DISEÑO DE UN MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN EL ESTÁNDAR ISO 27001:2013 PARA LA GESTIÓN DE LA INFORMACIÓN PARA EL CASO DE ESTUDIO EMPRESA QWERTY S.A

FLOR ESPERANZA BECERRA ARIAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD CEAD JOSE ACEVEDO Y GOMEZ
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIAS E INGENIERIAS ECBTI
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTÁ
2020

DISEÑO DE UN MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN EL ESTÁNDAR ISO 27001:2013 PARA LA GESTIÓN DE LA INFORMACIÓN PARA EL CASO DE ESTUDIO EMPRESA QWERTY S.A

FLOR ESPERANZA BECERRA ARIAS

Proyecto de grado aplicado para optar al título de Especialista en seguridad Informática

Director de trabajo de Grado

EDGAR MAURICIO LOPEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD CEAD JOSE ACEVEDO Y GOMEZ ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2020

Nota de aceptación:

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá, mayo 2019

AGRADECIMIENTOS

Mi agradecimiento

Al ing. Luis Fernando Zambrano por su valiosa asesoría durante el desarrollo de este proyecto.

A la Ing. Yenni Stella Núñez por su acompañamiento en este proceso de Aprendizaje.

Al Ing. Edgar Mauricio López por su interés en facilitar mi aprendizaje y valorar el esfuerzo realizado.

CONTENIDO

Lista de Tablas

Lista de Figuras

RESUMEN

A partir del escenario presentado para la empresa QWERTY SA. se realizará el diseño de un modelo de para gestionar de forma eficaz y sostenible la seguridad de su información, lo anterior basado en la norma ISO 27001:2013. El diseño incluye el análisis de riesgos, documentar el sistema de gestión (política, manual, procedimientos, plan de tratamiento de riesgos, documento de aplicabilidad), para lo cual se tendrá en cuenta las herramientas provistas por la metodología MARGERIT.

En cuanto a la metodología de investigación que se aplicará en el proceso para llevar a cabo el proyecto está determinado realizar el proceso bajo los siguientes lineamientos:
1. Observación de los hechos y definición del problema,
2. Investigación Documental y
3. Documentar el sistema de gestión seguridad de la información.

Palabras Clave

Seguridad de la información, sistema de gestión, Análisis de riesgo, vulnerabilidad, control.

ABSTRACT

From the scenario presented for the company QWERTY SA will design a model to efficiently and sustainably manage the security of your information, the above based on ISO 27001:2013. The design includes risk analysis, documenting the management system (policy, manual, procedures, risk treatment plan, applicability document), for which the tools provided by the MARGERIT methodology will be taken into account.

As for the methodology of research that will be applied in the process to carry out the project this is determined to carry out the process under the following guidelines: 1. Observation of the facts and definition of the problem, 2. Documentary Research and 3. Document the information security management system.

Keywords

Information security, management system, risk analysis, vulnerability, control.

INTRODUCCIÓN

El alcance de las tecnologías y la dependencia de esta permiten que se presenten distintas situaciones que obligan a realizar análisis, tanto de vulnerabilidades como de los impactos en caso de materializarse las condiciones que pueden afectar la confidencialidad, integridad y disponibilidad de la información.

Con este proyecto se pretende proponer el diseño de un modelo para gestionar la seguridad de la información basada en el estándar ISO 27001:2013 para el caso de estudio de la empresa QWERTY S.A.

Este proyecto tiene como finalidad principal analizar los activos de la información, el cual junto con el análisis de riesgos y su impacto puede ser utilizado para modelar un sistema de gestión de seguridad apropiado a las necesidades de la organización.

1. DEFINICIÓN DEL PROBLEMA

1.1. ANTECEDENTES

A través de la historia colombiana las comunicaciones evolucionaron y así mismo sucedió con los organismos del estado encargados de su regulación y por ello en su momento el ministerio de comunicaciones se transforma y convierte en el ministerio de las tecnologías de la información y las comunicaciones desde julio de 2009 mediante la ley 1341, esta ley además generó todo un marco normativo para el desarrollo del sector, la promoción y el uso de las TIC basado siempre en la protección de los derechos de los usuarios. (Comunicaciones, s.f.)

Si bien en Colombia y el mundo se viene utilizando los sistemas de información hace décadas solo hasta el año 2011 se constituyó un organismo la primera entidad del gobierno que se encargará de implementar mecanismos de atención de incidentes, alarmas tempranas y análisis de ciberseguridad que diera apoyo tanto a las entidades como al sector privado.

Una vez revisadas las estadísticas del DANE en su boletín técnico del tenencia y uso de tecnologías de la información y comunicación de las empresas del año 2018 se puede deducir estas herramientas han tomado importancia en todos sectores económicos evidenciado en que el 99.6% de las empresas encuestadas utilizan computadores, el 99.6% utilizan internet y el 73.3% cuenta con páginas web (estadísticas, 2019), con las cifras anteriores es claro que así como se cuenta con herramientas tecnológicas que facilitan las actividades de las organizaciones no se hace esperar la necesidad de administrar de forma adecuada asegurando la mitigación de riesgos basados en las premisas se garantizar la disponibilidad de la información a quienes están autorizado sin perder su confiabilidad e integridad.

Por lo anterior se optó en este trabajo de grado la revisión de uno de los casos de estudio propuesto por la universidad a través del que se realizará la presentación de una propuesta para un diseño viable para la implementación de un sistema de gestión de seguridad de la información.

1.1 PLANTEAMIENTO DEL PROBLEMA.

En la medida que la tecnología avanza también lo hacen las amenazas a la información que las organizaciones utilizan para tomar decisiones y comunicarlas; así mismo existen cada vez más herramientas para contrarrestar estas amenazas y evitar que se materialicen afectado el desempeño de las organizaciones.

A pesar de las numerosas medidas de seguridad que se tomen para proteger la

información no es posible estar 100% libres de ser atacados y que algunos de estos ataques tengan éxito. Ya que el objetivo de dichos ataques está orientado básicamente a obtener información, manipularla o modificarla para obtener beneficio o simplemente inutilizar el sistema.

El reto es crear las condiciones necesarias desarrollar confianza en el uso de medios electrónicos, a través de medidas que permitan garantizar la seguridad de los datos, las comunicaciones y los sistemas con los que se administran con controles eficientes, que no afecten la productividad de las organizaciones y que evolucionen con las necesidades de la organización.

Se requiere asegurar un proceso de implementación eficaz por lo que es necesario presentar el diseño del sistema de gestión con objetivos claros, dentro del contexto legal y con una metodología clara que permita identificar los riesgos, evaluar su impacto y definir los controles que se requieren para su mitigación.

1.2. FORMULACIÓN DEL PROBLEMA

¿Cuáles son los elementos fundamentales de un modelo de gestión de seguridad de la información para asegurar las condiciones de calidad de la información?

2. JUSTIFICACIÓN

Las organizaciones en general sin importar su tamaño recogen, procesan y transmiten información, enfrentando una serie de riesgos que pueden afectar sus condiciones, por lo que vienen adoptando una serie de medidas a través de controles que pueden perder su eficacia si no están definidos, implementados y evaluados dentro de un esquema de mejora continua, el cual se puede lograr mediante la implementación de un sistema de Gestión que permita asegurar las condiciones adecuadas para mantener la información segura, ya que este permite que permite que se implementen controles de forma ordenada, basada en prioridades por nivel de riesgo y direccionando tanto la inversión como los esfuerzos en función del aseguramiento de las condiciones para mantener su grado de confidencialidad, de que no se dude de su integridad y esté disponible a quien tenga los permisos para su uso.

La seguridad de la información se logra mediante la implementación de controles apropiados a las condiciones propias de cada organización, para poder establecer dichos controles es necesario entender la organización, los elementos que componen el sistema de información, las amenazas a la que está expuesto y los efectos que pueden desencadenarse de la materialización de los riesgos.

3. OBJETIVOS.

3.1 OBJETIVO GENERAL

Diseñar un modelo de gestión de la ciberseguridad para el caso de estudio empresa QWERTY SAS que permita asegurar las condiciones de calidad de la información mediante la aplicación de estándares y metodologías para la buena gestión de la información.

3.2. OBJETIVOS ESPECÍFICOS

- Identificar y clasificar las amenazas presentadas en los activos de información que afectan la calidad, integridad, disponibilidad y confiabilidad de la información para el caso de estudio de la empresa QWERTY

- Formular los controles a los activos de información para empresa QWERTY de acuerdo al anexo A de la norma ISO 27001:2013

- Establecer metodología de implementación del SGSI de la empresa QWERTY que asegure condiciones sostenibles de seguridad de la información y que a su vez promueva la evolución de las condiciones de seguridad de la información.

- Presentar documento con los recursos de tecnología, establecer medidas de seguridad apropiadas al menor costo con mecanismos apropiados de verificación de cumplimiento para mantener controles eficientes y apropiados sin afectar la productividad de la organización

4. MARCO REFERENCIAL

4.1 MARCO LEGAL

En los últimos 50 años se han generado diversas disposiciones de orden legal con relación a propiedad intelectual, regulación de telecomunicaciones y protección de la información, a continuación se relacionan algunas de ellas para ilustrar evolución en materia legal proporcionar el marco legal que hoy en día debe ser referente a la hora de entender derechos y deberes relacionados con las condiciones de seguridad de la información: “Desde el año 1968 se encuentran los primeros aportes del estado en generar un marco legal para el manejo de la información en el país con la ley 72 de 1968 con la incorporación a la legislación colombiana de los Pactos Internacionales de Derechos Económicos, Sociales y Culturales de la ONU y en el año 1975 con la adhesión a la convención universal de derechos de autor firmado en ginebra en 1952”[1]

Posteriormente en agosto de 1999 el congreso promulga la Ley 527 que regula el uso de Mensajes de Datos y Comercio Electrónico, e introduce claridad sobre el uso de firma digital

En el ámbito legal conceptos como: comercio electrónico, firma digital, sistema de información y se da reconocimiento jurídico a los mensajes de datos, establece las condiciones de valoración, conservación, presunción de originalidad y acuse de recibo entre otros.

El 5 de enero de 2009 el congreso promulga la ley 1273 modificando el código penal para introducir el concepto de protección de los datos, dando una amplia cobertura a la protección de la información tipificando escenarios que van desde acceso abusivo, obstaculización ilegitima de acceso a la información y redes, intercepción, daño informático, violación de datos personales, suplantación y circunstancias agravantes.

Es por esto que las organizaciones están obligadas a garantizar las condiciones de seguridad de la información de manera proactiva buscando siempre adelantarse a las condiciones que puedan afectar las condiciones de calidad de la información y más teniendo en cuenta que buena parte de la información de una compañía es

[1] REVISTA INFORMÁTICA JURÍDICA, Legislación informática de Colombia, Salamanca, 2016

proporcionada por sus interlocutores y que una vez la recibe es responsable de su custodia.[2]

Ley estatutaria 1581. DE 2012. Establece como derecho constitucional la protección de datos personales afianzando entre otros lo instituido en el artículo 15 y 20 de la actual constitución nacional.[3]

4.2 MARCO CONCEPTUAL

Antes de entrar en la revisión de conceptos metodológicos relacionados con el sistema de gestión vamos a exponer conceptos básicos necesarios para entender la necesidad de un sistema de gestión de seguridad de la información, los cuales fueron tomados de la norma ISO 27000:2016 (TÉCNICAS., 2017.).

Información: De manera simple puede definirse como un conjunto de datos que una vez interpretados toman sentido y son útiles para la toma de decisiones. Para la norma ISO 27000 la información se considera un Activo esencial que necesita ser protegida. Las tecnologías de la información surgen como respuesta a la necesidad de crear, procesar y almacenar, transmitir y protegerla.

Gestión: es el conjunto de acciones que permiten la realización de una actividad; estas acciones incluyen la capacidad de dirigir, supervisar controlar y mejorar de manera continua los recursos asignados para tal actividad.

Confidencialidad: Es la propiedad de la información que se asegura cuando en un sistema la información solo puede ser accedida por quien está autorizado.

Integridad: cualidad de un documento o archivo que no ha sido alterado y además permite demostrar que no se ha producido manipulación alguna sobre el mismo.

Disponibilidad: es asegurar que la información es accesible o está disponible en el momento que se requiere por usuarios o procesos autorizados.

---

[2]

[3] ALCALDIA MAYOR DE BOGOTA, ley 1581 de 2012, Régimen Legal de Bogotá, (octubre 17 de 2012) Colombia

Autenticación: es el mecanismo para verificar que un documento fue elaborado o pertenece a quien el documento indica.

No repudio: está asociado a la autenticación, el no repudio se produce frente a un tercero, donde el emisor no puede negar el envío y el receptor no puede negar que recibió el mensaje.

Elementos vulnerables de un sistema: En todo sistema de información se cuentan con tres elementos a proteger que son Hardware, software y datos. Los datos constituyen normalmente el principal elemento a proteger por ser el más amenazado y seguramente el más difícil de recuperar.

Amenazas: Se conoce como el peligro que surge de un hecho potencial, que al materializarse puede perjudicar a una persona, entidad u organización. En el campo de TI las amenazas pueden ser provocadas por Personas, fuentes lógicas, fuentes Físicas.

Riesgos: Es la probabilidad de que una amenaza ocurra, es decir que como producto de acciones intencionales o involuntarias se manifiesten efectos adversos o impactos sobre la información y por lo tanto sobre la operatividad del negocio.

Controles: se puede definir como la comprobación, inspección, fiscalización o intervención. También puede hacer referencia a la regulación sobre un sistema. El control debe ser Debe ser oportuno, debe estar ubicado estratégicamente de forma que se aplica sobre actividades específicas y críticas, Debe ser económico. Los controles pueden ser de técnicos (herramientas Software/hardware), de gestión (procedimiento, responsabilidades) o legales (Pólizas, cláusulas contractuales), es decir, están direccionados a la herramienta, El proceso y el cumplimiento de normas.

Gobierno de TI: Busca alinear estructuras, procesos, recurso y estrategias de las áreas de tecnología con la estrategia y objetivos trazados por el negocio para cumplir su misión o razón de ser mediante el establecimiento de relaciones y procesos que faciliten la comunicación entre los dos.

4.3 MARCO TEÓRICO

Cuando se habla de seguridad de la información es generar el ambiente propicio con medidas de control para “lograr la preservación de la confidencialidad, la

integridad, y la disponibilidad de los sistemas de información"[4].

Gestión de la seguridad: Corresponde a los planes, responsabilidades, prácticas, procedimientos y procesos realizados para dar cumplimiento a la política de seguridad y minimizar riesgos. Como proceso debe detectar incidentes, minimizar el impacto, recuperación rápida de los daños generados, revisión y actualización de las medidas de seguridad y minimizar incidentes de seguridad. Los estándares que pueden facilitar esta gestión son ITIL, ISO27001.

Características de la seguridad de la información: Define funciones o servicios de seguridad que debe proveer TI en términos de las características de la información, se debe realizar un análisis de la situación entendida como vulnerabilidades, servicios implementados, controles actuales; con esto se determina la gestión de riesgos a través de políticas de seguridad, gestión de cambios, procesos de comunicación de los distinto tipos de información, continuidad del negocio y seguridad del personal.

Buscar que los recursos para su implementación sean vistos como una inversión cuantificable mediante la revisión del retorno de inversión y no como un gasto.

Está orientada al entendimiento y compromiso del negocio (alta gerencia y directivos de la organización) y define la seguridad en términos de la gente, los procesos y las funciones del negocio. Mitiga riesgos organizacionales (ausencia de políticas, control de cambios, comportamiento de factor humano).

El riesgo tiene 4 posibles tratamientos: Evitar el riesgo eliminando la causa, Adoptar medidas para mitigar su efecto, compartir o transferir el riesgo, aceptar la existencia del riesgo y monitorearlo. "Los tipos de riesgo pueden ser: Ambientales, de mercado, financieros, operacionales, de cumplimiento, tecnológicos"[5]

Si bien existen diversas metodologías de análisis de riesgos que aplican a cualquier sistema que pueden ser aplicables en este diseño MAGERIT fue desarrollada específicamente para este análisis buscando dar uniformidad de los informes que recopilan los hallazgos y las conclusiones de las actividades de análisis y gestión

[4] TIPTON, 2006 Harold F. Tipton, Micki Krause (eds.), Information Security Management Handbook, 5th Ed., CRC Press, 2006

[5] GOMEZ FERNANDEZ, Luis, ANRES ALVAREZ, Ana, guía de aplicación de la norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes,España,AENOR,2012

de riesgos tales como: modelo de valor, mapa de riesgos, declaración de aplicabilidad, evaluación de salvaguardas (controles), estado de riesgo, informe de insuficiencias , cumplimento de normatividad y plan de seguridad[6]

Normas ISO 27000

Dentro de los estándares internacionales se cuenta con la ISO/IEC 27000:2016, correspondiente a la cuarta edición, en la que se basa a nivel nacional la NTC-ISO/IEC 27000:2016. “Este conjunto de normas tiene como objetivo ayudar a las organizaciones de todo tipo y tamaño a implementar y operar un Sistema de gestión orientada a garantizar la seguridad de la información.”[7]

Este conjunto de normas contiene una serie de componentes estructurales que permiten describir requisitos de un SGSI (ISO27001), requisitos para organismos de certificación(ISO 27006), y un marco de requisitos adicionales para sectores específicos; otras normas ofrecen orientación para aspectos de implementación tanto genéricos (ISO 27005)como condiciones para sectores específicos(ISO 27009).

Beneficios de las normas ISO27000

Entre los beneficios más significativos que menciona la norma NTC-ISO/IEC 27000 de la aplicación de esta familia de normas se destacan las siguientes:

1. Contar con un marco estructurado que soporte el proceso de especificar, implementar, operar y mantener la gestión de la seguridad de forma sostenible.
2. Promueve las buenas prácticas de seguridad de la información aceptadas a nivel mundial.
3. Aumenta la confianza en la organización por las partes interesadas
4. Alinea las prácticas de seguridad de la información a la gestión y gobierno del riesgo corporativo.

---

[6] **TECNICAS., INSTITUTO COLOMBIANO DE NORMAS.** *Tecnología de la información. Técnicas de seguridad de la información (SGSI). Visión general y vocabulario. Bogotá D.C.: ICONTEC, NTC-ISO/IEC 27000:2016.* 2017.

[7] **TECNICAS., INSTITUTO COLOMBIANO DE NORMAS.** *Tecnología de la información. Técnicas de seguridad de la información (SGSI). Visión general y vocabulario. Bogotá D.C.: ICONTEC, NTC-ISO/IEC 27000:2016.* 2017.

La norma ISO 27001 es una Metodología que al ser implementada facilita la administración de riesgos para asegurar que se mantengan las condiciones de calidad de la información en una organización. Se basa en la evaluación de riesgos e implementación de controles para mitigar los riesgos y a su vez asegurar que se mantienen vigentes en el tiempo mediante las auditorías o revisiones periódicas.

Su razón de ser primordial es proteger los activos de información, como consecuencia de ello se puede afirmar provee confianza en el manejo que la organización de la información proporciona un marco estructurado en la valoración de riesgos y los correspondientes controles, proporciona las condiciones para lograr un cumplimiento eficaz de las obligaciones Legales.

En la norma ISO 27005 se observa el ciclo de mejora donde se plasma la gestión del riesgo de forma cíclica,definiendo así la gestión de la seguridad de la información en términos de: planificar, implementar, monitorear, revisar y mejorar el sistema de gestión, define responsabilidades, exige la necesidad de objetivos medibles y exige la ejecución de auditorías internas. Los principios fundamentales de la norma son: Análisis de Riesgo, Compromiso de la alta gerencia, Definición de objetivos, estrategias, recursos y competencias.

