DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO/IEC 27001 PARA ENTIDADES DEL ESTADO

JUAN CARLOS DE LEON CAMELO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
RIOHACHA – LA GUAJIRA
2019

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO/IEC 27001 PARA ENTIDADES DEL ESTADO

JUAN CARLOS DE LEON CAMELO

TRABAJO DE GRADO PARA OPTAR EL TITULO DE ESPECIALISTA EN SEGURIDAD INFORMATICA

Esp. DANIEL FELIPE PALOMO LUNA
DIRECTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
RIOHACHA – LA GUAJIRA
2019

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Riohacha, 7 de marzo de 2019

DEDICATORIA

Este es un trabajo que se ha realizado con mucho esfuerzo, dedicación y cariño, lo dedico principalmente a Dios que es nuestro padre de la vida y todo poderoso, a mis padres José Alberto de León Vanegas y María Ignacia Camelo de León, que han sido la mayor motivación para seguir adelante en mi vida profesional, porque a pesar de los años y de ser adultos mayores se preocupan aun por el bienestar de sus hijos.

AGRADECIMIENTOS

Agradezco a Dios que es mi guía y mi fortaleza en todo momento para salir adelante, siempre está a mi lado protegiéndome y cuidándome de todo mal.

A mis padres José Alberto de León Vanegas y María Ignacia Camelo de León, por brindarme en todo momento el apoyo que necesito para salir adelante y esos valores que me hacen único en mi forma de ser.

A mi Director de Proyecto, Ingeniero Especialista Daniel Felipe Palomo Luna, por su colaboración y atención siempre oportuna, por impartir conocimiento de calidad y por realizar el correspondiente acompañamiento de forma magistral, apoyándome para culminar exitosamente el presente proyecto aplicado y obtener mi título como Especialista en Seguridad Informática.

A todos los que con su pequeño aporte en colaboración intelectual, anímica y en trabajo físico han contribuido a la consolidación de este proyecto y a lo que él puede generar si es aplicado en el área donde se desarrollará.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ACTIVO DE INFORMACIÓN: es el elemento de información que la organización recibe o produce en el ejercicio de sus funciones. Incluye todo lo que se encuentre presente en forma escrita, impresa, trasmitida o almacenada por cualquier medio electrónico en equipos de cómputo, incluyendo hardware, software, recurso humano, datos contenidos en registros, archivos, bases de datos, imágenes y videos.

AMENAZA: causa potencial de una acción negativa que puede ocasionar daños a un sistema de información.

AUTORIZACION: consentimiento previo para realizar una acción.

CONFIDENCIALIDAD: es la garantía de que la información será asegurada para que no sea divulgada sin consentimiento y únicamente será accesible por personal autorizado.

DAFP: son las siglas utilizadas para referirse al departamento administrativo de la función pública que proporciona la guía de riesgos para entidades públicas.

DISPONIBILIDAD: entendida como la garantía del acceso a la información en el instante en que el usuario la necesita.

.

DRP: son las siglas equivalentes en ingles a *Disaster Recovery Plan,* en español plan de recuperación ante desastres, es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos.

INTEGRIDAD: entendida como la preservación de la información de forma completa y exacta.

ISO27001: es una norma emitida por la Organización Internacional de Normalización (ISO) que describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

MAGERIT: metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

PDCA: son las siglas en inglés *plan-do-check-act* o Ciclo de Deming por ser Edwards Deming su creador.

PHVA: son las siglas en español del ciclo (planear, hacer, verificar y actuar), es una herramienta de mejora continua que permite planear, tomar acciones, verificar los resultados y actuar sobre los resultados esperados.

PRIVACIDAD: es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros.

RIESGO: es la posibilidad que una amenaza pueda causar cierto impacto negativo en un activo determinado que presenta una vulnerabilidad a dicha amenaza.

SGSI: son las siglas utilizadas para referirse al sistema de gestión de la seguridad de la Información e ISMS son las siglas equivalentes en ingles a *Information Security Management System*. Es una Herramienta de gestión que utiliza procesos sistemáticos y documentados para salvaguardar la seguridad de la información de una organización.

VULNERABILIDAD: puntos débil del equipamiento, aplicaciones, personal y mecanismos de control que facilitan la concreción de una amenaza.

RESUMEN

El presente documento se basó en la realización y diseño de una guía de buenas prácticas y procedimientos sistémicos, que consisten en minimizar los riesgos y salvaguardar la protección de la información, específicamente en organizaciones y entidades del estado, con la finalidad de preservar la confidencialidad, integridad y disponibilidad de la misma, a través de una herramienta de gestión relacionada con la seguridad y privacidad de los datos.

Es por ello que surgió la necesidad de desarrollar un sistema de gestión de seguridad de la información (SGSI) tomando como referencia la metodología que define la norma ISO/IEC 27001. Con el fin de ponerlo a disposición de las entidades del gobierno y que sea utilizado como guía para definir sus políticas de seguridad de la información.

