de puertos abiertos.

10. En cuanto al correo electrónico institucional se localizan debilidades tales como falsas noticias y Sendmail.

11. Los técnicos de mantenimiento poseen vulnerabilidades tales como: Ausencia de capacitaciones en temas relacionados con sistemas de seguridad de la información, como así misma falta de charlas informativas referentes a ingeniería social y de cómo evitarlas. De igual manera el exceso de confianza de los empleados con su entorno y finalmente falta de idoneidad en el personal contratado.

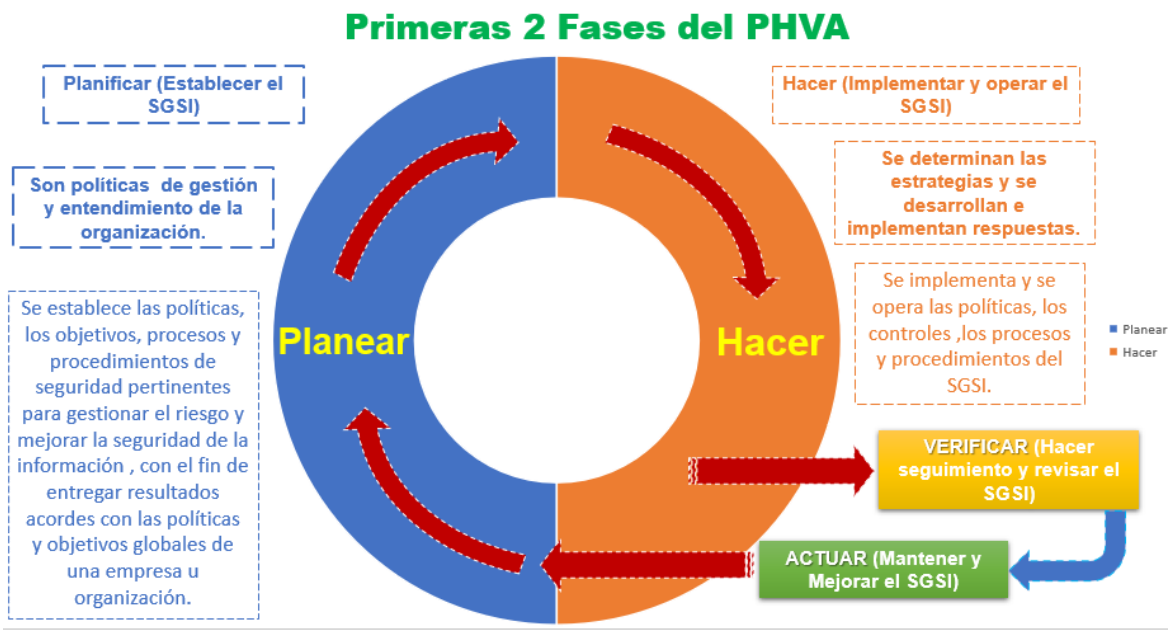
7.2. PROPUESTA DEL SGSI

En esta propuesta se diseña, se establece y mejora el sistema de gestión de la seguridad de la información del departamento de sistemas del caso de estudio de la empresa QWERTY S.A., en donde se lleva acabo la valoración y el tratamiento de los riesgos según los activos de información que posea la entidad y finalmente se adaptan a los requerimientos de la organización, para lo cual se tiene:

7.2.1. Diseño del plan del SGSI

Para llevar a cabo el diseño del modelo de seguridad y privacidad de la información para la empresa QWERTY S.A, se basa en la norma NTC-ISO/IEC 27001:2013. De acuerdo a lo anteriormente descrito, se establece, se gestiona y se implementa el SGSI para el caso de estudio de la empresa propuesto, basándose en las 2 primeras fases del modelo PHVA encontradas en suscrito estándar, la cual se describe de la siguiente forma:

Figura 1. Modelo PHVA aplicado a los procesos y estructura del SGSI.



Fuente: NTC-ISO/IEC 27001.

7.2.1.1. Contexto de la Organización.

En el contexto de la organización para la empresa QWERTY S.A, se efectúa el estudio y análisis del escenario, como así mismo la identificación de los activos de información presentados en la tabla 1 del descrito documento y finalmente el reconocimiento de los riesgos y vulnerabilidades de la organización mencionada.

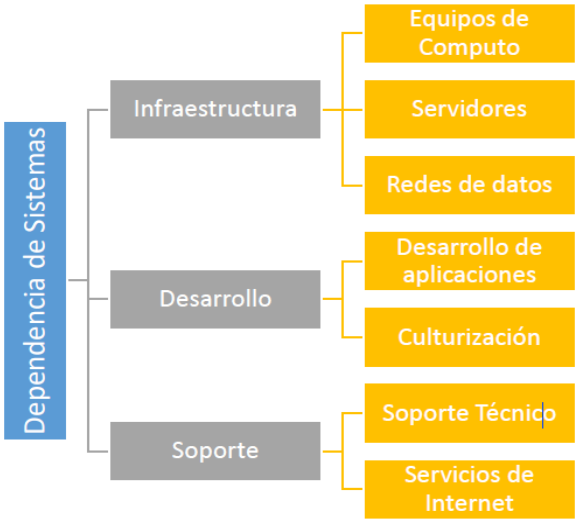
A. Estudio Del Escenario

I. Análisis del escenario.

En el departamento de sistemas de la empresa QWERTY S.A., nos presenta un escenario de una entidad del sector tecnológico que busca el desarrollo de la población colombiana con el uso de las TI. QWERTY S.A., cuenta con una comunidad de 120 trabajadores distribuidos en las diferentes dependencias de la empresa, entre los cuales se encuentran directivos, administrativos y operativos, quienes hacen uso de forma regular de los medios de información para consultar datos. Así mismo cuenta con unas dependencias del área de sistemas que son infraestructura, desarrollo y soporte, las cuales brindan apoyo a cualquier

requerimiento a su infraestructura tecnológica de un tiempo de 24/7, la cual se describe en el siguiente organigrama a continuación:

Figura 2. Organigrama de las dependencias de sistemas de la empresa QWERTY S.A.



Fuente: ECBTI-UNAD.

Además, Cada una de las dependencias del área de sistemas posee sus funciones y asistencias en la entidad como fueron descritas en el organigrama anterior, con el fin de mantener un óptimo desempeño en los servicios tecnológicos, como así mismo contar con un sistema de seguridad de la información en donde les brinde integridad, confidencialidad y disponibilidad en sus soluciones.

Igualmente, cabe mencionar que la empresa posee un canal de internet de 25 megas en ancho de banda dedicado para poder dar desarrollo a sus actividades rutinarias.

B. Compromiso.

La empresa QWERTY S.A., y su alta dirección desea demostrar liderazgo y compromiso ante cada uno de sus colaboradores y trabajadores que se encuentran en las diferentes dependencias de la institución, es decir que de acuerdo a la norma NTC-ISO/IEC 27001:2013, se da conocer la circular informativa No.001 del 2019 relacionada con los SGSI, en donde se establece los requerimientos mínimos de seguridad de la información, como dar cumplimiento de cada uno de sus criterios,

políticas de seguridad y controles, con el fin de brindar protección y seguridad a cada uno de los activos de información de suscrita empresa y todo lo anteriormente descrito, basados en la confidencialidad, integridad, disponibilidad y no repudio de la información.

De igual manera la alta dirección y cada uno de los responsables de las diferentes dependencias de la empresa QWERTY S.A., asigna responsabilidades y autoridad para asegurar el SGSI conforme a los requisitos del estándar de calidad, como de igual manera informa y documenta el desempeño y aplicabilidad del mismo.

C. Conocimiento de la organización y su contexto.

En el caso de estudio de la empresa QWERTY S.A., se fijan los términos necesarios para la realización de sus diferentes procesos y así conseguir la aprobación y conformidad de los artículos y prestaciones de servicios en cada una de sus fases y técnicas a ejecutar.

De acuerdo a lo anteriormente descrito, estos discernimientos o conocimientos que se mantienen actualizados y en disposición a personal nombrado y responsable de la prestación de estos servicios, ante las diferentes dependencias de la entidad tecnológica que se estudiando y así utilizar esta información para capacitar y dar a saber las diferentes políticas y normas que se están implementando para la protección de cada uno los activos de información de la organización QWERTY S.A., cuyas estrategias e instrumento a notificar son los siguientes:

- Documentación controlada por el sistema integrado de gestión de la empresa QWERTY S.A.
- Eventos realizados por la empresa como: capacitaciones, salidas pedagógicas y eventos comunales.
- Documentos que hacen referencia a unidades misionales de la empresa, como así mismo normas, políticas, estándares y circulares que informen a la comunidad institucional. (MANUAL DEL SISTEMA DE INTEGRADO DE GESTIÓN, 2018)[14]

[14] UNAD (2018). MANUAL DEL SISTEMA DE INTEGRADO DE GESTIÓN [Ebook] (11th ed., p. 7). Bogotá D.C. Recuperado de: https://sig.unad.edu.co/documentos/sgc/manuales/M-1.pdf?v10

D. Comprensión de las necesidades y expectativas de las partes interesadas.

La empresa QWERTY S.A., en compresión de las necesidades y de las partes interesadas tanto interna como externa se presenta de la siguiente manera:

Tabla 2. Matriz de partes interesadas internas.

Parte interesada	Necesidad/expectativa	¿Qué hace la empresa para atender el requisito?
Funcionarios	Asignación salarial justa.	Se determina código y el cargo jerárquico en el manual de funciones, requisitos, desafíos y competencias profesionales para las ocupaciones del personal de planta para el caso de estudio de la empresa QWERTY S.A, el cual se fundamenta en el Decreto Nacional para la determinación de salarios a los funcionarios públicos o administrativos.
	Contar con los recursos necesarios para cumplir con las funciones (fiscos y tecnológicos)	El capital es asignado y aprobado por la Junta Nacional para la vigencia del ministerio de trabajo, el cual compete al Plan Estratégico y las necesidades de las áreas de la entidad a cubrir.
	Cumplimiento en los pagos de nómina y de derechos laborales.	Se fija una fecha de pago de salario firme e integro para los 12 meses del año, donde integra cada uno de sus procedimientos y previsiones en el periodo de labor para fijar la liquidación y pago de prestaciones efectuadas. Así mismo se define las fechas de cierres financiero que implica a los procesos de nómina de QWERTY S.A.
	Programa de bienestar laboral que tenga en cuenta las necesidades de los funcionarios.	Plan de bienestar adoptado mediante Resolución nacional 667 de 2017.
	Cursos de preparación acorde a los requisitos y obligaciones de los cargos en la entidad.	Plan institucional de Capacitación empleado mediante Resolución Nacional del 2018.
	Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST).	SG-SST, mediante la Resolución Nacional 322 de 2017, Incorpora y define políticas y propósitos de la empresa como tal.

Junta Directiva	Cumplimiento de la misión de la Entidad	Se tiene definido el Plan Estratégico de la Entidad, en el cual se encuentra alineado a las directrices de la Entidad y el cual se concreta en las actividades definidas para cada vigencia y se le hace su respectivo seguimiento.
	Dar Cumplimiento a los objetivos y programas autorizados.	Informe y documentación de la gestión y tramites trimestrales. A través del Comité de Desarrollo Administrativo se efectúa el seguimiento y búsqueda del cumplimiento de la ejecución presupuestal, en donde se lleva un control de la realización del Plan Anual de Adquisiciones y de acción de vigencias, en la cual el registro de evidencia se realiza en las actas del Comité.
	Fases y procesos éticos y profesionales sustanciados y determinados acorde a los diferentes procedimientos, que respalden y aseguren la protección jurídica frente a una demanda que pueda afectar el patrimonio del caso de estudio de la empresa QWERTY S.A.	• Inspección de la segunda apelación sobre los fallos de primera apelación. • Comunicación de la directrices y normas jurídicas. • Emisión de las sugerencias técnicas. En caso de presentarse una demanda, como última instancia se debe efectuar un acuerdo ante el Comité de conciliación.
	Inspección y control ético profesional activo y efectivo de cada una de las actividades de ingeniería que se desenvuelvan internamente en la entidad y en la región.	Está incluido en el Plan de Acción 2018 de la empresa de caso de estudio.

Fuente: COPNIA (Concejo Profesional Nacional de Ingeniería).

Tabla 3. Matriz de partes interesadas externas.

Parte interesada	Necesidad/expectativa	¿Qué hace la empresa para atender el requisito?
Contratistas	Cumplimiento de lo pactado en los contratos	Nombramiento de un supervisor para que este sea la persona de oficio y sea el canal de comunicación entre la empresa QWERTY S.A y el contratista. Además, otra función del supervisor es efectuar tramites de los compromisos de la organización establecidos en el Contrato. Este Procedimiento se encuentra documentado en el acta de “Supervisión de contratos".
Entes de Control	Atención y vigilancia oportuna a cada uno de los requerimientos pertinentes.	Se envía por parte de la Dirección General la petición enviada por parte el ente de control a la Oficina de inspección Interno, con el fin de regular y compaginar con las áreas la respuesta y solución. Una vez aceptada, revisada, y consolidada el dictamen, se asignará el escrito a la Dirección General para firma y envió en las fechas establecidos para el requerimiento. Además, la Programación de entregas de informes de requerimientos de ley, se efectuará por parte de la Oficina de Control Interno para cada vigencia.
Investigados	Poder informarse y asesorarse de las actuaciones y fases en las que se encuentra el proceso ético profesional.	Se elaboran las notificaciones acordes a lo dispuesto en la Ley 1437 de 2011. Se atienden las solicitudes de consulta de los procesos e informes concernientes y correspondientes a la ley, procedimiento AC-pr-01 Peticiones, quejas y reclamos dentro de la organización.
	Los derechos al debido proceso, a la defensa técnica y a la economía procesal deben ser aplicados durante y en el curso del proceso.	Se cuenta con profesionales idóneos para adelantar los procesos disciplinarios. En la segunda apelación se verifica los fallos de la primera apelación y en caso de contemplar violaciones al debido juicio o proceso se procede a corregir las situaciones y circunstancias.

Oferentes	Información técnica clara y concisa de las obligaciones y necesidades de la organización con el fin de participar en los procesos de clasificación y selección.	Se dispone tanto en la investigación previa como en el pliego de condiciones los datos necesarios en relación al bien o servicio a estipular, como así mismo las condiciones que deben efectuar los oferentes para poder asociarse en el proceso de selección. Lo mismo se fija en la información de la convocatoria pública que se realiza. Además, constantemente se establece algunos requisitos técnicos del bien o servicio a contratar.
	Conocer e informarse del resultado de su participación en cada uno de los procesos de selección.	La dependencia de contratación pública dentro del término de ley, debe publicar las evaluaciones dentro de las fechas indicadas en el cronograma de actividades a lo que respecta a los términos legales para que oferentes efectúen observaciones al mencionado.
Profesionales competencia de la empresa QWERTY S.A (Nacionales y Extranjeros)	Conocimiento de las funciones del caso de estudio de la empresa QWERTY S. A	La publicación se realiza a través de los diferentes medios de comunicación de la entidad con el fin de llegar a los diferentes sectores públicos, según el plan de trabajo del área de comunicaciones. En el Plan de Acción de la empresa de estudio, se tiene determinada cada una de las actividades a Identificar, documentar, proponer y coordinar para los posibles espacios públicos y privados de la empresa QWERTY S.A., en donde la descrita entidad busca un reconocimiento ante la comunidad con el fin de socializar las funciones misionales.
	Conocimiento del Código de Ética.	Está incorporado y establecido en el plan de acción de la empresa en donde dice: • Desarrollar cátedra virtual de ética como articulación preventiva de la inspección, control y vigilancia de la empresa QWERTY S.A. •
	Conocimiento de las funciones de la empresa QWERTY S. A	Publicación a través de diferentes medios de comunicación con el fin de llegar a los distintos medios públicos, según lo establecido en el plan de trabajo de la dependencia de comunicaciones de la empresa QWERTY S.A.
	Página web de la empresa QWERTY S.A.	Diseño y estructuración del sitio web de dicha entidad y su publicación.

	Transparencia de los datos e información.	En el sitio web se implementaron los factores de táctica del Gobierno en Línea, en donde MINTIC describe lo siguiente: • Fiscalización de cada uno de los contenidos de la sección de Transparencia y acceso a la información pública. • Verificación y fiscalización de las acciones administrativas de cobranza por divulgación y reproducción de la información de la entidad. • Revisión y actualización de los inventarios de cada uno de los activos información según los mecanismos y normas de gobierno en línea. • Publicación de mecanismos de accesibilidad de los usuarios en situación de discapacidad a la información del sitio web de la descrita Entidad. •
Quejosos	Información sobre las quejas interpuestas.	Notificaciones que por ley se deben realizar al quejoso, Implementado en el procedimiento Procesos Ético profesionales.
Sociedad	Reconocimiento institucional	En el plan estratégico de la empresa QWERTY S.A., se fijó como táctica lo siguiente: • Diseño e implementación de tácticas de comunicación para el logro de reconocimiento institucional a nivel interno y externo de la entidad. •
	permitir e incentivar articulaciones para interponer quejas.	Por medio de la Área de Atención al Ciudadano, se establecieron canales de atención al usuario, los cuales pueden ser: • Telefónica • Presencial, • E-mail • Sitio Web y chat en línea.
	Actuación con imparcialidad y justicia.	Se tienen establecido los Principios y Valores, los cuales fueron adoptados e implantados mediante la Resolución Nacional 1446 del 21 de diciembre de 2015.

	Cumplimiento y ejecución de la Inspección y Control por parte de la empresa QWERTY S.A.	Las técnicas de Inspección, control y vigilancia, están descritas en cada articulación de sistema para la vigencia las actividades de inspección, control y vigilancia en su jurisdicción, área y dependencia. De igual manera se efectuará el análisis de la viabilidad jurídica, con el fin de recopilar la documentación para imposición y recaudo de multas derivadas del proceso de inspección, control y vigilancia de la Empresa QWERTY S.A.
	Investigaciones disciplinarias efectivas.	Seguimiento y búsqueda de los acuerdos y los términos de ley de cada uno de los procesos ético profesionales, de manera permanente por parte de los líderes de la investigación.
	Sanciones justas para los investigados	Los correspondientes Procesos ético profesionales adelantados por las 2 apelaciones.
	Uso racional de los recursos	Con el establecimiento de los regímenes de austeridad del gasto, este está amparado con Resolución Nacional 829 del 2016, en donde cada año se especifican lineamientos para que los gastos de la lista de pagos por nomina estos realicen acorde a las políticas ya establecidas, generen un ahorro de los bienes y así posean una mayor efectividad en el uso y utilización de los mismos. Además, cada año la obligación presupuestal de cada vigencia, debe ser tenida en cuenta en cada uno de los lineamientos de austeridad, como así mismo los contenidos políticos, la disponibilidad de los recursos líquidos y finalmente las limitaciones frente a la generación de ingresos propios.

(Álvarez Ledesma, torres Ruiz & Ochoa Arbeláez, 2018)[15]

Fuente: COPNIA (Concejo Profesional Nacional de Ingeniería).

[15] Álvarez Ledesma, A., torres Ruiz, G., & Ochoa Arbeláez, R. (2018). *Parte interesadas* [Ebook] (2nd ed., pp. 1-6). Bogotá D.C. Recuperado de: https://copnia.gov.co/sites/default/files/uploads/mapa-procesos/archivos/direccionamiento-estrategico/partes_interesadas.pdf

7.2.1.2. Liderazgo

A. Alcance

El desarrollo del SGSI de la empresa QWERTY S.A., poseerá como desarrollo las primeras 2 fases del PHVA de acuerdo a la norma ISO/27001:2013, la cual posee las siguientes actividades:

- Descripción de los activos de la información descritos en el caso de estudio propuesto, sobre los cuales se establecerán medidas de protección según el estándar NTC-ISO/IEC 27001:2013.
- Reconocimiento de contingencias, amenazas, vulnerabilidades y riesgos de seguridad hallados en cada uno de los activos de información del caso de estudio de la empresa QWERTY S.A propuesto.
- Ejecución de las acciones para el tratamiento de riesgos y oportunidades de la entidad.
- Establecimiento de propósitos y objetivos de seguridad de la información en las funciones y niveles pertinentes.
- Realización del análisis y peritaje de los riesgos con el fin de implementar una calificación y apreciación cuantitativa o cualitativa de las consecuencias del tratamiento a gestionar.
- Análisis y reconocimiento de los diferentes controles empleados para proteger y salvaguardar los activos de la información de la empresa QWERTY S.A.

7.2.1.3. Planificación.

A. Acciones para tratar riesgos y oportunidades.

I. Generalidades.

De acuerdo a la información dada del caso de estudio de la empresa QWERTY S.A., sobre el discernimiento de la organización y de su entorno, como así mismo del estudio de los requisitos y probabilidad de las partes interesadas, en donde se determinarán las contingencias y oportunidades que son indispensables de tratar, con el fin de asegurar el SGSI y prevenir los efectos indeseados a los activos de la información y finalmente lograr su mejora continua dentro de la entidad.

II. Valoración de riesgos de la seguridad de la información.

La empresa QWERTY S.A, define y aplica las fases de valoración y evaluación de riesgos de la seguridad, en donde se establece y se mantiene los criterios, como así mismo la identificación de los riesgos de la seguridad de los datos y finalmente el análisis y evaluación de los mismos.

De acuerdo a lo anterior, a continuación, se dará a conocer la información el mapa de riesgos de la entidad QWERTY S.A., según las acciones para tratar riegos y oportunidades y la valoración de riesgos de la seguridad de la información dándole clic en el siguiente Link:

https://drive.google.com/file/d/1Gz8Q3fOESyVFZio26Qb1A2gK33zVXVI-/view?usp=sharing ("Mapa de Riesgos - Gestión Tic 2016 - RISEM2016", 2016)[16]

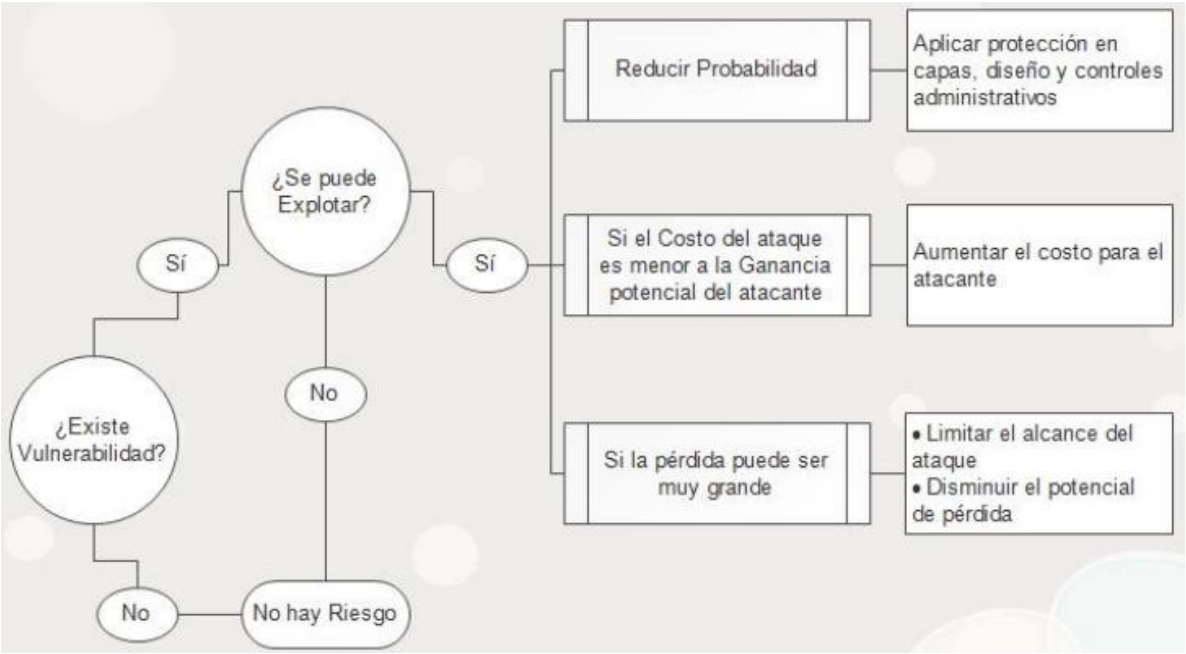
III. Tratamiento de riesgos de la seguridad de la información.

La empresa QWERTY S.A., define, aplica y adopta técnicas para la implementación de procedimientos con el fin de tener un control sobre los diferentes tratamientos de los riesgos y vulnerabilidades de la entidad; para así poder disponer de los controles necesarios para dicho tratamiento, los cuales permiten prevenir los riesgos y vulnerabilidades encontradas en nuestro sistema de información. A continuación, se explicará gráficamente el tratamiento del riesgo, en caso de que exista alguna vulnerabilidad:

---

[16] Mapa de Riesgos - Gestión Tic 2016 - RISEM2016. (2016). Recuperado de: http://www.fusagasuga-cundinamarca.gov.co/Transparencia/Paginas/MODELO-INTEGRADO-DE-PLANEACION-Y-GESTION.aspx?Paged=TRUE&PagedPrev=TRUE&p_SortBehavior=0&p_FileLeafRef=Mapa+Riesgos+-+Desarrollo+Integral+-+RISEM2016.xls&p_ID=69&PageFirstRow=31&&View=%7B870D54B1-13E5-4258-9453-DC58346CF7D3%7D

Figura 3. Estrategias para el tratamiento de riesgos en la empresa QWERTY.



Fuente: Facultad de Tecnología – Universidad Distrital Francisco José de Caldas.