Según la norma ISO27000, un sistema de Gestión de seguridad de la información consiste en un conjunto de políticas, procedimientos, directrices, recursos y actividades que son gestionados con el fin de proteger sus activos de información, La documentación requerida en un sistema de gestión (1) de seguridad de la información debe estar compuesta como mínimo de:

1. **Política de seguridad:** Contiene las líneas generales de actuación y el compromiso de la organización frente a velar por la confidencialidad, integridad y disponibilidad de los activos de información.

2. **Objetivos:** Describen de forma general lo que la organización busca lograr con la implementación del sistema en relación con las características de la información y los servicios.

3. **Alcance del sistema:** Define sobre que partes de la organización se aplicaran los procesos de gestión de la seguridad

4. **El proceso de evaluación de riesgos y resultados:** existen varias metodologías para hacer una evaluación de riesgos, sin embargo, La metodología MAGERIT es específica para la gestión de tecnología; en ella

se encuentra el marco para seguir un proceso de gestión de riesgos. Dentro de las principales secciones a desarrollar esta la elaboración del inventario de activos, identificación y valoración de amenazas, cálculo del impacto, cálculo del riesgo, identificación de los propietarios de los riesgos, determinación de las medidas de seguridad.

5. **Plan de tratamiento de riesgos:** Una vez establecidas las actividades se debe articular un plan que este compuesto básicamente por las actividades, los responsables de cada acción y el mecanismo para medir la eficacia de los controles a implantar. Estas mediciones deben ser definidas teniendo en cuenta que debido al esfuerzo que representa la toma de datos, por lo que se deben reducir y alinear a los objetivos de la organización." Las métricas deben ser pensadas en función de la confidencialidad, disponibilidad, e integridad. El plan de tratamiento de riesgos debe contener como mínimo los siguientes elementos: Objetivo, alcance, responsabilidades, tareas, seguimiento, indicadores"[8]

6. **Declaración de aplicabilidad:** corresponde a la documentación de las medidas de seguridad provistas en el anexo II de la norma indicando para cada (ESET, 2015) una de ellas si debe aplicarse o no, justificando las exclusiones[9], se desarrolla luego del tratamiento de riesgos, como beneficio principal es identificar la mitigación de riesgos que no han sido identificados y analizados en los pasos anteriores.

7. **Los procedimientos propios que la organización determine como necesarios.** Teniendo en cuenta que cada organización tiene diferentes necesidades y por lo tanto tiene tantas implementaciones tecnológicas como normas o condiciones de negocio diferente, una vez determinado el alcance es posible que se requieran procedimientos e instructivos propios para asegurar el control adecuado.

Tratamiento del Riesgo: Existen cuatro opciones para hacer el tratamiento de un riesgo, las cuales no son mutuamente excluyentes. estas opciones son: Reducción del riesgo mediante la selección de controles, Retención o aceptación del riesgo, Evitar el riesgo eliminando las acciones que pueden originar y para terminar

[8] GOMEZ FERNANDEZ, Luis, FERNANDEZ RIVERO Pedro Pablo. Como implantar un SGSI según UNE – ISO 27001: 2014 y su aplicación en el esquema Nacional de Seguridad, Madrid, Editorial AENOR, 2015, Pag 123

[9] ESET. (1 de Abril de 2015). WEliveSecurity. Obtenido de https://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/

transferir el riesgo que básicamente corresponde a compartir el riesgo con terceras partes, la cual se puede dar mediante pólizas de seguro, subcontratación[10].

MAGERIT

Es la metodología de análisis de gestión de riesgos de los sistemas de información, definida por el Ministerio de hacienda y administraciones públicas, como respuesta a la necesidad gestionar los riesgos propios de los sistemas de información, de los cuales se evidencia una creciente dependencia tanto de la administración pública como de toda la sociedad. (AMUTIO GOMEZ)

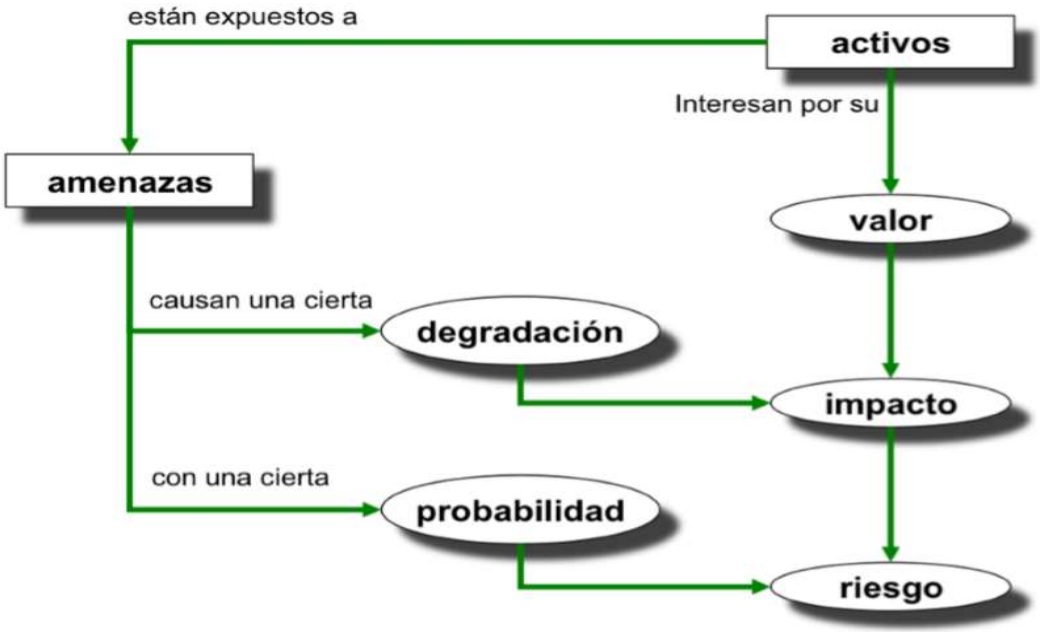
Magerit está documentado en tres libros, en los cuales se abarca el Método, el catálogo los elementos (tipos de activos, criterios de valoración, clasificación de amenazas) y las técnicas de valoración donde se describen algunas técnicas de análisis de gestión de riesgos

La clasificación de amenazas definida en el libro 2 es congruente con la tipificación de controles del anexo 1 de la norma ISO 27001

La siguiente gráfica (Diagrama 2.) Resume los conceptos básicos utilizados por la metodología y su flujo de trabajo para realizar el análisis de riesgos potenciales

[10] INSTITUTO COLOMBIANO DE NORMAS TECNICAS. Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información, Bogotá D.C.: ICONTEC, 2019. NTC-ISO/IEC 27005:2008, Pag 22-23

Fig. 1 Elementos del Análisis de riesgos Potenciales



Fuente: *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método*.

4.4 MARCO ESPACIAL

El proyecto será realizado en el marco de la empresa QWERTY S.A.S, la cual es una empresa del sector tecnológico que cuenta con tres dependencias encargadas de Infraestructura, Desarrollo y soporte. QWERTY SAS cuenta con 120 empleados, por lo que se puede considerar una PYME

4.5 MARCO TECNOLÓGICO

A continuación, se relacionan las metodologías específicas aplicables a cada una de las actividades a desarrollar para lograr la definición del Sistema de gestión de seguridad de la información

Tabla 1 Metodologías Aplicables

No	Etapa	Actividades críticas	Metodología Específica
1	Crear marco de referencia	Documentar antecedentes, casos de éxito, estudio de procesos y metodologías y buenas prácticas	Revisión documental de material académico foros, trabajos similares, sitios en internet relacionados con diseños de sistemas de gestión
2	Analizar situación de la organización	Revisión y análisis de caso de estudio establecer contexto interno y externo Establecer Población objetivo (Procesos, personas Activos)	Revisión de la documentación entregada en el Escenario dos para trabajo de proyecto aplicado Consulta de material relacionado con situación de ciberseguridad nacional
3	Estudiar problemática de gestión de seguridad	Identificar efectos no deseados, causas, tanto de la situación actual (vulnerabilidades actuales) como efectos del diseño, Definir tablas de valoración de riesgos	Análisis causa efecto Evaluación de riesgos con metodología MAGERIT.
4	Proponer alternativas de solución	Identificar alcance del sistema de gestión, política, Definir Marco Organizativo de la seguridad Establecer mediciones	Aplicar estándar ISO 27001 Matriz RACI para asignación de responsabilidades
5	Documentar el diseño propuesto	desarrollar los documentos requeridos para dar soporte al diseño del sistema de gestión desde	Aplicar estándar ISO 2001/ISO 27005 Metodología MAGERIT

Fuente: Presente Estudio

4.6 MARCO METODOLÓGICO

4.6.1 UNIDAD DE ANÁLISIS

La unidad de análisis corresponde a los posibles riesgos y vulnerabilidades a los cuales pueden estar sometidos los activos de la organización establecida como caso de estudio.

4.6.2. ESTUDIO METODOLÓGICO.

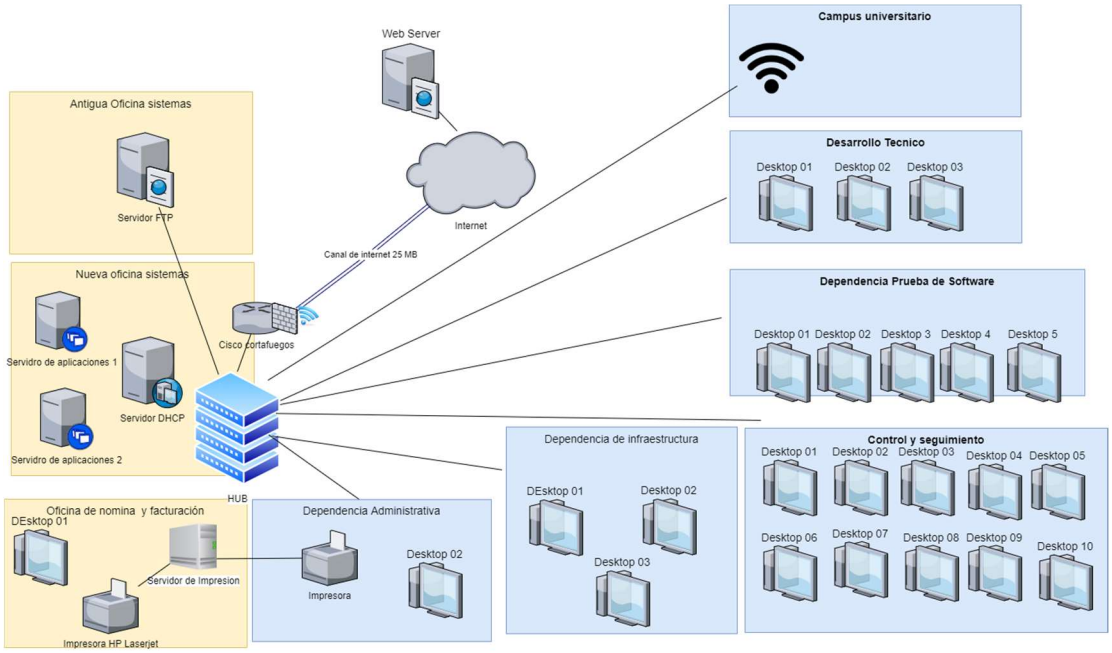
Para este proyecto aplicado la metodología seleccionada es la investigación por observación de un caso de estudio, esto teniendo en cuenta que el tipo de investigación que aplica al proyecto es La investigación aplicada, donde se busca resolver un problema práctico, El tipo de estudio es cualitativo en lo que se refiere a la identificación de activos, vulnerabilidades, clasificación del riesgo y se utilizarán escalas de valoración cuantitativa para la calificación de riesgos

Se tendrá como técnica el uso de levantamiento de información mediante observación y análisis de la misma con el objetivo de identificar los activos los cuales serán evaluados y así poder identificar sus riesgos con el objetivo que las entidades obtengan un diagnóstico que conlleven a la implementación de controles para conseguir el fortalecimiento del sistema de gestión de seguridad de la información basado en identificación y administración de riesgos.

5. IDENTIFICACIÓN DE ACTIVOS

Antes de dar paso a la clasificación de los activos se ilustra la arquitectura construida a partir del escenario presentado para facilitar la identificación de los activos.

Fig. 2 Arquitectura Inicial

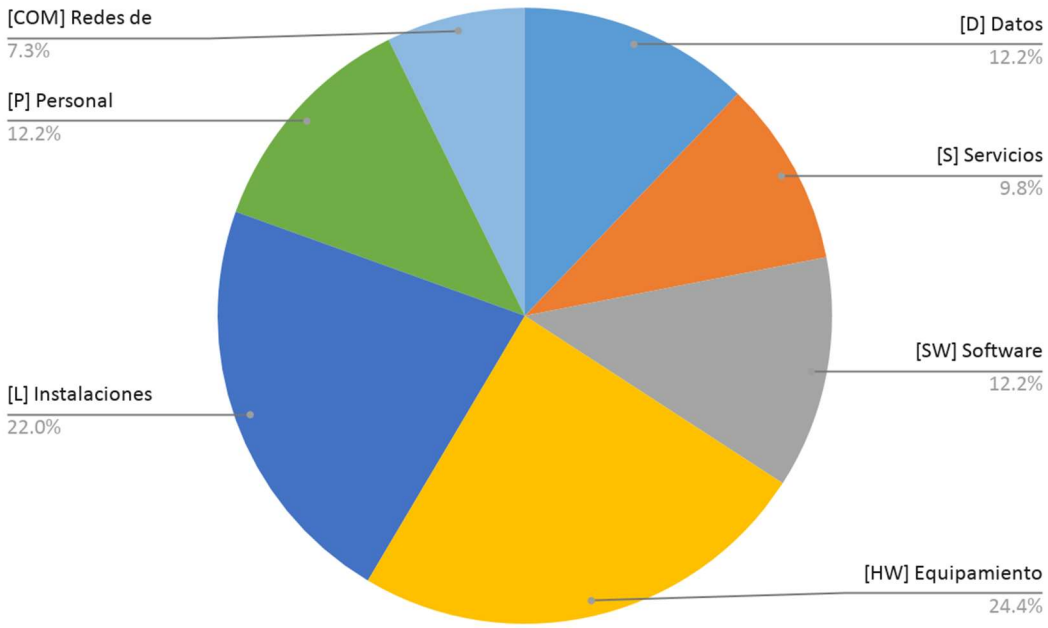


Fuente: Presente Estudio

Siguiendo la metodología y aplicando la nomenclatura de MAGERIT –Versión 3, se establecieron los Activos esenciales y paso seguido se identificaron los activos más relevantes que dan soporte a los servicios de tecnología. (Gobierno de España, Ministerio de Hacienda y administraciones públicas, 2012).

Los activos identificados Fueron Clasificados siguiendo según la metodología encontrando que el 24.4% corresponde a Equipos donde se incluyen tanto servidores como equipos de usuario final, el 12.2% corresponden a datos que incluyen desde datos registrados por usuarios finales, datos de seguimiento del servicio técnico hasta datos de configuración de red y de seguridad del sistema de información, 22% a instalaciones y 12.2% corresponde a personal. En la Figura 4 se presenta la totalidad de las categorías y su participación

Fig. 3 % Participación de Activos identificados



Fuente: Presente Estudio

5.1 ACTIVOS ESENCIALES

A continuación, se presentan dos clasificaciones que son datos y servicios los cuales se muestran a continuación en la tabla 2 y tabla 3.

La tabla 2 corresponde a los servicios que desde tecnología están disponibles para que la organización pueda realizar la labor social para la que fue constituida.[11]

[11] **AMUTIO GOMEZ, Miguel Angel, CANDAU, Javier.** *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método.* MAdrid : Editorial Ministerio de Hacienda y Administraciones Públicas Secretaría General

Tabla 2 servicios [S]

CODIGO	NOMBRE	CRITICIDAD	ACTIVO	DESCRIPCIÓN
[service]	SERVICIO	Nivel Alto [A]	Correo institucional	Comunicación con otros miembros de la entidad • Compartir archivos • Recibir comunicados oficiales • Brindar espacio de almacenamiento ilimitado • Dar prioridad a las actividades propuestas por el desarrollo académico del programa
[service]	SERVICIO	Nivel Alto [A]	Mantenimiento y gestión de activos	• Equipos de cómputo de escritorio, móviles y servidores, televisores, video proyectores • Software operativo y aplicativo • Servicio de Internet • Todo el equipamiento que se requiera para ayudar a dar cumplimiento al objeto social.
[service]	SERVICIO	Nivel Alto [A]	Gestión de usuarios y contraseñas	Administración de usuarios y contraseñas del correo y aplicativos utilizados
[service]	SERVICIO	Nivel Alto [A]	Gestión de talento humano	Generación de nómina de trabajadores • Generación de recibos de pago • Creación, alimentación y custodia de Hojas de vida • Control del seguimiento al talento humano • Generación certificados laborales y relacionados con el modelo de negocio

Fuente: Presente Estudio

En la tabla 3 que se presenta a continuación se clasifican los activos relacionados con información presente en la organización, para la clasificación se tuvo en cuenta

aspectos como datos personales que requieren tratamiento establecido en la ley de protección de datos, datos vitales que en caso de una situación catastrófica son requeridos para mantener la operación de la organización y datos que requieren tratamiento especial debido a que por su naturaleza y el riesgo que representa su divulgación pueden generar riesgos a la organización.

Tabla 3 Datos/información [D]

CÓDIGO	NOMBRE	CRITICIDAD	ACTIVO	DESCRIPCIÓN
[vr]	datos vitales	Nivel Alto [A] Publica [pub]	Datos del sistema de información	Registros realizados a través de los aplicativos que forman parte del sistema de información de la organización como inventarios, nómina, activos, estados financieros
[per]	Datos personales	Nivel Alto [A] difusión limitada [R]	Datos personales registrados en el sistema y en documentos físicos	Registros de datos personales requeridos para la identificación y/o autenticación de empleados, Estudiantes y proveedores
[Conf]	Datos de configuración	[R] Difusión limitada	configuración de red	Datos relacionados con configuración de equipos activos de red, segmentación, versión de sistemas operativos, parches, versiones de antivirus.
[Password]	Credenciales	[C] Confidencial	Usuarios y contraseñas	Datos relacionados con identificación de usuarios, contraseñas asignados a usuarios y administradores del sistema
[Conf]	Datos de configuración	[R] Difusión limitada	Configuración de niveles de permisos	Datos relacionados con la asignación de permisos a los perfiles de usuarios en los sistemas de información de la organización

Fuente: Presente estudio

5.2 OTROS ACTIVOS RELEVANTES

En esta sección se encuentran clasificados los activos que dan soporte a los activos de información o forman parte de los servicios. Un activo de esta clasificación puede ser soporte de uno o varios activos esenciales. Aquí se clasifican e identifican Aplicaciones de software, Equipos Informáticos, Instalaciones, Personal y Redes de comunicaciones.