De esta manera el presente documento busca proporcionar los lineamientos básicos y de forma general sobre cómo empezar a diseñar y dimensionar el alcance para realizar la implementación de un Sistema de Gestión de Seguridad de la Información en una organización del estado colombiano.

INTRODUCCIÓN

En la actualidad, es muy común escuchar por todos los medios el concepto de transformación digital, económica y social, esto se da como consecuencia del avance de las Tecnologías de la Información y las Comunicaciones (TIC) y el uso de Internet por millones de usuarios en todo el mundo. Esta posibilidad de conexión a nivel global ha permitido que la información esté tipificada como uno de los activos más valiosos e importantes para cualquier tipo de entidad, sin embargo, muchas organizaciones no la tienen asegurada.

Con el pasar del tiempo y el avance de la tecnología, la seguridad de los datos se ha vuelto un tema de suma importancia, por lo tanto, cualquier organización independientemente de que sea publica ó privada, debe ser consciente que están expuestas a un número de amenazas y riesgos que existen hoy en día, y aprovechan cualquier tipo de vulnerabilidad para someter a los activos críticos de información a ataques y espionajes, etc. Es por ello que para salvaguardar la información se deben utilizar herramientas de gestión a través de procesos sistémicos, documentados que garanticen la confidencialidad, integridad y disponibilidad de la misma.

La implementación de este tipo de herramientas en las entidades del estado tiene como objetivo primordial asegurar la protección de los datos y sus activos de información. En este proyecto se pretende entregar pautas de implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO27001:2013 que sirva como guía para cualquier entidad del gobierno.

En un entorno globalizado y competitivo, las entidades del estado dependen cada vez más de sus sistemas de información y de los datos almacenados en estos, de ahí radica la gran importancia de realizar una guía de un sistema de gestión de seguridad de la información que sirva como modelo de implementación para las entidades del gobierno.

El presente proyecto pretende mediante el uso de buenas prácticas y procedimientos adecuados, establecer una metodología de gestión de Seguridad de la información estructurada y clara, para que las entidades del estado puedan definir sus políticas de seguridad y realizar sus análisis de riesgos de una manera más eficiente y eficaz.

1. TITULO

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO/IEC 27001 PARA ENTIDADES DEL ESTADO

2. DEFINICIÓN DEL PROBLEMA

2.1 PLANTEAMIENTO DEL PROBLEMA

En un mundo conectado y globalizado, como el existente en la actualidad, y con el creciente uso de las tecnologías de la información y las comunicaciones (TIC), la seguridad de la información se ha considerado un aspecto esencial en las organizaciones de cualquier tamaño y tipo, específicamente en entidades del gobierno. Lo anterior, se refiere a un aspecto que tiene que ver con la protección de los datos contra accesos no autorizados y para salvaguardarlos de una posible corrupción durante todo su ciclo de vida. Las entidades hoy en día dependen cada vez más de sus sistemas de información y de los datos que estos administran, es por ello por lo que la información se ha convertido en un activo nuevo y de gran valor, sin embargo, muchas entidades no la tienen asegurada, y algunas ni siquiera saben cuál es el valor de sus activos intangibles.

Tendencias recientes han demostrado que los riesgos y amenazas están aumentando en frecuencia y en gravedad. Cada día las entidades están expuestas a todo tipo de ataques informáticos, accesos no autorizados, secuestro de información, vulnerabilidades, desastres naturales, siniestros y accidentes, etc. En su gran mayoría las entidades del gobierno no tienen delineadas sus políticas de seguridad de la información, esto conduce a resultados negativos en la protección de los datos y recursos de la Entidad, de esta manera incurren constantemente en fallas del servicio y comprometen los activos más críticos, la continuidad del negocio, el capital intelectual y la información confidencial de la organización.

En términos generales, se ve afectada la seguridad de los datos en las entidades del gobierno, por lo tanto, no se puede asegurar la integridad, disponibilidad y confiabilidad, al no contar en su mayoría con herramientas de gestión o políticas de seguridad definidas para el manejo de protección de la información.

2.2 FORMULACIÓN DEL PROBLEMA

¿Cómo el diseño de un Sistema de Gestión de Seguridad de la Información - SGSI permitirá minimizar los riesgos de seguridad y control de acceso a los usuarios al establecer políticas de seguridad y privacidad de la información en las entidades del estado?

3. JUSTIFICACIÓN

La seguridad de la información es un aspecto de suma importancia en todo tipo de organizaciones, más en las entidades del estado, donde la información se constituye en uno de los activos de mayor valor. Por este motivo, para garantizar la protección de la misma son necesarios unos sistemas de privacidad adecuados, así como una correcta gestión de la seguridad.

Teniendo en cuenta que las entidades están expuestas a todo tipo de riesgos y amenazas, el presente proyecto se centra en ayudar a preservar la confidencialidad, integridad y disponibilidad; a través del diseño de un sistema de gestión de seguridad de la información que sirva como guía para todo tipo de organizaciones. Por lo tanto, lo puedan utilizar como referencia para asegurar y proteger la información de los ciudadanos y funcionarios de la entidad.