Desde otra perspectiva, en el momento de que ocurra alguna vulnerabilidad es indispensable aplicar técnicas que aseguren la disminución de la posibilidad de que la debilidad sea utilizada, es decir que cuando esta sea explotada, esta deberá implementar capas de protección en sus diseños y controles con el fin de empequeñecer el riesgo o evitar que este ocurra.

Por otro lado, en caso de que el valor del ataque sea menor que el rendimiento potencial del mismo, es necesario aplicar protección con el fin de reducir la motivación, incrementando el valor del agresor.

De igual manera, cuando se sufra perdidas de gran magnitud, es necesario implementar técnicas y métodos para mitigar el riesgo, reduciendo así el potencial del daño.

Figura 4.Estrategias para el tratamiento de riesgos en la empresa QWERTY S.A.

ESTRATEGIAS PARA TRATAMIENTO DE RIESGO				
Probabilidad	**3 - Alta**	3.Zona de riesgo Moderado Tratamiento: Reducir la probabilidad de ocurrencia Evitar el riesgo	6. Zona de riesgo extremo Tratamiento: Reducir el riesgo Evitar el riesgo Compartir o transferir	9.Zona de riesgo Extremo Tratamiento: Reducir el riesgo Evitar el riesgo Compartir o transferir
	2 - Media	2. Zona de riesgo Bajo Tratamiento: Reducir la probabilidad de ocurrencia	4.Zona de riesgo Moderado Tratamiento: Reducir el riesgo Evitar el riesgo	6. Zona de riesgo extremo Tratamiento: Reducir el riesgo Evitar el riesgo Compartir o transferir
	1 - Bajo	1. Zona de riesgo Bajo Tratamiento: Asumir el riesgo	2. Zona de riesgo Bajo Tratamiento: Reducir el riesgo Evitar el riesgo	3.Zona de riesgo Moderado Tratamiento: Reducir el riesgo Evitar el riesgo
		1 - Bajo	**2 - Medio**	**3 - Alto**
		Impacto		

Fuente: Facultad de Tecnología – Universidad Distrital Francisco José de Caldas. (Plan de Implementación del SGSI basado en la norma ISO 27001:2013 para la empresa Interfaces y soluciones, 2017)[17]

De acuerdo a lo anteriormente descrito, a continuación, se procederá a efectuar el nivel de criticidad de cada uno de los activos de información de la dependencia de sistemas de la empresa QWERTY S.A., relacionados en la **Tabla 1,** los cuales se presentan de la siguiente manera:

[17] Plan de Implementación del SGSI basado en la norma ISO 27001:2013 para la empresa Interfaces y soluciones. (2017). [Ebook] (1st ed., pp. 52-53). Bogotá, D.C. Recuperado de: http://repository.udistrital.edu.co/bitstream/11349/6737/1/MoyanoOrjuelaLuzAdriana2017.pdf

Tabla 4. Nivel de Criticidad para evaluar los activos de información para la empresa QWERTY S.A.

CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD	
NIVEL DE CRITICIDAD	**DESCRIPCION**
Alto	La empresa QWERTY S.A., se verá seriamente afectada y puede generar sanciones elevadas y afectar la credibilidad de la entidad y de sus procesos.
Medio	El activo puede afectar de forma parcial una operación o un proceso. Las pérdidas o afectación pueden ser moderadas.
Bajo	El activo puede afectar una tarea aislada de la operación o del proceso. Las pérdidas o afectación serían menores y la entidad no incurriría en sanciones.

dado lo anterior, el propósito de efectuar el nivel de criticidad es de realizar un reconocimiento, una organización y una estimación de los activos de información de la entidad, en donde nos posibilitara puntualizar la criticidad y significación de un activo dentro de un SGSI, de tal manera que se proteja y se salvaguarde la información y que se garantice los controles apropiados de la seguridad de los datos y todo esto con el fin de protegerlos de los posibles riesgos que se puedan presentar. (Ramírez Rey, Martínez Rodríguez & Parrado Rodríguez, 2019) [18]

[18] Ramírez Rey, C., Martínez Rodríguez, M., & Parrado Rodríguez, V. (2019). GUÍA PARA EL LEVANTAMIENTO Y VALORACIÓN DE ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN [Ebook] (2nd ed., pp. 9-10). Bogotá. Recuperado de: https://www.minsalud.gov.co/Ministerio/Institucional/Procesos%20y%20procedimientos/ASIG03.pdf

Tabla 5. Nivel de Criticidad de los activos de información a cargo de la dependencia de sistemas de la empresa QWERTY S.A.

ID	Nombre del Activo	Tipo de Activo	Descripción	Ubicación	Cantidad	Nivel de Criticidad		
						Alto	Medio	Bajo
A1	Servidor de Impresión: Servidor marca Dell en torre PowerEdge T440 Ver ficha técnica	Hardware	Equipo de cómputo que conecta dos impresoras: Destinadas a: Una (1) Impresora HP LaserJet Enterprise serie 600, activo que brinda el servicio para la dependencia de nómina y facturación. Permite la concurrencia de hasta 25 usuarios y el volumen mensual de impresión es de 200 a 25000 páginas.	Oficina de nómina y facturación	1			
		Hardware	Una (1) Impresora SMART MultiXpress M4370LX, impresora que ofrece el servicio de escáner e impresión con un ciclo de trabajo de hasta 300000 páginas mensuales con capacidades de red alámbrica e inalámbrica. Impresora destinada para el servicio de directivos y administrativos y docentes.	Dependencia directiva y administrativa	1			
A2	Servidor de archivos FTP: Servidor marca Dell en torre PowerEdge T130	Hardware	Equipo de cómputo que tiene como función el almacenamiento y la administración de los archivos que se están generando en el interior de la organización como son: Digitalización de documento de entrada y de salida, audios generados en reuniones,	Oficina antigua de sistemas	1			

	Ver ficha técnica		asambleas y otro tipo de encuentros, video, generados por docentes y funcionarios. Dentro de las políticas de uso, para este servidor solo pueden tener acceso las personas autorizadas para los fines correspondientes.					
A3	Página web del Plan Máximo Ver ficha proveedor	Servicio de comercio electrónico	Servicio contratado con la empresa Godaddy.com La página web tiene como objeto la publicación de contenido relacionado con el modelo negocio. Está construida a partir del sistema gestor de contenidos dinámicos Joomla versión 2.5 El hospedaje web la infraestructura del servidor es Apache, PHP, MySQL.	Empresa Godaddy	1			
A4	Servidor de nómina y facturación Servidor marca Dell en torre PowerEdge T440 Características de servidor Apache 2.4.25 PHP 5.6.30 - 7.1.1 MySQL 5.7.17 PhpMyAdmin	Hardware	Plataforma de desarrollo propio. Tiene como función el almacenamiento y la administración de la nómina y facturación de la empresa QWERTY S.A.		2			

	4.6.6							
A5	Servidor DHCP Servidor marca Dell en torre PowerEdge T440	Hardware	Servidor que asigna y administra de forma dinámica el direccionamiento dentro de la organización		1			
A6	Equipos de cómputo para gestión del desarrollo tecnológico	Hardware	Equipos de cómputo donde se gestiona información online relacionada con el desarrollo del objeto social Presupuesto. Proveedores Órdenes de compra Inventarios.	Dependencia de desarrollo tecnológico	3			
A7	Cortafuegos Cisco ASA 5505 Ver ficha técnica	Hardware	Sistema de protección	Sistema de seguridad que está protegiendo a la red de datos, de intrusiones que se puedan presentar en la red	1			
A8	Equipos de Computo Sistemas operativos win10 Pro	Hardware-software	Equipos destinados para el desarrollo del objeto social	Dependencia de control y seguimiento	10			
A9	Equipos de Computo	Hardware	Equipos destinados para el desarrollo del objeto social	Dependencia de prueba de software.	5			
A10	Puntos de acceso alámbricos (hub)	Hardware	Dispositivos de red encargados de la interconexión de la red de datos.	Red de datos del centro.	4			

A11	Switch's cisco catalyst 2960	Hardware	Dispositivos de red encargados de la interconexión de la red de datos.	Red de datos del Centro.	6			
A12	Técnicos de mantenimiento	personal	Personal técnico encargado de realizar el mantenimiento preventivo y correctivo a los equipos PC.	Departamento de Sistemas.	2			
A13	Teléfonos IP	Hardware	Sistema de comunicación a través de teléfonos Voz IP, que comunica las oficinas y departamentos del centro.	Dependencias del centro	6			
A14	Puntos de acceso	Hardware	Puntos de acceso al servicio de internet en el campus universitario.	Departamento de sistemas[19]	2			

[19] Universidad Nacional Abierta y a Distancia Escuela de Ciencias Básicas de Tecnología e Ingeniera. (2019). *Escenario Dos (Enfoque Directivo - Administrativo)- Propuesta para el desarrollo de la alternativa de grado como Proyecto Aplicado* [Ebook] (1st ed.,Ibid., p. 3,4 y 5).

IV. Técnicas para el tratamiento del riesgo.

Según las prioridades de la empresa QWERTY S.A. y el nivel de riesgo descubierto y localizado, se establecen distintas técnicas para el tratamiento del riesgo detectado, el cual es el siguiente:

- **Evitar:** Para eludir un riesgo se parte del fundamento de que la probabilidad es alta y simboliza un alto peligro para la empresa, porque podría causar consecuencias muy dificultosas en caso de que suceda un siniestro.

Además, ciertas formas de evitar un riesgo son: no entablando un nuevo proyecto determinado como no factible, excluyendo la labor que genera una amenaza o reemplazándola por otra que no sea tan riesgosa o que no realice tantas perdidas, como la anulación de alguna línea de fabricación, comercio y finalmente canal de distribución o reparto.

- **Prevenir:** Cuando decimos de las medidas de prevención, nos referimos al establecimiento anticipadamente de las políticas, estándares, procedimientos que conlleven a que mencionado acontecimiento de riesgo no ocurra o reduzca su probabilidad de ocurrencia, tales como:
  - Controles y pruebas de seguridad.
  - Preparación.
  - Inversión en información.
  - Diversificación.
  - Reducción del nivel de exposición.
  - Mantenimiento preventivo y correctivo.
  - Medicina preventiva.

- **Proteger:** Cuando hablamos de protección pensamos en medidas preventivas que actúan en el instante de presentarse el riesgo, sobre los activos lógicos y físicos que se están amenazado. Las medidas de protección más comunes son las siguientes:
  - Sistemas automáticos de protección.
  - Dotación para protección personal.
  - Plan de contingencia y emergencia.

- **Aceptar:** Esto denota que se debe asumir los riesgos que este atraiga y en el instante que ocurra. Los riesgos se aceptan cuando la constancia es baja y el impacto leve, y no colocas en peligro el equilibrio de la empresa.

- **Retener:** Estos se detienen cuando en forma planificada y se establece un fondo para responder ante las posibles pérdidas causadas por su ocurrencia. (Mejía Quijano, n.d.)[20]

- **Transferir:** Comúnmente esta opción financiera es aceptada por la entidad en caso de algún acontecimiento o contingencia residual o riesgo inherente; es decir que en la organización tras el establecimiento de estas protecciones o salvaguardas ya definidas, se deben evitar pérdidas potenciales en la entidades a contratar estos servicios, ósea que X entidad externa está especializada para asumir estos controles y reducir estas incidencias que afecten y causen daños de los diferentes activos de información en susodicha entidad. Dado lo anterior, la organización adquirirá pólizas de seguros con el fin de cubrir gastos de los cuales se generen o produzcan en caso de algún riesgo o vulnerabilidad a los activos informáticos de la entidad QWERTY S.A.

  De acuerdo a lo anteriormente descrito, y una vez hallado los riesgos existentes en la empresa QWERTY S.A., se procederá a declarar la aplicabilidad más conocida como SOA.

[20] Mejía Quijano, R. MEDIDAS DE TRATAMIENTO DEL RIESGO [Ebook] (pp. 1-2). Recuperado de: http://www.eafit.edu.co/escuelas/administracion/consultorio-contable/Documents/Nota%20de%20Clase%2010%20Medidas%20de%20Tratamiento%20del%20Riesgo.pdf

Tabla 6. Declaración de aplicabilidad (SOA) la empresa QWERTY S.A

RL: Requerimiento legal, **CO:** Obligación contractual, **RN/BP:** Requerimiento del negocio/Buenas prácticas, **RER:** Resultado de la evaluación de riesgos.

Controles ISO 27001:2013		**Comentarios (Descripción de la implementación /Justificación de la exclusión)**	**Seleccionar la razón**			
			RL	**CO**	**RN/ BP**	**RER**
Sec	**Objetivo de control/control**					
5.1	Directrices de la Dirección en seguridad de la información.					
5.1.1	Grupo de políticas para la protección de los datos.	La Dirección de la empresa QWERTY S.A., deberá emplear un sistema de aprendizaje y concientización sobre seguridad informática para cada uno de los empleados públicos y administrativos de las distintas áreas que conforman la entidad.	**X**		**X**	
6.1	Estructura interna.					
6.1.4	Contacto con comunidades de interés singular.	Es necesario poseer y estimar un acercamiento con determinadas entidades con el fin de tener anotaciones en sitios web especializados en seguridad informática para así infundir conciencia y crear confianza en las diferentes composturas de seguridad de la información con el fin de que la QWERTY S.A sea una empresa más efectiva en su ámbito tecnológico.			**X**	
8.1	Compromiso sobre los activos de información.					
8.1.1	Registro y balance de los activos.	Técnicas y métodos automáticos que posibiliten vincular los inventarios a los agentes o cuentadantes que mantienen el control de cada una de las existencias de los diferentes activos informáticos y de información que fueron impuestos a encargo de funcionarios públicos y administrativos que desempeñen sus labores.			**X**	

8.1.2	Propiedad de los activos	Métodos y técnicas contables que examinan automáticamente, los daños o perjuicios en la disposición de los activos informáticos, con el fin de eludir el desorden de los datos al momento de tramitar los estados financieros de la empresa QWERTY S.A.				**X**
8.1.3	Uso razonable de los activos.	Métodos y técnicas que deben considerarse como un manual de pautas vinculado con las buenas prácticas, con noción habitual y que lo que determina en la legislación del ordenamiento jurídico del estado; es así precisamente en donde se manejan las obligaciones y normas fundamentales que deben perseguir, en el cumplimiento de sus funciones. Además, todos los funcionarios públicos y administrativos de la empresa QWERTY S.A., deben ayudar a contribuir a salvaguardar los sistemas de información e informáticos.	**X**			
8.1.4	Reintegro de los activos.	Se determina como un ejercicio que debe ser habitualmente desempeñada por un individuo que posea buenos conocimientos en las TI, con el fin de mejorar la gerencia y administración la valoración devolutiva.			**X**	
8.2	Organización de los datos.					
8.2.3	Manejo de los activos.	Inspección interna del área Informática que va a proporcionar una mejor fiscalización de las funciones o acciones efectuadas en el manual con el fin de prevenir y corregir irregularidades que puedan afectar la actividad de la empresa QWERTY S.A.			**X**	
9.1	Requerimientos para el control de ingreso a la entidad.					
9.1.1	Políticas de inspección de ingreso.	Se encuentra estipulado en el manual de políticas de la entidad, el cual no está concretado totalmente, por lo tanto, es indispensable su implementación con el fin de confortar el acceso únicamente a la nómina autorizada.	**X**		**X**	
13.2	Reciprocidad de los datos e información					

	con las partes externas.					
13.2.1	Políticas y técnicas de intercambio de datos.	La alta dirección debe considerar la ejecución de sistemas de formación y concientización en los diferentes técnicas y métodos de seguridad de la información, con el fin de resguardar apropiadamente la información y los activos informáticos de la empresa QWERTY S.A.	**x**		**X**	
18.1	Cumplimiento de los requerimientos legales y contractuales.					
18.2.1	Revisión independiente de la seguridad y protección de la información.	La implementación de las políticas de seguridad nos permiten efectuar pruebas de acceso de manera controlada, sin malicia y sin producir daño alguno, con una apropiada proyección y planeación del personal especializado de la dependencia de sistemas de la empresa QWERTY S.A., se evidenciara de una forma más efectiva las vulnerabilidades a los que están expuestos los activos de información, con el fin de implantar técnicas y acciones correctivas más eficaces y así aumentar el nivel de seguridad de la información en la entidad descrita.			**x**	

Fuente: ECBTI-UNAD (Ruiz Peña, 2018)[21]

[21] Ruiz Peña, J. (2018). DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION (SGSI) BAJO LA NORMA ISO/IEC 27001:2013, EN LA COOPERATIVA MULTIACTIVA DEL PERSONAL DEL SENA, EN BOGOTA [Ebook] (pp. 135-137). Bogotá, D.C. Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17300/1/80267708.pdf

B. Objetivos de seguridad de la información y planes para lograrlos.

- **Objetivo:** El objetivo primordial para la empresa QWERTY S.A., es implementar políticas de seguridad en donde se dispone de normas y estándares necesarios para asegurar y respaldar la confidencialidad, integridad, disponibilidad y no repudio de los datos en cada uno de los procesos y actividades de susodicha entidad.
- **Planes:** se implantará controles técnicos y organizativos como asimismo políticas de seguridad, listas de chequeo dentro del SGSI de la empresa QWERTY S.A., con el fin de garantizar confidencialidad, integridad, disponibilidad y no repudio de los datos en cada una de las actividades y procedimientos que efectué la organización.

De acuerdo a lo anteriormente descrito, se procede a describir las políticas de seguridad de la empresa QWERTY S.A., las cuales son:

I. POLITICAS DE SEGURIDAD

1) POLITICAS DE SEGURIDAD DE LAS COMUNICACIONES.

Para proteger los ataques a los datos de la empresa QWERTY S.A desde cualquier ubicación de red tanto interna como externa, se pretende asegurar y limitar el acceso a la intranet mediante el control de los procesos tecnológicos y servicios dentro de la red local, cumpliendo las siguientes responsabilidades en las áreas de la informática, comunicaciones y finalmente en su personal, tales como:

- La dirección de tecnología Informática y de Comunicaciones es responsable de acoger e implementar medidas de seguridad con la conclusión de mantener siempre en línea los activos de la empresa QWEERTY S.A.
- La dirección de tecnología Informática y de Comunicaciones es responsable de establecer inspecciones de defensa con el fin de mitigar las diferentes vulnerabilidades y riesgos de seguridad halladas en el sistema de información y así evitar que estas sean enviadas a través de las diferentes redes de datos de la empresa QWERTY S.A.
- La dirección de tecnología Informática y de Comunicaciones es responsable de que las redes de datos estén seccionadas por dominios, servicios, cuentas de usuarios, extensiones, zona geográfica entre otros, los cuales sean necesarios y requeridos para la empresa QWERTY S.A.

- La dirección de tecnología Informática y de Comunicaciones es responsable de garantizar la configuración óptima de los diferentes mecanismo e instrumentos de seguridad perimetral del sistema interno de la intranet de la compañía.
- La dirección de tecnología Informática y de Comunicaciones es responsable de reconocer, demostrar, acreditar y justificar los servicios, protocolos y puertos de comunicación, facultados por la empresa QWERTY S.A., y así evitar un riesgo sobre activos de la empresa.
- La dirección de tecnología Informática y de Comunicaciones es responsable establecer mecanismos de defensa y custodia de las redes internas de la empresa con el finde evitar cualquier ataque de la red externa.
- La dirección de tecnología Informática y de Comunicaciones es responsable de salvaguardar la confidencialidad de la información coherente con el direccionamiento IP y enrutamiento de paquetes, que incluye la LAN de la empresa QWERTY S.A., hacia y desde el exterior.

2) POLÍTICAS DE TRANSFERENCIA DE INFORMACIÓN.

Para certificar la transferencia de los datos dentro de la empresa QWERTY S.A., se debe cumplir una serie de lineamientos, inspecciones y técnicas con la solución de proteger la seguridad de los activos como son su Integridad, Disponibilidad, confidencialidad y no repudio de los datos dentro de la empresa ya descrita.

Dado lo anterior, se debe tener en cuenta las siguientes responsabilidades en las áreas, dependencias y personal que conforma la empresa QWERTYS.A.:

- La dirección de tecnología Informática y de Comunicaciones es responsable de brindar servicios de reprocidad de información confiable, como así mismo de establecer procedimientos y controles de cifrado de la información, las cuales aprueben la formalización de procedimientos para la permutación de Información Digital, y así finalmente asegurar la información frente a divulgación o alteraciones no autorizadas.
- Los intercesores con quienes se intercambia los datos de la empresa QWERTYS.A., deben facilitarles una aplicación adecuada a los datos captados, en ejecución de las Políticas de Seguridad de la empresa como

tal, de los requisitos estipulados y de las técnicas de reciprocidad de los datos Físicos y Digitales, determinados y autorizados por nuestra entidad.

- Los procedimientos de información y tarea de la empresa, no deben cambiar datos delicados de la empresa QWERTY S.A., vía y acceso telefónico.

3) POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN.

Para certificar que todos los activos de información de la empresa QWERTY S.A., tengan un custodio y respalden o respondan la a preservación de la confidencialidad, entereza y disponibilidad de los datos en cada uno de los sectores de la entidad.

Dado lo anterior, se debe tener en cuenta las siguientes responsabilidades en las áreas, dependencias y personal que conforma la empresa QWERTY S.A.

Propietarios de los Activos:

- Los responsables deben estar al pendiente periódicamente la validez de sus autenticaciones con el fin de siempre reservar las credenciales y así llevar control sobre los activos.
- Los responsables deben realizar roles y controles de accesos a la información que está bajo su custodia, asignándoles a los demás usuarios que hacen uso de la información, permisos o restricciones necesarias para conservar su permanencia e integridad además de su confidencialidad.
- Los responsables deben ser consecuentes que los recursos procesados de datos, estos deben estar siempre constantemente revisados y supervisados por internos de la compañía por ende siempre tiene que manejar disponibilidad en el caso que se le requiera una auditoría interna, esto se realiza previa notificación con días de anticipación.
- Los Propietarios de los Activos en caso de algún retiro de alguno de los funcionarios de la empresa, deben revisar el estado físico funcional de los activos entregados por los funcionarios que entregan el puesto, esto con el fin de velar por su normal funcionamiento y reportar alguna novedad sea por perdida o ausencia en el caso que fuere lugar.

Guardián de los Activos:

- Los Guardianes deben confrontar periódicamente que la información tenga los permisos y roles para los cuales le fueron asignados a cada funcionario de la empresa.
- Los Guardianes deben comprobar que los accesos a archivos, magnéticos u ópticos de información, tenga un manejo adecuado a la ocasión y que estos no sean mal utilizados, en el caso que se presencie un uso indebido son los encargados de reportar la novedad a los propietarios de la información.

Experto de Seguridad

- El Experto debe efectuar un examen de riesgos de seguridad de modo periódico, valorando con esto, las grietas de seguridad de los activos de información descriptos.
- El Experto debe detallar los contextos de uso y protección de la información, tanto física, como digital.
- El experto debe efectuar exploraciones habituales de los recursos de la plataforma tecnológica y los sistemas de la empresa Bangov.

Experto de seguridad / Propietarios de los Activos / Guardian de los activos

- El Experto de seguridad en conjunto con los Guardianes y el propietario de los activos deben certificar la identificación de los activos de información de la empresa QWERTY S.A., generando con esto, la relación conveniente, y con el revisar que los mantenimientos periódicos se realicen, así como las capacitaciones al personal con todos los temas de seguridad y cuidado de la información.

4) POLÍTICA DE GESTIÓN DE LA VULNERABILIDAD TÉCNICA.

Para certificar las vulnerabilidades fichadas, se deben implementar utilizando la aplicación de metodologías de pruebas de garantía, con esto se asegura que estas reciban un tratamiento óptimo para lograr aminorarlas, estas deben ser aplicada por personal profesional de la SI de la empresa QWERTY S.A.

De acuerdo lo anteriormente descrito, se debe tener en cuenta las siguientes responsabilidades en las áreas, dependencias y personal que conforma la empresa QWERTY S.A:

- El Experto de Seguridad debe desarrollar la Metodología y manuales de pruebas de garantía para la empresa QWERTY S.A.
- El Experto de Seguridad debe desarrollar los lineamientos y encargos para la atenuación de vulnerabilidades detectadas, todo a su vez de la aplicación de las pruebas de garantía.
- El Experto de Seguridad debe monitorear, periódicamente, el sometimiento de los procedimientos de acción, hechos y ejecutados por el personal TI de la empresa QWERTY S.A.
- El área de TI debe reconocer, habitualmente, la actualización de nuevas debilidades técnicas y reportarlas a los administradores TI y los developers de los sistemas de la empresa QWERTY S.A.
- El área de Informática debe transformar y elaborar procedimientos de acción, para aminorar las debilidades técnicas, manifestadas en la infraestructura tecnológica y sistemas de la QWWERTY S.A.
- El área de Informática y Comunicaciones debe avalar los recursos tecnológicos y profesionales para la proyección y cumplimiento de las pruebas de efectividad. (MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ETITC, 2017)[22]

5) POLÍTICA DE CRIPTOGRAFÍA

La empresa QWERTY S.A., implementará métodos criptográficos buscando brindar criterios de seguridad (Catalunya 2016) como los que se relacionan a continuación:

- Confidencialidad.
- Integridad de datos.
- Autenticación.
- Autorización
- Irrefutabilidad

Los criterios de seguridad relacionados anteriormente, están aprobados previamente por el Comité de Seguridad de la Información CSI. Las normas para

[22] Escuela Tecnológica Instituto Técnico Central. (2017). MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ETITC [Ebook] (2nd ed., pp. 55-95). Bogotá. Recuperado de: http://www.itc.edu.co/archives/manualpiliticassi.pdf

el desarrollo de la política, deben indicar para cada caso y escenario, cómo será la aplicación de la criptografía en casos como: cifrado, autenticación electrónica, firma electrónica y prueba electrónica[23].