Tabla 4 Instalaciones [L]

CODIGO	NOMBRE	CRITICIDAD	ACTIVO	DESCRIPCIÓN
[building]	Edificios	nivel alto [A]	oficina antigua de sistemas	ubicación de servidores
[building]	Edificios	nivel alto [A]	dependencia de desarrollo técnico	área de trabajo
[building]	Edificios	nivel alto [A]	Nueva oficina de sistemas	ubicación de servidores
[building]	Edificios	nivel alto [A]	Dependencia prueba de Software	área de trabajo
[building]	Edificios	nivel Medio [M]	Dependencia de control y seguimiento	área de trabajo
[building]	Edificios	nivel Medio [M]	Dependencia de infraestructura	área de trabajo
[building]	Edificios	nivel Bajo [B]	Dependencia Administrativa	área de trabajo
[building]	Edificios	nivel alto [A]	oficina nómina y facturación	área de trabajo
[building]	Edificios	nivel alto [A]	Campus universitario	área de acceso a estudiantes que utilizan los servicios del centro de estudios

Fuente: Presente Estudio

Tabla 5 Equipos informáticos [HW]

CÓDIGO	NOMBRE	CRITICIDAD	ACTIVO	DESCRIPCIÓN
[host]	grandes equipos	Nivel alto [A]	Servidor de impresión	Servidor marca dell en torre PowerEdge T440
[print]	Medios de impresión	Nivel medio [M]	Impresora area de nomina	Impresora HP LaserJet Enterprise serie 600
[print]	Medios de impresión	Nivel medio [M]	Impresora multifuncional, dependencia directiva y administrativa	Impresora SMART MultiXpress M4370LX
[host]	grandes equipos	Nivel alto [A]	Servidor de archivos FTP	Servidor marca dell en torre PowerEdge T130
[host]	grandes equipos	Nivel alto [A]	Servidor de facturación y nómina	Servidor marca dell en torre PowerEdge T44
[host]	grandes equipos	Nivel alto [A]	Servidor DHCP	Servidor marca dell en torre PowerEdge T440
[pc]	informática personal	Nivel alto [A]	Equipos de cómputo para dependencias de gestión del desarrollo tecnológico,infraestructura,control y seguimiento,pruebas y desarrollo de software	20 Equipos
[iphone]	telefonos IP	Nivel medio [M]	telefonos IP	Sistema de comunicación a través de teléfonos Voz IP, que comunica las oficinas y departamentos del centro
[firewall]	cortafuegos	nivel alto [A]	Cortafuegos Cisco ASA 5505	Sistema de seguridad que está protegiendo a la red de datos, de intrusiones que se puedan presentar en la red
[switch]	Conmutadores	nivel alto [A]	Switches cisco catalyst 296	red de datos del centro

Fuente: Presente Estudio

Tabla 6 Aplicaciones software [SW]

CÓDIGO	NOMBRE	CRITICIDAD	ACTIVO	DESCRIPCIÓN
[SW]	Aplicaciones	Nivel medio [M]	Página Web	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
[prp]	desarrollo propio	Nivel alto [A]	Software de Sistema de información	Software propio
[SW]	Aplicaciones	Nivel alto [A]	Apache 2.4.25	Software administrador para el sitio web
[av]	Antivirus	Nivel alto [A]	Antivirus	Software para control de virus
[os]	sistema operativo	Nivel alto [A]	licenciamiento de servidores y pc	Windows 10 phpMyAdmin 4.6.6 MySQL 5.7.17 PHP 5.6.30 - 7.1.1

Fuente: Presente estudio

Tabla 7 personal [P]

CÓDIGO	NOMBRE	CRITICIDAD	ACTIVO	DESCRIPCIÓN
[op]	Operadores	nivel alto [A]	técnicos de mantenimiento (2)	Personal técnico encargado de realizar el mantenimiento preventivo a los equipos de computo
[ui]	usuarios internos	nivel Medio [M]	Personal en practica	Personal en práctica que realiza registros en apl.de nómina y facturación
[des]	Desarrolladores	nivel alto [A]	Desarrolladores de software propio	Encargados de desarrollar y mantener software propio
[ui]	usuarios internos	nivel alto [A]	personal de nómina y facturación	Encargados de administración y registro de nómina y facturación
[ui]	usuarios internos	nivel Medio [M]	Usuarios del campus	estudiante que hacen uso del servicio del centro

Fuente: Presente Estudio

Tabla 8 Redes de comunicaciones [COM]

CÓDIGO	NOMBRE	CRITICIDAD	ACTIVO	DESCRIPCIÓN
[LAN]	Red local	nivel alto [A]	puntos de acceso inalámbrico	Dispositivos de red (4)
[internet]	Internet	nivel alto [A]	Canal de internet	Canal dedicado de 25 megas de ancho de banda
[LAN]	Red local	nivel alto [A]	puntos de acceso alámbrico	Acceso al Campus del centro de estudios

Fuente: Presente Estudio

6. VALORACIÓN DE ACTIVOS Y DEFINICIÓN DE AMENAZAS

6.1 DEFINICIONES

En la siguiente tabla se documentan los parámetros para determinar calificación tanto cuantitativa como cualitativa de los activos basados en el nivel de afectación o de interrupción del servicio.

Tabla 9 Escala de valoración

Valor	Criterio
1 Bajo	Daño menor o irrlevante ,Interrupción parcial de un grupo de Individuos en menos de un dia
2 Medio	Importante ,Interrupcion parcial de un grupo de individuos en 1 dia o mas
3 Alto	Grave , Interrupcion a toda la organización menos de un dia
4 Extremo	Extremadamente grave, Interrupcion a toda la orgamización mas de un dia o afecta organizaciones

Fuente: Presente Estudio

Esta escala se aplicó a todos los activos identificados evaluando de forma independiente en cada una de las condiciones de Confidencialidad, Integridad y Disponibilidad.

El segundo parámetro que se estableció para determinar el riesgo tiene que ver con la probabilidad de ocurrencia de las amenazas identificadas cada activo estableciendo cuatro niveles con rangos cuantitativos de 2 a 5 siendo 5 el más frecuente y de mayor impacto y 2 el menos probable.

Tabla 10 Escala de Probabilidad

Valor	**Descriptor**
2	Raramente
3	Ocasional
4	Probable
5	Frecuente

Fuente: Presente Estudio

En cuanto a la definición de las amenazas se utilizó como referente la codificación que presenta la metodología MAGERIT, en el libro II Catálogo de elementos página 25 a 47. [12]

Tabla 11 Probabilidad de ocurrencia (frecuencia)

	Raramente	ocasional	probable	Frecuente
Bajo	2	3	4	5
Medio	4	6	8	10
Alto	6	9	12	15
Extremo	8	12	16	20

Fuente: Presente Estudio

Los cuales se relacionan en la columna amenaza y que en el siguiente paso del ejercicio son los determinantes para establecer los controles (Gobierno de españa, Ministerio de Hacienda y administraciones Públicas, 2012).

Para tener en cuenta en la revisión de la calificación de activos esenciales es necesario tener en cuenta la siguiente interpretación.

C= Confidencialidad

I = Integridad

D=disponibilidad

Frecuencia, se refiere a la frecuencia con se pueden presentar eventos que afecten las condiciones de calidad de la información

[12] AMUTIO GOMEZ, Miguel Angel, CANDAU, Javier, MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos, Madrid, Editorial Ministerio de Hacienda y Administraciones Públicas Secretaría General Técnica Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones

Tabla 12 Calificación de activos esenciales

Código	Activo	C	I	D	Amenaza	Frecuencia
[vr]	Datos del sistema de información	4	4	4	[E20]	4
[service]	Correo institucional	1	1	3	[A8]	3
[service]	Mantenimiento y gestión de activos	3	1	1	[E23]	2
[service]	Gestión de usuarios y contraseñas	4	4	4	[E2]	3
[service]	Gestión de talento humano	3	4	4	[A7]	3
[per]	Datos personales registrados en el sistema y en documentos físicos	4	4	4	[E20]	4
[Conf]	configuración de red	3	3	4	[E2]	3
[Password]	Usuarios y contraseñas	4	3	4	[E20]	3
[Conf]	Configuración de niveles de permisos	4	3	4	[E2]	3

Fuente: Presente Estudio

En el activo Datos del sistema de información se incluyen los datos requeridos para la operación del negocio, tales como clientes, proveedores, inventarios, contratos costos y estados financieros.

Los datos personales se identifican como un activo aparte por el tratamiento legal que se tiene establecido aunque la amenaza que establece es la misma para los otros datos las consecuencias de su exposición a nivel legal es más *crítico.*

Tabla 13 Calificación de otros activos relevante

Código	Activo	C	I	D	Amenaza	Frecuencia
[SW]	Página Web	4	4	4	[A11]	5
[prp]	Software del sistema de información	4	4	2	[E20]	3
[SW]	Apache 2.4.25	4	4	3	[E.21]	2
[av]	Antivirus	3	2	1	[A.8]	3
[os]	licenciamiento de servidores y pc	3	1	2	[E.21]	4
[building]	oficina antigua de sistemas	3	3	3	[N*]	2
[building]	Empresa Godaddy	4	4	4	[N*]	2
[building]	dependencia de desarrollo tecnologico	3	3	3	[N*]	2
[LAN]	puntos de acceso alambrico	1	1	4	[I.8]	2
[MAN]	puntos de acceso inalambrico	1	1	4	[I.8]	2
[internet]	Canal de Internet	1	1	4	[I.8]	3
[op]	técnicos de mantenimiento (2)	2	2	2	[E28]	2
[ui]	Personal en practica	3	3	3	[E1]	3
[des]	Desarrolladores de software propio	2	2	2	[E28]	2
[host]	Servidor de impresión	4	4	4	[E.4]	3
[print]	Impresora área de nómina	1	1	4	[E.23]	3
[print]	Impresora multifuncional, dependencia directiva y administrativa	1	1	4	[E.23]	3
[host]	Servidor de archivos FTP	4	4	4	[E.4]	3
[host]	Servidor de facturación y nómina	4	4	4	[E.4]	3
[host]	Servidor DHCP	4	4	4	[E.4]	3
[pc]	Equipos de cómputo para gestión del desarrollo tecnológico	1	3	2	[N.*]	2
[pc]	Equipos de cómputo para dependencia de infraestructura	1	3	2	[N.*]	2
[pc]	Equipos de cómputo para dependencia de control y seguimiento	1	3	2	[N.*]	2
[pc]	Equipos de cómputo para dependencia de prueba de software	1	3	2	[N.*]	2
[ipphone]	teléfonos IP	1	1	1	[N.*]	2
[firewall]	Cortafuegos Cisco ASA 5505	4	4	4	[A.11]	2
[switch]	Switches cisco catalyst 296	4	3	4	[I.6]	2

Fuente: Presente Estudio

6.2 VULNERABILIDADES

A partir de la clasificación definida en el punto anterior a continuación se presenta un consolidado de las vulnerabilidades y los activos que afectan:

El Pareto de las amenazas está encabezado por el 28.3% por desastres naturales, el 20.75% corresponde vulnerabilidades de los programas de software, el 7.55.1 % a errores de configuración, en cuarto lugar, con 5.66 % encontramos 4 amenazas, que corresponden a Errores de mantenimiento/actualización de equipos, fallas de servicios de comunicación, errores en actualización o modificaciones de software y errores de los usuarios.

Tabla 14 Consolidado de amenazas.

Amenaza	Descripción	Cantidad de activos	%
[N*]	Desastres Naturales	15	28.30
[E.20]	Vulnerabilidades de los programas de software	11	20.75
[E.4]	Errores de configuración	4	7.55
[E.23]	Errores de mantenimiento/Actualización de Equipos	3	5.66
[I.8]	Fallo de servicios de comunicación	3	5.66
[E.21]	Errores en Actualización o modificaciones de programas (Software)	3	5.66
[E.1]	Errores de los usuarios	3	5.66
[A.11]	Acceso no autorizado	2	3.77
[A.8]	Difusión de malware	2	3.77
[E.28]	Indisponibilidad del personal	2	3.77
[E.15]	Alteración Accidental de la información	2	3.77
[I.6]	Corte del suministro eléctrico	1	1.89
[E.2]	Errores del administrador	1	1.89
[A.7]	Uso no previsto	1	1.89

Fuente: Presente Estudio

7. EVALUACIÓN DE RIESGOS

El primer paso en la valoración de riesgos una vez se tiene definido el inventario de activos está en la identificación de amenazas y vulnerabilidades y para su adecuada cuantificación se definen valores de frecuencia de ocurrencia de cada una de las amenazas con referencia a los activos e impacto acumulado.

7.1. CRITERIOS DE EVALUACIÓN

A continuación, se define la escala de valoración para determinar la probabilidad de que se materialice un riesgo. Básicamente se define una combinación del impacto y la probabilidad y se establece una matriz como medida de comparación.

Tabla 15 Matriz de calificación de riesgo

Riesgo			Probabilidad			
			Raramente	Ocasional	Probable	Frecuente
			2	3	4	5
	Bajo	1	2	3	4	5
	Medio	2	4	6	8	10
	Alto	3	6	9	12	15
Impacto	Extremo	4	8	12	16	20

Fuente: Presente Estudio

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

Tabla 16 Nivel de riesgo

Rango	Riegos
menor a 4	Despreciable
De 5 a 8	Bajo
de 9 a 12	Alto
mayor a 12	Critico

Fuente: Presente Estudio

7.2. CALIFICACIÓN DEL RIESGO

Aplicando los parámetros de calificación definidos tenemos lo siguiente: cuatro riesgos de nivel crítico, tres de nivel Alto y uno de nivel bajo en los activos esenciales.

Tabla 17 Calificación del riesgo para activos esenciales

Código	Activo	Amenaza	Frecuencia	Riesgo
[vr]	Datos del sistema de información	[E20]	4	16
[service]	Correo institucional	[A8]	3	2
[service]	Mantenimiento y gestión de activos	[E23]	2	6
[service]	Gestión de usuarios y contraseñas	[E2]	3	8
[service]	Gestion de talento humano	[A7]	3	6
[per]	Datos personales registrados en el sistema y en documentos físicos	[E20]	4	16
[Conf]	configuración de red	[E2]	3	8
[Password]	Usuarios y contraseñas	[E20]	3	8
[Conf]	Configuración de niveles de permisos	[E2]	3	8

Fuente: Presente Estudio

A partir de la calificación anterior de riesgo se puede establecer que los activos con mayor riesgo corresponden a los datos relacionados con proveedores, compras y nómina.

Tabla 18 Calificación del riesgo para otros activos (1)

Código	Activo	Amenaza	Frecuencia	Riesgo
[des]	Desarrolladores de software propio	[E28]	2	8
[host]	Servidor de impresión	[E.4]	3	12
[print]	Impresora área de nómina	[E.23]	3	12
[print]	Impresora multifuncional, dependencia directiva y administrativa	[E.23]	3	12
[host]	Servidor de archivos FTP	[E.4]	3	12
[host]	Servidor de facturación y nómina	[E.4]	3	12
[host]	Servidor DHCP	[E.4]	3	12
[pc]	Equipos de cómputo para gestión del desarrollo tecnológico	[N.*]	2	6
[pc]	Equipos de cómputo para dependencia de infraestructura	[N.*]	2	6
[pc]	Equipos de cómputo para dependencia de control y seguimiento	[N.*]	2	6
[pc]	Equipos de cómputo para dependencia de prueba de software	[N.*]	2	6
[ipphone]	teléfonos IP	[N.*]	2	2
[firewall]	Cortafuegos Cisco ASA 5505	[A.11]	2	8
[switch]	Switches cisco catalyst 296	[I.6]	2	8

Fuente: Presente Estudio

Como nivel de riesgo alto se identifican software del sistema de información, el antivirus, que se identifica no se está administrando de manera adecuada, licenciamiento de servidores, el canal de internet y el personal en práctica y el personal que utiliza el sistema de información.

Tabla 19 Calificación del riesgo para otros activos (2)

Código	Activo	Amenaza	Frecuencia	Riesgo
[SW]	Página Web	[A11]	5	8
[prp]	Software del sistema de información	[E20]	3	12
[SW]	Apache 2.4.25	[E.21]	2	8
[av]	Antivirus	[A.8]	3	12
[os]	licenciamiento de servidores y pc	[E.21]	4	12
[building]	oficina antigua de sistemas	[N*]	2	6
[building]	Empresa Godaddy	[N*]	2	2
[building]	dependencia de desarrollo tecnológico	[N*]	2	8
[LAN]	puntos de acceso alámbrico	[I.8]	2	8
[MAN]	puntos de acceso inalámbrico	[I.8]	2	8
[internet]	Canal de Internet	[I.8]	3	12
[op]	técnicos de mantenimiento (2)	[E28]	2	4
[ui]	Personal en practica	[E1]	3	12

Fuente: Presente Estudio

Los servidores y equipos de impresión ubicados en la sede tienen un nivel de riesgo alto, tanto por las condiciones físicas que le pueden llevar a verse expuestos a desastres naturales, como posible exposición a amenazas por fallas generadas en el mantenimiento físico o deficiencias de configuración.

8. FORMULACIÓN DE CONTROLES.

La formulación de controles se realiza a partir de la identificación de los riesgos del capítulo anterior y el anexo A de la norma ISO 27001.

8.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

Se debe definir las políticas, que, una vez aprobadas por la dirección, deben ser divulgadas para que sirvan de guía en el comportamiento de los empleados y faciliten la toma de decisiones.

Estas políticas deben ser revisadas a intervalos planificados para asegurar que se mantienen vigentes en función de la evolución de las amenazas.

Esta política debe incluir las medidas de seguridad para uso de dispositivos móviles que se tengan para la prestación del servicio, que si bien no son relevantes en la revisión de vulnerabilidades hay que tener en cuenta que la razón de ser del negocio es el desarrollo tecnológico de las comunidades que asesora y esta es hoy un elemento fundamental.[13]

8.2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Se debe establecer un marco de referencia de gestión de la seguridad que articule la implementación y operación de la misma. Para esto se debe definir Roles y responsabilidades asociados a la seguridad, en esta definición se debe incluir la segregación de funciones, evitando así conflictos que no permitan un sano control, e incluir como condición obligatoria en todo proyecto que se emprenda la validación de las condiciones de seguridad de la información.

8.3 SEGURIDAD DEL RECURSO HUMANO

En la identificación de activos se identifican cuatro grupos de interés específicos sobre los cuales se deben implementar medidas de control para asegurar las condiciones de calidad de la información, estos grupos son: Proveedores, Operadores Usuarios internos y Desarrolladores.

Ya que en el grupo de usuarios internos se destaca en personal en práctica para el registro de información en el sistema de nómina se debe contar con un control en el proceso de selección que incluya verificación de antecedentes, acuerdos

[13] INSTITUTO COLOMBIANO DE NORMAS TECNICAS. Tecnología de la información. Técnicas de seguridad de la información. Sistemas de seguridad de la información. Requisitos Bogotá D.C.: ICONTEC, 2013. NTC-ISO/IEC 27001:2013

contractuales con respecto a la confidencialidad de la información y las responsabilidad de cada individuo frente al adecuado manejo de la información que debe mantenerse durante la contratación y la confidencialidad una vez se termina el contrato; se debe establecer una prueba técnica que evidencie las habilidades del personal para desarrollar la labor para la que se contrata.

Una vez es contratado el personal es necesario hacer constante sensibilización al personal frente a las necesidades de seguir mantener condiciones de seguridad adecuadas de la información a la que tienen acceso por para realizar las labores que se les asigna y el establecimiento y la debida comunicación de procesos disciplinarios a que hay lugar ante incumplimiento de políticas y procedimientos que resulten en afectación de la información.

8.4 GESTIÓN DE ACTIVOS

Para una adecuada gestión se debe tener en cuenta tanto los enunciados en el Anexo A[14] de la norma que se vienen desarrollando como las buenas prácticas de ITIL, en las cuales se cuenta con los lineamientos para documentar de forma adecuada el catálogo de los servicios, el cual facilita la aplicación de los siguientes controles:

1. Contar con la identificación clara de los activos de información
2. Establecer el propietario del servicio tanto cliente como (negocio) como desde el punto de vista técnico.
3. Disponibilidad.
4. Acuerdos de nivel de servicio
5. Nivel de criticidad del activo

Una vez se establece esta clasificación se debe definir, comunicar e implementar el procedimiento para el manejo de los activos, que debe incluir el mecanismo para solicitar el acceso, mantenimiento, renovación, políticas de uso.