Para implementar dicha política, es necesario contar previamente con el procedimiento para la clasificación de la información que maneja la empresa, así como un correcto etiquetado de ésta.

Política de controles criptográficos

Estas permiten el aseguramiento de la forma apropiada y eficaz en que se hace uso de la criptografía en la empresa QWERTY S.A., en busca de la confidencialidad, la autenticidad y/o integridad de la información.

Controles de criptografía.

- Velar porque la información que esté clasificada como ultrasecreta, secreta y confidencial se encuentre cifrada para su uso. Los administradores del sistema deben realizar revisiones periódicas de las implementaciones tecnológicas de cifrado de acuerdo con la clasificación de los datos, para proteger su confidencialidad e integridad.
- El CSI debe verificar toda transmisión de información etiquetada como ultrasecreta, secreta, confidencial y restringida; previó análisis de su criticidad, además debe contar con herramientas de cifrado de datos. El desarrollo y establecimiento de estándares para la aplicación de controles criptográficos.
- Las soluciones criptográficas para los datos de negocio críticos se deben revisar anualmente.
    - Las comunicaciones que implican datos de negocio sensibles deben cumplir con los requerimientos criptográficos dispuestos por el CSI.
    - Las soluciones criptográficas para el acceso remoto se deben revisar anualmente.

- La información de negocio (información confidencial o información privada), definida por las regulaciones o leyes, debe ser cifrada en los sitios de almacenamiento y siempre que viaje sobre cualquier red.

---

[23] Catalunya, Universidad Oberta de. «Política de seguridad criptográfica de la Universitat Oberta de Catalunya.» 2016. https://seu-electronica.uoc.edu/portal/_resources/ES/documents/seu-electronica/Politica_Seguretat_Criptogrxfica_UOC-cat_ES.pdf.

- La información pública o que no necesite de protección de la confidencialidad, no requiere de cifrado.
- Los colaboradores no deben instalar ningún software de cifrado no validado y aprobado por el CSI.
- El CSI, debe verificar que la información sea clasificada por cada dependencia; previo análisis de su criticidad, y propender por la confiabilidad, seguridad y control de los respaldos de esta información.
- Los desarrolladores para todos los desarrollos deben hacer uso de los controles de criptografía establecidos por el CSI.

Gestión De Llaves

El CSI debe establecer los lineamientos para la administración y manejo de llaves de cifrado, en caso de requerirse.

La autenticidad y la integridad de documentos electrónicos se pueden verificar usando firmas digitales. Las siguientes consideraciones se deben tener en cuenta al utilizar firmas digitales:

- Proteger la confidencialidad de la llave criptográfica privada y la integridad de la llave pública.
- La calidad del algoritmo criptográfico usado.
- La legislación nacional que define la personalidad jurídica de estas firmas.

El CSI debe establecer los lineamientos para la gestión de llaves criptográficas de acuerdo con las necesidades de la entidad:

- Generación de llaves.
- Gestión de certificados digitales.
- Distribución de llaves.
- Almacenamiento de llaves.
- Revocación de llaves.
- Recuperación de llaves.
- Resguardo de llaves.
- Destrucción de llaves.
- El departamento de Infraestructura, con el apoyo del CSI, es responsable de supervisar todas las actividades con respecto a la gestión de llaves.
- Todas las herramientas para la creación de llaves criptográficas deben ser protegidas con los más altos niveles de Seguridad.

- Las llaves de cifrado deben ser gestionadas y protegidas. Esta protección debe incluir:
    - La creación y emisión de llaves
    - La confidencialidad de llaves privadas.
    - La integridad de llaves públicas.
    - La revocación de llaves.
    - La recuperación de llaves perdidas.
    - El resguardo de llaves viejas.
    - La destrucción de llaves obsoletas.

II. CONTROLES INDICADOS.

Atraves del reconocimiento, valoración y primacía de los riegos identificados, se ha fomentado un estudio e investigación sobre los controles a usar en su procedimiento y tratamiento.

Para el análisis y la inspección de controles de la empresa QWERTY S.A., nos hemos fundamentado en el anexo A del estándar de calidad ISO/IEC 27001:2013, el cual describe las pautas para efectuar la descripción y condición del sistema de información de la entidad relacionada anteriormente.

7.3. ADMINISTRACION Y GESTIÓN DE RIESGOS DE LA CIBERSEGURIDAD DE LA EMPRESA QWERTY S.A.

7.3.1. Metodología para el análisis y gestión de la seguridad de la información de la empresa QWERTY S.A., basada en MARGERIT.

7.3.1.1. Identificación y clasificación de los activos de información del caso de estudio de la empresa QWERTY S.A.

La identificación de los activos de información dentro de una empresa u organización son de gran importancia, ya que los descritos poseen un gran valor e la importancia para la entidad, es decir que hace referencia a las diferentes tipologías en las cuales se categorizan según el activo en donde se presentan. A continuación, los enunciaremos:

- [D] Datos
- [K] Claves criptográficas
- [S] Servicios
- [SW] Software
- [HW] Equipamento informático
- [COM] Redes de comunicaciones
- [Media] Soporte de información
- [AUX] Equipamento auxiliar
- [L] Instalaciones
- [P] Personal[24]

De acuerdo a lo anterior, en la tabla 1., se identificaron cada uno de los activos de información a cargo del departamento de sistemas del caso de estudio de la empresa QWERTY S.A.

7.3.1.2. Identificación de los riesgos que se exponen en el escenario 2 del caso de estudio de la empresa QWERTY S.A.

Partiendo que el riesgo es el “Grado de exposición de un activo que cual permite la materialización de una amenaza ocasionando daños a la compañía”. (Institución

---

[24] Amutio Gomez, M., Candau, J., Mañas, J., & Gonzales Barroso, J. (2012). Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. [Ebook] (3rd ed., p. 3). Recuperado de: https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html.

Universitaria Politécnico Gran Colombiano, 2016, p. 7)[25]. Dado lo anterior en el ítem *7.1.1.3. Identificación de los riesgos que presentan en el caso de estudio de la empresa QWERTY S.A.,* se describen cada una de las contingencias que se presentan en la entidad descrita anteriormente.

7.3.1.3. Identificación de la vulnerabilidades, amenazas y salvaguardas para la protección de manera eficaz y eficiente de los activos de información de la empresa QWERTY S.A.

Antes de presentar cada una de las vulnerabilidades, amenazas y salvaguardas de nuestro caso de estudio de la empresa QWERTY S.A., para la protección de cada uno de los activos de información de descrita entidad, como primera instancia se describirá un poco más el análisis y gestión de riesgos con el fin de entender su importancia e impacto que pueda generar en una empresa u organización.

Dado lo anteriormente descrito y partiendo que la seguridad informática se define como la preservación de la confidencialidad, la integridad y la disponibilidad de los sistemas de información [Tipton, 2006] (Manjarrez, Mogollón, Cortes & Dussan, 2016) [26] y reconociendo que en una organización se puede presentar diferentes riesgos y amenazas que comprometen cada uno de los activos de información y principalmente a los pilares de la seguridad informática que rigen a una organización. Dado lo anteriormente descrito, podemos decir que dentro de una entidad ya sea privada o pública, existe el estudio del análisis, gestión y control de riesgos dentro de la arquitectura de seguridad de su organización.

Cuando hablamos del proceso de gestión de riesgos, decimos que es la forma de comprender la evaluación previa de los riesgos del sistema informático y para ello debe efectuarse con una objetividad y rigurosidad, con el fin de dar cumplimiento a

---

[25] Fajardo Diaz, C. (2017). ANÁLISIS DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DE UN APLICATIVO DE GESTIÓN DOCUMENTAL LIDER EN EL MERCADO COLOMBIANO. [Ebook] (p. 15). Recuperado 5 marzo 2020, de: https://fliphtml5.com/zexxp/wfas/basic.

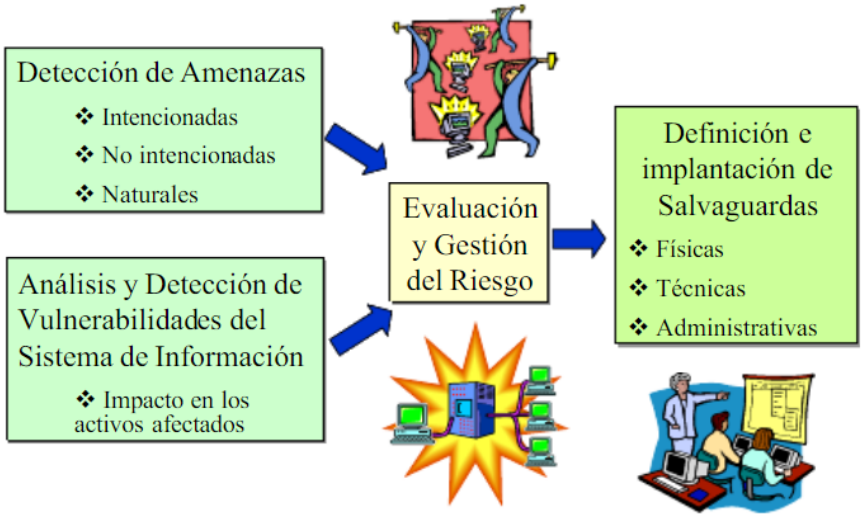
[26] Manjarrez, c., mogollón, e., cortes, i., & Dussan, l. (2016). identificación de riesgos en el tratamiento de datos personales a nivel de usuarios clientes de aplicaciones móviles en el sector del transporte público individual en Bogotá. recuperado el 25 agosto 2019, de: https://repository.ucatolica.edu.co/bitstream/10983/7831/4/identificacion%20de%20riesgos%20en%20el%20uso%20de%20apps%20de%20transporte%20publico.pdf

su funcionamiento con todas las garantías de ley; es decir que debe existir un equipo responsable de la evaluación de cada uno de los procesos propiamente dicho.

La gestión de riesgos se puede definir como el plan de implementación de ciertas salvaguardas en el sistema informático, la cual nos permite disminuir la probabilidad de que se materialice la amenaza o bien reducir la vulnerabilidad o el imposible impacto en la organización.

A continuación, mediante la siguiente figura se describirá el análisis y gestión de riesgos dentro de una organización.

Figura 5. Análisis y gestión de riesgos en una organización y para el caso de estudio de la empresa QWERTY.



Fuente: Álvaro Gómez Vieites. Anexo III Análisis y Gestión de Riesgos en un Sistema Informático.

De igual manera para poseer un mejor concepto y definición del estudio del análisis y gestión de riesgos en una organización, como lo es en nuestro caso de estudio de la empresa QWERTY S.A., debemos entender los siguientes términos:

1. **Recurso del sistema**
   Los **recursos** del sistema son los activos a proteger del sistema informático de la organización.
2. **Amenazas.**
   Se considera una **Amenaza a** cualquier evento accidental o intencionado que pueda ocasionar algún daño en el sistema informático, provocando pérdidas materiales, financieras o de otro tipo en la organización.

3. **Vulnerabilidades.**
   Una **Vulnerabilidad** es cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarles daños y producir perdidas en la organización.
4. **Incidente de seguridad.**
   Un **Incidente de Seguridad**, es cualquier evento que tenga o pueda tener como resultado la interrupción de los servicios suministrados por un sistema informático y/o posibles pérdidas físicas, de activos o financieras. Es decir, se considera un incidente, es a la materialización de una amenaza.
5. **Impactos.**
   El **Impacto**, es la medición y valoración del daño que podría producir a la organización un incidente de seguridad.
6. **Riesgos.**
   El **Riesgo** es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto en la organización.
7. **Defensas, Salvaguardas o medidas de seguridad.**
   Una **Defensa, Salvaguarda o medida de seguridad,** es cualquier medio empleado para eliminar o reducir un riesgo. Su objetivo es reducir las vulnerabilidades de los activos, la probabilidad de ocurrencia de las amenazas y/o el nivel de impacto en la organización.
8. **Transferencia del riesgo a terceros.**
   Como alternativa a la implantación de una serie de medidas de seguridad, una organización también podría considerar la transferencia del riesgo a un tercero, ya sea mediante la contratación de una póliza de seguros especializada o bien sea a través de la subcontratación de un proveedor especializado en ofrecer en determinados servicios de seguridad informática. (Gómez Vieites, n.d.)[27]

De acuerdo a lo anterior y una vez aclarado los términos y conceptos para el Análisis y gestión de riesgos en una organización y especialmente para nuestro caso de estudio de la empresa QWERTY S.A, a continuación, los describiremos:

---

[27] Gómez Vieites, A. Anexo III Análisis y Gestión de Riesgos en un Sistema Informático. Recuperado el 25 de agosto 2019, de: https://www.academia.edu/5971566/Anexo_III_An%C3%A1lisis_y_Gesti%C3%B3n_de_Riesgos_en_un_Sistema_Inform%C3%A1tico

Tabla 7. Identificación de las amenazas, vulnerabilidades y salvaguardas que se presenta a cargo del departamento de sistemas del caso de estudio de la empresa QWERTY S.A.

Nombre del Activo	Categorización[.] Cantidad(.)	Amenazas	Vulnerabilidades	Salvaguardas
Servidor de Impresión: **Servidor marca Dell en torre PowerEdge T440** **Ver ficha técnica**	[HW] Equipamento Informático - (2)	• Averías de origen físico y lógico. • Accesos no autorizados. • Errores de mantenimiento preventivo y correctivo. • Errores de actualización de equipos en cuanto a su parte de software. • Condiciones inadecuadas de temperatura o humedad. • Cortes eléctricos	• Falta de mantenimiento. • Daños por desgaste o defectos de fábrica. • Daños del servidor por falta de equipos que regulen variaciones de voltajes e idas de energía eléctrica.	• Protección de equipos. • Actualización constante del antivirus. • Listas de chequeo en los mantenimientos de software y hardware. • Diseño y aplicación de políticas de seguridad • Establecer equipos de protección de variación de voltajes (UPS, supresores de picos, estabilizadores etc.).
Servidor de archivos FTP: **Servidor marca Dell en torre PowerEdge T130**	[D] Datos - (1)	• Manipulación de hardware. • Robo de información. • Errores de administración de	• Carencia de configuraciones de seguridad en el servidor • Las copias de seguridad se encuentran en el mismo servidor, los cuales restablecen los datos e	• Diseñar y/o actualizar la política de seguridad de la información de la organización. • Definir un plan de tratamiento de incidentes

Ver ficha técnica		los sistemas y de su seguridad. • Errores de mantenimiento tanto de hardware como de software. • Desastres naturales • Averías de origen físico y lógico. • Daños por agua y fuego. • Indisponibilidad temporal en el acceso la información contenida en los servidores generada por un tercero no autorizado. • Modificación y/o alteración de la información y los servicios alojados en los servidores por un empleado con exceso de privilegios. • Fallos no intencionales causado por un empleado de la organización.	información en caso de daño o perdida. • El antivirus instalado en los servidores no se encuentra activo ni actualizado. • La configuración y administración de los servidores no se encuentra centralizada. • Ausencia de sistemas de control ambiental que permitan controlar variables como temperatura y humedad relativa en el área donde se encuentran instalados los servidores. • falta de mantenimiento de las políticas de seguridad en credenciales y cifrado de la información.	de seguridad de la información. • Establecer el procedimiento para el backup de la información, el cual debe estar en un contenedor de información diferente al cual le están realizando el backup. • Actualizar y depurar los directorios existentes, identificando las cuentas de usuario que no cumplan con las políticas de seguridad

		• Ataque destructivo • Caída del sistema por agotamiento de recursos.		
Servidor de nómina y facturación **Servidor marca Dell en torre PowerEdge T440** **Características de servidor** **Apache 2.4.25** **PHP 5.6.30 - 7.1.1** **MySQL 5.7.17** **PhpMyAdmin 4.6.6**	[SW] Software - (2)	• Denegación de servicio. • Errores de los usuarios. • Errores de mantenimiento y actualización de equipos. • Errores del administrador. • DoS. • Caída del sistema por agotamiento de recursos • Ataque destructivo • Manipulación de hardware. • Robo de información.	• Daños por desgaste. • Daños por variaciones de voltajes protección eléctrica regulada. • falta de mantenimiento de las políticas de seguridad en credenciales y cifrado de la información • Daños por mal uso o falta de capacitación en el manejo. • Mantenimiento inadecuado o ausencia. • Daño en la copia de seguridad. • El antivirus desactualizado.	• Definir un plan de tratamiento de incidentes de seguridad de la información. • Establecer el procedimiento para el backup de la información, el cual debe estar en un contenedor de información diferente al cual le están realizando el backup. • Actualización constante del antivirus. • Listas de chequeo en los mantenimientos de software y hardware. • Definir un plan de tratamiento de incidentes de seguridad de la información.
Servidor DHCP. Servidor marca Dell en torre PowerEdge T440	[HW] Equipamento Informático - (1)	• Averías de origen físico y lógico. • Accesos no autorizados. • Errores de mantenimiento	• Falta de mantenimiento. • Daños por desgaste o defectos de fábrica. • Daños del servidor por falta de equipos que regulen variaciones de	• Crear una política de seguridad para el manejo, uso y mantenimiento de equipos.

		preventivo y correctivo. • Errores de actualización de equipos en cuanto a su parte de software. • Condiciones inadecuadas de temperatura o humedad. • Cortes eléctricos • Caída del sistema por agotamiento de recursos	voltajes e idas de energía eléctrica. • falta de mantenimiento de las políticas de seguridad en credenciales y cifrado de la información • Daños por mal uso o falta de capacitación en el manejo.	• Actualización contante de las versiones del servidor. • Capacitación al personal técnico. • Listas de chequeo de los equipos. • Establecer equipos de protección de variación de voltajes (UPS, supresores de picos, estabilizadores etc.).
Página web del Plan Máximo **Ver ficha proveedor**	Servicios [S] - (1)	• Modificación y/o alteración de la información y los servicios alojados en los servidores por un empleado con exceso de privilegios. • Accesos no autorizados. • Denegación de servicios. • Alteración accidental de la información. • Difusión de software dañino.	• Errores en la gestión de recursos y configuraciones. • Fallos en la depuración de alguna aplicación o en la misma programación del sitio web. • Permisos, privilegios y/o control de acceso. • Ejecución de códigos malintencionados, SQL injection • Factor Humano	• Identificación de los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red que se contraten con el proveedor del servicio. • Contante actualización con el contrato de soporte del servicio con el proveedor.

		• Perdidas de autenticación. • Redirección y reenvió no validos • Fallo de servicios de comunicación. • Caída del sistema por agotamiento de recursos.		
***Equipos de cómputo para gestión del desarrollo tecnológico** *****Equipos de Computo (Dependencia de prueba de software) ***Equipos de Computo Sistemas operativos win 10 Pro (Equipos destinados para el desarrollo del objeto social).**	**[HW] Equipamento Informático - (3)** [HW] Equipamento Informático - (5**)** **[HW] Equipamento Informático - (10)**	• Falla de hardware. • Falla de software. • Delincuentes informáticos. • Virus, gusanos, troyanos, spyware, DDoS, ransomware etc. • Acceso de información no debida. • Cortes eléctricos • Suplantación de la identidad del usuario • Accesos no autorizados • Caída del sistema por agotamiento de recursos. • Difusión de software dañinos.	• Falta de mantenimiento. • Daños caudados por desgate o defectos de fabrica • Mala configuraciones de los equipos • Falta de mantenimiento a las políticas de credenciales • Factor humano • Daños de los equipos por variaciones de voltajes e idas de energía eléctrica	• Control de acceso. • Gestión de privilegios. • Configuración y mantenimiento de equipos. • Realizar revisiones periódicas en los equipos de cómputo para prevenir desactualizaciones en el software instalado (Sistema operativo, Antivirus y aplicaciones).
*Puntos de acceso alámbricos (hub)	[COM] redes de comunicaciones.	• Fuga de información debido al acceso de	• Ausencia de procesos que establezcan los	• Implementar controles de acceso físico y lógico que

***Puntos de acceso (AP servicio de internet en el campus universitario).** * Switches cisco catalyst 2960	(4) **[COM] redes de comunicaciones. (2)** [COM] redes de comunicaciones. (2)	usuarios no autorizados a la infraestructura de red de la organización. • Indisponibilidad del servicio de la red inalámbrica y alámbrica, debido a ataques de denegación de servicios (DoS). • Fallas en el hardware y software de los dispositivos de red. • Caída del servicio • Errores de software • Daños de equipos	procedimientos para habilitar o deshabilitar las cuentas de usuario. • Deficiencias en las configuraciones de seguridad de la red inalámbrica y alámbrica, empleando un cifrado débil. • Falta de políticas de seguridad de la información dentro de la red de la organización. • Perdida de confidencialidad de información que puede ser sensible para la entidad debido a que es compartida a través de la infraestructura de red de la organización, permitiendo su visualización a personas no autorizadas.	restrinjan los accesos no autorizados a los repositorios de información. • Implementar configuraciones de seguridad orientadas a salvaguardar la información e infraestructura de red de la organización (Router, Switch's, redes inalámbricas). • Gestión de claves y cifrado • Controles de acceso. • Registro de actuaciones. • Implementar configuraciones de seguridad orientadas a salvaguardar la información e infraestructura de red de la organización.
Cortafuegos Cisco ASA 5505 **Ver ficha técnica**	[HW] Equipamento Informático - (1)	• Accesos no autorizados. • Manipulación del hardware. • Errores de administración del sistema y de seguridad.	• Denegación de servicios en el tratamiento de paquetes. • Validación de certificados SSL. • Autenticación de acceso remotos (VPN).	• Efectuar actualizaciones permanentes. • Controles de acceso. • Gestión de claves y cifrado • Gestión de privilegios. • Listas de chequeo de los equipos.

		• Errores de mantenimiento y actualización de equipos. • Averías de origen lógico o físico. • Condiciones inadecuadas de temperatura y humedad. • Daños por Agua y fuego. • Desastres naturales.	• Autenticación de la administración y configuración del equipo. • Insuficiente entropía en la generación de claves criptográficas. • Secuestros de sesión. • Escalda de privilegios.	• Crear una política de seguridad para el manejo, uso y mantenimiento de equipos. • Diseñar y aplicar políticas de seguridad. • Listas de chequeo en los mantenimientos de software y hardware. • Capacitación constante al personal técnico.
Técnicos de mantenimiento	[P] Personal (2)	• Empleado descontento de la organización. • Exempleado de la organización aun con accesos y privilegios habilitados para acceder a la infraestructura física y lógica de la organización. • Terceros interesados en generar ataques que provoquen la indisponibilidad del servicio y/o producto que brinda la	• Ausencia de capacitación al personal en temas relacionados con los sistemas de seguridad de la información. • Ausencia de un programa de sensibilización al personal sobre la importancia de su rol en la seguridad de la información. • Exceso de confianza de los empleados con su entorno (Dentro y fuera de las instalaciones de la entidad). • No hay lineamientos claros de seguridad orientados al personal debido a la	• Formación continua. • Selección de personal. • Especificación del puesto de trabajo. • Condiciones contractuales: responsabilidad en la seguridad en los Sistemas de información. • Establecer acuerdos de confidencialidad con los empleados, proveedores y terceros para el manejo de la información institucional.

		organización de estudio. • Extorciones por información • Ingeniería Social • Robo de información	ausencia de una política de seguridad de la información. • Extracción de información confidencial. • Falta de charlas informativas referente a la ingeniería social y de cómo evitarlas. • Falta de idoneidad en el personal contratado. • Falta de mantenimiento de las políticas de seguridad en credenciales y cifrado de información.	
Teléfonos IP	[HW] Equipamento Informático - (6)	• Caídas del servicio • Robo de llamadas • Sniffer • Fallas de hardware	• falta de cifrado de información • falta de actualización • Falta de mantenimiento. • Daños por desgaste o defecto de fábrica.	• Listas de chequeo en los mantenimientos de software y hardware. • Registro de actuaciones. • Establecer acuerdos de confidencialidad con los empleados, proveedores y terceros para el manejo de la información institucional a través de este servicio. • Definir un plan de tratamiento de incidentes de seguridad de la información.

7.3.1.4. Evaluación del riesgo.

A. Valoración de los activos de información según el impacto.

La metodología **MARGERIT,** las dimensiones de valoración para un activo de información según sus características y sus atributos se clasifican de la siguiente manera:

1) Disponibilidad [D]
2) Integridad [I]
3) Confidencialidad [C]
4) Trazabilidad [T]

De acuerdo a lo descrito anteriormente, la **Valoración de riesgos según el impacto**, nos permite examinar y relacionar los diferentes riesgos permitiendo tener un análisis para cada una de las dimensiones, es decir que la valoración de riesgos da un valor a cada uno de los activos de información teniendo en cuenta cada una de sus dimensiones y finalmente su importancia en cuanto al nivel de seguridad.

Partiendo que para el desarrollo de nuestro caso de estudio de la empresa QWERTY S.A., es de suma importancia efectuar **La valoración de la escala Cualitativa,** con la cual se dará inicio a la valoración de los activos de acuerdo al impacto que pueda generar daño.

Figura 6. Valoración de acuerdo al impacto.

IMPACTO	NOMENCLATURA	VALOR	DESCRIPCIÓN
MUY ALTO	[MA]	10	Daño muy grave
ALTO	[A]	7-9	Daño grave
MEDIO	[M]	4-6	Daño importante
BAJO	[B]	1-3	Daño menor
MUY BAJO	[MB]	0	Irrelevante a efectos prácticos

Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos.

Teniendo en cuenta la anterior tabla sobre la valoración del impactó, a continuación, se realizará la valoración de activos información según el impacto que pudieren tener y la descripción de la escala de acuerdo a nuestra

metodología implantada y todo lo anteriormente descrito basados en el departamento de sistemas del caso de estudio de la empresa QWERTY S.A.

Tabla 8. Valoración de los activos de información del departamento de sistemas del caso de estudio de la empresa QWERTY S.A., según su impacto.

Nombre del Activo de la Información	Categorización[.] Cantidad(.)	Impacto	Criterios de valoración (Descripción escalas estándar)
Servidor de Impresión: Servidor marca Dell en torre PowerEdge T440 Ver ficha técnica	[HW] Equipamento Informático - (2)	**[B]**	**(1.olm):** Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)
Servidor de archivos FTP: Servidor marca Dell en torre PowerEdge T130 Ver ficha técnica	[D] Datos - (1)	**[MA]**	**(5. da):** Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones.
Página web del Plan Máximo Ver ficha proveedor	Servicios [S] - (1)	**[M]**	**(1. da):** Pudiera causar la interrupción de actividades propias de la Organización.
Servidor de nómina y facturación. Servidor marca Dell en torre PowerEdge T440 Características de servidor Apache 2.4.25 PHP 5.6.30 - 7.1.1 MySQL 5.7.17 PhpMyAdmin 4.6.6	[SW] Software - (2)	**[A]**	**(3. da):** Probablemente cause la interrupción de actividades propias de la Organización.
Servidor DHCP. Servidor marca Dell en torre PowerEdge T440	[HW] Equipamento Informático - (1)	**[M]**	**(1. da):** Pudiera causar la interrupción de actividades propias de la Organización.
Equipos de cómputo para gestión del desarrollo tecnológico	[HW] Equipamento Informático - (3)	**[A]**	**(3.adm):** probablemente impediría la operación efectiva de una parte de la Organización.

Cortafuegos Cisco ASA 5505 Ver ficha técnica	[HW] Equipamento Informático - (1)	**[MA]**	**(10.si):** probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios.
Equipos de Computo (Dependencia de prueba de software)	[HW] Equipamento Informático - (5)	**[M]**	**(10.olm):** Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.
Equipos de Cómputo Sistemas operativos win 10 Pro (Equipos destinados para el desarrollo del objeto social).	[HW] Equipamento Informático - (10)	**[B]**	**(1. da):** Pudiera causar la interrupción de actividades propias de la Organización.
Puntos de acceso alámbricos (hub)	[COM] redes de comunicaciones. (4)	**[B]**	**(7.si):** probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
Puntos de acceso (AP servicio de internet en el campus universitario).	[COM] redes de comunicaciones. (2)	**[B]**	**(7.si):** probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
Switches cisco catalyst 2960	[COM] redes de comunicaciones. (2)	**[M]**	**(9.si):** **P**robablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios.
Técnicos de mantenimiento	[P] Personal (2)	**[A]**	**(4.pi2):** probablemente quebrante leyes o regulaciones.
Teléfonos IP	[HW] Equipamento Informático - (6)	**[MB]**	**(1.olm):** Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local).[28]

[28] © Ministerio de Hacienda y Administraciones Públicas. (2012). MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [Ebook] (3rd ed., pp. 19-23). España. Recuperado de: https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

B. Valoración de los activos de información según el impacto y sus dimensiones de seguridad.

Basados en la anterior tabla, a continuación, se efectuará tabla de Valoración de los activos de información del departamento de sistemas del caso de estudio de la empresa QWERTY S.A., según su impacto y sus dimensiones de seguridad, para así dar valor a las consecuencias de materialización de una amenaza según el caso de estudio propuesto.

Tabla 9. Valoración de los activos de información del departamento de sistemas del caso de estudio de la empresa QWERTY S.A., según su impacto y sus dimensiones de seguridad.

Nombre del Activo de la Información	Categorización[.] Cantidad(.)	Valoración de los activos				
		[D]	[C]	[I]	[A]	[T]
Servidor de Impresión: Servidor marca Dell en torre PowerEdge T440 Ver ficha técnica	[HW] Equipamento Informático - (2)	[B]	[MB]	[B]	[MB]	[MB]
Servidor de archivos FTP: Servidor marca Dell en torre PowerEdge T130 Ver ficha técnica	[D] Datos - (1)	[MA]	[MA]	[MA]	[A]	[A]
Página web del Plan Máximo Ver ficha proveedor	Servicios [S] - (1)	[A]	[M]	[M]	[B]	[B]
Servidor de nómina y facturación. Servidor marca Dell en torre PowerEdge T440 Características de servidor Apache 2.4.25 PHP 5.6.30 - 7.1.1 MySQL 5.7.17 PhpMyAdmin	[SW] Software - (2)	[M]	[M]	[A]	[M]	[B]

4.6.6						
Servidor DHCP. Servidor marca Dell en torre PowerEdge T440	[HW] Equipamento Informático - (1)	**[M]**	**[B]**	**[B]**	**[MB]**	**[B]**
Equipos de cómputo para gestión del desarrollo tecnológico	[HW] Equipamento Informático - (3)	**[M]**	**[A]**	**[A]**	**[A]**	**[M]**
Cortafuegos Cisco ASA 5505 Ver ficha técnica	[HW] Equipamento Informático - (1)	**[MA]**	**[MA]**	**[MA]**	**[A]**	**[A]**
Equipos de Computo (Dependencia de prueba de software)	[HW] Equipamento Informático - (5)	**[MB]**	**[B]**	**[M]**	**[B]**	**[MB]**
Equipos de Cómputo Sistemas operativos win 10 Pro (Equipos destinados para el desarrollo del objeto social).	[HW] Equipamento Informático - (10)	**[B]**	**[MB]**	**[B]**	**[B]**	**[MB]**
Puntos de acceso alámbricos (hub).	[COM] redes de comunicaciones. (4)	**[B]**	**[B]**	**[B]**	**[B]**	**[MB]**
Puntos de acceso (AP servicio de internet en el campus universitario).	**[COM] redes de comunicaciones. (2)**	**[B]**	**[B]**	**[B]**	**[MB]**	**[MB]**
Switches cisco catalyst 2960.	[COM] redes de comunicaciones. (2)	**[M]**	**[B]**	**[M]**	**[B]**	**[MB]**
Técnicos de mantenimiento	[P] Personal (2)	**[M]**	**[M]**	**[A]**	**[A]**	**[A]**
Teléfonos IP	[HW] Equipamento Informático - (6)	**[A]**	**[B]**	**[B]**	**[B]**	**[MB]**

C. Análisis de riesgos y su impacto de los activos.

I. Valoración de riesgos según el impacto y la probabilidad del riesgo de cada uno de los activos de información del caso de estudio de la empresa QWERTY S.A.

Para efectuar un análisis de riesgos y su impacto de los activos de debe efectuar una valoración de acuerdo a la probabilidad de ocurrencia de los riesgos (número de veces por periodo de tiempo) y finalmente el impacto (las consecuencias de llegar a concretarse el riesgo). Dado lo anterior se procederá a efectuar la estimación del riesgo según el impacto para nuestro caso de estudio de la empresa QWERTY S.A.

Tabla 10. Calificación del impacto.

VALOR	IMPACTO	DESCRIPCIÓN
5	Leve	Si el hecho llegara a presentarse tendría bajo impacto o efecto en la Institución.
10	Moderado	Si el hecho llegara a presentarse tendría medianas consecuencias o efectos en la Institución.
20	Catastrófico o Grave	Si el hecho llegara a presentarse tendría alto impacto o efecto en la Institución

De acuerdo a los anterior, debemos tener en cuenta los siguientes conceptos claros para así dar inicio a la calificación, evaluación y solución a los riesgos.

- **Probabilidad.** Es el análisis cualitativo y cuantitativo de la eventualidad se verifique y examine un acontecimiento. Esta puede ser medida con los siguientes criterios:
    - **Frecuencia** que es si el riesgo se ha materializado o **Factibilidad** que es en donde se puede propiciar el riesgo según los factores internos y externos dentro de una organización.

De igual manera, para efectuar este análisis de riegos y su impacto se debe tener en cuenta la siguiente tabla de calificación de probabilidad, la cual se presenta de la siguiente manera:

Tabla 11.Calificación de Probabilidad.

VALOR	PROBABILIDAD	DESCRIPCIÓN
1	Baja	Puede ocurrir algunas veces o bajo circunstancias excepcionales (P<=30%).
2	Media	Puede ocurrir (P>30% y <=70%).
3	Alta	Probabilidad de ocurrencia en la mayoría de Circunstancias (P>70%).

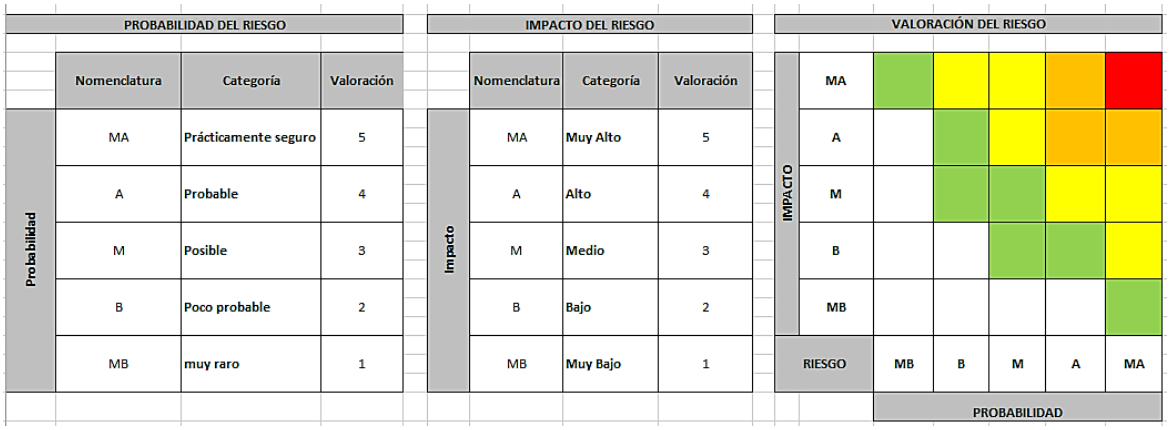
Dado lo anterior, se procede a **evaluar el riesgo** que pueden ser Riesgos aceptables, tolerables, moderados, importantes o inaceptable, mediante la siguiente formula:

EVALUACIÓN = Impacto x Probabilidad

En conclusión, para efectuar el análisis de riesgos como primera medida se debe determinar la gravedad del riesgo en la organización que para nuestro caso de estudio se hará para determinar la identificación, calificación y evaluación de los riesgos como se está efectuando en la matriz de análisis de riesgos que veremos en el **Anexo A** del presente documento.

Para efectuar este proceso e implementarlo en el departamento de sistemas del caso de estudio de la empresa QWERTY S.A., debemos tener en cuenta la siguiente figura 4 de tablas para la valoración de riesgos según el impacto y la probabilidad del riesgo existe dentro de la organización de acuerdo a la implementación de la metodología Margerit.[29]

Figura 7. Tablas para la valoración de riesgos según el impacto y la probabilidad del riesgo existe dentro de una organización.



PROBABILIDAD DEL RIESGO

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

IMPACTO DEL RIESGO

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

VALORACIÓN DEL RIESGO

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

Fuente: Luis Fernando Zambrano Hernández. Curso Riesgos y Control Informático UNAD 2019.

[29] MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO. (2016). [Ebook] (5th ed., pp. 12-20). Bucaramanga. Recuperado de: https://www.uis.edu.co/webUIS/es/administracion/controlGestion/documentos/2015/MSE.01manualAdministracionRiesgo.pdf

Tabla 12. Hoja de Excel sobre la valoración de riesgos según el impacto y la probabilidad del riesgo existe de cada uno de los activos de información dentro del departamento de sistemas del caso de estudio de la empresa QWERTY S.A.

IDENTIFICACIÓN DEL RIESGO						ANÁLISIS Y EVALUACIÓN DEL RIESGO		
Nombre del activo de Informacion	Activo de informacion	Riesgo			Clases de Riesgo 1. Estratégico 2. Imagen 3. Operativo 4. Financiero 5.Cumplimiento 6.Tecnología	Probabilidad de materialización	Impacto	Valoracion del riesgo de los activos
		Tipo Riesgo	Vulnerabilidades	Amenaza				
Servidor de Impresión: Servidor marca dell en torre PowerEdge T440	[HW] EQUIPAMENTO INFORMÁTICO	Institucional	*falta de mantenimiento *Daños por desgaste o defectos de fabrica. *• Daños del servidor por falta de equipos que regulen variaciones de voltajes e idas de energía eléctrica.	[I5] Avería de origen físico o lógico	6.Tecnología	2	2	ACEPTABLE (MUY BAJO)
Servidor de archivos FTP: Servidor marca dell en torre PowerEdge T130	[HW] EQUIPAMENTO INFORMÁTICO	Institucional	*Carencia de configuraciones de seguridad del servidor. *La configuracion y la administracion de los servidores no se encuentra centralizada. *El antivirus instalado en el servidor no	[E2] Errores del administrador	6.Tecnología	3	2	TOLERABLE (BAJO)
Página web	[S] SERVICIOS	Institucional	* Errores en la gestion de recursos y configuraciones. * Fallos en la depuracion de alguna aplicación o en la misma programacion del sitio web. * Ejecucion de codigo malintencionados. * Factor	[I8] Fallo de servicios de comunicaciones	6.Tecnología	2	2	ACEPTABLE (MUY BAJO)

A continuación, se presentará link de acceso de la tabla anterior en caso de que la hoja de Excel no acceda dentro del documento: https://drive.google.com/file/d/16sM4s1E3NSD7Ura6h3pbmpeRXeKdx7Xz/view?usp=sharing

7.3.1.5. Tratamiento del riesgo

Partiendo del caso de estudio propuesto y del Análisis de riesgos de cada uno de los procesos del departamento de sistemas del caso de estudio de la empresa QWERTY S.A., y basándonos en la metodología **MARGERIT,** A continuación, se procederá a efectuar el **plan de tratamiento de riesgos** de acuerdo a la clasificación y valoración del riesgo, como así mismo las estrategias a implementar de acuerdo a los activos de información que posee la entidad descrita. A continuación, se presentará Guía de estrategias para el tratamiento de los riesgos del caso de estudio propuesto:

Tabla 13. Guía de estrategias para el tratamiento de los riesgos.

CLASIFICACIÓN DEL RIESGO	ESTRATEGIAS	DESCRIPCIÓN DE LA ESTRATEGIA
Alto (Importante).	**Mitigar o Implantar.**	Es una estrategia de respuesta a los riesgos, según la cual se actúa para reducir la frecuencia de ocurrencia o impacto de un riesgo.
Muy Alto (Inaceptables)	**Evitar o eliminar**	Es una estrategia de respuesta a los riesgos, con el fin de eliminar la amenaza para protegerse de su impacto. En esta estrategia el riesgo no se asume
	Transferir	Es una estrategia de respuesta a los riesgos, según la cual se traslada el impacto de una amenaza a un tercero, junto con la responsabilidad de la respuesta. Ejemplo: el aseguramiento de activos mediante una compañía aseguradora
Medio (Moderados).	**Aceptar**	Es una estrategia de respuesta a los riesgos en la cual se decide reconocer el riesgo y monitorearlo
Bajos (Tolerable)	**Aceptar y monitorear**	Es una estrategia de respuesta a los riesgos en la cual se decide reconocer el riesgo y no tomar ninguna medida, a menos que el riesgo se materialice.
Muy Bajos (Aceptable).		

[30] Velásquez Restrepo, P., Velásquez Restrepo, S., Velásquez Lopera, M., & Villa Galeano, J. (2017). Implementación de la gestión de riesgo en los procesos misionales de la Sección de Dermatología de la Universidad de Antioquia (Medellín, Colombia) siguiendo las directrices de la norma ISO 9001:2015 [Ebook] (pp. 88-89). Bogotá, Colombia. Recuperado de: http://www.scielo.org.co/pdf/rgps/v16n33/1657-7027-rgps-16-33-00078.pdf

Tabla 14. Hoja de Excel con el Plan de tratamiento de riesgos, de acuerdo a la identificación, valoración y clasificación de los riesgos según las estrategias descritas dentro del departamento de sistemas del caso de estudio de la empresa QWERTY S.A.

IDENTIFICACIÓN DEL RIESGO					ANÁLISIS Y EVALUACIÓN DEL RIESGO			ESTRATEGIAS PARA EL PLAN DE TRATAMIENTO DE RIESGOS.	
Nombre del activo de Informacion	Activo de informacion	Riesgo			Probabilidad de materialización	Impacto	Valoracion del riesgo de los activos	Estrategia del riesgo	Criterios del tratamiento del riesgo de acuerdo al controles a aplicar a partir de la norma ISO 27001
		Tipo Riesgo	Vulnerabilidades	Amenaza					
Servidor de Impresión: Servidor marca dell en torre PowerEdge T441	[HW] EQUIPAMENTO INFORMÁTICO	Institucional	*falta de mantenimiento *Daños por desgaste o defectos de fabrica	[I5] Avería de origen físico o lógico	2	2	ACEPTABLE (MUY BAJO)	Aceptar	**A11.2.4 Mantenimiento de los equipos**: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
Servidor de archivos FTP: Servidor marca dell en torre PowerEdge T131	[HW] EQUIPAMENTO INFORMÁTICO	Institucional	*Carencia de configuraciones de seguridad del servidor. *La configuracion y la administracion de los servidores no se encuentra centralizada. *El antivirus instalado	[E2] Errores del administrador	3	2	TOLERABLE (BAJO)	Aceptar	**A5.1.1 Politicas para la seguridad de la informacion:** Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
Página web	[S] SERVICIOS	Institucional	* Errores en la gestion de recursos y configuraciones. * Fallos en la depuracion de alguna aplicación o en la misma programacion del sitio	[I8] Fallo de servicios de comunicaciones	2	2	ACEPTABLE (MUY BAJO)	Aceptar	**A13.1.2 seguridad de los servicios de red**: 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

A continuación, se presentará link de acceso de la tabla anterior en caso de que la hoja de Excel no acceda dentro del documento: https://drive.google.com/file/d/11W9vMLZ5WGx8O3lQQcC_ReUcZgrOu1hp/view?usp=sharing

De acuerdo a la identificación, valoración y clasificación de los riesgos según las estrategias descritas dentro del departamento de sistemas del caso de estudio de la empresa QWERTY S.A., para la implementación del plan de tratamientos de riesgos, se concluye que las acciones o estrategias para tratar los riesgos son: **“Aceptar” y “ Aceptar y Monitorear”**; es decir que cuando los daños provocados por la materialización del riesgo no han afectado mayormente las actividades regulares del departamentos de sistemas de descrita entidad, como así mismo la toma de la decisión es **“aceptar”** dicho riesgo y finalmente los riesgos que son de baja prioridad se deben **“aceptar y monitorear”,** pero se recomienda aplicar controles basados en la norma ISO/IEC 27001 y 27002 para evitar que los riesgos, amenazas y vulnerabilidades se materialicen.[31]

[31] Guanoluisa Huertas, J., & Maldonado Soliz, I. (2015). *Análisis de Riesgos de un plan de seguridad de la información para el concejo nacional de igualdad de discapacidades "CONADIS"* [Ebook] (pp. 51-52). Quito, Ecuador. Recuperado de: https://bibdigital.epn.edu.ec/bitstream/15000/10499/1/CD-6217.pdf

7.4. MODELO DE GESTIÓN DE LA CIBERSEGURIDAD DE LA EMPRESA QWERTY S.A., BASADOS EN LA NTC-ISO/IEC 27032.

7.4.1. Contextualización de la norma.

La NTC-ISO/IEC 27032 es la estándar calidad basado en la ciberseguridad, el cual ayuda a preparar a las empresas y organizaciones con el fin de detectar, controlar y responder a los ciberataques, como así mismo se enfoca a lo que tiene que ver con las tecnologías de la información, técnicas de seguridad y finalmente las directrices para la ciberprotección. Dado a lo anteriormente descrito, este estándar de calidad suministra guías de técnicas en donde se afrontan los diferentes tipos de riesgos de la ciberprotección tales como: ataque de ingeniería social, malwares, hackeos, spyware, software no deseados. Igualmente posee guías técnicas que dispone de controles para abordar los diferentes tipos de riesgos y responder a los ataques. Además, esta norma pose una segunda extensión de domino que es la colaboración, es decir, que es una necesidad de compartir y coordinar información de manera eficiente y efectiva para manejar los incidentes que ocurren entre los diferentes actores en el ciberespacio. De igual manera la presente norma incluye un marco para compartir información, manejar incidentes y ejercer coordinación. Dado lo anterior la norma ISO 27032 emerge como un complemento de la norma ISO 27001, cuyo propósito es brindar y destacar las mejores prácticas para la seguridad y cuidado de activos virtuales, los cuales son primordiales para el desarrollo operacional dentro de la organización.

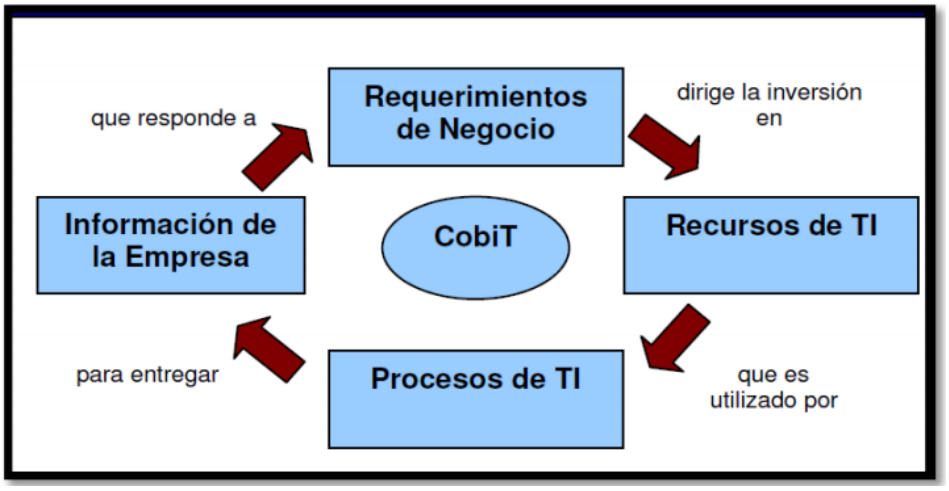
7.4.2. Entendimiento de la organización (Caso de estudio de la empresa QWERTY S.A.)

Basándonos en la información dada del escenario 2 (enfoque directivo - administrativo) de nuestro proyecto aplicado, lo que se pretende es efectuar una identificación de la empresa del caso de estudio que se está implementando, con el fin de generar un entendimiento el cual nos permitirá conocer las diferentes funciones de las áreas, dependencias, sistemas de gestión como ISO27001, Metodologías para el análisis de gestión de riesgos (MARGERIT), aspectos regulatorios, infraestructura tecnología, entre otros elementos los cuales nos permitirán no solo conocer la entidad sino ver qué tan organizados y dispuestos se encuentran frente a la Ciberseguridad.

A continuación, se definirá métodos y principios que nos posibilitaran reconocer los ítems que se van aplicar en nuestro proyecto de acuerdo a la norma ISO27032. Como de igual manera se dará inicio a un reconocimiento o un recorderís de cada

uno de los activos de información ligado a su criticidad y su nivel de exposición de riesgo dentro de la organización. Dado a lo anteriormente descrito y basados en las Buenas prácticas COBIT, se diseñará e implementará una plantilla en donde se vera de cómo está conformada la entidad, cuál es su infraestructura, niveles y políticas de seguridad, según los criterios y principios del COBIT que veremos en la siguiente figura:

Figura 8. Principios Básicos del COBIT



Fuente: COBIT 4.1[32].

Dado a lo anteriormente escrito, a continuación, se aplicará plantilla que se realizó con el fin de poseer una mejor compresión según los parámetros descritos previamente, los cuales serán base para la implementación del estándar de calidad NTC-ISO/IEC 27032.

[32] CobIT 4.1 Spanish. (2007). [Ebook] (p. 10). Recuperado, de: https://biblioteca.info.unlp.edu.ar/uploads/docs/cobit.pdf.

Tabla 15. Conocimiento del caso de estudio de la empresa QWERTY S.A.

Conocimiento del caso de estudio de la empresa QWERTY S.A.	
OBJETIVO: Tener y poseer conocimiento del caso de estudio de la empresa QWERTY S.A., con el fin de conocer actividad comercial, tipo de organización, tipo de tecnologías, entre otros aspectos que permitirán disponer el mejor rumbo de la organización y así implementar las buenas prácticas de la NTC-ISO/IEC 27032.	
Nombre de la organización:	Departamento de sistemas del caso de estudio de la empresa QWERTY S.A.
Sector:	Tecnológico (uso de las TI)
Tipo de organización:	Formal.
Actividad comercial:	Corresponde al desarrollo tecnológico de las comunidades colombianas a través del uso de Tecnologías de Información para la consulta de datos.
Dependencias:	**SISTEMAS** (Infraestructura, desarrollo y soporte).
Estructura y organización de TI y Seguridad	
Comprender como está determinada estructura de empresa QWERTY S.A., a nivel de TI y de seguridad de los activos de información.	
¿Qué áreas existen en TI?	Área de infraestructura, Área de desarrollo y Área de soporte.
¿Cuenta con especialistas de Seguridad de la información e informática?	El departamento de sistemas y sus diferentes áreas de las TI de la empresa QWERTY S.A., no cuenta con personal capacitado y especializado para afrontar ataques de los ciberdelincuentes dentro de la infraestructura de red y finalmente no cuenta con protección de la diferentes amenazas, riesgos y vulnerabilidades de cada uno de los activos información del Si.
¿Cuentan con área de Riesgos?	La entidad descrita y de caso de estudio no cuenta, ni posee con una dependencia o área de riesgos para la ciberprotección y seguridad de los datos.
Inventario y descripción tecnológica	
Conocimiento de los equipos, sistemas y servicios con los que cuenta la empresa QWERTY S.A.	
Equipos, sistemas y servicios.	En la tabla 1 de los activos de información a cargo del departamento de sistemas de la empresa QWERTY S.A, se encuentra la identificación de cada uno de los servicios, equipos y sistemas tecnológicos con lo que cuenta la descrita entidad.
Seguridad informática y de la información	
Conocimiento de los mecanismos de protección y de la seguridad informática e información.	
Hardware - software	La empresa en estudio, cuenta con mecanismo de protección tanto físicos como lógicos los cuales se dan a conocer en el numeral 7 sobre la propuesta del SGSI basados en la norma NTC-ISO/IEC 27001:2013, en el ítem 7.1.3.3 sobre los objetivos de seguridad de la información y planes para lograrlos, en donde se describen: • Políticas de seguridad de las comunicaciones.