8.4.1 EQUIPOS

Para prevenir daños o pérdida que puedan impedir contar con los equipos disponibles cuando se requiere su utilización.

Se debe implementar el procedimiento que asegure la ejecución de los mantenimientos preventivos (A11.2.4), de igual forma este procedimiento debe tener alcance a establecer las condiciones para mantener o retirar activos para renovación y las condiciones para hacer la reutilización y/o disposición final de los

[14] INSTITUTO COLOMBIANO DE NORMAS TECNICAS. Tecnología de la información. Técnicas de seguridad de la información. Sistemas de seguridad de la información. Requisitos Bogotá D.C.: ICONTEC, 2013. NTC-ISO/IEC 27001:2013

mismos sin afectar la seguridad o divulgación de la información que contienen los equipos.

8.5 SEGURIDAD FÍSICA Y DEL ENTORNO

Con este control se busca prevenir el acceso a las instalaciones en donde se hace el procesamiento de la información por personas que no cuentan con la debida autorización.

Se debe implementar espacio exclusivo para ubicación de servidores DHCP, HTTP y PBX con condiciones ambientales controladas (A.11.1.4) y evitando el acceso no autorizado (A11.2.1) o en su defecto trasladar estos servidores a un centro de datos (hosting o cloud).

Para tal efecto es necesario implementar el uso de control con validación por medio biométrico (A11.1.2 y A11.1.3), para restringir el acceso.

8.6 CONTROL PARA DESARROLLO DE SOFTWARE

Ya que se cuenta con desarrollo de software propio es necesario restringir el acceso a los códigos fuente, para evitar daños intencionales o manipulación por personal si el conocimiento es adecuado. (A9.4.5)

Se debe realizar el control de cambios que permita asegurar que un cambio en el software no afecte el procesamiento de la información para el que es utilizado. (A12.1.2).

Ante un evento que implique fallas en el ambiente en producción es necesario contar tanto con las copias de los elementos de software de los servicios como la documentación de la configuración necesaria para asegurar restauración de los servicios, por lo que es necesario alinear el proceso de liberación de versiones del software y su implementación de forma que se convierta en una práctica estándar donde se asegure la planificación de los cambios, validación de incidentes y problemas frente a los objetivos definidos para las implementaciones, asegurar un inventario completo de estos activos asignando un responsable de mantenerlo actualizado, con la debida documentación al momento de su puesta en producción.

Ahora para asegurar que el software cuenta con las medidas apropiadas de seguridad se debe evaluar que se cuenta con un sistema apropiado de acceso y con la debida gestión de contraseñas que aplique las buenas prácticas de contraseñas fuertes (A9.4.3), De igual forma se debe asegurar que las aplicaciones

cuentan con restricciones de acceso basado en privilegios asociados a los perfiles derivados de los roles que ejecuta cada usuario por las responsabilidades asignadas (A9.4.1).

9. ADMINISTRACIÓN Y GESTIÓN DE RIESGO

Hasta aquí se puede decir que cuenta con un contexto y diagnóstico inicial de la situación de la organización con respecto a sus activos, valoración de riesgos y definición global de controles a aplicar, ahora se desarrollara a partir de lo anterior el plan de tratamiento de riegos, la declaración de aplicabilidad basados en el Anexo 1 de la norma ISO 27001.[15]

Seguidamente se dará soporte a los controles con la inclusión de documentos como la política de seguridad, el procedimiento para manejo de activos, la política de seguridad para proveedores y el control de software entre otros.

9.1 PLAN DE TRATAMIENTO DE RIESGOS

9.1.1 OBJETIVO

Establecer la ruta para la implementación de controles que permitan reducir el nivel riesgos identificados en la evaluación preliminar, facilitando la organización de la seguridad que se requiere para dar el tratamiento adecuado a la información en QWERTY SAS.

9.1.2 ALCANCE

Este plan incluye las actividades para definir el modelo de gestión de riesgos de QWERTY SAS.

9.1.3 RESPONSABILIDADES

El equipo directivo es responsable de revisar y aprobar el plan, los objetivos del sistema de gestión de seguridad de la información y facilitar los recursos necesarios que aseguren su ejecución.

Oficial de seguridad: Debe realizar la supervisión de las distintas actividades.

El responsable de la dependencia de sistemas se encarga de la implementación y ejecución de las tareas técnicas previstas en el plan.

[15] INSTITUTO COLOMBIANO DE NORMAS TECNICAS. Tecnología de la información. Técnicas de seguridad de la información. Sistemas de seguridad de la información. Requisitos Bogotá D.C.: ICONTEC, 2013. NTC-ISO/IEC 27001:2013

Cuadro Actividades plan de tratamiento de riesgos

Actividad	Responsable	Plazo	Activos afectados	Recursos
Definir Responsble de SGSI, el oficial de seguridad y comité de seguridad de la informacipon	Dirección	1 mes	Todos	Horas Direccion Economico en caso de requerir contratación
Establecer Declaración de aplicabilidad	Responsable del SGSI	1 mes	Todos	horas responsable SGSI
Aprobar y difundir la politica de seguridad	Dirección	1 mes	Todos	Horas Direccion
Aprobar y definir la politica de seguridad para proveedores	Dirección	1 mes	todos	Horas Direccion
Elaborar procedimiento para clasificacioón de información	Responsable del SGSI	1mes	todos	horas responsable SGSI
elaborar procedimientos para el control de activos	responsable de seguridad	4 meses	todos	Horas responsables de seguridad
Llevar acabo actividades de formación especificas en seguridad para la dependencia de sistemas (administracion del antivirus, Administracion del Firewall, seguridad de aaplicaiones)	responsable de seguridad	3meses	todos	Horas responsables de seguridad
Llevar a cabo actividades de socialización al interior de la organización con respecto a la importancia de la seguridad y los procedimientos a adoptar.	responsable de seguridad	2 meses	todos	Horas responsables de seguridad
Implementar requistos de control de acceso y claves	Responsable dependencia de sistemas	2 meses	Aplicaciones y usuarios	horas responsable de dependencia de sistemas
Definir implementación de controles de acceso fisico y logico	responsable de sistemas	1 mes	Areas criticas	horas responsable de dependencia de sistemas
Definir plan de continuidad de negocio	Responsable del SGSI Resposable de sistemas	4 meses	todos	HorasResponsable del SGSI Horas Resposable de sistemas
Implemnetar contingencia para equipos servidores de mision Critica	Responsable del SGSI Resposable de sistemas	4 meses	Equipos de procemiento de mision critica	HorasResponsable del SGSI Horas Resposable de sistemas
Definir el procedimiento asegurar el adecuado gestión de cambios.	responsable de seguridad	1 mes	Todos	horas responsable SGSI
Definir el plan de auditoria.	Responsable del SGSI	1 mes	Todos	horas responsable SGSI

Fuente: Presente Estudio

9.2 Declaración de Aplicabilidad

A continuación, se presenta la revisión de los controles propuesto en La norma ISO27001, junto con la evidencia del cumplimiento del requisito en caso de que aplique dicho control. En el siguiente se presenta para cada control el objetivo, sub

controles, Si aplica o no, la justificación y se relaciona el documento que evidencia su cumplimiento.

Cuadro Declaración de aplicabilidad

A5	POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION		Aplica		
A5.1	Orientación de la dirección para la gestión de la seguridad de la				
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes			si	no	Justificación /Evidencia
A5.1.1	Políticas para la seguridad de la información	Control: documentar en las politicas de la compañis tanto el compormiso como las directrices establecidas por la organizacion para regir las condiciones de seguridad de la información esta debe estar aprobada por la dirección,y asegurar que todas las partes interesadas (empleados, proveedores, clientes, accionistas) la conocen	X		**Justificacion:** Son requeridas ya que ellas se definen las directrices que regulan comportamiento, restricciones,desiciones y autoridad.Asi como cambia la tecnologia, las condiciones del negocio , las vulenrabilidades, se debe revisar las politicas periodicamente para asegurar que mantienen su efectividad. **Evidencia:** Politica
A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Para asegurar que se mantienen vigentes en el tiempo y con los cambios tecnologicos a los que se ven enfrentadas las organizaciones se deben revisar a intervalos planificados o cuando se considere pertinente por cambios drasticos en la organización	X		
A6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION		Aplica		
A6.1	Organización interna				
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.			si	no	Justificación /Evidencia
A6.1.1	Roles y responsabilidades	Control: para garntizar que cada actividad que afecteN las conduciones de la informacíón se deben definir todas las responsabilidades y deben ser asignadas claramente	X		**Justificación:** Dependiendo del cargo que se desempeñe, se deben tener claro las responsabilidddes frente a la seguridad de la información La segregación de funciones es vital para asegurar que se reducen riegos de uso indebido de los activos **Evidencia:** Politica de seguridad de la información, donde se especifican
A6.1.2	Separación de deberes	Control: Se debe aplicar el principio de segregación de funciones simpres que se definan los deberes, roles y responsabilidades	X		
A6.1.3	Contacto con las autoridades	Control: Se deben establcer y mantener contactos con las autoridades que faciliten la revision y toma de acciones tanto en eventos de materializacion de riesgos como en prevención conociendo las tendencias y nuevas forma tanto de los delitos informaticos	X		**Justificación:** Esto facilita que se cuenten con el reconocimiento oportuno de cambios y mecanismos de implementación de dichos cambios.
A6.1.4	Contacto con grupos de interés especial	Control: Realizr suscricpión a organizaciones especializadas idpendientes y fabricantes de los productos de tecnologia utilizados para recibir información constante de innovaciones, cambios y alertas posibles ataques y medidas para enfrentarlos.	X		**Justificación:** identificar nuevas vulnerabilidades y mecanismos de control es mas facil cuando es el trabajo mancomunado de individuos con el mismo interes
A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: Cada proyecto que se inicie en la orgnaizacion debe tener en cuenta las directrices de seguridad de la información establecidas y debe forma parte del analisis de riegos de los proyectos	X		**Justificacion:** Ya que la razon de ser de QWERTY SAS es el desarrollo tecnologico de comunicaciones es imprecindible contar con esta factor en la formulacion de dichos proyectos **Evidencia:** Politica de seguridad de la información

Fuente: Anexo A, ISO 27001:2013

Cuadro Declaración de aplicabilidad (continuación)

A6.2	Dispositivos móviles y teletrabajo		Aplica		Justificación /Evidencia
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles			si	no	
A6.2.1	Política para dispositivos móviles	Control: Se debe adoptar las medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles, los cuales deben quedar documentados.	X		**Justificación:** Aplica, ya que dentro de los equipos utilizados para prestar servicios tecnologico se se encuentran equipos Moviles. **Evidencia:** politica de seguridad de dispositivos moviles
A6.2.2	Teletrabajo	Control:Control para almacenamiento de archivos resultado de teletrabajo y mecanismos de transporte de los mismos		x	**Justificación:** No existe en la organización esta modalidad de trabajo, por lo que el control no es aplicable.
A7	SEGURIDAD DE LOS RECURSOS HUMANOS		Aplica		Justificación /Evidencia
A7.1	Antes de asumir el empleo				
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.			si	no	
A7.1.1	Selección	Control: Durante la selección se debe tener contemplado el procedimientos, los mecanismos y los recursos para realizar La verificación de antecedentes de todos los candidatos a un empleo segun las leyes actuales y las necesidades de validacion segun las reponsabilidades y la informacion a la que va a tener acceso.	X		**Justificacion:** es fundamental asegurar que se cuenta no solo con las competencias, sino tambien revision de antecedentes y experiencia previa en negocioas anteriores. Se deben establecer responsabilidades claras, acuerdos de confidencialida y demas según el cargo.
A7.1.2	Términos y condiciones del empleo	Control: Incluir tanto en contrato laboral como en contratos de servicios externos los articulos necesarios que dejen explicito tanto el compromiso del manejo apropiado de la información, como las responsabilidades frente a su confidencialidad y las consecuencias legales frente su incumplimiento	X		**Evidencia:** Política de seguridad informática sección Responsabilidad
A7.2	Durante la ejecución del empleo		Aplica		Justificación /Evidencia
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.			si	no	
A7.2.1	Responsabilidades de la dirección	Control: Documentar, publicar y demostrar el compromiso de la direccion y su exigencia a todos los colaboradores para que cumplan las normas.	X		**Justificación:** Es necesario esta declaratoria, ya que sin el respaldo de la direccion no se contaran con recursos ni con respaldo para la aplicación debida de controles **Evidencia:** Politica de seguridad informatica
A7.2.2	Formación en la seguridad de la información.	Control: establcer plan de sensibilizacion y capacitación según aplique al personal de forma regular para segurar que se mantiene actualizados los conocimientos de políticas y procedimientos que apliquen a cada cargo.	X		**Justificación:** es necesario asegurar el manejo adecuado de la información por todos aquellos que de una u otra forma pueden afectarla **Evidencia:** Politica de seguridad de la información
A7.2.3	Proceso disciplinario	Control: Las faltas o violaciones a la seguridad de la información deben estar contempladas en los procesos disciplinarios Formales definidos en la organización y debe aplicarse la divulgación apropiada	X		**Justificación:** Deben existir sanciones para quienes infrinjen normas, proliticas, procedimientos o no cumplen con sus responsabilidades **Evidencia:** politica de seguridad de la información

Fuente: Anexo A, ISO 27001:2013

Cuadro Declaración de aplicabilidad (continuación)

A7.3	Terminación y cambio de empleo		Aplica		Justificación /Evidencia
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo			si	no	
A7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Incluir tanto en contrato laboral como en contratos de servicios externos los articulos necesarios que dejen explicito Las responsabilidades frente a la confidencialidad posterior a la terminacion del contrato	X		**Justificación:** Es necesario mantener claridad en lo que tiene que ver con compromisos con el manejo de información que se tenga posterior a la terminacion del empleo o cambio de responsabilidades (revisar clausulas contractuales)
A8	GESTION DE ACTIVOS		Aplica		Justificación /Evidencia
A8.1	Responsabilidad por los activos				
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de			si	no	
A8.1.1	Inventario de activos	Control: establecer nomenclatura para identificacionde activos de información, realziar la marcación fisica y documentar registro con el inventario de especificando: codigo, tipo, descripcion general responble y ubicación.	X		**Justificacion:** Solo si se conoce el inventario de activos se puede establecer su criticidad, vulnerabilidades y nivel de riesgo, ahora el tener un propietario claro facilita el manejo de los activos. Esto facilita la aplicacion del control de uso y devolucion de los activos **Avidencia:** Procedimiento de control de activos
A8.1.2	Propiedad de los activos	Control: a cada activo se le debe asignar en el inventario tanto los al como los autorizados a que pueden acceder al mismo	X		
A8.1.3	Uso aceptable de los activos	Control: Establecer normas de uso de equipos y software que delimiten y fciliten el uso de los mismos	X		
A8.1.4	Devolución de activos	Control: tanto para empleados como contratistas para gestionar el cierre se su contrato y pago de liquidaciones y saldos de contrato se debe presentar paz y salvo con respecto a activos a sua cargo resistrados en el inventario (tanto fisicos, como logicos, en los cuales se debe entregar claves de acceso)	X		
A8.2	Clasificación de la información		Aplica		Justificación /Evidencia
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.			si	no	
A8.2.1	Clasificación de la información	Control: Definir procedimiento para La clasificación de la información teniendo e en cuenta como parametros los requisitos legales, valor, criticidad en caso de su divulgación.	X		**Justificación:** Este grupo de controles aplica debido a que si bien toda la información requiere cuidado, no se cuentan siempre con recursos suficientes, por lo que es necesario su clasificacion, etiquetado y definicion de procedimiento para su manejo **Evidencia:** Procedimientode clasificación de información
A8.2.2	Etiquetado de la información	Control: definir procedimiento para el etiquetado de la información, de acuerdo con el esquema de clasificación definido en el control Anterior (A.8.2.1)	X		
A8.2.3	Manejo de activos	Control: Basados en la clasificación de numeral A.8.2.1 definir procedimiento para el manejo de activos.	X		

Fuente: Anexo A, ISO 27001:2013

Cuadro Declaración de aplicabilidad (continuación)

A8.3	Manejo de medios		Aplica		Justificación /Evidencia
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios			si	no	
A8.3.1	Gestión de medio removibles	Control: definir procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación de activos establecido y a los roles y responsabilidades.	X		**Justificación:** La organización cuenta con medios removiles debido que deben tener un control establecido ya que la perdida de los mismos puede afectar la confidencialidad de la informacion interna y de clientes **Evidencia:** Politica de seguridad
A8.3.2	Disposición de los medios	Control: EL procedimiento de gestion de medios removibles debe incluir el protocolo a segur para dar disposicion final a dichos medios	X		
A8.3.3	Transferencia de medios físicos	Control: Implementar mecanismo de proteccion a discos duros de portatilesa traves de encripcion desde el antivirus	X		
A9	CONTROL DE ACCESO		Aplica		Justificación /Evidencia
A9.1	Requisitos del negocio para el control de acceso				
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.			si	no	
A9.1.1	Política de control de acceso	Control: documentar y divulgar una política de control de acceso que se ajuste a los requisitos del negocio y a las condiciones de clasificacion de la información	X		**Justificación:** Requerido para asegurar el debido control en el acceso a los activos de QWERTY SAS y alos lugares donde se procesan datos. **Evidencia:** Politica de control de acceso
A9.1.2	Acceso a redes y a servicios en red	Control: definir el la politica de accesos la forma de asignación de permisos y como gestionar las autorizaciones de ingreso.	X		**Justificación:** Para dar cumplimiento a la politica de acceso es necesario implementar los controles de acceso. **Evidencia:** Politica de seguridad de la información
A9.2	Gestión de acceso de usuarios		Aplica		Justificación /Evidencia
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.			si	no	
A9.2.1	Registro y cancelación del registro de usuarios	Control: Documetar e implementar procedimiento para definir el formato y como tramitar la solicitud y cancelación de derechos de acceso a los aplicativos.	X		**Justificación:** La asignacion de usuarios y claves es el mecanismo usual para dar el acceso a la información que se requiere para dearrollar una labor y a su vez restringir el acceso y/o modificacion de aquella que forma parte de un sistema de información y que ya sea por su clasificación o por segregación de funciones no puede ser expuesta. **Evidencia:** Procedimiento de gestion de claves y acceso
A9.2.2	Suministro de acceso de usuarios	Control: Establcer en el procedimiento del control A.9.2.2, tiempos, mecanismos y repsonsables de la asignacipon de permisos	X		
A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	X		
A9.2.4	Gestión de información de autenticación secreta de usuarios	Control: establecer el mecanismo de entrega de usuarios y claves asegurando la confidencialidad de la misma en el proceso de entrega.	X		
A9.2.5	Revisión de los derechos de acceso de usuarios	Control: establecer plan de auditoria de los derechos de acceso asignados vs los autorizados periodicamente	x		
A9.2.6	Retiro o ajuste de los derechos de acceso	Control: establecer en procedimiento de gestion de recurso humano y la validación de cancelación de permisos tanto a aplicativos como el acceso fisico. Para contratos de servicio establecer acuerdo acuerdo de cancelacio de permisos de acceso al terminar la prestacion del servicio.	X		

Fuente: Anexo A, ISO 27001:2013

Cuadro Declaración de aplicabilidad (continuación)