	• Políticas de transferencia de información.
	• Políticas de gestión de activos de información.
	• Políticas de gestión de la vulnerabilidad técnica.
	• Políticas de criptografía
	  ○ Controles criptográficos
	  ○ Gestión de llaves.

Controles lógicos	Cabe resaltar que la entidad del caso de estudio propuesto, no cuenta con roles y perfiles para el acceso a cada uno de los sistemas empresa, como así mismo no tienen definidos mecanismos para el acceso de terceros a los diferentes sistemas de información de la descrita organización.
Parte jurídica y de formalización.	
Conocimiento del ambiente regulatorio en el cual se desenvuelve la empresa QWERTY S.A., con el fin de reconocer la regulación y así disponerla con el manejo e implementación de las buenas prácticas de la ciberseguridad.	
Circulares, decretos y leyes	La empresa QWERTY S.A., no cuenta con un área de regulación y reglamentación buenas prácticas de ciberseguridad tales como: • Políticas y normativas. • Controles de acceso lógicos. • Copias de seguridad. • Protección antimalware. • Actualización de software. • Registros de actividad. • Controles de acceso a la red y seguridad de la misma. • Movilidad de la información. • Gestión de soportes. • Continuidad del negocio (Prevención, protección y reacción ante incidentes de seguridad). (guia_decalogo_ciberseguridad_metad, 2017)[33] Dado lo anteriormente descrito se dan a conocer con el fin de mejorar los sistemas de información y de las redes de comunicación del caso de estudio de la empresa QWERTY S.A y así promover la confianza y éxito de la organización.
Sistemas y metodologías gestión implementados	
Que sistemas y metodologías de gestión se tienen implementadas en la empresa de estudio.	
ISO 27001	Es un estándar de calidad enfocado a proteger y preservar la confidencialidad, integridad y disponibilidad de la información dentro de un

[33] guia_decalogo_ciberseguridad_metad. (2017). [Ebook] (1st ed., p. 4). Recuperado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf.

	SGSI como lo es en el caso de nuestro caso de estudio de la empresa QWERTY S.A., y cuya información la encontramos en el presente documento en su numeral 7 sobre la propuesta del SGSI basadas en las 2 primeras fases del modelo PHVA.
MARGERIT	Es una metodología de análisis y gestión de riesgos, es una herramienta para la minimización de los riesgos, amenazas y vulnerabilidades de las tecnologías de información de una entidad y la cual fue dispuesta y aplicada al departamento de sistemas del caso de estudio de la empresa QWERTY S.A., y cuya información la encontramos en el presente documento en su numeral 8.2.
Manejo de Incidentes	
La descrita entidad del caso de estudio planteado sobre la empresa QWERTY S.A., no posee un área o centro de operaciones de seguridad (SOC), en donde se efectué un análisis y seguimiento de las diferentes labores y funciones en las redes internas y externas de la misma, como de igual manera en las bases de datos, sistemas de información, aplicaciones y sitios web en donde indiquen anomalías o compromisos con los datos e información que vulneren y amenacen los mismos. Pero de igual manera los diferentes activos de información ya cuentan con algunas políticas de seguridad y unas salvaguardas según la normatividad ISO 27001 y a la metodología de análisis y gestión de riesgos MARGERIT.	
Concientización y capacitación	
El caso de estudio de la empresa QWERTY S.A., no posee un cronograma de capacitación respecto a temas y campañas de concientización sobre contenidos de ataques cibernéticos.	

7.4.3. Pautas a tener en cuenta.

De acuerdo a la información y análisis efectuado anteriormente sobre el entendimiento y conocimiento de la organización, tenemos como criterios para la implementación de la norma NTC-ISO/IEC 27032 las siguientes pautas:

- Administración y gestión del riesgo.
- Manejo de incidentes.
- Conciencia y capacitación.
- Monitoreo y detección.
- Protección de datos (terceras partes)
- Gestión de cumplimiento.
- Operación y continuidad.

Dado lo anteriormente descrito, estas pautas o criterios nos permite guiar y encaminar la implementación del estándar de calidad basados en aspectos importantes para cualquier entidad o empresa sin importar el tipo de negocio.

7.4.4. Implementación de la NTC-ISO/IEC 27032 al departamento de sistemas del caso de estudio de la empresa QWERTY S.A.

Partiendo que la norma NTC-ISO/IEC 27032 nos enseña y nos expone las buenas prácticas de la ciberseguridad y que las descritas nos permiten aplicar a cualquier empresa u organización, con el fin de generar criterios y pautas para la protección de cada uno de los activos de información que posee el caso de estudio de la empresa QWERTY S.A y que se encuentran en el ciberespacio.

De acuerdo a lo anterior y al entendimiento de nuestra empresa, se implementará y fortalecerá los diferentes controles y aspectos de seguridad en la red, información, internet e infraestructura críticas de los datos e información (CIIP)[34], las cuales se exponen en los 13 numerales de la norma NTC-ISO/IEC 27032 que se dan a conocer a continuación:

Tabla 16. Estructura norma NTC-ISO/IEC 27032.

Numeral	Descripción
1.	Alcance y campo de aplicación
2.	aplicabilidad
3.	Referencias normativas
4.	Términos y definiciones
5.	Términos abreviados
6.	Generalidades o Visión general.
7.	Partes interesadas en el ciberespacio.
8.	Activos del ciberespacio.
9.	Amenazas contra la seguridad y protección del ciberespacio.
10.	Roles de las partes interesadas de la ciberseguridad o ciberprotección.
11.	Directrices para las partes interesadas.
12.	Controles de ciberseguridad o ciberprotección.
13.	Marco del intercambio y coordinación de información.

Fuente: norma ISO 27032[35].

[34] ISO/IEC 27032:2012 Tecnología de la información. Técnicas de seguridad. Directrices para la ciberseguridad. ISO. (2012). Recuperado de: https://www.iso.org/standard/44375.html.

[35] ISO/IEC 27032:2012 Tecnología de la información. Técnicas de seguridad. Directrices para la ciberseguridad. ISO. (2012). Recuperado de: https://www.iso.org/standard/44375.html.

Dada la anterior tabla, se describe los diferentes numerales la cual conforman la estructura general de la norma ISO 27032, con base a lo descrito se implementará dicha guía para aplicación de las buenas prácticas de la ciberseguridad al departamento de sistemas del caso de estudio de la empresa QWERTY S.A.

De acuerdo a lo descrito, se procederá a plasmar y aplicar cada uno de los numerales del estándar calidad, mediante la estructura de los anteriores ítems e información sobre el entendimiento de la organización (Caso de estudio de la empresa QWERTY S.A.). Además, y con respecto al ítem 1-6 no se requiere aplicación al escenario propuesto, ya que es información de conocimiento de la norma, pero si se debe resaltar para el desarrollo del proyecto aplicado, el cual se presenta a continuación:

7.4.4.1. Alcance y campo de aplicación.

Este estándar de calidad ofrece una guía para mejorar el estado de la ciberseguridad o ciberprotección de la empresa u organización, destacando aspectos exclusivos de descrita acción, como en otros entornos de protección y confianza tales como:

- Seguridad de la información.
- Seguridad de las redes.
- Seguridad de internet.
- Protección de la infraestructura critica de información (CIIP).

Además, este estándar de calidad abarca todo lo que tiene que ver con las prácticas de protección online en base de las partes interesadas del ciberespacio.

7.4.4.2. Aplicabilidad.

Audiencia: Esta norma se aplica a los proveedores de servicios en el ciber espacio, pero también incluye a los consumidores que utilizan este servicio.

Limitaciones: Este estándar no aborda.

- Ciberseguridad.
- Cibercrimen.
- Seguridad de internet.
- CIIP
- Crímenes relacionados a internet

En resumen, este estándar se limita al entendimiento del ciberespacio en internet.

7.4.4.3. Referencias normativas.

La presente norma tiene como referencia el documento del estándar de calidad ISO/IEC 27000, que trata Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Descripción general y vocabulario.

7.4.4.4. Términos y definiciones.

El estándar de calidad se apropia de los términos y conceptos indicados en la norma ISO/IEC/27000 y los que utiliza propiamente la descrita.

7.4.4.5. Términos abreviados.

En este ítem se detallan los términos abreviados que se aplican en esta norma.

7.4.4.6. Generalidades o visión general

La seguridad y protección de los datos e información en Internet y en el Ciberespacio ha sido un asunto ascendiente y de preocupación. Las partes interesadas han venido estableciendo su presencia en el Ciberespacio a través de sitios web y ahora están tratando de aprovechar aún más el mundo virtual proporcionado por el Ciberespacio.

Dentro de este ítem se explica la condición y universo del Ciberespacio, Ciberseguridad, el prototipo o plantilla general en la que se ha basados en el desarrollo de la presente norma, la cual se enfoca y se enmarca en las principales estrategias para cada una de las partes interesadas.

Dado a lo anteriormente descrito, la implementación de las buenas prácticas de la ciberprotección o ciberseguridad se implementará según los numerales 7-13 de la NTC-ISO/IEC 27032 para departamento de sistemas del caso de estudio de la empresa QWERTY S.A., los que se dan a continuación:

7.4.4.7. Partes interesadas en el ciberespacio.

El propósito de este ítem, es generar un reconocimiento de las partes interesadas del departamento de sistemas del caso de estudio de la empresa QWERTY S.A., los cuales se dan según los lineamientos y propósitos de esta norma, las partes

interesadas que se presentan en el escenario propuesto son proveedores y consumidores.

Partiendo que los **consumidores**, son los usuarios individuales y organizaciones tantos públicas como privadas, las cuales se vuelven clientes o consumidores en el momento en que accede en el ciberespacio o cualquier servicio disponible en este.

Cuando hablamos de los **Proveedores**, decimos que son aquellos que facilitan el servicio en el ciberespacio tales como IPS (proveedores de servicio de internet y servicios de aplicaciones.

Dado lo anteriormente descrito y de acuerdo al caso de estudio, el departamento de sistemas de la empresa QWERTY S.A, en cada uno de sus procesos y actividades que efectúa como consumidor, como así mismo cada uno de sus sistemas de información que aplica, estos generan un impacto que pueden ser altos, medios o bajos según su proceso o servicio que preste la entidad. Para este proceso la empresa de caso de estudio, es consumidora de altos anchos de banda de servicio internet (canal dedicado de 25 MB) el cual es destinado para el desarrollo de las actividades rutinarias de la empresa descrita. Pero también es una proveedora de servicios a través del ciberespacio, ya que la descrita atraves de su sitio web, publica y realiza marketing de cada una de las tecnologías información que ofrece a través de este sistema implantado, el cual va dirigido a las diferentes comunidades colombianas.

De acuerdo a lo anterior podemos afirmar que atraves del proveedor de servicio de internet (ISP) podemos tener varios niveles críticos y no críticos de seguridad, los cuales pueden afectar la confidencialidad, integridad y disponibilidad de la información de la organización descrita.

7.4.4.8. Activos del ciberespacio.

Basándonos en los activos de información presentados en el escenario 2 y en la tabla 1 de la propuesta del SGSI del caso del estudio de la empresa QWERTY S.A a cargo del departamento de sistemas y como ya sabemos los activos de información son aquellos que tienen valor para un individuo u organización, dado este principio los activos del ciberespacio se clasifican en personales y organizacionales pero también si lo vemos más descriptivamente lo podemos catalogar como activos físicos y activos virtuales; cuando decimos de activo virtual, son aquellos que solo existen en el ciberespacio ósea que no se pueden ver o tocar

(intangibles), esto nos lleva a identificarlos y a efectuar un inventario de acuerdo a nuestro caso de estudio propuesto.

Partiendo de este enunciado, los activos del ciberespacio que se identifican en nuestro caso de estudio son los siguientes:

A. Activo 1.

- **Nombre del Activo:** Proveedor de servicio de internet (ISP)
- **Proceso al cual está asociado:** a todas las dependencias y áreas del caso de estudio de empresa QWERTY S.A
- **Categoría del activo:** Servicios [S]
- **Ubicación del activo:** Virtual
- **Tipo:** Terciario
- **Criticidad:** bajo
- **Valor del activo:** 3 → [Confidencialidad]
  1→ [Integridad]
  2→[Disponibilidad]

*** Escala de calificación de 1 a 4 donde:**

1: La pérdida no impedirá la continuidad de la operación.

2: La pérdida causara un impacto bajo en la operación.

3: La pérdida causara un impacto medio en la operación.

4: La pérdida causara un impacto alto en la operación.

- **Calificación del activo**: (2)

B. Activo 2.

- **Nombre del Activo:** Página Web
- **Proceso al cual está asociado**: a las dependencias o áreas de desarrollo, como así mismo las áreas directivas, administrativas y operativas.
- **Categoría del activo:** Servicios [S]
- **Ubicación del activo:** Virtual.
- **Tipo:** Terciario.
- **Criticidad:** Bajo
- **Valor del activo:** 2 → [Confidencialidad]
  1→ [Integridad]

2→[Disponibilidad]

*** Escala de calificación de 1 a 4 donde:**

1: La pérdida no impedirá la continuidad de la operación.

2: La pérdida causara un impacto bajo en la operación.

3: La pérdida causara un impacto medio en la operación.

4: La pérdida causara un impacto alto en la operación.

- **Calificación del activo:** (1)

C. Activo 3.

- **Nombre del Activo:** Equipos de cómputo para gestión del desarrollo tecnológico. (Objeto Social).
- **Proceso al cual está asociado:** Gestión de la información online para el desarrollo del objeto social (proveedores, órdenes de compra e inventarios).
- **Categoría del activo:** [HW] Equipamento Informático
- **Ubicación del activo:** Físico
- **Tipo:** Propio.
- **Criticidad:** Medio
- **Valor del activo:** 3 → [Confidencialidad]
  2→ [Integridad]
  2→[Disponibilidad]

*** Escala de calificación de 1 a 4 donde:**

1: La pérdida no impedirá la continuidad de la operación.

2: La pérdida causara un impacto bajo en la operación.

3: La pérdida causara un impacto medio en la operación.

4: La pérdida causara un impacto alto en la operación.

- **Calificación del activo:** (3)

D. Activo 4.

- **Nombre del Activo:** Correo Electrónico Institucional.

- **Proceso al cual está asociado:** Servicio que busca: Comunicación con otros miembros de la entidad, compartir archivos, recibir comunicaciones oficiales, brindar espacio de almacenamiento ilimitado y finalmente dar prioridad a las actividades propuestas por el desarrollo académico de la entidad.
- **Categoría del activo:** [S] servicios
- **Ubicación del activo:** Virtual
- **Tipo:** Terciario.
- **Criticidad:** Bajo.
- **Valor del activo:** 3 → [Confidencialidad]
  2→ [Integridad]
  2→[Disponibilidad][36]

*** Escala de calificación de 1 a 4 donde:**

1: La pérdida no impedirá la continuidad de la operación.

2: La pérdida causara un impacto bajo en la operación.

3: La pérdida causara un impacto medio en la operación.

4: La pérdida causara un impacto alto en la operación.

- **Calificación del activo:** (1).

7.4.4.9. Amenazas contra la seguridad y protección del ciberespacio.

Las amenazas existentes en el ciberespacio se estudian y se examinan según los activos del ciberespacio, estas amenazas se clasifican en 2 campos:

1. **Amenazas a los activos personales**. Estos se dan especialmente en los problemas de identidad, producidos por la filtración o usurpación de la información.

---

[36] Ramírez Rey, C., Martínez García, M., & Parrado Rodríguez, V. (2019). *GUÍA PARA EL LEVANTAMIENTO Y VALORACIÓN DE ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN* [Ebook] (2nd ed., pp. 7,8,9). MinSalud. Recuperado de: https://www.minsalud.gov.co/Ministerio/Institucional/Procesos%20y%20procedimientos/ASIG03.pdf .

2. **Amenazas a los activos de la organización**. La existencia de negocios y organizaciones en línea, suelen ser objetivos de los cibercriminales, ya que sus intenciones van más allá de un simple pasatiempo.

Desde otra perspectiva encontramos también los Agentes de Amenaza, que es un elemento de amenaza individualmente o grupalmente, los cuales poseen algún rol en la ejecución o apoyo de un ataque. De igual manera se localizan las Vulnerabilidades, que son las debilidades de un activo o control, los cuales son aprovechadas por una amenaza; pero de igual forma, existen mecanismos de ataque los cuales son categorizados así:

- Ataques desde el interior de la red privada (Pueden ser causados por los empleados o por un tercero que tenga acceso a la red interna de la entidad).
- Ataques desde fuera de la red privada (Internet, explotación de los activos dentro de la red de la organización).

Además, las amenazas contra la seguridad y protección del ciberespacio se efectúan de acuerdo a la implementación de la metodología del análisis y gestión de riesgos de los sistemas de información (MARGERIT), en su libro II del catálogo de elementos, así como lo fue ejecutado en el presente proyecto en todo su contenido y procedimiento denotado en el ítem **8.1 sobre la metodología para el análisis y gestión de la seguridad de la información de la empresa QWERTY S.A., basada en Margerit.**

Dado a lo anteriormente descrito, se procederá a efectuar dicho proceso a los activos del ciberespacio faltantes de acuerdo a la metodología implementada.

1. **Identificación y clasificación de los activos del ciberespacio del caso de estudio de la empresa QWERTY S.A.**

Tabla 17. Reconocimiento y Categorización de los activos del ciberespacio del caso de estudio de la empresa QWERTY S.A.

Activo del ciberespacio	Categorización
Proveedor de servicio de internet (ISP)	**[S]**
Página Web	**[S]**
Equipos de cómputo para la gestión del desarrollo tecnológico (Objeto Social)	**[HW]**
Correo electrónico Institucional	**[S]**

2. **Identificación de los riesgos de los activos del ciberespacio que se pueden presentar en el caso de estudio de la empresa QWERTY S.A.**

- Riesgos del internet relacionado con la información tales como:
    - Acceso a la información poco fiable y falsa.
    - Dispersión, pérdida de tiempo.
    - Acceso a la información inapropiada.
    - Acceso a la información peligrosa, inmoral, ilícita.

- Riesgos del internet relacionado con las actividades económicas.
    - Estafas.
    - Robo
    - Negocios ilegales.
    - Delitos de propiedad intelectual.

- Riesgos del internet relacionado con la tecnología
    - Actos de sabotaje y piratería

- Riesgos del internet relacionado con las adiciones.
    - Demasiado tiempo conectado en la red.
    - Compras compulsivas.
    - Juegos online
    - Pornografía.
- Riesgos relacionados con la comunicación del correo institucional
    - Bloqueo temporal del buzón de correo.
    - Perdida de intimidad.
    - Acciones ilegales.
    - Malas compañías
    - Recepción de mensajes personales ofensivos.[37]

- Riesgos relacionados con la seguridad de las páginas web.
    - Inyección
    - Autenticación rota.
    - Exposición de datos sensibles.
    - XML Entidades externas XXE (inyección de código, la cual analiza los datos XML)

---

[37] *Riesgos de Internet*. Cefire.edu.gva.es. Recuperado de: http://cefire.edu.gva.es/file.php/1/Comunicacion_y_apertura/B1_Navegacion_Internet/5_riesgos_de_internet.html.

- Control de acceso con falla.
- Configuración incorrecta de seguridad.
- Cross-Site Scripting (XSS).
- Deserialización insegura (adulteración de datos serializados).
- Utilización de componentes con vulnerabilidades conocidas.
- Insuficiente registro y monitoreo. (Gimenes, 2017) [38]

- Riesgos relacionados con la seguridad de los equipos de cómputo para la gestión del desarrollo tecnológico (Objeto Social).
  - Robos por computadora.
  - Errores y averías (Daños producidos virus y ladrones informáticos.
  - Fraudes y ataques cibernéticos (Phishing). Fugas de datos o perdidas de información.
  - Sabotaje.
  - Aunque los equipos de cómputo cuentan con sistemas de antivirus actualizado, no se hace un seguimiento a sus actualizaciones o estado.

3. Identificación de las vulnerabilidades, amenazas y salvaguardas para la protección de los activos del ciberespacio del caso de estudio de la empresa QWERTY S.A.

[38] Gimenes, N. (2017). *Top 10 Riesgos de Seguridad en la Web (OWASP) y como atenuarlos con API Management - Sensedia*. Recuperado de: https://sensedia.com/es/apis/10-riesgos-seguridad-apis/.

Tabla 18. Reconocimiento de las vulnerabilidades, amenazas y salvaguardas de los activos del ciberespacio del caso de estudio de la empresa QWERTY S.A.

Nombre del activo	Categorización	Amenazas	Vulnerabilidades	Salvaguardas
Proveedor de servicio de internet (ISP)	Servicios [S] - (1)	• Lentitud del servicio de comunicación. • Intermitencia del servicio. • Caída parcial o total del servicio. • Problemas de seguridad.	• Errores en la configuración. • Gran número de puertos abiertos. • Fugas de información. • Acceso a la información poco fiable y falsa • Accesos no autorizados al servicio.	• Listas de chequeo en los mantenimientos de software y hardware de la infraestructura de la ISP. • Aplicación de filtros de contenidos. • Política de seguridad para el manejo y uso de los servicios del internet.
Página Web	Servicios [S] - (1)	• Modificación y/o alteración de la información y los servicios alojados en los servidores por un empleado con exceso de privilegios. • Accesos no autorizados. • Denegación de servicios. Alteración accidental de la información. • Difusión de software dañino. • Perdidas de autenticación. • Redirección y reenvió no validos	• Errores en la gestión de recursos y configuraciones. • Fallos en la depuración de alguna aplicación o en la misma programación del sitio web. • Permisos, privilegios y/o control de acceso. • Ejecución de códigos malintencionados, SQL injection. • Factor Humano	• Identificación de los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red que se contraten con el proveedor del servicio. • Contante actualización con el contrato de soporte del servicio con el proveedor.

		• Fallo de servicios de comunicación. • Caída del sistema por agotamiento de recursos.		
Equipos de cómputo para la gestión del desarrollo tecnológico (Objeto Social)	**[HW] Equipamento Informático - (10)**	• Falla de hardware. • Falla de software. • Delincuentes informáticos. • Virus, gusanos, troyanos, spyware, DDoS, ransomware etc. • Acceso de información no debida. • Cortes eléctricos • Suplantación de la identidad del usuario • Accesos no autorizados • Caída del sistema por agotamiento de recursos. • Difusión de software dañinos.	• Falta de mantenimiento. • Daños caudados por desgate o defectos de fabrica • Mala configuraciones de los equipos • Falta de mantenimiento a las políticas de credenciales • Factor humano. • Daños de los equipos por variaciones de voltajes e idas de energía eléctrica.	• Control de acceso. • Gestión de privilegios. • Configuración y mantenimiento de equipos. • Realizar revisiones periódicas en los equipos de cómputo para prevenir desactualizaciones en el software instalado (Sistema operativo, Antivirus y aplicaciones).
Correo electrónico Institucional	Servicios [S] - (1)	• Denegación de Servicios (DoS) • Spam • Fugas de información. • Ingeniería Social • Phishing	• Sendmail (envió, recepción y redireccionamiento del mail). • Bulos (falsa noticias)	• Aplicación de protocolos de transporte de correo electrónico. • Protocolos de acceso. • Creación y aplicación de políticas para el uso de correo electrónico. • Roles de seguridad del correo electrónico. • Seguridad del servidor de correo institucional. • Actualizaciones permanentes. • Listas de chequeo.

De acuerdo al Reconocimiento de las vulnerabilidades, amenazas y salvaguardas de los activos del ciberespacio del caso de estudio de la empresa QWERTY S.A, se procederá a evaluar el riesgo según la valoración de los activos del ciberespacio y su impacto; en la tabla 15, se reconoce dicha valoración de acuerdo al catálogo de elementos establecidos en el libro II de la metodología de MARGERIT en su versión No.3, dado lo anterior se procederá a efectuar dicha estimación:

Tabla 19. Valoración de los activos del ciberespacio del caso de estudio de la empresa QWERTY S.A; según su impacto.

Nombre del Activo del ciberespacio	Categorización[.] - Cantidad (.)	Impacto	Criterios de Valoración (Descripción escalas estándar).
Proveedor de servicio de internet (ISP).	**Servicios [S] - (1)**	**[B]**	**(5. da):** Probablemente cause la interrupción de actividades propias de la Organización, con impacto en otras organizaciones.
Página Web.	**Servicios [S] - (1)**	**[M]**	**(1. da):** Pudiera causar la interrupción de actividades propias de la Organización.
Equipos de cómputo para la gestión del desarrollo tecnológico (Objeto Social).	**[HW] Equipamento Informático - (10)**	**[A]**	**(3.adm):** probablemente impediría la operación efectiva de una parte de la Organización.
Correo electrónico Institucional.	**Servicios [S] - (1)**	**[M]**	**(3. da):** Probablemente cause la interrupción de actividades propias de la Organización.