A9.3	Responsabilidades de los usuarios		Aplica		Justificación /Evidencia
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información			si	no	
A9.3.1	Uso de información de autenticación secreta	Control: Definir sanciones laborales frente al incumplimiento del Procedimiento de gestion de claves y acceso	X		**Justificación:** este control es requerido proque fortalece los controles de la seccion A9.2 **Evidencia:** Procedimiento de gestion de claves y acceso
A9.4	Control de acceso a sistemas y aplicaciones		Aplica		Justificación /Evidencia
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.			si	no	
A9.4.1	Restricción de acceso a la información	Control: definir roles y nivel de acceso que debe ser documentado y debidamente autorizado por los propietarios de la información	X		**Justificación:** Este grupo de controles va mas alla de la gestion claves y contraseñas del numeral a9.2, incluyendo la regulación del uso de utilitarios, y el manejo de codigos fuente. **Evidencia:** politica de seguridad de la información
A9.4.2	Procedimiento de ingreso seguro	Control: definir procedimiento y publicar el Procedimiento de gestion de claves y acceso.	X		
A9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben	X		
A9.4.4	Uso de programas utilitarios privilegiados	Control: Definir responsables y eventos en los que esta permitido el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	X		
A9.4.5	Control de acceso a códigos fuente de programas	Control: Definir pefiles que pueden tener el acceso a los códigos fuente de los desarrollos propios y los tipos de acceso que pueden tener a estos.	X		
A10	CRIPTOGRAFIA		Aplica		Justificación /Evidencia
A10.1	Controles criptográficos				
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la			si	no	
A10.1.1	Política sobre el uso de controles criptográficos	Control: política sobre el uso de controles criptográficos para la protección de la información.		X	No aplica porque no se usan estos controles en el sistema de la empresa QWERTY
A10.1.2	Gestión de llaves	Control: Política sobre el uso, protección y tiempo de vida de las llaves criptográficas.		X	No aplica porque no se manejan codigo encriptados en la empresa QWERTY
A11	SEGURIDAD FISICA Y DEL ENTORNO		Aplica		Justificación /Evidencia
A11.1	Áreas seguras				
Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la			si	no	
A11.1.1	Perímetro de seguridad física	Control: Establecer anillos de seguridad fisica para proteger zonas que contengan información confidencial o activos criticos como centro de cableado, centro de servidores	x		**Justificación:** Buen parte de la seguridad de la información radica en contar con restricciones de acceso adecuadas y evitar exponer equipos de procesamiento criticos a personas no autorizadas y su conservación ante situaciones provocadas por fenomenos natirales. **Evidencia:** Politica de control de acceso y plan de continuidad
A11.1.2	Controles de acceso físicos	Control: Implementar control de acceso fisico para las áreas seguras con control electronico	x		
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	x		
A11.1.4	Protección contra amenazas externas y ambientales.	Control: establcer contingencia protección física contra desastres naturales, ataques maliciosos o accidentes.			
A11.1.5	Trabajo en áreas seguras.	Control: Establecer y aplicar procedimientos con las normas para trabajo en áreas seguras.	x		
A11.1.6	Áreas de carga, despacho y acceso público	Control: Implemnetar control y registro de acceso en puntos de acceso publico	x		

Fuente Anexo A ISO 27001: 2013

Cuadro Declaración de aplicabilidad (continuación)

A11.2	Equipos		Aplica		Justificación /Evidencia
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.			si	no	
A11.2.1	Ubicación y protección de los equipos	Control: mantener equipos servdores en areas restingidas y con control de acceso apropiado	x		**Justificación:** Como bien lo indica el objetivo con estos se previene perdida,da;o o compromiso de activos, teniendo en cuenta que hoy en dia la información no solo esta en los servidores , sino tambien hay una sere de información no necesariamente estructurada en los equipos de usuario final y que desde alli se puede tener acceso a información privilegiada. por lo que se importante asegurar durante el ciclo de vida de una equipo de sus dispotivos el adecuado manejo. **Evidencia:** politica de seguridad de la información
A11.2.2	Servicios de suministro	Control: Implementar cotingencia para fluido electrico y asegurar su mantenimiento Implementar contingencia para canal de acceso a internet	x		
A11.2.3	Seguridad en el cableado.	Control: proteger contra interceptación, interferencia o daño el cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información.	x		
A11.2.4	Mantenimiento de los equipos.	Control: establecer y ejecutar plan para mantenimiento preventivo de equipos de computo y perifericos anual	x		
A11.2.5	Retiro de activos	Control: Establecer procedimiento para autorización de retiro de equipos computo de las instalaciones.	x		
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	x		
A11.2.7	Disposición segura o reutilización de equipos	Control: establecer lista de chequeo de los pasos a seguir cuando se reasigna un equipo o cuando se hace disposicion final	x		
A11.2.8	Equipos de usuario desatendido	Control: implementar directiva desde el directorio activo bloquear equipo por inactividad .	x		
A11.2.9	Política de escritorio limpio y pantalla limpia	Control: implementar politica de escritorio limpio y determinar frecuencia de auditoria de su cumplimiento	x		
A12	SEGURIDAD DE LAS OPERACIONES		Aplica		Justificación /Evidencia
A12.1	Procedimientos operacionales y responsabilidades				
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de			si	no	
A12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	x		**Justificación:** este grupo de controles permite asegurar que se realiza monitoreo de uso de los recursos y asu vez cambios bajo condiciones de control. **Evidencia:** Procedimiento de control de cambios.
A12.1.2	Gestión de cambios	Control: Definir procedimienro con responsables y protocolo a seguir en la implementación y documentación de cambios.	x		
A12.1.3	Gestión de capacidad	Control: Implementar Herramienta para monitoreo de recursos que permitan identificar cambios de cosumo de forma oportuna y predecir cambios para capacidades futuras.	x		
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Definir e implmentar ambiente de prueba para desarrollo y modificaciones de software.	x		

Fuente Anexo ISO 27001:2013

Cuadro Declaración de aplicabilidad (continuación)

A12.7	Consideraciones sobre auditorias de sistemas de información		Aplica		Justificación /Evidencia
Objetivo: Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos			si	no	
A12.7.1	Controles de auditorías de sistemas de información	Control: Definir plan anual de auditorias, que incluya definicion de requisitos, recursos, cronograma y alcance de cada evaluación.	x		**Justificación:** Una forma de saber si los controles estan bien implementados y si son efectivos es mediante la verficación, por lo que es necesaria sin que esto no afecte el comportamiento general del sistema. **Evidencia:** Procedimiento para Planificacion de auditoria del sistema
A13	SEGURIDAD DE LAS COMUNICACIONES		Aplica		Justificación /Evidencia
A13.1	Gestión de la seguridad de las redes				
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.			si	no	
A13.1.1	Controles de redes	Control: Definir e implementar herramienta para monitoreo de redes	x		**Justificación:** Este grupo de controles inlcuye tres elementos fundamentales en cualquier gestión que son: Ordenamiento, control y comunicación para asegurar su cumplimiento.
A13.1.2	Seguridad de los servicios de red	Control: Definir y documentar los acuerdos de nivel de servicio con tiempos, responsables, datos de contacto y niveles de escalamiento tanto interno como externo.	x		
A13.1.3	Separación en las redes	Control: Implementar el uso de VLANs, para separar servicios en las REDES	x		
A13.2	Transferencia de información		Aplica		Justificación /Evidencia
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.			si	no	
A13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	x		**Justificación:**Una de las vulnerabilidades que puede ser aprovechada en cualquier sistema

Fuente: Anexo A. ISO 27001:2013

Cuadro Declaración de aplicabilidad (continuación)

A14	Adquisición, desarrollo y mantenimiento de sistemas		Aplica		
A14.1	Requisitos de seguridad de los sistemas de información				
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes .			si	no	Justificación /Evidencia
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Establecer directriz de elementos de segurida a tener en cuenta en nuevos requerimientos de la información en los nuevos proyectos que inv tecnologia.	x		**Justificación:** En La planeación del desarrollo de software es fundamental asegurar que se cuentan con todos los elementos para que su arquitectura se consistente y posteriormente soporte el cumplimiento de todos los requisistos, es por eso que se deben tener en cuenta desde la definicion de requisitos las condiciones de seguridad.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: establecer requisitos en manejo de información para los servicios contratados sobre redes públicas	x		
A.14.1.3	Protección de transaccciones de los servicios de las aplicaciones.	Control: establecer mecanismos para encripción de datos trasmitidos en redes publicas.	x		
A14.2	Seguridad en los procesos de Desarrollo y de Soporte		Aplica		
Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.			si	no	Justificación /Evidencia
A.14.2.1	Política de desarrollo seguro	Control: definir instructivo con requierimientos de seguridad atener en cuente en desarrollo y pruebas de los mismos.	x		**Justificacion:** Como en todo proceso se requieren la definicion de pautas minimas para el desarrollo apropiado, en este caso el desarrollo de software de debe ser contemplado desde su defincion, fabricacion hasta su puesta en marcha contemplando tanto las pruebas como el control de cmabios ya mencionado en controles anteriores. Se debe tener en cuenta que es atraves de los aplicativos es que los usuarios tienen contacto con los datos y al vez es en donde se pueden implementar las restricciones que se tenga definidas en el control de acceso de los mismos. La organizacion cuenta con un area dentro de la dependencia de sistemas encargada del desarrollo de aplicaciones. **Evidencia:** procedimiento de desarrollo de aplicaciones
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Establcer procedimiento para registro aprobación y liberacion de cambios en desarrollo de software.	x		
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Definir listas de chequeo para validación de cambios en aplicaciones y herramientas de tecnolgia en general y establecer forma de prueba, responsable y casos de uso a revisar.	x		
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control:establecer criterios para revision y acepatación de cambios en las herramientas de software.	x		
A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Control: Se deben establecer, documentar y mantener principios para la construcción e implemnetacion de sistemas de información bajo condiciones de seguridad adecuados.	x		
A.14.2.6	Ambiente de desarrollo seguro	Control: Definir ambiente con derechos de acceso especiales para fuentes, bases dedatos y doucmentacion tecnica de requerimiento y resultados de pruebas.	x		
A.14.2.7	Desarrollo contratado externamente	Control: Establecer instructivo para definir mecanismos de planificación, prueba, implementación y seguimiento de software contratado, asi como mecanismo para transferencia de conocimiento	x		
A.14.2.8	Pruebas de seguridad de sistemas	Control: definir tanto lista de chequeo como casos de prueba en relación con las seguridad de herramientas de software.	x		
A.14.2.9	Prueba de aceptación de sistemas	Control: Definir tanto lista de chequeo e instructivo para pruebas de aceptación como casos de prueba de herramientas de software.	x		

Fuente: Anexo A. ISO 27001:2013

Cuadro Declaración de aplicabilidad (continuación)

A14.2	Seguridad en los procesos de Desarrollo y de Soporte		Aplica		Justificación /Evidencia
Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.			si	no	
A.14.2.1	Política de desarrollo seguro	Control: definir instructivo con requierimientos de seguridad atener en cuente en desarrollo y pruebas de los mismos.	x		**Justificacion:** Como en todo proceso se requieren la definicion de pautas minimas para el desarrollo apropiado, en este caso el desarrollo de software de debe ser contemplado desde su defincion, fabricacion hasta su puesta en marcha contemplando tanto las pruebas como el control de cmabios ya mencionado en controles anteriores. Se debe tener en cuenta que es atraves de los aplicativos es que los usuarios tienen contacto con los datos y al vez es en donde se pueden implementar las restricciones que se tenga definidas en el control de acceso de los mismos. La organizacion cuenta con un area dentro de la dependencia de sistemas encargada del desarrollo de aplicaciones. **Evidencia:** procedimiento de desarrollo de aplicaciones
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Establcer procedimiento para registro aprobación y liberacion de cambios en desarrollo de software.	x		
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Definir listas de chequeo para validación de cambios en aplicaciones y herramientas de tecnolgia en general y establecer forma de prueba, responsable y casos de uso a revisar.	x		
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control:establecer criterios para revision y acepatación de cambios en las herramientas de software.	x		
A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Control: Se deben establecer, documentar y mantener principios para la construcción e implemnetacion de sistemas de información bajo condiciones de seguridad adecuados.	x		
A.14.2.6	Ambiente de desarrollo seguro	Control: Definir ambiente con derechos de acceso especiales para fuentes, bases dedatos y doucmentacion tecnica de requerimiento y resultados de pruebas.	x		
A.14.2.7	Desarrollo contratado externamente	Control: Establecer instructivo para definir mecanismos de planificación, prueba, implementación y seguimiento de software contratado, asi como mecanismo para transferencia de conocimiento	x		
A.14.2.8	Pruebas de seguridad de sistemas	Control: definir tanto lista de chequeo como casos de prueba en relación con las seguridad de herramientas de software.	x		
A.14.2.9	Prueba de aceptación de sistemas	Control: Definir tanto lista de chequeo e instructivo para pruebas de aceptación como casos de prueba de herramientas de software.	x		
A14.3	Datos de prueba		Aplica		Justificación /Evidencia
Objetivo: Asegurar la protección de los datos usados para pruebas.			si	no	
A.14.3.1	Protección de datos de prueba	Control:Los datos de prueba se deben seleccionar, proteger y controlar bajo derechos de acceso solo a quienes realizar el rol de tester de sofwware.	x		**Justificación:** Teniendo en cuenta que se desarrolla software propio es necesario darle manejo adecuado a los datos utilizados para sus pruebas
A15	RELACIONES CON LOS PROVEEDORES		Aplica		Justificación /Evidencia
A15.1	Seguridad de la información en las relaciones con los proveedores.				
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.			si	no	
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Definir e implementar politica para Los requisitos de seguridad de la información para proveedores, asegurando manejo confidencial de la información.	x		**justificacion:** Estos controls son el mecanismo para segurar que la información que se entrega a terceros para que puedan desarrollar su labor adecuadamente sea custodiada de la forma correcta y que los medios contratados , tanto productos como servicios cuentan con el respaldo necesario para el manejo adecuado de la información **evidencia:**Politica de seguridad para proveedores
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: realizar estudio de seguridad a proveedores, e incluir en los acuerdos de confidencialidad para manejo de la información. Establecer reglas minimas de manejo de información.	x		
A15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	x		

Fuente: ISO IEC 27001:2013, Anexo A.

Cuadro Declaración de aplicabilidad (continuación)

A15.2	Gestión de la prestación de servicios de proveedores		Aplica		Justificación /Evidencia
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores			si	no	
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Establecer plan de auditoria y lista de chequeo para asegurar revision de servicios prestados por proveedores.	x		**justficacion:**Estos dos controles aplican porque son complementarios a los controles A15.1, ya que permiten asegurar tanto seguimiento como el cierre del proceso de la prestacion de servicios de tecnologia
A15.2.2	Gestión del cambio en los servicios de los proveedores	Control: Establcer procedimiento para registro aprobación y liberacion de cambios en servicios de proveedores	x		
A16	GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION		Aplica		Justificación /Evidencia
A16.1	Gestión de incidentes y mejoras en la seguridad de la información				
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y			si	no	
A16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	x		**Justificación:** para asegurar tanto el adecuado manejo para minimizar el impacto de un incidente como la recolección de información para asegurar su valoracion que permita tomar acciones de fondo es necesario asegurar que se cuenta con un procedimiento apropiado que establezca tanto responsabilidades como los mecanismos para reporte, evlauacion y repuesta. **Evidencia:** Procedimiento de gestion de inicdentes
A16.1.2	Reporte de eventos de seguridad de la información	Control: establecer y divulgar los canales de la que se deben utilizadps para comunicar incidentes o eventos que puedan afectar la seguridad.	x		
A16.1.3	Reporte de debilidades de seguridad de la información	Control: socializar la importancia y establecer compromiso de usuarios para que comuniquen incidentes	x		
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: establcer paramtros de clasificacion de incidentes y definir formato de registro. Definir acciones inmediatas según su clasificación.	x		
A16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	x		
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: establecer periodicidad y metodo de revsion de incidentes de seguridad para establecer accion medianta analisis de causa Raiz	x		
A16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	x		
A17 Aspectos de seguridad de la información y gestion de la continuidad de negocio			Aplica		Justificación /Evidencia
A17.1	Continuidad de Seguridad de la información				
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.			si	no	
A17.1.1	Planificación de la continuidad de la seguridad de la información	Control: definir lista de chequeo de controles que se deben mantener activos aun en caso de habilitación de contingencia.	x		**Justificacion:** Estos controles aplican y se deben soportar con un plan que Asegure la continuidad del negocio apropiado a sus necesidades, debido a que sin importan los controles que se implementen pueden existir sistuaciones como condiciones medio ambientales o desastres naturales poco predecibles pero probables,
A17.1.2	Implementación de la continuidad de la seguridad de la información	Control: Definir plan de continuidad de operacion de los sistemas de información para servicios de mision critica estableciendo protolocolo tanto de habilitacion de la contingencia como mecanismos para retorno al ambiente normal.	x		
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: establecer plan de auditoria interna intervalos trimestralmentes para validar el cumplimientos de controles de la seguridad y su eficacia. Realizar pruebas de las contingencias establecidas para asegurar su cumplimiento	x		

Fuente: ISO IEC 27001:2013, Anexo A.

Cuadro Declaración de aplicabilidad (continuación)

A17.2	Redundancias		Aplica		Justificación /Evidencia
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de			si	no	
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control: impelmentar redundancia para Las instalaciones de procesamientos de información con prioridad en los servicios criticos	x		**justificacion:** para asegurar alta disponibilidad es necesario establecer contingecia para equipos de mision critica.
A18	CUMPLIMIENTO		Aplica		Justificación /Evidencia
A18.1	Cumplimiento de requisitos legales y contractuales				
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.			si	no	
A18.1.1	Identificación de la legislación aplicable.	Control: Documentar matriz de requisitos legales vigentes , establcer responsables de cumplimiento de requisito, entidad encargada de su validacion	x		**justificación:** El cumplimiento de requisitos legales y contractuales es un tema que a en ocasiones no se la da improtancia que merece sin tener en cuenta que esto puede generar dificultades a nivel de reputación y multas que pueden causar mas daño que la misma perdida de información. **evidencia:** politica de seguridad de la informacion
A18.1.2	Derechos propiedad intelectual (DPI)	Control: implementar procedimientos para asegurar el cumplimiento de los requisitos relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. Restringir permisos para instalacion de software.	x		
A18.1.3	Protección de registros	Control: Establcer los procedimientos requeridos para cumpli requisitos de ley y contractuales relacionados con perdida, destrucción, falsificación o acceso no autorizado.	x		
A18.1.4	Privacidad y protección de información de datos personales	Control: definir procedimiento para dar cumplimiento a la ley de proteccion de datos personales.	x		
A18.1.5	Reglamentación de controles criptográficos.	Control: Usar controles criptográficos solicitados por requiaitoa legales actuales o por acuerdos contractuales con clientes o proveedores		x	
A18.2	Revisiones de seguridad de la información		Aplica		Justificación /Evidencia
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.			si	no	
A18.2.1	Revisión independiente de la seguridad de la información	Control: Establecer plan de auditoria de cumplimiento de procedimientos, instructivos y politicas definidos para mantener la seguridad de la información	x		**Justificación:** Una forma de saber si los controles estan bien implementados y si son efectivos es mediante la verficación, por lo que es necesaria sin que esto no afecte el comportamiento general del sistema. **Evidencia:** Procedimiento para Planificacion de auditoria del sistema
A18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Realizar revision gerencial de forma peridica del cumplimiento de procedimientos de información dentro de cada area con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	x		
A18.2.3	Revisión del cumplimiento técnico	Control: Establecer plan de auditoria de cumplimiento de procedimientos, instructivos y politicas definidos para mantener que se mantiene el cumplimiento tecnico.	x		

Fuente: ISO IEC 27001:2013, Anexo A.

9.3 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

9.3.1 ALCANCE

Aplica a todas las dependencias de la empresa QWERTY SAS y sus procesos internos sus recursos a la totalidad de procesos internos y tercerizados vinculados a través de acuerdos o contratos y todo el personal con contratación directa que utilicen o afectan las condiciones de calidad de la información.

9.3.2 OBJETIVOS

1. Proteger tanto la información de la empresa QWERTY SAS, como los activos utilizados para su procesamiento, almacenamiento y acceso con el fin de asegurar que la información se mantiene íntegra, disponible y es confiable.
2. Definir las directrices de la empresa QWERTY SAS para el análisis y evaluación de riesgos de seguridad de la información.
3. Establecer responsabilidades en la administración de los activos de información.

9.3.3 RESPONSABILIDADES

La junta directiva de la empresa QWERTY SAS dan aprobación a esta política y son los únicos responsables de autorizar cualquier modificación a la misma.

Los propietarios de los activos: Son responsables de establecer y documentar la clasificación de la información y de establecer los permisos de acceso de acuerdo a funciones y competencia de los usuarios de la organización.

El área de soporte es responsable de cumplir las funciones asignadas en los procedimientos que dan soporte a la política de seguridad como son la administración de usuarios, actividades operativas asignadas en el SGSI.

El área de infraestructura debe garantizar el cumplimiento de los procedimientos que dan soporte a la implementación de controles de la infraestructura que incluye equipos, redes, cableado, equipos activos y su configuración.

El área de desarrollo debe garantizar la ejecución de prácticas seguras de desarrollo de software y seguir las pautas establecidas para el control de cambios.

Los usuarios de la información son responsables de conocer y cumplir las normas establecidas para mantener la información vigente en cuanto a Manejo de usuario y contraseñas, Uso adecuado de los activos y acatar las normas establecidas para asegurar la confidencialidad de la información a la que tiene acceso.

Jefe dependencia de Nómina tiene como responsabilidad Notificar a todo empleado que se vincula a la empresa QWERTY SAS la política de seguridad de la información, suscribir los acuerdos de confidencialidad, desarrollar plan de

capacitación continua a cerca de la seguridad y asegurar que se cumplan de los procedimientos de selección y desvinculación definidos en el SGSI.

Jefe de compras Hacer la divulgación de la política de seguridad para proveedores, Suscribir los acuerdos de confidencialidad con proveedores que requieren información de QWERTY SAS para realizar la actividad para la que son contratados.

El gestor de Proyectos con comunidades debe seguir las buenas prácticas de seguridad de la información en la definición e implementación de proyectos para las comunidades.

9.3.4 SISTEMA OPERATIVO Y APLICACIONES

1. Es responsabilidad del área de soporte:
    1. Mantener actualizados los sistemas operativos de los equipos, asegurando que en la medida que estos pierdan soporte del fabricante se debe planificar y asegurar la renovación con la debida anticipación.
    2. Asegurar que los usuarios no tienen permisos de administrador del equipo que les permita instalar software o cambiar parámetros del sistema

2. Es responsabilidad de los usuarios atender las siguientes obligaciones:

    1. No Instale Software desconocido sin la aprobación de dependencia de sistemas.
    2. No cambie los parámetros del sistema operativo sin el visto bueno de la dependencia de tecnología.
    3. Todo software, paquete, programa, aplicación que se instale en la compañía por cuenta propia y cause errores en el sistema, será responsabilidad del usuario.
    4. Si se presentan comportamientos inusuales en sus archivos o en las memorias USB o en el equipo de cómputo asignado debe informar al área de soporte para su análisis y diagnóstico.

9.3.5 CONTROL DE ACCESO

El acceso a la infraestructura de QWERTY SAS para personal externo debe ser autorizado al menos por un director de QWERTY SAS, quien deberá notificarlo a la Dirección de la dependencia de sistema quien cuenta con la discreción para autorizar su habilitación.
Todo el personal es responsable del IDusuario y contraseña asignada para el uso y acceso, el cual es único e intransferible, por lo que está prohibido compartirlo con otras personas

Está prohibido proporcionar información a personal externo, de los mecanismos de control de acceso de QWERTY SAS

La utilización de dispositivos extraíbles para almacenamiento de información (memorias USB, CD R/RW, DVD R/RW, discos duros extraíbles.) debe ser autorizada por el director y supervisada por la Dirección de Tecnología.

9.3.6 DISPOSITIVOS REMOVIBLES

Los puertos USB de los equipos de la compañía están restringidos para los usuarios y sólo serán habilitados con la debida justificación de la necesidad de su uso, en cuyo caso se deben atender las siguientes indicaciones:

No abrir Memorias USB en el equipo sin examinar con el antivirus.

Evite conectar memorias USB de personas ajenas a la compañía sin antes consultar con el área de soporte para evitar propagación de virus por este medio.

No conecte dispositivos diferentes a los autorizados por la dependencia de sistemas y para los que fueron habilitados los puertos USB a los equipos bajo su responsabilidad.

9.4 MANTENIMIENTO Y DESARROLLO DE APLICACIONES

9.4.1 OBJETIVO

Definir y ejecutar tareas con el propósito de brindar a los usuarios a través del Software herramientas de trabajo funcionales que garanticen, automaticen y agilicen la operatividad de sus labores.

9.4.2 ALCANCE Y RESPONSABLES

Este procedimiento inicia desde la solicitud de mantenimiento y/o creación de aplicaciones de software hasta su implementación y seguimiento.

- **Director Dependencia de Sistemas**

Responsable de evaluar la posibilidad del mantenimiento y desarrollo del software dado el requerimiento de las áreas de la organización, Generar planes de trabajo, revisar su ejecución y generar acciones para su cumplimiento. Validar cumplimiento de cronogramas y definir prioridades en actividades de desarrollo.

- **Ingeniero de desarrollo**

Responsable del mantenimiento del Software, es decir, de escribir código fuente, realizar pruebas de escritorio y generar los archivos ejecutables. Reportar cronograma y seguimiento de actividades a la dirección de sistemas, realizar la

actividad de codificación de software observando las condiciones de seguridad de la información.

- **Analista Tester**

Encargado de definir y ejecutar pruebas funcionalidad y de seguridad de las aplicaciones desarrolladas a partir del requerimiento de desarrollo y la lista de chequeo definida para validar la seguridad de las aplicaciones.

9.4.5 DEFINICIONES

Software: Es un conjunto de instrucciones compiladas que dependiendo de la secuencia de las mismas y los parámetros ingresados procesa datos para generar un resultado, son utilizados para simplificar procesamiento de información. En esta clasificación encontramos los sistemas operativos, utilitarios, antivirus, aplicaciones específicas, ERP, malware, virus troyanos y toda suerte de elementos que pueden alterar los datos.

Programas Fuente: Para el caso de QWERTY SAS todo el Software Operativo a excepción de la Nómina, la Contabilidad y los inventarios, son desarrollos propios, es decir los aplicativos son escritos y mantenidos por personal de QWERTY SAS. Las fuentes, son archivos escritos en un lenguaje de programación que contienen toda la funcionalidad de los aplicativos.

9.4.6 GENERALIDADES

Solicitudes

En términos generales los usuarios generan una necesidad de mantenimiento o desarrollo de nuevas aplicaciones de Software que puede convertirse en una corrección puntual de un ejecutable, la modificación de un listado o reporte, un nuevo reporte, una nueva opción dentro del sistema, un módulo nuevo, una nueva funcionalidad y hasta un nuevo aplicativo. Estas necesidades se generan a través de un e-mail o una solicitud escrita.

Las solicitudes de desarrollo deben contener como mínimo la siguiente información: Alcance, Propósito, descripción detallada de la funcionalidad, Usuarios y permisos sobre la funcionalidad, Definición de términos que requieran explicación para facilitar el entendimiento de la descripción Funcional.

Arquitectura de la solución y Desarrollo

A partir de la solicitud aprobada por el director de sistemas El ingeniero de desarrollo debe definir y documentar diseño de la solución teniendo en cuenta: Funcionalidad, capacidades de los recursos de procesamiento y condiciones de seguridad de la

información, en caso de estimar que los recursos de procesamiento no son suficientes debe informar a la dirección de sistemas antes de continuar con el desarrollo.

Una vez presentado el diseño y aprobado por la dirección de sistemas se debe proceder con la codificación del aplicativo.

Pruebas de Desarrollo

A partir del requerimiento del usuario y del diseño definido por el Ing de desarrollo el Tester debe construir la lista de chequeo para las pruebas de funcionalidad, con respecto a las pruebas de seguridad de la aplicación debe aplicar la lista de chequeo de seguridad de las aplicaciones definidas para esta validación

Ambiente de Pruebas

Para la realización de las pruebas se cuenta con una base de datos que debe contener la información necesaria para realizar las pruebas del software, los ingenieros de desarrollo deben entregar los scripts para la creación de objetos a que haya lugar y el Tester debe probar que estos funcionen correctamente y a partir de los objetos generados realizar la aplicación de las pruebas.

Todo software desarrollado de forma externa debe pasar por el mismo procedimiento de pruebas a cargo del Tester antes de su aceptación y despliegue en producción.

Custodia Archivos Fuente

Solamente los ingenieros de desarrollo tienen acceso para modificación de los archivos fuente, de los cuales se debe realizar copia de seguridad a diario por parte del área de soporte.

9.5 POLÍTICA DE SEGURIDAD PARA PROVEEDORES.

9.5.1 ALCANCE

Esta política aplica a todas las actividades realizadas por quien preste servicios como proveedor a QWERTY SAS, independientemente del tipo de servicio que preste.

9.5.2 OBJETIVO

Establecer las directrices frente a la seguridad de la información aplicable a Proveedores de la Empresa QWERTY SAS, para evitar la pérdida o usos indebidos de información que como consecuencia pueda dañar la reputación de la organización o afectar su funcionamiento.

9.5.3 PRESTACIÓN DEL SERVICIO

Todo proveedor, ya sea persona natural o jurídica, que realice labores para QWERTY SAS debe cumplir con las normas establecidas en este documento.

Los proveedores deben asegurar que todo su personal tiene la formación y capacitación apropiada para el desarrollo del servicio prestado, tanto para lo que fue contratado como en el manejo confidencial de la información que se le entrega para realizar su labor y es su responsabilidad garantizar que siguen las directrices definidas para gestión de usuarios y contraseñas de la política de seguridad informática de QWEERTY SAS.

Es responsabilidad del proveedor informar cualquier cambio en el personal de su organización que afecte el servicio que presta a QWEERTY SAS

9.5.4 CONFIDENCIALIDAD DE LA INFORMACIÓN

La información de QWERTY SAS se debe considerar por defecto, tiene el carácter de confidencial, con excepción de aquella que se encuentra en medios masivos de difusión, o que expresamente así lo defina QWERTY SAS.

Salvo autorización expresa de QWWERTY SAS los proveedores deben mantener confidencialidad de la información a la que tiene acceso de forma indefinida.

Cuando se trate de datos personales, los proveedores sólo tendrán acceso datos necesarios para el desempeño de su labor, de los cuales se debe asegurar que se guarda la debida confidencialidad y una vez terminada la labor deben devolver los archivos y destruir cualquier medio lógico de la misma que tengan en su poder.

En el tratamiento de datos de carácter personal fuera de las instalaciones de QWERTY SAS, debe garantizarse por parte del proveedor el nivel de seguridad apropiado al tipo de archivo.

9.5.5 PROPIEDAD INTELECTUAL

Para garantizar el cumplimiento de las normas de propiedad intelectual está estrictamente prohibido el uso de software en los sistemas de información de QWERTY SAS sin la correspondiente licencia.

9.5.6 INTERCAMBIO DE INFORMACIÓN

En el intercambio (Transmisión o recepción) de información entre las partes, se considerarán no autorizadas los siguientes tipos de archivos y por lo tanto generan sanciones a los proveedores que las permitan en su personal:

- Material protegido por las leyes de Protección Intelectual sin la debida autorización.
- Material pornográfico.
- Envío de archivos a terceras partes de información de la organización sin la debida autorización de QWERTY SAS
- Archivos que atentan contra la normativa de protección de datos personales.

- Software o aplicativos no relacionados con el negocio.

9.5.7 **UTILIZACIÓN DE LOS RECURSOS**

Los recursos que QWERTY SAS pone a disposición del proveedor deben ser utilizados exclusivamente para el cumplimiento de las obligaciones para la que le fueron proporcionados, estos recursos son objeto de auditoria y se aplicaran los mecanismos de control que se requieran para validar su utilización dentro de lo acordado.

Para que un equipo de cómputo del proveedor sea conectado a la red de QWERTY SAS deberán estar homologados (sistemas operativos, Antivirus), debidamente licenciados y le aplican las políticas de restricción de navegación a través del servicio de internet de la Organización

Está prohibido introducir voluntariamente en la red de QWERTY SAS o de sus clientes cualquier tipo de malware.

Se debe registrar en bitácora de acceso fecha, hora identificación y motivo del acceso a las áreas restringidas en las que se realice procesamiento de datos.

Está prohibido distorsionar o falsear tanto la información de QWERTY SAS a la que tienen acceso como los registros de auditoría de los Sistemas de Información de QWERTY SAS.

9.6 GESTIÓN DE CLAVES Y ACCESO

- **Alcance**

  Aplica a todos los medios utilizados por los usuarios para acceder a la información de la organización QWERTY SAS.

- **Objetivos**

  Establecer directrices para el manejo de contraseñas y administración de privilegios para evitar el acceso no autorizado a los sistemas de información de QWERTY SAS.

- **Administración de Privilegios**

  Cada propietario de la información debe establecer los niveles de acceso a la información y basado en esta definición el área de soporte asigna los perfiles a los usuarios asignados.
  Cualquier cambio en las funciones del usuario o de área que implique modificar el perfil del usuario con respecto a las aplicaciones de QWERTY SAS, deberán ser notificados al área de soporte para realizar los cambios respectivos.

  Cuando un empleado se retire de la organización este evento debe ser notificado para la deshabilitar el usuario de Red, Correo y usuario de aplicaciones.

- **Equipo Desatendido**
  Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como password y protectores de pantalla cuando se retiren de su puesto de trabajo.

- **Administración de usuario y password**

  La asignación de permisos será solicitada por el jefe directo del usuario y una vez validado con los niveles de acceso definidos por los propietarios de la información será asignado por el área de soporte.

  Las contraseñas no pueden dejarse de forma legible en cualquier medio impreso y en un lugar donde las personas no autorizadas puedan accederlas.

  Aplicar las siguientes condiciones en la definición de contraseñas por parte de los usuarios

  - Debe estar compuestos de al menos 6 caracteres alfanuméricos
  - No deben ser iguales al usuario
  - Las contraseñas no se deben relacionar con trabajo o la vida personal del usuario
  - No debe ser igual a las tres contraseñas anteriormente definidas.

  No está permitido compartir usuario y contraseña con otros empleados, es único e intransferible, cualquier acción realizada por otros es responsabilidad de quien tiene asignado este usuario y clave.

9.7 Clasificación de información

Alcance

Aplica al 100% de los activos de información para las actividades de identificación, clasificación en función de su confidencialidad y mecanismo de etiquetado.

Los medios en que se encuentra la información objeto de esta clasificación son: Documentos electrónicos, bases de datos, documentos impresos, información verbal.

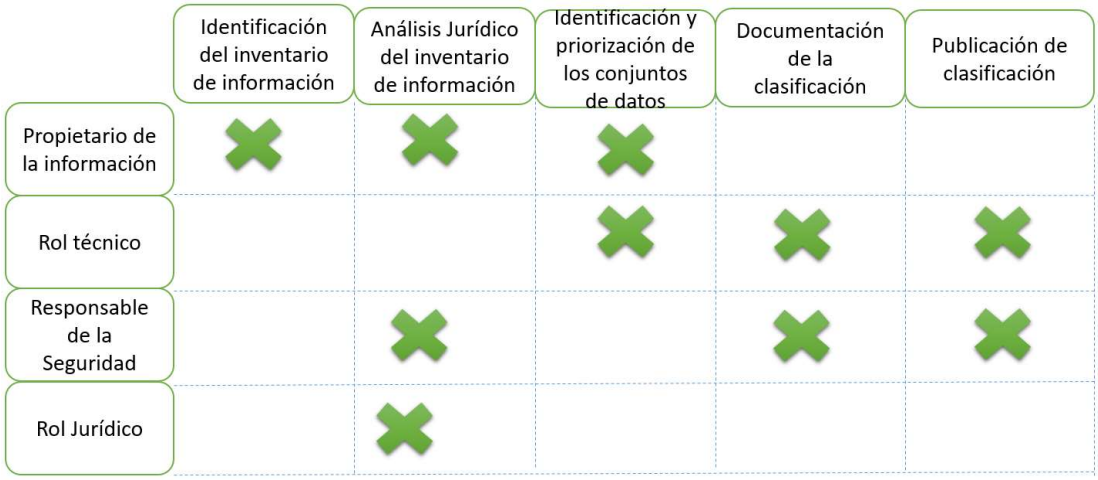
Objetivo

Identificar y clasificar adecuadamente la información de la organización QWERTY SAS, para reducir la afectación negativa de la seguridad de la información por un tratamiento no apropiado.

Roles y responsabilidades

En la siguiente figura se ilustra de manera global los roles frente a las actividades de identificación de la información

Fig. 4 Roles y Responsabilidades



Fuente: Presente Estudio

Identificación de la información:

La revisión del inventario se debe revisar una vez al año, para mantenerlo actualizado. Para el registro de este inventario se debe utilizar el siguiente formato:

Formato Para registro de Inventario

ID	Área	descripción	Tipo	ubicación	Clasificación	criticidad	propietario
			Impreso Electrónico B. datos		Nivel de confidencialidad	Alta Media Baja	

Fuente: Presente Estudio

Clasificación de la información

Para la clasificación de la información de debe tener en cuenta los siguientes niveles de clasificación, que están alineados a lo establecido en la ley 1712 de 2014

Tabla 20 Tipos de información

Tipo	Descripción
Pública Reservada	Disponible solo para un proceso o área de la organización, si es conocidas por terceros puede generar impacto negativo a la reputación de la organización o de tipo legal por condiciones contractuales
Pública Clasificada	Información disponible únicamente los procesos internos, si es conocida por personas externas a la organización puede afectar de forma negativa a los procesos o perder ventajas competitivas del negocio
Pública	Información que puede ser entregada o publicada sin restricciones dentro o fuera de la organización sin que perjudique los procesos, la reputación o la competitividad de la organización
No Clasificada	Activos de información que se deben incluir en el inventario y que aún no han sido clasificados, deben ser tratados como PUBLICA RESERVADA hasta que asigne la clasificación definitiva

Fuente: Presente Estudio

Etiquetado: es el mecanismo utilizado para identificar a que nivel de confidencialidad pertenece la información.

Para el etiquetado de la información se utilizará las siguientes abreviaturas. Para archivos en medios electrónicos se registrará el nombre del archivo con estas iniciales y luego el nombre del archivo separado por un carácter "- ".

Para los documentos impresos se registrará en la margen inferior izquierda las abreviaturas de su clasificación.

En el siguiente cuadro se identifica el tipo de información

Tabla 21 Etiquetado

Tipo	Abreviatura	Ejemplo
Publica Reservada	PR	PR-planestartegico2019.doc
Publica Clasificada	PC	PC-programamantenimientoPreventivo.XLS
Publica	PP	PP-Protafolioservicios.PPT

Fuente: Presente Estudio

La información que no tenga esta identificación se considera como no clasificada y se le dar el tratamiento establecido para dicha información.