Basado en lo anteriormente efectuado, se procederá a realizar la valoración de los activos del ciberespacio del departamento de sistemas del caso de estudio de la empresa QWERTY S.A., según su impacto y dimensiones de seguridad, con el fin de conocer y valorar cada una de las consecuencias de su materialización de la amenaza según el escenario propuesto.

Tabla 20. Valoración de los activos del ciberespacio del departamento de sistemas del caso de estudio de la empresa QWERTY S.A; según su impacto y dimensiones de seguridad.

Nombre del Activo del ciberespacio	Categorización[.]- Cantidad (.)	Valoración de los activos				
		[D]	[C]	[I]	[A]	[T]
Proveedor de servicio de internet (ISP)	**Servicios [S] - (1)**	**[A]**	**[B]**	**[B]**	**[B]**	**[MB]**
Página Web	**Servicios [S] - (1)**	**[A]**	**[M]**	**[M]**	**[B]**	**[B]**
Equipos de cómputo para la gestión del desarrollo tecnológico (Objeto Social)	**[HW] Equipamento Informático - (10)**	**[B]**	**[MB]**	**[B]**	**[B]**	**[MB]**
Correo electrónico Institucional	**Servicios [S] - (1)**	**[M]**	**[A]**	**[M]**	**[M]**	**[B]**

De lo anteriormente descrito, a continuación, se procederá a realizar el análisis de riesgos de acuerdo a su valoración, impacto y probabilidad de riesgo, conforme a la matriz de análisis de riesgos y la cual se anexará las observaciones y estudios de los activos del ciberespacio acorde a la metodología implementada y la cual se verá reflejada en el **Anexo A,** según el nombre del activo del ciberespacio y su categorización.

Una vez efectuada la matriz de análisis de riesgos, se realizará la valoración de riesgos según el impacto y la probabilidad del riesgo existe dentro del departamento de sistemas del caso de estudio de la empresa QWERTY S.A., la cual se ve reflejada en el **Anexo B**, según la información dada allí.

A continuación, se procederá a realizar el tratamiento del riesgo de los activos del ciberespacio, según los riesgo y estrategias descrita en el caso de estudio de la empresa QWERTY S.A., el cual se encuentra reflejado en el Anexo C del presente documento.

Dada la anterior información, podemos decir que los activos del ciberespacio del departamento de sistemas del caso de estudio de la empresa QWERTY S.A., se va a implementar un plan de tratamiento de riesgos, en donde se ejecutaran acciones o estrategias como son **"Aceptar" y "Aceptar y Monitorear"** los riesgos**,** con el fin de evitar los riesgos, amenazas y vulnerabilidades dentro de nuestro sistema de información.

7.4.4.10. Controles de ciberseguridad o ciberprotección.

Una vez identificados los riesgos de ciberseguridad, se procederá a establecer lineamientos y controles apropiados para así poder implementarlos de acuerdo a la presente norma.

Para dar inicio e implementación de los controles se debe definir unas políticas que normalicen la creación recolección, almacenamiento, trasmisión, distribución, procesamiento y uso general de la información del caso de estudio de la empresa QWERTY S.A, especialmente con los activos de información del ciberespacio. Dado lo anterior, los controles de ciberseguridad según la norma que se deben implementar dentro de la entidad de acuerdo a sus lineamientos son:

Tabla 21. Controles de ciberseguridad para los activos del ciberespacio para el departamento de sistemas del caso de estudio de la empresa QWERTY S.A.

Activos del ciberespacio	Categorización	Controles de Ciberseguridad
• **Proveedor de servicio de internet (ISP).**	**[S]**	**<u>A Nivel Servidor:</u>** **Control 01.** Configuración de servidores, incluyendo los sistemas operativos subyacentes de acuerdo a la guía de configuración de seguridad, incluyendo una

• **Página Web** • **Correo electrónico Institucional**	**[S]** **[S]**	definición adecuada de los usuarios del servidor versus los administradores, como así mismo la aplicación de controles de acceso a los directorios, archivos de programas, sistemas y la habilitación de rastros para los procesos de auditoria, en particular, para la seguridad y otros eventos de fallo en el sistema. **Control 02.** Implementación de un sistema para probar y desplegar actualizaciones de seguridad para asegurar que el sistema operativo y las aplicaciones del servidor la cuales mantienen al día y con prontitud las nuevas actualizaciones de seguridad que este disponibles. **Control 03.** Supervisión del desempeño de seguridad del servidor a través de revisiones periódicas de los rastros para los procesos de auditoria. **Control 04.** Revisiones de las configuraciones de seguridad. **Control 05.** Ejecución de los controles de software anti-malicioso (tales como antivirus y anti-spyware) en el servidor. **Control 06.** Llevar a cabo evaluaciones de vulnerabilidad regulares y pruebas de seguridad de los sitios y aplicaciones en línea con el fin de asegurar que la seguridad se mantiene adecuadamente. **Control 07.** Realizar exploraciones regularmente en búsqueda de elementos comprometidos.
Equipos de cómputo para la gestión del desarrollo tecnológico (Objeto Social)	**[HW]**	**<u>A nivel de Usuario Final:</u>** **Control 01.** Utilización de sistemas operativos compatibles que posean los parches de seguridad más actualizados e instalados. Además, los consumidores organizacionales tienen la responsabilidad de estar al tanto y observar las políticas de la organización con respecto a los sistemas operativos compatibles. **Control 02.** Utilización de las ultimas aplicaciones soportadas y que tengan los parches más actualizados e instalados.

		Control 03. Uso de herramientas antivirus y anti-spyware. **Control 04.** Habilitación de bloqueadores de scripts o configuraciones de seguridad web superior, con el fin de garantizar que solo los scripts de fuentes confiables se ejecuten en una computadora local. **Control 05.** Utilización de filtros phishing, es decir que los navegadores web comunes y las herramientas del navegador, incorporan a menudo la capacidad de determinar si un sitio que un usuario está visitando se encuentra dentro de una base de datos de sitios web de Phishing conocidos o contienen patrones de scripts que son similares a aquellos típicos sitios web de phishing. **Control 06.** Habilitación de firewall personal y finalmente el uso de un sistema de detección de intrusos basado en el host (HIDS).[39]

[39] Gomez Morales, G. (2017). Gestión de la Ciberseguridad según el ISO/IEC 27032:2012. Linkedin.com. Recuperado de: https://www.linkedin.com/pulse/gesti%C3%B3n-de-la-ciberseguridad-seg%C3%BAn-el-isoiec-gianncarlo-g%C3%B3mez-morales.

8. CONCLUSIONES

- Con la implementación del SGSI en el caso de estudio de la empresa QWERTY S.A., de acuerdo al estándar de calidad ISO 27001:2013, se concluye que cualquier tipo de entidad, pymes u organización que implemente estas normas, proporcionara seguridad en cada uno de los activos de la información y prolongara la existencia y valoración de los mismos.

- Mediante el análisis de las amenazas, riesgos, vulnerabilidades y la aplicación de procedimientos o controles se puede garantizar una mayor vida útil a los activos de información tanto físicos como del ciberespacio y todo esto a partir de las estrategias de protección tanto físicos como virtuales basándonos en los principios de confidencialidad, integridad, disponibilidad y no repudio de la información.

- Al momento de evaluar el nivel de riesgo en una empresa u organización, se debe determinar como primera medida la metodología a implementar, para así proceder a definir el alcance del departamento o área que va a analizar y finalmente diagnosticar el estado actual de la seguridad informática de cada uno de los activos de información de la empresa QWERY S.A.

- Para un buen análisis de riesgos se debe tener en cuenta la evaluación y cálculo de riesgos sobre cada uno de los activos de información y finalmente se debe aplicar medidas o controles para materializar la protección sobre cada uno de los activos de información de una entidad u organización.

- Es importante identificar los activos de informacion, como asi mismo las amenazas, riesgos y vulnerabilidades que posean la organización, con el fin implementar y mejorar medidas de seguridad dentro de la entidad, teniendo en cuenta las políticas y controles funcionales, los cuales conllevan al cumplimiento de cada uno de los objetivos del SGSI dentro de la entidad.

9. RECOMENDACIONES

- Se recomienda que para la implementación del presente proyecto se tenga en cuenta cada uno de los argumentos que están contenidos en el presente documento es decir cada uno de los parámetros descritos en el diseño del plan de gestión de riesgos y vulnerabilidades del caso de estudio de la empresa QWERTY S.A., basados en los estándar NTC-ISO/IEC 27001, tales como:
    - Políticas de seguridad de la empresa
    - Técnicas, Procedimientos, objetivos y controles para la gestión de riesgos.

- Para efectuar un buen análisis de riesgos en cada uno de los procesos de una empresa u organización se recomienda que, como primera medida, seleccionar una metodología a aplicar, una vez realizado lo anterior se procede a definir el alcance del departamento o área que va a analizar y enseguida se procede a identificar los activos de información más relevantes para el funcionamiento de la empresa u organización, una vez hecho lo anterior se procede a identificar las amenazas que puedan afectar los activos de información de la entidad, como así mismo la identificación de las vulnerabilidades y salvaguardas que son implantadas como medidas y controles de seguridad en el área o dependencia del sistema de seguridad de informática.

- Se recomienda que al momento de efectuar un buen análisis de riesgos se debe tener en cuenta la evaluación y cálculo de riesgo sobre cada uno de los activos de información así cuenten medidas de protección o no las que cuenten y finalmente se debe aplicar medidas o controles para materializar la protección sobre cada uno de los activos de información de la entidad tanto físicos como del ciberespacio y se aconseja emplear la metodología MARGERIT, la cual fue empleada en este proyecto.

REFERENCIAS BIBLIOGRÁFICAS

- AGUIRRE TOVAR, Ricardo Andrés y ZAMBRANO ORDOÑEZ, Andrés Fernando. Estudio para la implementación del sistema de gestión de seguridad de la información para la secretaria de educación departamental de nariño basado en la norma ISO/IEC 27001 [en línea]. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3655/1/13039116.pdf

- ALCALDÍA MUNICIPAL DE SOPO.SECRETARIA DE DESARROLLO. Plan de gestión del riesgo en seguridad y privacidad de la información [sitio web]. Junio de 2018. Archivo pdf. Disponible en: http://www.sopo-cundinamarca.gov.co/Transparencia/PlaneacionGestionyControl/PLAN%20DE%20GESTION%20DEL%20RIESGO%20EN%20SEGURIDAD%20Y%20PRIVACIDAD%20DE%20LA%20INFORMACION.pdf

- ALEMAN NOVOA, Helena y RODRÍGUEZ BARRERA, Claudia. Metodologías para el análisis de riesgos en los SGSI [en línea]. Disponible en: https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1754

- ALVAREZ RIAÑO, Jerzon Herley. 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, que incluye: asesoría, planeación [en línea]. Bogotá (2016). Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/11950/1/17348959.pdf.

- ALLISON RAMOS PRODUCCIÓN AUDIOVISUAL. Riesgos informáticos [Video]. Perú: YouTube. (17 de febrero 2016).10:32 minutos. Disponible en: https://www.youtube.com/watch?v=vZ5Dr1nSSRY

- ARDILA GARCIA, Álvaro Javier y CARDONA TOVAR Lorena Patricia. Desarrollo de un marco de trabajo para la gestión del SGSI en PYMES desarrolladoras de software en Bogotá basado en la metodología MGSM -PYME [en línea]. Disponible en: http://repository.udistrital.edu.co/bitstream/11349/2807/1/CardonaTovarLorenaPatricia2016.pdf

- Álvarez, Angela; Torres, Gloria y Ochoa, Rubén. Matriz de partes interesadas internas [en línea]. 2 ed. Colombia: Concejo profesional nacional de ingeniería 2018. Disponible en: https://www.copnia.gov.co/sites/default/files/uploads/mapa-procesos/archivos/direccionamiento-estrategico/partes_interesadas.pdf

- Bastidas, Henry; López, Iván y Peña, José. Análisis de riesgos y recomendaciones de seguridad de la información al área de información y tecnología del hospital susana López de valencia de la ciudad de Popayán [en línea]. Disponible en: https://www.copnia.gov.co/sites/default/files/uploads/mapa-procesos/archivos/direccionamiento-estrategico/partes_interesadas.pdf

- BENAVIDES SEPÚLVEDA, Alejandra María y BLANDÓN JARAMILLO, Carlos Arturo. Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico. [en línea]. Disponible en: http://eds.a.ebscohost.com.bibliotecavirtual.unad.edu.co/eds/pdfviewer/pdfviewer?vid=1&sid=0d8ee77b-ce77-4578-bcff-7e41aa16469d@sdc-v-sessmgr05

- BIRARDA, Carina y BALDERRAMA, Julio Cesar. ISO IEC 27032 Ciberseguridad [Video]. YouTube (19 de septiembre de 2019).49:36 minutos. Disponible en: https://www.youtube.com/watch?v=7Y6_2HzU4p8

- BOCANEGRA QUINTERO, Yamilet. Análisis y gestión de riesgos de los sistemas de información de la alcaldía municipal de Tuluá aplicando la metodología MAGERIT [en línea]. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3632/1/66728456.pdf

- BOTERO VEGA, David Humberto. Diseño del sistema de gestión de seguridad informática y de la información (SGSI) para la empresa BELISARIO LTDA. de la ciudad de Bogotá D.C [en línea]. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/12925/1/80259558.pdf

- Buesaquillo, Mónica; López, Darwin y García, Andrés. Diseño del sistema de gestión de seguridad de la información para una agencia de viajes y turismo [en línea]. Bogotá. (29 de mayo de 2017). Disponible en:

http://repository.poligran.edu.co/bitstream/handle/10823/999/entregafinal.pdf?sequence=1&isallowed=y

- CAMARGO RAMIREZ, Juan David. 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]. (p.9-12) Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/11992/1/75104100.pdf.

- Canal En VIVO - Universidad EAFIT. Administración de Riesgos Cibernéticos: Nuevos desafíos relacionados con la dependencia tecnológica [Video]. Medellín Colombia: YouTube. (23 de mayo de 2018).1:11 hrs. Disponible en: https://www.youtube.com/watch?v=bb8gzgkJutk

- Cárdenas, Leidy; Martínez, Hugo y Becerra, Luis. Gestión de seguridad de la información: revisión bibliográfica [en línea]. (24 de octubre de 2016). Disponible en: http://eds.b.ebscohost.com.bibliotecavirtual.unad.edu.co/eds/pdfviewer/pdfviewer?vid=2&sid=76e5dfd6-7afe-4a67-8e7c-3e0779fe2163@pdc-v-sessmgr02 E-SSN: 1699-2407.

- CASTRO QUINDE, Carlos Oswaldo. Elaboración de un Sistema de Gestión de Seguridad de la Información (SGSI) para la Empresa Radical Cía. Ltda. En la Ciudad de Quito para el año 2014. [en línea]. Disponible en: http://dspace.udla.edu.ec/handle/33000/3376

- CISCO. Soluciones de seguridad para redes empresariales y Cisco DNA [sitio web]. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

- COLOMBIA, BOGOTA D.C. INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION (ICONTEC). Norma técnica NTC-ISO/IEC colombiana 27001 [en línea]. (22 de marzo de 2006). Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

- COMISIÓN DE REGULACIÓN DE COMUNICACIONES (CRC). Revisión del marco regulatorio para la gestión de riesgos de seguridad digital: Análisis y

propuesta [sitio web]. República De Colombia. (noviembre de 2017). Archivo pdf. Disponible en: https://www.crcom.gov.co/recursos_user/2017/actividades_regulatorias/ciberseguridad/Documento_CRC_Seguridad_Digital_Vpublicar.pdf

- CORTES BORRERO, Rodrigo. Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia [en línea]. Villavicencio (febrero de 2015). Disponible en: https://repository.usta.edu.co/bitstream/handle/11634/14032/2015rodrigocortes.pdf?sequence=1&isAllowed=y

- CORDOBA BITCOIN. Documental sobre seguridad informática [Video]. YouTube (14 de octubre de 2017). 44:26 minutos. Disponible en: https://www.youtube.com/watch?v=Dp_iBcfFftM

- CÓRDOBA SUAREZ, Alba Elisa. Diseño e implementación de un SGSI para el área de informática de la curaduría urbana segunda de pasto bajo la norma ISO/IEC 27001 [en línea]. San Juan de Pasto (mayo de 2015). Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3627/1/59650050.pdf

- DIAZ, Andrés; COLLAZOS, Gloria; CORTEZ, Hermes; ORTIZ, Leidy y HERAZO, Gustavo A. Implementación de un sistema de gestión de seguridad de la información (SGSI) en la comunidad nuestra señora de gracia, alineado tecnológicamente con la norma ISO 27001 [en línea]. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3627/1/59650050.pdf

- ESCUELA DE ORGANIZACIÓN INDUSTRIAL (EOI). Administración y gestión de la seguridad en los sistemas [Video]. YouTube (06 de junio de 2016). 01:58:21 hrs. Disponible en: https://www.youtube.com/watch?v=D2rFxvxcSEA

- ESCUELA TECNOLOGICA, INSTITUTO TECNICO CENTRAL. Política general de seguridad de la información y objetivos del SGSI y MSPI [sitio web]. 3 ed. Bogotá D.C, (19 de abril de 2017). Disponible en: http://www.itc.edu.co/archives/politicaobjetgsimspi.pdf

- FAJARDO DIAZ, Carmen Elizabeth. Análisis de los riesgos de seguridad de la información de un aplicativo de gestión documental líder en el mercado colombiano [en línea]. Bogotá (2 de junio de 2017) (p.15). [Consultado el 05 de marzo de 2020]. Disponible en: http://alejandria.poligran.edu.co/bitstream/handle/10823/995/3.%20Documento%20Final%20Opci%c3%b3n%20de%20grado%20II.pdf?sequence=1&isAllowed=y

- Florez, Fanny; Jiménez, Diana y Hidalgo, Pablo. diseño de un sistema de gestión de seguridad de la información para la empresa MEGADATOS S.A. en la ciudad de quito, aplicando las normas ISO 27001 e ISO 27002 [en línea]. Disponible en: http://bibdigital.epn.edu.ec/bitstream/15000/4885/1/Diseño de un sistema.PDF

- GARCÍA RAMÍREZ, German y CASTRO ANGARITA, Jaime. Diseñar un sistema de gestión de la seguridad de la información (SGSI) a la empresa UNITRANSA S.A. ubicada en la ciudad de Bucaramanga [en línea]. Trabajo de grado para optar al título de Especialista en Seguridad Informática. Bucaramanga. Universidad Nacional Abierta y a Distancia (UNAD). Escuela de ciencias básicas, tecnología e ingeniería (ECBTI). 2017. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/11914/4/5685072.pdf

- GARRIDO CAMARGO, Cristóbal. Elaboración de plan de implementación de la ISO/IEC 27001:2013 [sitio web]. Universitat Oberta de Catalunya (UOC). (diciembre de 2018) (p.7-12). Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/88265/10/cgarridocaTFM0119memoria.pdf

- Gobierno de Colombia, MINTIC. Modelo Nacional de gestión de riesgos de seguridad digital. Archivo pdf. Disponible en: https://mintic.gov.co/portal/604/articles-61854_documento.docx

- Global Standards. ISO 27001 - Seguridad de la Información [Video]. YouTube. (14 de noviembre de 2017). 32:56 minutos. Disponible en: https://www.youtube.com/watch?v=WJm1qHHuMr0

- GÓMEZ MORALES, Gianncarlo. (Ciberseguridad según el ISO/IEC 27032:2012) [en línea]. G55CIO Edición No. 14. p.14. ISSUU. Disponible en: https://issuu.com/g55cio/docs/g55cio_issuu_edicion_14_9mayo

- GÓMEZ VIEITES, Álvaro. Anexo III Análisis y Gestión de Riesgos en un Sistema Informático [sitio web]. Academia.edu. Disponible en: https://www.academia.edu/5971566/Anexo_III_An%C3%A1lisis_y_Gesti%C3%B3n_de_Riesgos_en_un_Sistema_Inform%C3%A1tico

- GUERRERO JULIO, Marlene Lucila y GÓMEZ FLOREZ, Luis Carlos. Gestión de riesgos y controles en sistemas de información: del aprendizaje a la transformación organizacional [en línea]. ScienceDirect. (13 de diciembre de 2012) Disponible en: https://www-sciencedirect-com.bibliotecavirtual.unad.edu.co/science/article/pii/S0123592312700116?via=ihub

- GUANOLUISA HUERTAS, Jhon Erik y MALDONADO SOLIZ, Ivonne Fernanda. Análisis de Riesgos de un plan de seguridad de la información para el concejo nacional de igualdad de discapacidades "CONADIS" [en línea]. Quito Ecuador; mayo de 2015. (p.51-52). Disponible en: https://bibdigital.epn.edu.ec/bitstream/15000/10499/1/CD-6217.pdf

- GUZMAN SILVA, Carlos Alberto. Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso [en línea]. Funza Cundinamarca, noviembre de 2015. Disponible en: http://alejandria.poligran.edu.co/bitstream/handle/10823/654/Proyecto%20de%20Grado%20SGSI%20-%20IGM-%20CarlosGuzman%20%28FINAL%29.pdf?sequence=1&isAllowed=y

- GUZMAN SOLANO, Sandra Liliana. Guía para la implementación de la norma ISO 27032 [en línea]. Universidad Católica de Colombia. Bogotá D.C, junio de 2019. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/23385/1/Proyecto%20Guia%20ISO%2027032.pdf

- HATHAYWAY, Melissa. Gestión del riesgo cibernético nacional [sitio web]. Organización de los estados americanos (OEA). White paper series. 2 ed. Archivo pdf. Disponible en: https://www.oas.org/es/sms/cicte/ESPcyberrisk.pdf

- INSTITUTO COLOMBIANO AGROPECUARIO (ICA), Oficina tecnologías de la información. Plan Estratégico de Seguridad de la Información PESI [sitio web]. Bogotá D.C, (noviembre de 2017). Disponible en: https://www.ica.gov.co/transparencia-y-acceso-a-la-informacion/2018/plan-estrategico-de-seguridad-de-la-informacion_ic.aspx

- INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). SGSI - 05 Implantación de un SGSI [Video]. España: YouTube. (22 de marzo 2010).06:14 minutos. Disponible en: https://www.youtube.com/watch?v=i_3z68QGaJs

- INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). SGSI - 07 Los activos de Seguridad de la Información [Video]. España: YouTube. (27 de abril de 2010). 05:22 minutos. Disponible en: https://www.youtube.com/watch?v=THnQ2FH7NtU

- INSTITUTO NACIONAL DE NORMALIZACIÓN (INN). NCh iso-27032:2015. 1st ed., Santiago de chile. (2015). p. 3-8.

- INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN (INTECO). Guía de apoyo de un SGSI: Implantación de un SGSI en la empresa [sitio web]. Gobierno de España. Archivo pdf. Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

- INSTITUCIONES, SERVICIOS DE CREACIÓN DE SITIOS WEB INSTITUCIONALES OFICINA DE SEGURIDAD PARA LAS REDES INFORMÁTICAS. Metodología para la gestión de la seguridad informática (Proyecto). Archivo pdf. Disponible en: https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf

- ISO 27000.es [sitio web]. Serie “27000”. Disponible en: https://www.iso27000.es/iso27000.html

- ISO 27000.es [sitio web]. SGSI. Disponible en: https://www.iso27000.es/sgsi.html

- LUNA LASSO, Juan Francisco Respondiendo a la amenaza: hacia el fortalecimiento de las políticas de ciberseguridad en Colombia a través de la comunidad internacional [en línea]. Trabajo de grado para optar al título de politólogo. Bogotá D.C. Pontifica Universidad Javeriana. Escuela de ciencias políticas y relaciones internacionales. 2016. Disponible en: https://repository.javeriana.edu.co/bitstream/handle/10554/35658/Juan%20Francisco%20Luna%20Lasso.pdf?sequence=1&isAllowed=y

- LIZARAZO LOZANO, Kevin Orlando. Planteamiento de un SGSI basado en la norma ISO 27001:2013 para la empresa de servicios de tecnología SITECH DE COLOMBIA SAS en los procesos gestión financiera, gestión de logística y gestión de IT [en línea]. Trabajo de grado para optar al título de especialista en seguridad informática. Bogotá D.C. Universidad Piloto de Colombia. Facultad de Ingeniería. 2016. Disponible en: http://polux.unipiloto.edu.co:8080/00003412.pdf

- Manjarrez, Cristina; Mogollón, Edgar; Cortes, Iván y Dussan, Leonardo. Identificación de riesgos en el tratamiento de datos personales a nivel de usuarios clientes de aplicaciones móviles en el sector del transporte público individual en Bogotá [en línea]. Trabajo de grado para obtener el título de especialista en auditoria de sistemas. Bogotá D.C. Universidad Católica de Colombia. Facultad de Ingeniería. 2016. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/7831/4/Identificacion%20de%20Riesgos%20en%20el%20Uso%20de%20Apps%20de%20Transporte%20Publico.pdf

- MAYA ARANGO, Paula Andrea. Desarrollo de un Plan Director de Seguridad para la implementación de un SGSI basado en la norma ISO/IEC 27001 [en línea]. Universitat Oberta de Catalunya (UOC). Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC). (06 de junio de 2016). Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/11914/4/5685072.pdf

- MEJÍA QUIJANO, Rubí Consuelo y NÚÑEZ PATIÑO, María Antonia. Administración de riesgos empresariales en Colombia, México y Argentina. [en línea]. Medellín, Colombia. Universidad EAFIT. Agosto de 2017. Disponible en:

https://repository.eafit.edu.co/bitstream/handle/10784/11721/administracion_riesgos_empresariales_colombia_mexico_argentina.pdf?sequence=1&isAllowed=y ISBN: 978-958-720-441-4

- MERCADO PALENCIA, Yolima. Tercera web conferencia del curso de Aspectos Éticos Y legales de la seguridad informática. Universidad Nacional Abierta y a Distancia (UNAD). Abril de 2020. Disponible en: http://conferencia2.unad.edu.co/pgepdmgxi3u0/?proto=true

- MOYANO ORJUELA, Luz Adriana y SUAREZ CARDENAS, Yasmin Elena. Plan de implementación del SGSI basado en la norma ISO 2701:2013 para la empresa INTERFACES Y SOLUCIONES [en línea]. Trabajo de grado para obtener el título de ingeniera telemática. Bogotá D.C (2017). Universidad Distrital Francisco José Caldas. Facultad de telemática. Disponible en: http://repository.udistrital.edu.co/bitstream/11349/6737/1/MoyanoOrjuelaLuzAdriana2017.pdf

- MUÑOZ MARTÍN, Manuel. Guía de implantación de un SGSI basado en la norma UNE-ISO/IEC 27001 [en línea]. Universitat Oberta de Catalunya. (junio de 2015). Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/42965/7/mmanozTFC0615memoria.pdf

- MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS [sitio web]. Gobierno de España. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (3rd ed., pp. 19-23). Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

- MINTIC. Guía de gestión de riesgos - seguridad y privacidad de la información [sitio web]. Bogotá D.C, (01 de abril de 2016). Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

- MONCAYO RACINES, Diana Elizabeth. Modelo de evaluación de riesgos en activos TIC´S para pequeñas y medianas empresas del sector automotriz [en línea]. Escuela Politécnica Nacional. Quito, Ecuador (agosto de 2014). Disponible en: https://bibdigital.epn.edu.ec/bitstream/15000/8499/3/CD-5741.pdf

- PERAFÁN RUIZ, John Jairo y CAICEDO CUCHIMBA, Mildred Caicedo. Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca [en línea]. Tesis de grado para obtener el título de Especialista en Seguridad Informática. Popayán (2015). Universidad Nacional Abierta y a Distancia (UNAD). Escuela de ciencias básicas tecnología e ingeniería (ECBTI). Disponible en: http://repository.udistrital.edu.co/bitstream/11349/6737/1/MoyanoOrjuelaLuzAdriana2017.pdf

- PORRAS DIAZ, Daniel Andrés. Mapa de Riesgos - Gestión Tic 2016 - RISEM2016 [en línea]. Alcaldía de Fusagasugá. 15 de noviembre de 2017, Disponible en: http://webcache.googleusercontent.com/search?q=cache:oy8NNkG9zoAJ:www.fusagasuga-cundinamarca.gov.co/Transparencia/MODELO%2520INTEGRADO%2520DE%2520PLANEACION%2520Y%2520GESTION/Mapa%2520de%2520Riesgos%2520-%2520Gesti%25C3%25B3n%2520Tic%25202016%2520-%2520RISEM2016.xls+&cd=6&hl=es-419&ct=clnk&gl=co

- REVISTA IBÉRICA DE SISTEMAS E TECNOLOGÍAS DE INFORMACIÓN (RISTI): Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000 [en línea]. Rio tinto Portugal. 01 de mayo de 2017. Disponible en: http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1646-98952017000200006&lng=en&tlng=en ISSN 1646-9895

- RIVEROS CARDENAS, Fredy Orlando. Administración del riesgo cibernético un enfoque desde la alta gerencia empresarial en Colombia [en línea]. Universidad militar nueva granada. Facultad de estudios a distancia. Trabajo de grado para optar al título de Especialista en Alta Gerencia. Bogotá D.C (2016). Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/15837/RiverosCardenasFredyOrlando2017.pdf;jsessionid=080C9D80D77334EE32CA96476069E485?sequence=1

- RODRÍGUEZ CONDE, Luis. Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013 [en línea]. Universitat Oberta de Catalunya (UOC). Máster Universitario en Seguridad de las Tecnologías de la Información y de las

Comunicaciones (MISTIC). (junio de 2017). Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/64545/1/liziyoTFM0617-Resumen%20Ejecutivo-Memoria.pdf

- ROJAS HERNANDEZ, Yoisel; TORRES, David Leonardo y CONTRERAS, José Gregorio. Manual de políticas de seguridad y privacidad de la información ETITC [sitio web]. Escuela tecnológica instituto técnico central. Bogotá, (2nd ver., p.55-95). Disponible en: http://www.itc.edu.co/archives/manualpiliticassi.pdf

- ROJAS PEÑA, Hernán Mauricio. Aplicación de la metodología MAGERIT para el análisis de riesgos de los sistemas de control en la estación TENAY del oleoducto [en línea]. (p.10-14). Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/27758/1/1075211684.pdf

- RUIZ PEÑA, José Higinio. Diseño de un sistema de gestión de seguridad de la información (SGSI) bajo la norma ISO/IEC 27001:2013, en la cooperativa multiactiva del personal del Sena, en Bogotá [en línea]. Monografía con miras a obtener el título de especialista en seguridad informática. Bogotá D.C (18 de febrero de 2018). Universidad Nacional Abierta y a Distancia (UNAD). Escuela de ciencias básicas tecnología e ingeniería (ECBTI). Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17300/1/80267708.pdf

- SANCHEZ PACHECO, Emilio Antonio y REBOLLEDO HINOJOSA, Faver Lisandro. Diseño de un modelo de gestión de la seguridad de la información en el área de talento humano de la secretaría de educación [en línea]. Trabajo de grado para obtener el título de especialista en seguridad de la Información. Arauca, 17 de septiembre de 2017. Institución universitaria politécnico grancolombiano. facultad de ingeniería y ciencias básicas. Disponible en: http://repository.poligran.edu.co/bitstream/handle/10823/1039/DISE%C3%91O%20DE%20UN%20MODELO%20DE%20GESTI%C3%93N%20DE%20LA%20SEGURIDAD%20DE%20LA%20INFORMACI%C3%93N%20EN%20EL%20%C3%81....pdf?sequence=1&isAllowed=y

- SUAREZ, Oswaldo. SGSI Sistema de Gestión de Seguridad de la Información [Video]. Colombia: YouTube. (13 de julio 2014). 07:23 minutos. Disponible en: https://www.youtube.com/watch?v=wIe01QIFA8Q

- SUAREZ GONZÁLEZ, Rafael. Análisis de activos de información para un sistema misional basados en la metodología MAGERIT v3 y la norma ISO 27001:2013 [en línea]. Monografía para optar el título de especialista en seguridad informática. Bogotá D.C (18 de julio de 2018). Universidad Nacional Abierta y a Distancia (UNAD). Escuela de ciencias básicas tecnología e ingeniería (ECBTI). Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/19571/3/80803746.pdf

- UNIR ESTUDIOS AVANZADOS. Riesgos de ciberseguridad y su impacto en negocio [sitio web]. Gobierno de España, Madrid. Archivo pdf. Disponible en: https://static.unir.net/ingenieria/ciberseguridad-y-estrategia-corporativa-para-la-alta-direccion/Curso_Ciberseguridad-CEA_es.pdf

- UNIVERSIDAD INDUSTRIAL DE SANTANDER (UIS). Manual para la administración del riesgo [en línea]. Bucaramanga, octubre de 2016. (5th ed., p. 12-20). Disponible en: https://www.uis.edu.co/webUIS/es/administracion/controlGestion/documentos/2015/MSE.01manualAdministracionRiesgo.pdf

- UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD). Manual del sistema de integrado de gestión [sitio web]. Bogotá, (18nd ver). (18 de agosto 2020). Disponible en: https://sig.unad.edu.co/documentos/sgc/manuales/M-1.pdf?v10

- UNIVERSIDAD OBERTA DE CATALUNYA (UOC). Política de seguridad criptográfica de la Universitat Oberta de Catalunya [sitio web]. Barcelona España. Disponible en: https://www.uoc.edu/portal/_resources/ES/documents/seu-electronica/Politica_Seguretat_Criptogrxfica_UOC-cat_ES.pdf

- VELÁSQUEZ; Paula; VELÁSQUEZ, Sandra; VELÁSQUEZ, Margarita y VILLA, Jhon. Implementación de la gestión de riesgo en los procesos misionales de la Sección de Dermatología de la Universidad de Antioquia (Medellín, Colombia) siguiendo las directrices de la norma ISO 9001:2015 [en línea]. (p. 88-89). Bogotá D.C, 30 de mayo de 2017. Disponible en: http://www.scielo.org.co/pdf/rgps/v16n33/1657-7027-rgps-16-33-00078.pdf

- YÁÑEZ CÁCERES, Nelson Alejandro. Sistema de gestión de seguridad de la información para la subsecretaria de economía y empresas de menor tamaño [en línea]. tesis para optar al grado de magister en tecnologías de la información. Santiago de chile (2017). Universidad de Chile. Facultad de ciencias físicas y matemáticas. Departamento de ciencias de la computación. Disponible en: http://repositorio.uchile.cl/bitstream/handle/2250/147976/Sistema-de-gestion-de-seguridad-de-la-informacion-para-la-Subsecretaria-de-Economia-y-Empresas.pdf?sequence=1&isAllowed=y

ANEXOS

ANEXO A

MATRIZ DE ANALISIS DE RIESGOS DEL DEPARTAMENTOS DE SISTEMAS DEL CASO DE ESTUDIO DE LA EMPRESA QWERTY S.A.

El descrito Anexo A, da a conocer la Evaluación del nivel riesgo de cada uno de los activos informáticos del departamento de sistemas del caso de estudio de la empresa QWERTY S.A., mediante el uso de una metodología de análisis de riesgos MAGERIT, con el fin de determinar el estado actual de la seguridad informática de la organización. Dado lo anterior a continuación se describe detalladamente el proceso de análisis de riesgos de cada uno de los procesos relacionados en nuestro caso de estudio seleccionado

A.1 INFORMACION.

OBJETIVO	Evaluar el nivel riesgo de los activos informáticos del departamento de sistemas del caso de estudio de la empresa QWERTY S.A., mediante el uso de una metodología de análisis de riesgos MAGERIT, con el fin de determinar el estado actual de la seguridad informática de la organización.
ALCANCE :	Análisis de riesgos sobre los procesos ddel departamento de sistemas del caso de estudio de la empresa QWERTY S.A.
Nombre de la Organización:	Departamento de sistemas del caso de estudio de la empresa QWERTY S.A.
CONTEXTO LEGAL:	NTC ISO/IEC 27001 - NTC ISO/IEC 27005 - NTC ISO/IEC 31000
Actividad Comercial:	Corresponde al desarrollo tecnológico de las comunidades colombianas a través del uso de Tecnologías de Información para la consulta de datos.
ENFOQUE METODOLOGICO	El enfoque de gestión de riesgos a aplicar está basado en la metodología **MAGERIT**
TRATAMIENTO	**Se tratarán los riesgos cuyos niveles sean:**
	NIVEL A TRATAR: 6 a 15 MODERADO (M)
	Se aceptarán los riesgos cuyo resultado después de la valoración de riesgos sean: MODERADO (M)
	Niveles de aceptación del riesgo (1 a 5 aceptable (A), 6 a 15 moderado (M), 16 a 26 inaceptable(I))
	Una vez aplicados los controles se acepta un riesgo de residual en niveles **APRECIABLE** o **IMPORTANTE**
	Criticidad residual (1 a 4 despreciable (d), 5 a 9 baja (B), 10 a 15 apreciable (a), 16 a 20 importante (i), 21 a 25 crítico(C))

A.2 METODOLOGIA MARGERIT.

MATRIZ DE INVENTARIO; PROBABILIDAD, IMPACTO Y VALORACIÓN DEL RIESGO DE ACTIVOS DE INFORMACIÓN

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

PROBABILIDAD DEL RIESGO

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

IMPACTO DEL RIESGO

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

VALORACIÓN DEL RIESGO

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

VALORACIÓN DEL RIESGO

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

A.3 ACTIVOS Y VALORACION CUALITATIVA.

Por el tamaño de la matriz de levantamiento de la información de los activos de información del departamento de sistemas del caso de estudio de la empresa QWERTY S.A, según la metodología MAGERIY y de la norma NTC/ISO/IEC 27001:2013, la descrita se puede detallar minuciosamente en el archivo de google drive cuyo link se encuentra al finalizar este anexo.

A.4 VALORACION CUANTITATIVA.

Nombre	Riesgo	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
Servidor de Impresión: Servidor marca Dell en torre Po	BAJO	4	4	4	9	9	6
Servidor de archivos FTP: Servidor marca Dell en torre	IMPORTANTE	15	15	20	20	15	17
Página web	APRECIABLE	9	9	15	15	20	14
Servidor de nómina y facturación.Servidor marca Dell e	APRECIABLE	15	9	15	20	15	15
Servidor DHCP: Servidor marca dell en torre PowerEdg	BAJO	4	9	9	9	15	9
Equipos de cómputo para gestión del desarrollo tecno	IMPORTANTE	20	15	20	20	15	18
Cortafuegos Cisco ASA 5505	APRECIABLE	20	9	9	15	9	12
Equipos deComputo (Dependencia de prueba de softw	BAJO	9	4	9	15	4	8
Equipos de Cómputo Sistemas operativos win 10 Pro (	BAJO	9	4	4	9	9	7
Puntos de acceso alámbricos (hub)	BAJO	9	4	9	9	9	8
Switches cisco catalyst 2960	APRECIABLE	9	4	9	15	15	10
Técnicos de mantenimiento	IMPORTANTE	20	20	15	20	15	18
Teléfonos IP	BAJO	4	4	4	9	9	6
Puntos de acceso (AP servicio de internet en el campu	BAJO	9	4	9	9	15	9
0	FALSO	FALSO	FALSO	FALSO	FALSO	FALSO	0
Proveedor de servicio de internet (ISP)	APRECIABLE	9	4	9	9	20	10
Correo electrónico Institucional	APRECIABLE	15	9	20	15	15	15

A.5 AMENAZAS Y PLAN DE TRATAMIENTO.

Dado el mismo principio del anexo A.3, en este numeral se relacionara la matriz de análisis y tratamiento de riesgos en donde se identifican las amenazas, vulnerabilidades, análisis de riesgos, estrategias de controles y finalmente el plan de tratamiento a aplicar y todo esto para cada uno de los activos de información presentados en el departamento de sistemas del caso de estudio de la empresa QWERTY S.A. Dado lo anterior, esto también aplica para cada una de las hojas elaboradas y encontradas en el archivo de Excel en donde se fija cada uno de los procedimientos y así poder evaluar el nivel de riesgo que posee la entidad de estudio; los cuales se ven reflejados y contenidos en el archivo de Excel que se encuentra publicado en **google drive** atraves del siguiente link:

https://drive.google.com/file/d/10OcgboeoEi-7aFZljHaRjxitDH2ZpGuz/view?usp=sharing

ANEXO B

TABLA DE LA VALORACION DE LOS RIESGOS SEGÚN EL IMPACTO Y LA PROBABILIDAD DEL RIESGO QUE EXISTE DENTRO DEL DEPARTAMENTO DE SISTEMAS DEL CASO DE ESTUDIO DE LA EMPRESA QWERTY S.A.

La valoración de los riesgos según el impacto y la probabilidad están dados atraves de la frecuencia de ocurrencia de un evento dentro de la empresa u organización, como así mismo en la materialización del riesgo. De acuerdo a lo anteriormente descrito a continuación se presenta la valoración de riesgos según el impacto y la probabilidad de riesgo existente dentro del caso de estudio propuesto.

B.1 IMPACTO Y PROBABILIDAD DE RIESGO.

IDENTIFICACIÓN DEL RIESGO						ANÁLISIS Y EVALUACIÓN DEL RIESGO		
Nombre del activo de Informacion	Activo de informacion	Riesgo			Clases de Riesgo 1. Estratégico 2. Imagen 3. Operativo 4. Financiero 5.Cumplimiento 6.Tecnología	Probabilidad de materialización	Impacto	Valoracion del riesgo de los activos
		Tipo Riesgo	Vulnerabilidades	Amenaza				
Servidor de Impresión: Servidor marca dell en torre PowerEdge T440	[HW] EQUIPAMENTO INFORMÁTICO	Institucional	*falta de mantenimiento *Daños por desgaste o defectos de fabrica. *• Daños del servidor por falta de equipos que regulen variaciones de voltajes e idas de energía eléctrica.	[I5] Avería de origen físico o lógico	6.Tecnología	2	2	ACEPTABLE (MUY BAJO)
Servidor de archivos FTP: Servidor marca dell en torre PowerEdge T130	[HW] EQUIPAMENTO INFORMÁTICO	Institucional	*Carencia de configuraciones de seguridad del servidor. *La configuracion y la administracion de los servidores no se encuentra centralizada. *El antivirus instalado en el servidor no se encuentra activado ni actualizado.	[E2] Errores del administrador	6.Tecnología	3	2	TOLERABLE (BAJO)
Página web	[S] SERVICIOS	Institucional	* Errores en la gestion de recursos y configuraciones. * Fallos en la depuracion de alguna aplicación o en la misma programacion del sitio web. * Ejecucion de codigo malintencionados. * Factor Humano	[I8] Fallo de servicios de comunicaciones	6.Tecnología	2	2	ACEPTABLE (MUY BAJO)

Dado lo anterior, para esta sesión, sobre el impacto y probabilidad de riesgo, la valoración del riesgo de cada uno de los activos de información y del ciberespacio se encuentran reflejados y contenidos en el archivo de Excel que se encuentra publicado en **google drive** atraves del siguiente link:

https://drive.google.com/file/d/16sM4s1E3NSD7Ura6h3pbmpeRXeKdx7Xz/view?usp=sharing

B.2 MATRIZ DE INVENTARIO: PROBABILIDAD, IMPACTO Y VALORACION DEL RIESGO DE LOS ACTIVOS DE INFORMACION.

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

PROBABILIDAD DEL RIESGO

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

IMPACTO DEL RIESGO

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

VALORACIÓN DEL RIESGO

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

VALORACIÓN DEL RIESGO

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

ANEXO C

PLAN DE TRATAMIENTO DE RIESGOS, DE ACUERDO A LA IDENTIFICACIÓN, VALORACIÓN Y CLASIFICACIÓN DE LOS RIESGOS DEL CIBERESPACIO SEGÚN LAS ESTRATEGIAS DESCRITAS DENTRO DEL DEPARTAMENTO DE SISTEMAS DEL CASO DE ESTUDIO DE LA EMPRESA QWERTY S.A.

Con la implementación del plan de tratamiento de riesgos de los activos del ciberespacio, se realiza con el fin de efectuar y aplicar estrategias de aceptación y monitorización de los riesgos y así evitar las vulnerabilidades y amenazas que puedan afectar nuestro sistema de información.

C.1 IMPACTO Y PROBABILIADAD DE RIESGO.

IDENTIFICACIÓN DEL RIESGO					ANÁLISIS Y EVALUACIÓN DEL RIESGO			ESTRATEGIAS PARA EL PLAN DE TRATAMIENTO DE RIESGOS.	
Nombre del activo de Informacion	Activo de informacion	Riesgo			Probabilidad de materialización	Impacto	Valoracion del riesgo de los activos	Estrategia del riesgo	Criterios del tratamiento del riesgo de acuerdo al controles a aplicar a partir de la norma ISO 27001
		Tipo Riesgo	Vulnerabilidades	Amenaza					
Servidor de Impresión: Servidor marca dell en torre PowerEdge T440	[HW] EQUIPAMENTO INFORMÁTICO	Institucional	*falta de mantenimiento *Daños por desgaste o defectos de fabrica	[I5] Avería de origen físico o lógico	2	2	ACEPTABLE (MUY BAJO)	Aceptar	**A11.2.4 Mantenimiento de los equipos**: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
Servidor de archivos FTP: Servidor marca dell en torre PowerEdge T130	[HW] EQUIPAMENTO INFORMÁTICO	Institucional	*Carencia de configuraciones de seguridad del servidor. *La configuracion y la administracion de los servidores no se encuentra centralizada. *El antivirus instalado en el servidor no se encuentra activado ni actualizado.	[E2] Errores del administrador	3	2	TOLERABLE (BAJO)	Aceptar	**A5.1.1 Politicas para la seguridad de la informacion:** Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
Página web	[S] SERVICIOS	Institucional	* Errores en la gestion de recursos y configuraciones. * Fallos en la depuracion de alguna aplicación o en la misma programacion del sitio web. * Ejecucion de codigo malintencionados. * Factor Humano	[I8] Fallo de servicios de comunicaciones	2	2	ACEPTABLE (MUY BAJO)	Aceptar	**A13.1.2 seguridad de los servicios de red**: 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.

Dado lo anterior, para esta sesión, sobre el plan de tratamientos de riesgos para cada uno de los activos de información que se encuentran en el ciberespacio, los descritos detalladamente en el archivo de Excel que se encuentra publicado en **google drive** atraves del siguiente link:

https://drive.google.com/file/d/11W9vMLZ5WGx8O3lQQcC_ReUcZgrOu1hp/view?usp=sharing

C.2 MATRIZ DE INVENTARIO: PROBABILIDAD, IMPACTO Y VALORACION DEL RIESGO DE LOS ACTIVOS DE INFORMACION.

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

PROBABILIDAD DEL RIESGO

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

IMPACTO DEL RIESGO

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

VALORACIÓN DEL RIESGO

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

VALORACIÓN DEL RIESGO

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

ANEXO D

RESUMEN ANALÍTICA ESPECIALIZADO -RAE

Fecha de Realización:	13/05/2020
Programa:	Especialización en seguridad Informática
Línea de Investigación:	Infraestructura tecnológica y seguridad en redes.
Título:	Diseño de un plan de gestión de riesgos y vulnerabilidades del caso de estudio de la empresa QWERTY S.A., basados en los estándar NTC-ISO/IEC 27001 y NTC-ISO/IEC 27032.
Autor(es):	SAAVEDRA AGUDELO, Jorge Emilio.
Palabras Claves:	Ciberseguridad, Sistema de gestión de seguridad de la información (SGSI), análisis de riesgos, gestión de riesgos, Activos de información
Descripción:	En el trabajo de grado, se diseñó de un plan de gestión de riesgos y vulnerabilidades del caso de estudio de la empresa QWERTY S.A., basados en los estándar NTC-ISO/IEC 27001 y NTC-ISO/IEC 27032.el cual permitió tener una base para mejorar la seguridad de las tecnologías de información y las comunicaciones (TICs). En el desarrollo de este proyecto, se pudo identificar el estado actual del departamento de sistemas de la empresa QWERTY S.A., en cuanto al tema de la seguridad de la información de cada uno de los activos tanto físicos, virtuales y del

	ciberespacio, en donde se realizó un análisis de riesgos el cual permitió identificar los puntos fuertes y débiles de las áreas del departamento de sistemas, como así mismo la elaboración del análisis de gestión de riesgos atraves de la metodología Margerit, con el fin de mitigar los riesgos, dando así la aplicación de la buenas prácticas de la seguridad y finalmente la una propuesta de políticas de seguridad de la información para cada uno de los activos de entidad de estudio, basados en las normas NTC-ISO/IEC 27001 y NTC-ISO/IEC 27032 y así Proporcionándole a la empresa del caso de estudio una idea del efecto de las vulnerabilidades, amenazas y riesgos que allí pueden existir.

Fuentes bibliográficas destacadas:

- Aguirre Tovar, R., & Zambrano Ordoñez, A. (2015). STUDIO PARA LA IMPLEMENTACION DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA LA SECRETARIA DE EDUCACION DEPARTAMENTAL DE NARIÑO BASADO EN LA NORMA ISO/IEC 27001. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3655/1/13039116.pdf
- Alejaldre García, V. (2017). Implantación de un SGSI en una administración local. [online] Openaccess.uoc.edu. Recuperado de: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/59427/7/valejaldregTFM0117memòria.pdf
- Alemán Novoa, H., & Rodríguez Barrera, C. (2015). Metodologías para el análisis de riesgos en los sgsi. Recuperado de: http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435
- Ardila García, A., & Cardona Tovar, l. (2016). DESARROLLO DE UN MARCO DE TRABAJO PARA LA GESTIÓN DEL SGSI EN PYMES DESARROLLADORAS DE SOFTWARE EN BOGOTÁ BASADO EN LA METODOLOGÍA MGSM -PYME. Recuperado de: http://repository.udistrital.edu.co/bitstream/11349/2807/1/CardonaTovarLorenaPatricia2016.pdf

- Álvarez Ledesma, A., Torres Ruiz, G., & Ochoa Arbeláez, R. (2018). Partes interesadas [Ebook] (2nd ed., pp. 1-6). Bogotá D.C. Recuperado de: https://copnia.gov.co/sites/default/files/uploads/mapa-procesos/archivos/direccionamiento-estrategico/partes_interesadas.pdf
- APLICACION DE LA METODOLOGÍA MAGERIT PARA EL ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE CONTROL EN LA ESTACIÓN TENAY DEL OLEODUCTO. (2019). [Ebook] (1st ed., pp. 10-14). Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/27758/1/1075211684.pdf.
- BASTIDAS PARUMA, H., LÓPEZ ORTIZ, I., & PEÑA HIDALGO, H. (2014). ANÁLISIS DE RIESGOS Y RECOMEDACIONES DE SEGURIDAD DE LA INFORMACIÓN AL AREA DE INFORMACIÓN Y TECNOLOGÍA DEL HOSPITAL SUSANA LÓPEZ DE VALENCIA DE LA CIUDAD DE POPAYÁN. Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/2668/5/76323713.pdf
- Benavides Sepúlveda, A., & Blandón Jaramillo, C. (2018). Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico. Recuperado de: http://eds.a.ebscohost.com.bibliotecavirtual.unad.edu.co/eds/pdfviewer/pdfviewer?vid=1&sid=0d8ee77b-ce77-4578-bcff-7e41aa16469d@sdc-v-sessmgr05
- Bocanegra Quintero, Y. (2015). ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDIA MUNICIPAL DE TULUÁ APLICANDO LA METODOLOGÍA MAGERIT. Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3632/1/66728456.pdf
- Botero Vega, D. (2016). DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN (SGSI) PARA LA EMPRESA BELISARIO LTDA. DE LA CIUDAD DE BOGOTÁ D.C. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/12925/1/80259558.pdf
- Camargo Ramírez, J. (2017). DISEÑO DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) EN EL ÁREA TECNOLOGICA DE LA COMISIÓN NACIONAL DEL SERVICIO CIVIL - CNSC BASADO EN LA NORMA ISO27000 E ISO27001 [Ebook] (1st ed., pp. 9-12). Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/11992/1/75104100.pdf.