Para la información de Base de datos o a la que se tiene acceso a través de aplicativos una vez se tenga identificada la información se debe registrar por parte del propietario los usuarios que tendrán acceso a la información y con qué tipo de permiso mediante el registro de la siguiente Matriz:

Formato para Registro de Permisos de Base de datos

ID	Descripción	Usuario	Consultar	Registrar	Modificar	Eliminar

Fuente: Presente Estudio

9.8 GESTIÓN DE INCIDENTES

Objetivo

Definir el procedimiento para asegurar el reporte, la recopilación y análisis de los incidentes para mantener la mejora continua del sistema de gestión de seguridad de la información de QWERTY SAS.

Alcance

Este procedimiento aplica a todos los empleados que por sus funciones tienen acceso a los sistemas de información de la compañía.

Responsabilidades

Usuarios: Deben reportar toda anomalía o comportamiento fuera de lo normal que identifiquen en el sistema de información.

Área de soporte: Registrar todo evento que sea reportado por los usuarios, tomar las medidas del caso, consolidar y reportar los casos al responsable de seguridad de la información.

Responsable de seguridad: Debe analizar los casos, identificar las vulnerabilidades o causas del incidente y proponer las acciones a seguir.

Desarrollo

Notificación y registro

Se incluirán en el registro de incidentes todas aquellas anomalías reportadas por los usuarios que afecten o puedan afectar a la seguridad de los datos.

Cuando el área de soporte identifique una vulnerabilidad o debilidad en el sistema también debe incluirlo en el reporte de incidentes.

El reporte debe contener como mínimo la siguiente información:

Formato Reporte de incidentes

Fecha de la notificación	
Usuario que hace el reporte	
Descripción detallada del incidente o debilidad	
Fecha y hora en que se presentó el incidente	
Acciones iniciales realizadas	

Fuente: Presente Estudio

Gestión y tratamiento

Con la información recopilada se debe iniciar la identificación de posibles causas y los efectos producidos por la situación presentada.

El responsable de seguridad debe evaluar si la acción inicialmente tomada por soporte es suficiente correctivo o si se deben tomar otras acciones, luego determinar las acciones preventivas para evitar la repetición del incidente o la reducción de la vulnerabilidad.

Una vez tomadas las acciones tanto correctivas como preventivas deben tener seguimiento para determinar su efectividad.

10. MANUAL DE SEGURIDAD DE LA INFORMACIÓN

10.1 OBJETIVOS

- El objetivo del presente documento es establecer los lineamientos para garantizar la confidencialidad, integridad y disponibilidad de la información de QWERTY SAS, entendida esta como un activo de la organización.
- Establecer buenas prácticas para la preservación de la infraestructura tecnológica y normas aplicables a la gestión segura de la misma.
- Garantizar la protección de datos que se encuentran bajo custodia de la organización QWERTY SAS en sus bases de datos.
- Establecer el alcance de SGSI.

10.2 ALCANCE DEL SGSI

Aplica a todas las dependencias de la empresa QWERTY SAS y sus procesos internos sus recursos a la totalidad de procesos internos y tercerizados vinculados a través de acuerdos o contratos y todo el personal con contratación directa que utilicen o afectan las condiciones de calidad de la información.

10.3 MEDIDAS DE SEGURIDAD

Los recursos informáticos, los sistemas de información y en general todas las bases de datos estarán accesibles por las personas asignadas por QWERTY SAS.

Los propietarios de los datos son los responsables de gestionar los permisos de acceso a los usuarios garantizando siempre el principio de segregación de funciones y siguiendo las pautas del procedimiento establecido por QWERTY SAS.

A continuación se enumeran y detallan los lineamientos y medidas de seguridad implementadas por LA organización QWERTY SAS.

10.4 ESTRUCTURA DEL SGSI

En el siguiente gráfico se representan los componentes principales requeridos para asegurar el cumplimiento de los objetivos del sistema de gestión de seguridad, están organizados de forma jerárquica de las instrucciones generales (políticas) a las instrucciones específicas (Procedimientos)

Fig. 5 Estructura sistema de gestión

Fuente : Presente Estudio

Basados en lo anterior se establece entonces que estos 7 elementos dan cobertura al alcance del propuesto para el sistema de la organización QWERTY SAS.

10.5 ENFOQUE DE LA EVALUACIÓN DE RIESGOS

Como punto de partida para poder establecer una adecuada gestión de riesgos es entender que la gestión de actividades para lograr un resultado eficaz debe estar basado en procesos que a partir de entradas genera transformación y resultados que pueden a la vez ser la entrada a otros procesos, el sistema de gestión de seguridad de la información de la empresa QWERTY SAS no es la excepción y por ello es el primer concepto a aplicar a la hora de hacer la evaluación de riesgos.

Como segundo aspecto a tener en cuenta en el enfoque de la evaluación de riesgos está en Identificar los requisitos, valorar los riesgos, realizar el seguimiento para hacerlo sostenible e identificar las oportunidades de mejora de forma periódica.[16]

Por lo anterior la valoración de riesgos para QWERTY SAS tiene basa en identificar, cuantificar y priorizar riesgos basados en criterios de aceptación de riesgos, los objetivos de la organización y deba facilitar la priorización de los riesgos identificados para facilitar la implementación de controles alineados a las necesidades de la organización y a las posibilidades de costos que se pueden asumir.

[16] GOMEZ FERNANDEZ, Luis, FERNANDEZ RIVERO Pedro Pablo. Como implantar un SGSI según UNE – ISO 27001: 2014 y su aplicación en el esquema Nacional de Seguridad, Madrid, Editorial AENOR, 2015

10.6 SEGUIMIENTO

Para asegurar el cumplimiento de las medidas establecidas en el SGIS y evaluar la evolución continua es necesario establecer métricas a las acciones relevantes del sistema. Para ello se define la siguiente plantilla para la definición de los indicadores.

Formato para registro de indicadores

Objetivo		
Métrica		
Indicador		
Frecuencia		
Formula		
Mediciones		
Fecha	**Valor**	**Análisis**

Fuente: Presente Estudio

Objetivo: Corresponde a las características de la información que se deben asegurar, como, por ejemplo: Preservar la integridad de la información.

Métrica: Descripción de la identificación, como número de incidentes de seguridad provocados por virus.

Indicador: Meta o parámetro de comparación.

Frecuencia: Periodicidad con la que se va a tomar.

Formula: Forma de cálculo del indicador, como por ejemplo número de incidentes asociados a perdida de información.

Fecha: Según la frecuencia establecida se registra la fecha de cada toma del dato del indicador.

Valor: resultado del indicador obtenido a partir de la formulación

Análisis: Explicación del resultado y definición de posibles acciones

11. PROPUESTA DE IMPLEMENTACIÓN

Para establecer las medidas de seguridad apropiadas al menor costo posible es necesario entender que el factor humano es el elemento más vulnerable y por lo tanto se convierte en el principal objetivo de los ataques informáticos mediante el uso de la ingeniería social y por lo tanto debe ser fundamental al momento de definir las acciones para lograr el fortalecimiento sin descuidar otros factores que sin duda son necesarios. Como respuesta al cuarto objetivo de este trabajo a continuación se presentan las medidas de seguridad más apropiadas a aplicar en el escenario propuesto para la organización QWERTY.

Como primera medida es necesario recurrir a construir cultura organizacional en torno a los principios de la seguridad de la información[17] basados en creencias y acciones que muestren con el ejemplo y a partir de lecciones aprendidas tanto internas como de otras organizaciones para ilustrar las consecuencias de tomar a la ligera las medidas de seguridad, procedimientos y políticas establecidas por la organización. Para esto es necesario indagar sobre prácticas actuales vigentes e introducirlas en la cultura de la organización.

Como tercera medida sacar provecho de los recursos con los que ya se cuenta realizando Revisión de configuraciones y claves para eliminar posibles configuraciones y claves por defecto. Actualizar firmware y sistema operativos de los servidores, Equipos de red activos y software como antivirus, estas actividades toman tiempo y requieren personal con los conocimientos apropiados para ello, por lo que en la medida que se presente la necesidad de renovación de equipos tecnológicos y software se debe incluir en la evaluación la posibilidad de adquirirlos como servicio y no como activos, minimizando obsolescencia, administración, asegurando alta disponibilidad, todo esto basado en acuerdos apropiados de nivel de servicio y de confidencialidad tanto sobre la información como de los eventos o incidentes de seguridad.

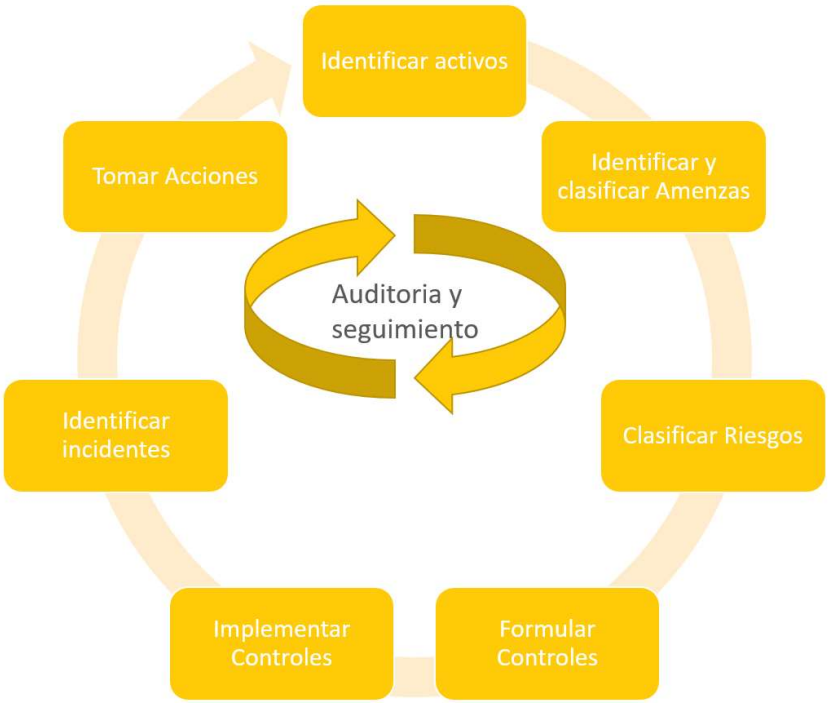
[17] CANO m, Jeimy J Cano M, Manual de un ciso , Bogotá D.C,Ediciones de la U, Colombia, 2016

11. RESULTADOS Y DISCUSIÓN

La decisión de implementar un sistema de gestión de seguridad de la información responde hoy en día a dos grandes necesidades de las organizaciones, en primera instancia es la respuesta a la necesidad de la dirección de tener mayor gobernabilidad de las distintas áreas de tecnología y de los recursos utilizados, y en segundo lugar permite generar una respuesta más eficaz ante los incidentes de seguridad de información por parte de los responsables de tecnología.

A través del desarrollo de este trabajo, aunque basado en un modelo de empresa teórico claramente se puede observar que es un proceso largo que se va construyendo con el tiempo y se fortalece con la observación constante del modelo y de cómo los cambios afectan su comportamiento.

Fig. 6 Ciclo de implementación



Fuente: Presente Estudio

A través de la documentación realizada para llegar a los objetivos propuestos se evidencia que la implementación de un sistema de gestión de seguridad permite poner en claro no solo el inventario de los activos, sino también su uso, las implicaciones de no contar con él y declarar los responsables de su administración, así como mitigar una de las causas que hoy en día generan las vulnerabilidades

más Frecuentes que son la obsolescencia de las herramientas y las deficiencias en configuraciones ya sea por el uso de parámetros por defecto por el exceso de funcionalidad no administrada de forma correcta.

Para terminar, como todo sistema gestión el de la seguridad de la información no es la excepción con respecto a que el primer paso es el compromiso del capital humano basado en la conciencia de lo que representa en esta caso el valor de la información, y una vez se desarrolla el primer modelo su auditoría y seguimiento constante comparando con frecuencia el estado del sistema frente a factores externos como los avances tecnológicos, competidores, y factores internos como las nuevas necesidades del negocio, evolución de sus procesos internos, son los que marcan la evolución del mismo sistema de gestión de seguridad.

12. RECOMENDACIONES

Para la definición de cualquier sistema de gestión de seguridad es necesario aplicar el principio de seguridad integral que esto permite no solo fortalecer unos mecanismos con otros, sino que además no se deja nada al azar.

Se debe asegurar que se tienen claramente establecidas, identificadas y monitoreadas las distintas líneas de defensa con las que se cuentan

Para este y cualquier sistema de gestión es necesario la evaluación periódica de su comportamiento, cambios representativos que puedan afectar la seguridad de la información y la efectividad de los mecanismos de control.

Las medidas de seguridad a implementar deben ser apropiadas al sistema de información de a proteger, el tamaño de la organización y el nivel de riesgo generado por el contexto en que se desenvuelve.

12. CONCLUSIONES

La metodología MAGERIT facilita la identificación de amenazas y a la vez provee un estándar que facilita la clasificación de las amenazas.

Como resultado de la identificación de amenazas es establecen 14 elementos que agrupan los resultados permitiendo consolidar y simplificar el análisis

Como resultado de la evaluación del riesgo se establecieron los siguientes elementos de nivel crítico: Datos de proveedores, datos de órdenes de compra, datos de empleados y datos de inventario, Software página Web.

Como nivel de riesgo bajo se identifican: Gestión de usuarios y contraseñas, Gestión de talento humano, correo institucional, Software de facturación y nómina, licenciamiento de servidores y pc, canal de internet, Personal en Práctica, servidores y equipo de impresión

BIBLIOGRAFIA

ABRIL Ana, PULIDO Jarol y BOHADA Jhon A., Análisis de Riesgos en Seguridad de la Información (2013), Fundación Universitaria Juan DE Castellanos Colombia .

AMUTIO GÓMEZ, Miguel Angel, CANDAU, Javier**.** *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método.* Madrid : Editorial Ministerio de Hacienda y Administraciones Públicas Secretaría General.

AMUTIO GÓMEZ, Miguel Angel, CANDAU, Javier, MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos, Madrid, Editorial Ministerio de Hacienda y Administraciones Públicas Secretaría General Técnica Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones

AMUTIO GÓMEZ, Miguel Angel, CANDAU, Javier, MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III -Guia de Tecnicas, Madrid, Editorial Ministerio de Hacienda y Administraciones Públicas Secretaría General Técnica Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones

ALCALDIA MAYOR DE BOGOTA, ley 1581 de 2012, Régimen Legal de Bogotá, (octubre 17 de 2012) Colombia

ALEMAN NOVOA,Helena, Rodriguez BARRERA, Claudia, Metodologias para el análisis de riesgos de los SGSI,[en linea], Disponible en:

http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

ALEXANDER, A Diseño de un Sistema de Gestión de Seguridad de Información, óptica ISO 27001:2005, Bogotá, Alfaomega.,2007

BAENA PAZ, Guillermina María Eugenia. Metodología de la investigación, Grupo Editorial Patria, 2014.

BILBAO LAZARO, Enrique, Modelo unificado de análisis de riesgos de seguridad Física y Lógica, [en línea,], Inteco, disponible en:

https://www.cuevavaliente.com/sites/default/files/ponencia_inteco_2011.pdf

BISOGNO, María Victoria. Metodología para el aseguramiento de entornos informatizados – MAEI. Buenos Aires – Argentina. Universidad de Buenos Aires, 2004

Blog especializado en Sistemas de Gestión de Seguridad de la Información. SGSI PMG [En línea] disponible en: http://www.pmg-ssi.com/2015/07/quees-sgsi/.

CANO m, Jeimy J Cano M, Manual de un ciso , Bogotá D.C,Ediciones de la U, Colombia, 2016

CARRANZA CASTRO, Marlon, proyecto de investigación exploratorio sobre la gestión de la seguridad lógica en los sistemas de información de las pymes, del sector de comercio de la ciudad de santa marta,2008

COLOMBIA, CONGRESO DE LA REPUBLICA**.** *Ley 1273, Bogotá.* Bogota : s.n., 5 de Enero de 2009.

CIFUENTES Garzón, Guillermo Análisis de seguridad en base de datos: Aplicación Oracle versión. Maestría en Evaluación y Auditoría de Sistemas Tecnológicos. Universidad de las Fuerzas Armadas ESPE. Sede Sangolquí, (2014).

ECRIVA GASCO,Gema, ROMERO SERRANO, Rosa Maria, RAMADA, David, Seguridad Informatica,[Online], Madrid, Macmillan iberia, 2013

https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/detail.action?docID=3217398

ELVIRA Mifsud, Introducción a la seguridad informática {En línea} (2012), disponible en: http://recursostic.educacion.es/observatorio/web/en/software/softwaregeneral/1040-introduccion-a-la-seguridad-informatica?showall=1.

ESET. (1 de Abril de 2015). WEliveSecurity. Obtenido de https://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/

FERNANDEZ SANCHEZ, Carlos Manuel, PIATTINI VHELTUIS, Mario. Modelo para el gobierno de las TIC, basado en las Normas ISO, España, AENOR, 2012

FUNDACION DE EGRESADOS U.D, ITIL foundation V3, Version 2.2.3, Bogotá, 2009

GAONA VASQUEZ, Karina del Rocio, Aplicación de la metodología Magerit para el análisis y gestion de riesgos de la seguridad de la información aplicado a la empresa pesquera e industrial Bravito s.a en la ciudad de machala,cuenca, Universidad politécnica salesiana sede cuenca, 2013

GOMEZ FERNANDEZ, Luis, FERNANDEZ RIVERO Pedro Pablo. Como implantar un SGSI según UNE – ISO 27001: 2014 y su aplicación en el esquema Nacional de Seguridad, Madrid, Editorial AENOR, 2015

GOMEZ FERNANDEZ, Luis, ANRES ALVAREZ, Ana, guía de aplicación de la norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para

pymes,España,AENOR,2012

GOMEZ LOPEZ, Julio, GOMEZ LOPEZ, Oscar David. Administración de sistemas operativos, Bogotá, Ra-Ma EDITORIAL, 2014.

GOMEZ VIEITES, Alvaro. Seguridad de lo equipos informaticos, RA-MA editorial, 2014

INSTITUTO COLOMBIANO DE NORMAS TECNICAS. Tecnología de la información. Técnicas de seguridad de la información. Sistemas de seguridad de la información. Requisitos Bogotá D.C.: ICONTEC, 2013. NTC-ISO/IEC 27001:2013

INSTITUTO COLOMBIANO DE NORMAS TECNICAS. Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información, Bogotá D.C.: ICONTEC, 2019. NTC-ISO/IEC 27005:2008

KATZ,Matias, Redes y seguridad,Bogotá, Alfaomega, 2016

KOSUTIC, DEJAN, La importancia de la declaración de aplicabilidad para la norma iso 27001, [Online], 2013, https://advisera.com/27001academy/es/knowledgebase/la-importancia-de-la-declaracion-de-aplicabilidad-para-la-norma-iso-27001/

LARDENT, Alberto R, sistemas de información para la gestión empresaria: Procedimientos, seguridad y auditoria, Bogotá D.C., Prentice Hall, 2001.