- Canal En VIVO - Universidad EAFIT. (2018). Administración de Riesgos Cibernéticos: Nuevos desafíos relacionados con la dependencia tecnológica [Video]. Recuperado de: https://www.youtube.com/watch?v=bb8gzgkJutk
- Castro Quinde, C. (2014). Elaboración de un Sistema de Gestión de Seguridad de la Información (Sgsi) para la Empresa Radical Cia. Ltda. En la Ciudad de Quito para el año 2014. Recuperado de: http://dspace.udla.edu.ec/handle/33000/3376
- Cárdenas Solano, L., Martínez Ardila, h., & Becerra Ardila, L. (2016). GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: REVISIÓN BIBLIOGRÁFICA. Recuperado de: http://eds.b.ebscohost.com.bibliotecavirtual.unad.edu.co/eds/pdfviewer/pdfviewer?vid=2&sid=76e5dfd6-7afe-4a67-8e7c-3e0779fe2163@pdc-v-sessmgr02
- Catalunya, Universidad Oberta de. Política de seguridad criptográfica de la Universitat Oberta de Catalunya.» 2016. https://seu-electronica.uoc.edu/portal/_resources/ES/documents/seu-electronica/Politica_Seguretat_Criptogrxfica_UOC-cat_ES.pdf.
- Certificacion360. (2018). ISO/IEC 27032 Ciberseguridad [Video]. Recuperado de: https://www.youtube.com/watch?v=4Qoqcz9ojrw
- © Ministerio de Hacienda y Administraciones Públicas. (2012). MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [Ebook] (3rd ed., pp. 19-23). España. Recuperado de: https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html
- Cortés Borrero, R. (2015). Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia. Recuperado de: http://eds.b.ebscohost.com.bibliotecavirtual.unad.edu.co/eds/pdfviewer/pdfviewer?vid=2&sid=fcc64185-ea4b-46d6-8aa9-de9b98d7f107@pdc-v-sessmgr03
- Buesaquillo Osorio, M., López Herrera, D., & García Henao, A. (2017). DISEÑO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA UNA AGENCIA DE VIAJES Y TURISMO. Recuperado de: http://repository.poligran.edu.co/bitstream/handle/10823/999/EntregaFinal.pdf?sequence=1&isAllowed=y

- Córdoba Suarez, A. (2015). DISEÑO E IMPLEMENTACIÓN DE UN SGSI PARA EL ÁREA DE INFORMÁTICA DE LA CURADURÍA URBANA SEGUNDA DE PASTO BAJO LA NORMA ISO/IEC 27001. Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3627/1/59650050.pdf
- Díaz, A., Collazos, G., Cortez Lozano, H., Ortiz, L., & Herazo Pérez, G. IMPLEMENTACION DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LA COMUNIDAD NUESTRA SEÑORA DE GRACIA, ALINEADO TECNOLÓGICAMENTE CON LA NORMA ISO 27001. Recuperado: http://www.konradlorenz.edu.co/images/stories/articulos/SGSI.pdf
- DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI BASADO EN LA NORMA ISO27001 PARA EL COLEGIO PROCOLOMBIANO DE LA CIUDAD DE BOGOTÁ, QUE INCLUYE: ASESORIA, PLANEACIÓN. (2016). [Ebook] (1st ed., pp. 32-33). Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/11950/1/17348959.pdf.
- DNA), A. (2019). Soluciones de seguridad para redes empresariales y Cisco DNA. Disponible: https://www.cisco.com/c/es_co/solutions/enterprise-networks/enterprise-network-security/index.html?CCID=cc000009&DTID=pseggl000015&POSITION=SEM&COUNTRY_SITE=co&CAMPAIGN=sc-00&CREATIVE=CO_SEM_SEC_Security-SPA_PM_NB-Cibersegur&REFERRING_SITE=Google&KEYWORD=ciberseguridad&ds_rl=1261909&gclid=EAIaIQobChMIv4-y96Ki4QIVgh6GCh2d8AeaEAMYASAAEgLyW_D_BwE#~stickynav=3
- Documental sobre seguridad informática. (2017). Recuperado de: https://www.youtube.com/watch?v=Dp_iBcfFftM
- Fajardo Diaz, C. (2017). ANÁLISIS DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DE UN APLICATIVO DE GESTIÓN DOCUMENTAL LIDER EN EL MERCADO COLOMBIANO. [Ebook] (p. 15). Recuperado 5 marzo 2020, de: https://fliphtml5.com/zexxp/wfas/basic.
- Garrido Camargo, C. (2018). Elaboración de plan de implementación de la ISO/IEC 27001:2013 [Ebook] (1st ed., pp. 7-12). Universitat Oberta de Catalunya (UOC). Recuper http://openaccess.uoc.edu/webapps/o2/bitstream/10609/88265/10/cgarridocaTFM0119memoria.pdf

- Guía de gestión de riesgos- seguridad de la información. (2016). [Ebook] (7th ed.). Bogotá D.C. Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf
- Global Standards. (2017). ISO 27001 - Seguridad de la Información [Video]. Disponible en: https://www.youtube.com/watch?v=WJm1qHHuMr0
- Gómez Morales, G. (2017). G55CIO Edición N° 14 (Ciberseguridad según el ISO/IEC 27032:2012). Recuperado de: https://issuu.com/g55cio/docs/g55cio_issuu_edicion_14_9mayo
- Gómez Vieites, A. Anexo III Análisis y Gestión de Riesgos en un Sistema Informático. Recuperado el 25 de agosto 2019, de: https://www.academia.edu/5971566/Anexo_III_An%C3%A1lisis_y_Gesti%C3%B3n_de_Riesgos_en_un_Sistema_Inform%C3%A1tico
- Guerreo Julio, M., & Gómez Flórez, L. (2012). Gestión de riesgos y controles en sistemas de información: del aprendizaje a la transformación organizacional. Disponible en: https://www-sciencedirect-com.bibliotecavirtual.unad.edu.co/science/article/pii/S0123592312700116?via=ihub
- Guanoluisa Huertas, J., & Maldonado Soliz, I. (2015). Análisis de Riesgos de un plan de seguridad de la información para el concejo nacional de igualdad de discapacidades "CONADIS" [Ebook] (pp. 51-52). Quito, Ecuador. Recuperado de: https://bibdigital.epn.edu.ec/bitstream/15000/10499/1/CD-6217.pdf
- Guzmán Silva, C. (2015). DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA UNA ENTIDAD FINANCIERA DE SEGUNDO PISO. Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3655/1/13039116.pdf
- GUZMÁN SOLANO, S. (2019). GUÍA PARA LA IMPLEMENTACION DE LA NORMA ISO 27032. [Ebook] (1st ed., pp. 7-17). Universidad católica de Colombia. Retrieved 27 April 2020, from https://repository.ucatolica.edu.co/bitstream/10983/23385/1/Proyecto%20Guia%20ISO%2027032.pdf.
- EOI Escuela de Organización Industrial. (2016). Administración y gestión de la seguridad en los sistemas [Video]. Recuperado de: https://www.youtube.com/watch?v=D2rFxvxcSEA

- Escuela Tecnológica Instituto Técnico Central. (2017). MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ETITC [Ebook] (2nd ed., pp. 55-95). Bogotá. Recuperado de: http://www.itc.edu.co/archives/manualpiliticassi.pdf
- Flórez Estévez, F., Jiménez Núñez, D., & Hidalgo Lascano, P. (2012). DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA MEGADATOS S.A. EN LA CIUDAD DE QUITO, APLICANDO LAS NORMAS ISO 27001 E ISO 27002. Disponible en: http://bibdigital.epn.edu.ec/bitstream/15000/4885/1/Diseño de un sistema.PDF
- GARCÍA RAMÍREZ, G., & CASTRO ANGARITA, J. (2017). DISEÑAR UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) A LA EMPRESA UNITRANSA S.A. UBICADA EN LA CIUDAD DE BUCARAMANGA. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/11914/4/5685072.pdf
- Hathaway, M. (2018). Gestión del riesgo cibernético nacional. Recuperado de: https://www.oas.org/es/sms/cicte/ESPcyberrisk.pdf
- Instituto Nacional de normalización (INN). NCh iso-27032:2015. 1st ed., Santiago de chile. (2015). pp. 3-8.
- Implantación de un SGSI en la empresa. Recuperado de: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf
- Iso27000.es. (n.d.). Sistema de Gestión de la Seguridad de la Información. [online] disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf
- ISO/IEC 27032:2012. (2012). Recuperado de: https://webstore.iec.ch/preview/info_isoiec27032{ed1.0} en.pdf
- Luna Lasso, J. (2016). Respondiendo a la amenaza: hacia el fortalecimiento de las políticas de ciberseguridad en Colombia atraves de la comunidad internacional. Recuperado de: https://repository.javeriana.edu.co/bitstream/handle/10554/35658/Juan Francisco Luna Lasso.pdf?sequence=1&isAllowed=y
- Lizarazo Lozano, K. (2016). PLANTEAMIENTO DE UN SGSI BASADO EN LA NORMA ISO 27001:2013 PARA LA EMPRESA DE SERVICIOS DE TECNOLOGÍA SITECH DE COLOMBIA SAS EN LOS PROCESOS GESTIÓN

FINANCIERA, GESTIÓN DE LOGÍSTICA Y GESTIÓN DE IT [E-book] (1st ed.). Bogotá D.C: Polux.unipiloto.edu.co. Recuperado de: http://polux.unipiloto.edu.co:8080/00003412.pdf

- López, A. (2020). Serie 27k. Iso27000.es. Recuperado de: http://www.iso27000.es/iso27000.html.
- Manjarrez, c., mogollón, e., cortes, i., & Dussan, l. (2016). identificación de riesgos en el tratamiento de datos personales a nivel de usuarios clientes de aplicaciones móviles en el sector del transporte público individual en Bogotá. recuperado el 25 agosto 2019, de: https://repository.ucatolica.edu.co/bitstream/10983/7831/4/identificacion%20de%20riesgos%20en%20el%20uso%20de%20apps%20de%20transporte%20publico.pdf
- MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO. (2016). [Ebook] (5th ed., pp. 12-20). Bucaramanga. Recuperado de: https://www.uis.edu.co/webUIS/es/administracion/controlGestion/documentos/2015/MSE.01manualAdministracionRiesgo.pdf
- Mapa de Riesgos - Gestión Tic 2016 - RISEM2016. (2016). Recuperado de: http://webcache.googleusercontent.com/search?q=cache:oy8NNkG9zoAJ:www.fusagasuga-cundinamarca.gov.co/Transparencia/MODELO%2520INTEGRADO%2520DE%2520PLANEACION%2520Y%2520GESTION/Mapa%2520de%2520Riesgos%2520-%2520Gesti%25C3%25B3n%2520Tic%25202016%2520-%2520RISEM2016.xls+&cd=6&hl=es-419&ct=clnk&gl=co
- Maya Arango, P. (2016). Plan de implementación del SGSI basado en la norma ISO 27001:2013. Eds.a.ebscohost.com.bibliotecavirtual.unad.edu.co. Recuperado de: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/53466/8/pmayaaTFM0616memoria.pdf.
- Mejía Quijano, R. MEDIDAS DE TRATAMIENTO DEL RIESGO [Ebook] (pp. 1-2). Recuperado de: http://www.eafit.edu.co/escuelas/administracion/consultorio-contable/Documents/Nota%20de%20Clase%2010%20Medidas%20de%20Tratamiento%20del%20Riesgo.pdf
- Mercado, Y. (2020). Tercera web conferencia del curso de Aspectos Éticos Y legales de la seguridad informática. Lecture, Adobe Connect recuperado de: http://conferencia2.unad.edu.co/pgepdmgxi3u0/?proto=true

- Metodología para la gestión de la seguridad informática (Proyecto). Recuperado de: https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf
- Modelo Nacional de gestión de riesgos de seguridad digital. Disponible en: https://mintic.gov.co/portal/604/articles-61854_documento.docx
- Molina Cañamero, B. (2018). Desarrollo de un Plan Director de Seguridad para la implementación de un SGSI basado en la norma ISO/IEC 27001. [online] Openaccess.uoc.edu. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/88386/6/bmolinacaTFM1218memoria.
- Moncayo Racines, D. (2014). https://bibdigital.epn.edu.ec/bitstream/15000/8499/3/CD-5741.pdf [Ebook]. Quito, Ecuador. Recuperado de: https://bibdigital.epn.edu.ec/bitstream/15000/8499/3/CD-5741.pdf
- Moyano Orjuela, L., & Suárez Cárdenas, Y. (2017). Botero Vega, D. (2016). DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN (SGSI) PARA LA EMPRESA BELISARIO LTDA. DE LA CIUDAD DE BOGOTÁ D.C. Recuperado de: http://repository.udistrital.edu.co/bitstream/11349/6737/1/MoyanoOrjuelaLuzAdriana2017.pdf
- Muñoz Martin, M. (2015). Guía de implantación de un SGSI basado en la norma UNE-ISO/IEC 27001. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/42965/7/mmanozTFC0615memoria.pdf
- NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001. (2006). Recuperado de: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma. NTC-ISO-IEC 27001.pdf
- Optiv Security anuncia el nuevo Risk Transformation Service™, que ayudará a las empresas a mitigar el riesgo empresarial. (2019). Disponible en: https://www.businesswire.com/news/home/20190308005157/es/
- Perafán Ruiz, J., & Caicedo cuchimba, M. (2014). Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/2655/3/76327474.pdf
- Plan Estratégico de Seguridad de la Información PESI. (2017). Disponible en: https://www.ica.gov.co/transparencia-y-acceso-a-la-informacion/2018/plan-estrategico-de-seguridad-de-la-informacion_ic.aspxPlan Estratégico de Seguridad de la Información PESI. (2017). Recuperado de:

https://www.ica.gov.co/transparencia-y-acceso-a-la-informacion/2018/plan-estrategico-de-seguridad-de-la-informacion_ic.aspx

- Plan de Implementación del SGSI basado en la norma ISO 27001:2013 para la empresa Interfaces y soluciones. (2017). [Ebook] (1st ed., pp. 52-53). Bogotá, D.C. Recuperado de: http://repository.udistrital.edu.co/bitstream/11349/6737/1/MoyanoOrjuelaLuzAdriana2017.pdf
- Política general de seguridad de la información y objetivos del SGSI y MSPI. (2017). Recuperado de: http://www.itc.edu.co/archives/politicaobjetgsimspi.pdf
- Ramos, a. (2016). RIESGOS INFORMÁTICOS. Disponible en: https://www.youtube.com/watch?v=vZ5Dr1nSSRY
- Revisión del marco regulatorio para la gestión de riesgos de seguridad digital. (2017). Disponible en: https://www.crcom.gov.co/recursos_user/2017/actividades_regulatorias/ciberseguridad/Documento_CRC_Seguridad_Digital_Vpublicar.pdf
- Riesgos de ciberseguridad y su impacto en negocio. Recuperado de: https://static.unir.net/ingenieria/ciberseguridad-y-estrategia-corporativa-para-la-alta-direccion/Curso_Ciberseguridad-CEA_es.pdf
- Riveros Cárdenas, F. (2016). ADMINISTRACION DEL RIESGO CIBERNETICO UN ENFOQUE DESDE LA ALTA GERENCIA EMPRESARIAL EN COLOMBIA. Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/15837/RiverosCardenasFredyOrlando2017.pdf;jsessionid=080C9D80D77334EE32CA96476069E485?sequence=1
- Rodríguez Conde, L. (2017). Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013. [online] Openaccess.uoc.edu. disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/64545/1/liziyoTFM0617-Resumen%20Ejecutivo-Memoria.pdf
- Ruiz Peña, J. (2018). DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION (SGSI) BAJO LA NORMA ISO/IEC 27001:2013, EN LA COOPERATIVA MULTIACTIVA DEL PERSONAL DEL SENA, EN

BOGOTA [Ebook] (pp. 135-137). Bogotá, D.C. Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17300/1/80267708.pdf

- SANCHEZ PACHECO, E., & REBOLLEDO HINOJOSA, F. (2017). DISEÑO DE UN MODELO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE TALENTO HUMANO DE LA SECRETARÍA DE EDUCACIÓN. Recuperado de: http://repository.poligran.edu.co/bitstream/handle/10823/1039/DISE%C3%91O%20DE%20UN%20MODELO%20DE%20GESTI%C3%93N%20DE%20LA%20SEGURIDAD%20DE%20LA%20INFORMACI%C3%93N%20EN%20EL%20%C3%81....pdf?sequence=1&isAllowed=y
- SGSI - 05 Implantación de un SGSI. (2010). Recuperado de: https://www.youtube.com/watch?v=i_3z68QGaJs
- SGSI - 07 Los activos de Seguridad de la Información. (2010). Recuperado de: https://www.youtube.com/watch?v=THnQ2FH7NtU
- Suarez González, R. (2018). ANALISIS DE ACTIVOS DE INFORMACION PARA UN SISTEMA MISIONAL BASADOS EN LA METODOLOGÍA MAGERIT V3 Y LA NORMA ISO 27001:2013. [Ebook] (pp. 48-52). Bogotá. Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/19571/3/80803746.pdf
- Suarez, O. (2014). SGSI Sistema de Gestión de Seguridad de la Información [Video]. Disponible en: https://www.youtube.com/watch?v=wIe01QIFA8Q
- UNAD (2018). MANUAL DEL SISTEMA DE INTEGRADO DE GESTIÓN [Ebook] (11th ed., p. 7). Bogotá D.C. Recuperado de: https://sig.unad.edu.co/documentos/sgc/manuales/M-1.pdf?v10
- Valencia Duque, F. and Orozco Álzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. [online] RISTI - Revista Ibérica de Sistemas e Tecnologías de Información. Disponible en: http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1646-98952017000200006&lng=en&tlng=en
- Vanegas Ramírez, w., Quiroga Rodríguez, S., León Beltrán, D., & Rodríguez Camargo, J. (2018). PLAN DE GESTION DEL RIESGO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Disponible en:

<table>
<tr><td colspan="2">http://www.sopo-cundinamarca.gov.co/Transparencia/PlaneacionGestionyControl/PLAN DE GESTION DEL RIESGO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.pdf
• Velásquez Restrepo, P., Velásquez Restrepo, S., Velásquez Lopera, M., & Villa Galeano, J. (2017). Implementación de la gestión de riesgo en los procesos misionales de la Sección de Dermatología de la Universidad de Antioquia (Medellín, Colombia) siguiendo las directrices de la norma ISO 9001:2015 [Ebook] (pp. 88-89). Bogotá, Colombia. Recuperado de: http://www.scielo.org.co/pdf/rgps/v16n33/1657-7027-rgps-16-33-00078.pdf
• Yáñez Cáceres, N. (2017). SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA SUBSECRETARIA DE ECONOMÍA Y EMPRESAS DE MENOR TAMAÑO. Recuperado de: http://repositorio.uchile.cl/bitstream/handle/2250/147976/Sistema-de-gestion-de-seguridad-de-la-informacion-para-la-Subsecretaria-de-Economia-y-Empresas.pdf?sequence=1&isAllowed=y</td></tr>
<tr><td>Contenido del documento:</td><td>El desarrollo de este trabajo consta de:

Planteamiento de problema

¿Cómo proteger de manera eficaz y eficiente los activos de información de la empresa QWERTY S.A., a partir de la implementación el estándar NTC-ISO/IEC 27001 y NTC-ISO/IEC 27032?

Objetivo general

Diseñar un plan de gestión de riesgos y vulnerabilidades para el caso de estudio de la empresa QWERTY S.A., basados en los estándar NTC-ISO/IEC 27001 y NTC-ISO/IEC 27032.</td></tr>
</table>

	Objetivos Específicos • Diseñar un modelo de seguridad y privacidad de la información para la empresa QWERTY S.A, basado en la norma NTC-ISO/IEC 27001. • Identificar estrategias de protección para los activos de información de la empresa QWERTY S.A., con base en los principios de confidencialidad, integridad, disponibilidad y no repudio de la información. • Establecer un modelo de gestión de ciberseguridad de la empresa QWERTY S.A., haciendo uso de los metodologías y estándares basados NTC-ISO/IEC 27032 para la buena gestión de la información. • Proponer metodologías para la gestión de seguridad de la información, en la cual se gestione los riesgos y vulnerabilidades a la cuales están expuestas la empresa del caso de estudio propuesto desde el punto de vista cibernético. **Marco Referencial:** El cual se divide en: marco teórico, marco conceptual, antecedentes, marco legal y marco contextual. **Diseño Metodológico:** Es la fase donde se encuentra la explicación del desarrollo e implementación de la solución del caso de estudio sobre la empresa QWERTY S.A según las normas, metodologías y estándares de calidad que rigen y protegen los activos de informaciones de las organizaciones. **Desarrollo del proyecto:** En esta fase se mostrará el desarrollo del proyecto según los objetivos planteados, se divide en: Propuesta del SGSI basada en la NTC-ISO/IEC 27001:2013., metodología para el análisis y gestión de la seguridad de la información de la empresa QWERTY S.A, basada en MARGERIT y finalmente el

	modelo de gestión de la ciberseguridad de la empresa QWERTY S.A, basada en la NTC-ISO/IEC 27032. **Resultados:** En esta fase se mostrará los resultados obtenidos con desarrollo del proyecto. **Divulgación:** Manera en que se realizara la divulgación del proyecto de grado. **Conclusiones.** **Recomendaciones.** **Referencia Bibliográficas y Anexos.**
Marco Metodológico:	El desarrollo de este proyecto se llevó a cabo en 4 etapas según los objetivos planteados: **Etapa 1.** Diseño del modelo de seguridad y privacidad de la información. **Etapa 2.** Identificación de las estrategias de protección de los activos de información, basados en los principios de confidencialidad, integridad, disponibilidad, y no repudio de la información. **Etapa 3.** Establecimiento del modelo de gestión de la ciberseguridad, basados en la norma NTC/ISO /IEC 27032.

	Etapa 4. Propuesta de la metodología para la gestión de la seguridad de la información, para el análisis y gestión de los riesgos basado en MARGERIT.
Conceptos adquiridos:	**Amenaza:** cualquier evento accidental o intencionado que pueda ocasionar algún daño en el sistema informático, provocando pérdidas materiales, financieras o de otro tipo en la organización. **Análisis de riesgos**. Empleo sistemático o metódico de los datos para determinar las fuentes y evaluar los riesgos. **Activo de información.** Conocimiento o información que posee o tiene valor para un individuo u organización. **Ciberespacio**: entorno complejo que resulta de la interacción de personas, softwares y servicios en Internet por medio de dispositivos y redes de tecnología conectados a éste, los que no existen en forma física **Ciberseguridad:** Acción de proteger en contra de consecuencias, físicas, sociales financieras, ocupacionales, educacionales o de otro tipo que resultan del daño, error, accidente, perjuicio o cualquier otro evento que se pueda considerar no deseable en el ciberespacio. **MAGERIT**: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

	SGSI. Sistema de gestión de la seguridad de la información, que cita a un conjunto de políticas de seguridad en cuanto a la administración de la información.
Conclusiones:	• Con la implementación del SGSI en el caso de estudio de la empresa QWERTY S.A., de acuerdo al estándar de calidad ISO 27001:2013, se concluye que cualquier tipo de entidad, pymes u organización que implemente estas normas, proporcionara seguridad en cada uno de los activos de la información y prolongara la existencia y valoración de los mismos. • Mediante el análisis de las amenazas, riesgos, vulnerabilidades y la aplicación de procedimientos o controles se puede garantizar una mayor vida útil a los activos de información tanto físicos como del ciberespacio y todo esto a partir de las estrategias de protección tanto físicos como virtuales basándonos en los principios de confidencialidad, integridad, disponibilidad y no repudio de la información. • Al momento de evaluar el nivel de riesgo en una empresa u organización, se debe determinar como primera medida la metodología a implementar, para así proceder a definir el alcance del departamento o área que va a analizar y finalmente diagnosticar el estado actual de la seguridad informática de cada uno de los activos de información de la empresa QWERY S.A. • Para un buen análisis de riesgos se debe tener en cuenta la evaluación y cálculo de riesgos sobre cada uno de los activos de información y finalmente se debe

	aplicar medidas o controles para materializar la protección sobre cada uno de los activos de información de una entidad u organización. • Es importante identificar los activos de informacion, como asi mismo las amenazas, riesgos y vulnerabilidades que posean la organización, con el fin implementar y mejorar medidas de seguridad dentro de la entidad, teniendo en cuenta las políticas y controles funcionales, los cuales conllevan al cumplimiento de cada uno de los objetivos del SGSI dentro de la entidad.