MAQUERA Quispe, Henry George, Serpa Guillermo, Paola Nhataly, GESTIÓN DE ACTIVOS BASADO EN ISO/IEC 27002 PARA GARANTIZAR SEGURIDAD DE LA INFORMACIÓN**,** Perú 2018, CIENCIA & DESARROLLO

MATALOBOS, Juan , Analisis de riesgos de seguridad de la información,Tesis Universidad Politecnica de Madrid Facultad de informatica,Madrid, mayo de 2009

MENDEZ ALVAREZ, Carlos Eduardo. Metodología, Diseño y desarrollo del proceso de investigación 4ª. Edicion,Mexico,Limusa,2008

Portal administración Metodología de análisis {En línea} (2012), disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_ Metodolog/pae_Magerit.html#.WRIcMEWGPIU

MINISTERIO DE LAS TICS,Guia para la preparación de las TICS para la continuidad de Negocio, Seguridad y privacidad de la información [en linea],2010, Disponible en:

https://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf

SISTEMAS Y CALIDAD TOTAL, 15 Etapas para la Implementación y Desarrollo de un Sistema de Gestión de Calidad ISO 9001:2008 [Online]

http://www.sistemasycalidadtotal.com/calidad-total/15-etapas-implementacion-sistema-gestion-de- calidad-iso-9001/

REVISTA INFORMATICA JURIDICA, Legislación informática de Colombia, Salamanca, 2016

http://www.informatica-juridica.com/legislacion/colombia/

RAMOS VARON, Antonio angel, BARBERO MUÑOZ, Carlos,MARUGAN RODIRGUEZ,David, GONZALEZ DURAN, Ismael, Hacking con Ingenieria social Tecnicas para hackear humanos, Madrid, RA-MA Ediciones de la U, 2015.

ROA BUENDIA, José Fabián. Seguridad informática, Madrid, MG Graw Hill, 2013

ROJAS CORSICO, Ivana Soledad, Trabajo de Auditoria normas COBIT, Bogotá, El CID editor, 2009

ROSS, Jeanne , WEILL, Peter, Seis decisiones de TI que no debe dejar en manos del departamento de TI, Ediciones Deusto,2014

SUAREZ GONZALEZ. Rafael, Analisis de activos de información para un sistema misional basados en metodología MAGERIT v 3. Y la norma ISO 27001:2013, Bogotá D.C. Universidad Nacional abierta y a distancia UNAD, 2018

STALLINGS, William, Comunicaciones y redes de computadores, Bogotá, Pearson Educación, 2004

TERAN PEREZ, David Moises, Administración y seguridad en redes de computadoras, Bogotá,Alfaomega,2018

VANEGAS Devia, Gonzalo Andrés, PARDO, César, Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT, sistemas y telematica,universidad ICESI, 2014, Cali, Valle del cauca.

RESUMEN RAE

1. Información General	
Tipo de Documento	Informe final trabajo de grado
Acceso al documento	Universidad Nacional Abierta y a Distancia UNAD Escuela de Ciencias Básicas tecnológicas e ingenierías Especialización en seguridad Informática
Título	Diseño de un modelo de gestión de seguridad de la información basado en el estándar iso 27001:2013 para la gestión de la información para el caso de estudio empresa qwerty s.a
Autor	Flor Esperanza Becerra Arias
Director	
Publicación	Digitado en Computador
Unidad Patrocinante	Universidad Nacional Abierta y a Distancia UNAD Escuela de Ciencias Básicas tecnológicas e ingenierías Especialización en seguridad Informática
Palabras Clave	Seguridad de la información, sistema de gestión, Análisis de riesgo, vulnerabilidad, control.

2. Descripción
Trabajo de grado para optar al título de especialista en seguridad informática, a partir del escenario presentado para la empresa QWERTY SA se establece un modelo de para gestionar de forma eficaz y sostenible la seguridad de su información, lo anterior basado la norma ISO 27001:2015, Cuenta con análisis de riesgos, documentar el sistema de gestión (política, manual, procedimientos, plan de tratamiento de riesgos, documento de aplicabilidad), para lo cual se tendrá en cuenta las herramientas provistas por la metodología MARGERIT.

3. Información General	
Tipo de Documento	Informe final trabajo de grado
Acceso al documento	Universidad Nacional Abierta y a Distancia UNAD Escuela de Ciencias Básicas tecnológicas e ingenierías Especialización en seguridad Informática
Título	Diseño de un modelo de gestión de seguridad de la información basado en el estándar iso 27001:2013 para la gestión de la información para el caso de estudio empresa qwerty s.a
Autor	Flor Esperanza Becerra Arias
Director	
Publicación	Digitado en Computador
Unidad Patrocinante	Universidad Nacional Abierta y a Distancia UNAD Escuela de Ciencias Básicas tecnológicas e ingenierías Especialización en seguridad Informática
Palabras Clave	Seguridad de la información, sistema de gestión, Análisis de riesgo, vulnerabilidad, control.

4. Descripción
Trabajo de grado para optar al título de especialista en seguridad informática, a partir del escenario presentado para la empresa QWERTY SA se establece un modelo de para gestionar de forma eficaz y sostenible la seguridad de su información, lo anterior basado la norma ISO 27001:2015, Cuenta con análisis de riesgos, documentar el sistema de gestión (política, manual, procedimientos, plan de tratamiento de riesgos, documento de aplicabilidad), para lo cual se tendrá en cuenta las herramientas provistas por la metodología MARGERIT.

5. Fuentes
TECNICAS., INSTITUTO COLOMBIANO DE NORMAS. *Tecnología de la información. Técnicas de seguridad de la información (SGSI). Visión general y vocabulario. Bogotá D.C.: ICONTEC, NTC-ISO/IEC 27000:2016.* 2017. **AMUTIO GOMEZ, Miguel Angel, CANDAU, Javier.** *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método.* MAdrid : Editorial Ministerio de Hacienda y Administraciones Públicas Secretaría General. **COLOMBIA, CONGRESO DE LA REPUBLICA.** *Ley 1273, Bogotá.* Bogota : s.n., 5 de Enero de 2009. MENDEZ ALVAREZ, Carlos Eduardo. Metodología, Diseño y desarrollo del proceso de investigación 4ª. Edicion,Mexico,Limusa,2008 BAENA PAZ, Guillermina María Eugenia. Metodología de la investigación, Grupo Editorial Patria, 2014. https://bibliotecavirtual.unad.edu.co:2538/lib/unadsp/detail.action?docID=3228423. INSTITUTO COLOMBIANO DE NORMAS TECNICAS. Tecnología de la información. Técnicas de seguridad de la información. Sistemas de seguridad de la información. Requisitos Bogotá D.C.: ICONTEC, 2013. NTC-ISO/IEC 27001:2013 INSTITUTO COLOMBIANO DE NORMAS TECNICAS. Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información, Bogotá D.C.: ICONTEC, 2019. NTC-ISO/IEC 27005:2008 GOMEZ LOPEZ, Julio, GOMEZ LOPEZ, Oscar David. Administración de sistemas operativos, Bogotá, Ra-Ma EDITORIAL, 2014. AMUTIO GOMEZ, Miguel Angel, CANDAU, Javier, MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos, Madrid, Editorial Ministerio de Hacienda y Administraciones Públicas Secretaría General Técnica Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones AMUTIO GOMEZ, Miguel Angel, CANDAU, Javier, MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III -Guia de Tecnicas, Madrid, Editorial Ministerio de Hacienda y Administraciones Públicas Secretaría General Técnica Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones CANO m, Jeimy J Cano M, Manual de un ciso , Bogotá D.C,Ediciones de la U, Colombia, 2016

SISTEMAS Y CALIDAD TOTAL, 15 Etapas para la Implementación y Desarrollo de un Sistema de Gestión de Calidad ISO 9001:2008 [Online] http://www.sistemasycalidadtotal.com/calidad-total/15-etapas-implementacion-sistema-gestion-de- calidad-iso-9001/

KOSUTIC, DEJAN, La importancia de la declaración de aplicabilidad para la norma iso 27001, [Online], 2013 https://advisera.com/27001academy/es/knowledgebase/la-importancia-de-la-declaracion-de-aplicabilidad-para-la-norma-iso-27001/

GOMEZ VIEITES, Alvaro. Seguridad de lo equipos informaticos, RA-MA editorial, 2014

GOMEZ FERNANDEZ, Luis, FERNANDEZ RIVERO Pedro Pablo. Como implantar un SGSI según UNE – ISO 27001: 2014 y su aplicación en el esquema Nacional de Seguridad, Madrid, Editorial AENOR, 2015

ROA BUENDIA, José Fabián. Seguridad informática, Madrid, MG Graw Hill, 2013

ECRIVA GASCO,Gema, ROMERO SERRANO, Rosa Maria, RAMADA, David, Seguridad Informatica,[Online], Madrid, Macmillan iberia, 2013 https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/detail.action?docID=3217398

REVISTA INFORMATICA JURIDICA, Legislación informática de Colombia, Salamanca, 2016 http://www.informatica-juridica.com/legislacion/colombia/

GOMEZ FERNANDEZ, Luis, ANRES ALVAREZ, Ana, guía de aplicación de la norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes,España,AENOR,2012

GOMEZ VIEITES, Álvaro, Gestión de incidentes de seguridad informática, España, RA-MA Editorial, 2014

FERNANDEZ SANCHEZ, Carlos Manuel, PIATTINI VHELTUIS, Mario. Modelo para el gobierno de las TIC, basado en las Normas ISO, España, AENOR, 2012

ROJAS CORSICO, Ivana Soledad, Trabajo de Auditoria normas COBIT, Bogotá, El CID editor, 2009

ROSS, Jeanne , WEILL, Peter, Seis decisiones de TI que no debe dejar en manos del departamento de TI, Ediciones Deusto,2014

FUNDACION DE EGRESADOS U.D, ITIL foundation V3, Version 2.2.3, Bogotá, 2009

RAMOS VARON, Antonio angel, BARBERO MUÑOZ, Carlos,MARUGAN RODIRGUEZ,David, GONZALEZ DURAN, Ismael, Hacking con Ingenieria social Tecnicas para hackear humanos, Madrid, RA-MA Ediciones de la U, 2015.

CARRANZA CASTRO, Marlon, proyecto de investigación exploratorio sobre la gestión de la seguridad lógica en los sistemas de información de las pymes, del sector de comercio de la ciudad de santa marta,2008

STALLINGS, William, Comunicaciones y redes de computadores, Bogotá, Pearson Educación, 2004

LARDENT, Alberto R, sistemas de información para la gestión empresaria: Procedimientos, seguridad y auditoria, Bogotá D.C., Prentice Hall, 2001.

LARDENT, Alberto R, sistemas de información para la gestión empresaria: Planeamiento, Tecnología y calidad I, Bogotá D.C., Prentice Hall, 2001.

SUAREZ GONZALEZ. Rafael, Analisis de activos de información para un sistema misional basados en metodología MAGERIT v 3. Y la norma ISO 27001:2013,Bogotá D.C. Universidad Nacional abierta y a distancia UNAD, 2018

ABRIL Ana, PULIDO Jarol y BOHADA Jhon A., Análisis de Riesgos en Seguridad de la Información (2013), Fundación Universitaria Juan D Castellanos Colombia .

BISOGNO, María Victoria. Metodología para el aseguramiento de entornos informatizados – MAEI. Buenos Aires – Argentina. Universidad de Buenos Aires, 2004
CIFUENTES Garzón, Guillermo Análisis de seguridad en base de datos: Aplicación Oracle versión. Maestría en Evaluación y Auditoría de Sistemas Tecnológicos. Universidad de las Fuerzas Armadas ESPE. Sede Sangolquí, (2014).
ELVIRA Mifsud, Introducción a la seguridad informática {En línea} (2012), disponible en: http://recursostic.educacion.es/observatorio/web/en/software/softwaregeneral/1040-introduccion-a-la-seguridad-informatica?showall=1.
Portal administración Metodología de análisis {En línea} (2012), disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_ Metodolog/pae_Magerit.html#.WRIcMEWGPIU
Blog especializado en Sistemas de Gestión de Seguridad de la Información. SGSI PMG [En línea] disponible en: http://www.pmg-ssi.com/2015/07/quees-sgsi/.
Análisis de riesgos de la seguridad de la información para la institución universitaria colegio mayor del cauca, [En línea] (2014), tesis posgrado, disponible en: http://www.academia.edu/24661883/An%C3%A1lisis_ de_Riesgos_de_la_Seguridad_de_la_Informaci%. (s.f.)
Generalidades de la informática, [En línea], disponible en: https://sites.google.com/site/navegadorteleinformatico/navegadorteleinformatico
Sistemas de Gestion de seguridad de la informacion, [en línea], disponible en: https://www.isotools.org./pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf
Que es la declaración de Aplicabilidad, [en linea], disponible en: https://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/
Iso 27001 y la declaración de aplicabilida, [en linea], disponible en: https://www.pmg-ssi.com/2014/03/iso-27001-la-declaracion-de-aplicabilidad
Norma y leyes que existen en Colombia para delitos informáticos, [en linea], disponible en: https://es.slideshare.net/santiagocisneros6/normas-y-leyes-que-existen-en-colombia-para-delitos-informaticos
TERAN PEREZ, David Moises, Administracion y seguridad en redes de computadoras, Bogotá,Alfaomega,2018
KATZ,Matias, Redes y seguridad,Bogotá, Alfaomega, 2016
ALEMAN NOVOA,Helena, Rodriguez BARRERA, Claudia, Metodologias para el análisis de riesgos de los SGSI,[en linea], Disponible en: http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874
BILBAO LAZARO,Enrique, Modelo unificado de análisis de riesgos de seguridad Fisica y Logica, [en línea,], Inteco, disponible en: https://www.cuevavaliente.com/sites/default/files/ponencia_inteco_2011.pdf
Alexander, A Diseño de un Sistema de Gestión de Seguridad de Información, óptica ISO 27001:2005, Bogotá, Alfaomega.,2007
MINISTERIO DE LAS TICS,Guia para la preparación de las TICS para la continuidad de Negocio, Seguridad y privacidad de la informacion [en linea],2010, Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf

GAONA VASQUEZ, Karina del Rocio, Aplicación de la metodología Magerit para el análisis y gestion de riesgos de la seguridad de la información aplicado a la empresa pesquera e industrial Bravito s.a en la ciudad de machala,cuenca, Universidad politécnica salesiana sede cuenca, 2013

MATALOBOS, Juan , Analisis de riesgos de seguridad de la información,Tesis Universidad Politecnica de Madrid Facultad de informatica,Madrid, mayo de 2009
VANEGAS Devia, Gonzalo Andrés, PARDO, César, Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT, sistemas y telematica,universidad ICESI, 2014, Cali, Valle del cauca.

ALCALDIA MAYOR DE BOGOTA, ley 1581 de 2012, Régimen Legal de Bogotá, (octubre 17 de 2012) Colombia

Maquera Quispe, Henry George, Serpa Guillermo, Paola Nhataly, GESTIÓN DE ACTIVOS BASADO EN ISO/IEC 27002 PARA GARANTIZAR SEGURIDAD DE LA INFORMACIÓN, Peru 2018, CIENCIA & DESARROLLO

6. Contenidos

El documento cuenta con 11 capítulos en los que se desarrolla la propuesta para establecer los mecanismos necesarios para gestionar la seguridad de la organización de forma Eficaz. En los primeros capítulos se establece el planteamiento del problema y se resume en la siguiente pregunta el punto de partida el desarrollo del trabajo: "Cuáles son los elementos fundamentales de un modelo de gestión de seguridad de la información para asegurar las condiciones de calidad de la información?"
Es establecen los siguientes 4 objetivos específicos bajo los que se oriente la estructuración del trabajo:

- Identificar y clasificar las amenazas presentadas en los activos de información que afectan la calidad , integridad, disponibilidad y confiabilidad de la información para el caso de estudio de la empresa QWERTY
- Formular los controles a los activos de información para empresa QWERTY de acuerdo al anexo A de la norma ISO 27001:2013
- Establecer metodología de implementación del SIGS de la empresa QWERTY que asegure condiciones sostenibles de seguridad de la información y que a su vez promueva la evolución de las condiciones de seguridad de la información.
- Presentar documento con los recursos de tecnología, establecer medidas de seguridad apropiadas al menor costo con mecanismos apropiados de verificación de cumplimiento para mantener controles eficientes y apropiados sin afectar la productividad de la organización

Se da respuesta a estos objetivos en los capítulos 6 a 11, donde básicamente se encuentran consignados los siguientes elementos para el escenario propuesto así:

1. Identificación de Activos, así como su valoración, la determinación de las vulnerabilidades y evaluación de riesgos, en donde se realiza la clasificación de los activos esenciales como servicios y datos de información y otros activos como son Aplicaciones de software, equipos informáticos, instalaciones, Personal y redes de comunicaciones.
2. Formulación de controles, a partir de la evaluación de riesgos se identifican los controles de mayor impacto para el escenario propuesto
    - ✓ Política de seguridad de la información
    - ✓ Organización de la seguridad de la información
    - ✓ Seguridad del recurso humano
    - ✓ Gestión de activos
    - ✓ Equipos
    - ✓ Seguridad física y del entorno

- ✓ Control para desarrollo de software

3. Administración del riesgo, que incluye: Plan de tratamiento de riesgos, declaración de aplicabilidad y la política de seguridad.
   En el plan de tratamiento de riesgos se define como objetivo del plan establecer la ruta de implementación de controles requeridos en QWERTY SAS, para esto se establece alcance, responsabilidades y actividades con plazos, recursos y activos afectados en cada actividad.
   En cuanto a la declaración de aplicabilidad se toma como base el anexo 1 de la norma ISO27001, en donde se establece el control para cada ítem, si aplica o no este escenario, la justificación de su aplicación o no y en caso de aplicar la evidencia o el documento en el que queda documentado el control ya sea política, procedimiento o formato.
4. Se definen los procedimientos fundamentales para dar respuesta a las condiciones de seguridad como son: Mantenimiento y desarrollo de aplicaciones, Gestión de claves de acceso, clasificación de información y gestión de incidentes.
   Manual de seguridad de la información que cuenta con los siguientes elementos: Objetivo, Alcance Del SGSI, Medidas de seguridad, estructura del SGSI, enfoque utilizado para la evaluación de riesgos y seguimiento al Sistema de gestión mediante la definición de formato para los indicadores.

7. Metodología

Para este proyecto aplicado la metodología seleccionada es la investigación por observación de un caso de estudio, esto teniendo en cuenta que el tipo de investigación que aplica al proyecto es La investigación aplicada, donde se busca resolver un problema practico, El tipo de estudio es cualitativo en lo que se refiere a la identificación de activos, vulnerabilidades, clasificación del riesgo y se utilizaran escalas de valoración cuantitativa para la calificación de riesgos

8. Conclusiones

La metodología MAGERIT facilita la identificación de amenazas y a la vez provee un estándar que en facilita la clasificación de las amenazas.
Como resultado de la identificación de amenazas es establecen 14 elementos que agrupan los resultados permitiendo consolidar y simplificar el análisis.
Como resultado de la evaluación del riesgo se establecieron los siguientes elementos de nivel crítico: Datos de proveedores, datos de órdenes de compra, datos de empleados y datos de inventario, Software página Web.
Como nivel de riego bajo se identifican: Gestión de usuarios y contraseñas, Gestión de talento humano, correo institucional, Software de facturación y nomina, licenciamiento de servidores y pc, canal de internet, Personal en Práctica, servidores y equipo de impresión.

Para la definición de cualquier sistema de gestión de seguridad es necesario aplicar el principio de seguridad integral que esto permite no solo fortalecer unos mecanismos con otros, sino que además no se deja nada al azar.
Se debe asegurar que se tienen claramente establecidas, identificadas y monitoreadas las distintas líneas de defensa con las que se cuentan

Para este y cualquier sistema de gestión es necesario la evaluación periódica de su comportamiento, cambios representativos que puedan afectar la seguridad de la información y la efectividad de los mecanismos de control. Las medidas de seguridad a implementar deben ser apropiadas al sistema de información de a proteger, el tamaño de la organización y el nivel de riesgo generado por el contexto en que se desenvuelve.

Elaborado Por	Flor esperanza Becerra Arias
Revisado Por	

Fecha de elaboración	2019	11	30