Con un sistema de gestión de seguridad de la Información y utilizando como marco de referencia el código de buenas prácticas de la norma ISO/IEC 27001, las entidades conocen los riesgos y las amenazas a los que está sometida la información y sus activos, de esta manera los asume, minimiza, protege y controla mediante unos procedimientos sistémicos, documentados y conocido por todos.

Para las entidades del estado es fundamental contar con políticas de seguridad alineadas a las necesidades y objetivos estratégicos del negocio, compuesto por una estructura organizacional con roles, responsabilidades y un conjunto coherente de procesos gestionados correctamente, con el objetivo de promover y extender una cultura de seguridad en todos los niveles de la organización, y de esta forma gestionar adecuadamente la protección de la información.

Establecer un sistema de gestión de seguridad de la Información define el comportamiento personal y profesional de los funcionarios, ciudadanos, contratistas o terceros sobre la información procesada por la organización, así mismo, permite que la entidad trabaje bajo los mejores estándares y prácticas de seguridad y protección de datos; con lo cual evidentemente el presente documento es un aporte valioso para cada una de estas entidades.

4. OBJETIVOS DEL PROYECTO

4.1 OBJETIVO GENERAL

Diseñar un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC 27001 que permita preservar la integridad, confidencialidad y disponibilidad de la información en las entidades del estado.

4.2 OBJETIVOS ESPECÍFICOS

- Identificar los activos informáticos comunes que se manejan en las entidades del estado para determinar los dominios del estándar que serán aplicados para el diseño del SGSI.

- Determinar los factores de amenaza, las vulnerabilidades y riesgos de seguridad informática y de la información que afectan a las entidades del estado.

- Aplicar la metodología de análisis y evaluación de riesgos para determinar el impacto de los riesgos detectados.

- Verificar la existencia de controles de seguridad informática y de la información de acuerdo a la norma ISO 27001:2013 en las entidades del estado

- Diseñar las Políticas de Seguridad de la información para las entidades del estado basado en la ISO 27001:2013.

5. MARCO DE REFERENCIA

5.1 ANTECEDENTES

Para ilustrar la investigación sobre el diseño de un sistema de gestión de seguridad de la información que sirva como modelo para entidades del estado, se realizó una revisión bibliográfica basada en documentos claves que aporten para el desarrollo del presente proyecto de grado.

A continuación, se establecen los diferentes trabajos e investigaciones relacionadas con el desarrollo del presente trabajo:

Articulo Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000, elaborado por Francisco Javier Valencia Duque y Mauricio Orozco Álzate de la Universidad Nacional de Colombia, sede Manizales, Departamento de Informática y Computación, Campus La Nubia. Revista ibérica de Sistemas y Tecnologías de Información. RISTI Nº 22, 06/2017.

Este artículo ofrece información acerca de la implementación de un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC 27001 para entidades del estado en Colombia, acorde con la normatividad vigente en el país.

Norma Técnica Colombiana NTC-ISO/IEC 27001:2013, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos

El objetivo de esta norma técnica colombiana esta en especificar los requisitos para implementar, establecer, mantener y mejorar cada día un sistema de gestión de la seguridad de la información dentro del contexto de la entidad.

Articulo 5482 Modelo de Seguridad y Privacidad de la Información, elaborado por parte del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, Gobierno de Colombia.

Documento presentado por el gobierno de Colombia que sirve como modelo para que sea adoptado por las entidades de orden nacional y territorial, es una guía de buenas prácticas que suministra requisitos para la implementación de un sistema de gestión de seguridad de la información.

Articulo Método para implementar un SGSI según el ISO/IEC 27001:2013, elaborado por Gianncarlo Gómez Morales.

El propósito del artículo es desarrollar y proponer un método que permita implementar un Sistema de Gestión de Seguridad de la Información aplicable a cualquier tipo de entidad, incluyendo el proceso de certificación del ISO/IEC 27001:2013.

Proyecto de grado, Diseño de un Sistema de Gestión de seguridad de la información (SGSI) basado en ISO27001 para laboratorios servicios farmacéuticos de calidad SFC Ltda. Presentada por el ingeniero Jorge Leonardo Rodríguez Correa, Especialización en Seguridad Informática de la Universidad Nacional Abierta y a Distancia UNAD. Año 2017.

Este proyecto de grado utiliza en su estructura la norma ISO27001:2013, adicionalmente ofrece información acerca de la metodología de implementación de un Sistema de Gestión de seguridad de la información (SGSI).

Proyecto de grado, Diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI) en el área tecnológica de la Comisión Nacional del Servicio Civil - CNSC basado en la norma ISO27000 e ISO27001, presentada por Juan David Camargo Ramírez, Especialización en Seguridad Informática de la Universidad Nacional Abierta y a Distancia UNAD. Año 2017.

Proyecto de grado realizado a una entidad del estado colombiano donde se implementó un Sistema de Gestión de Seguridad de la Información en el área tecnológica, por lo tanto utilizo como referencia la norma ISO27001 en su metodología.

5.2 MARCO CONTEXTUAL

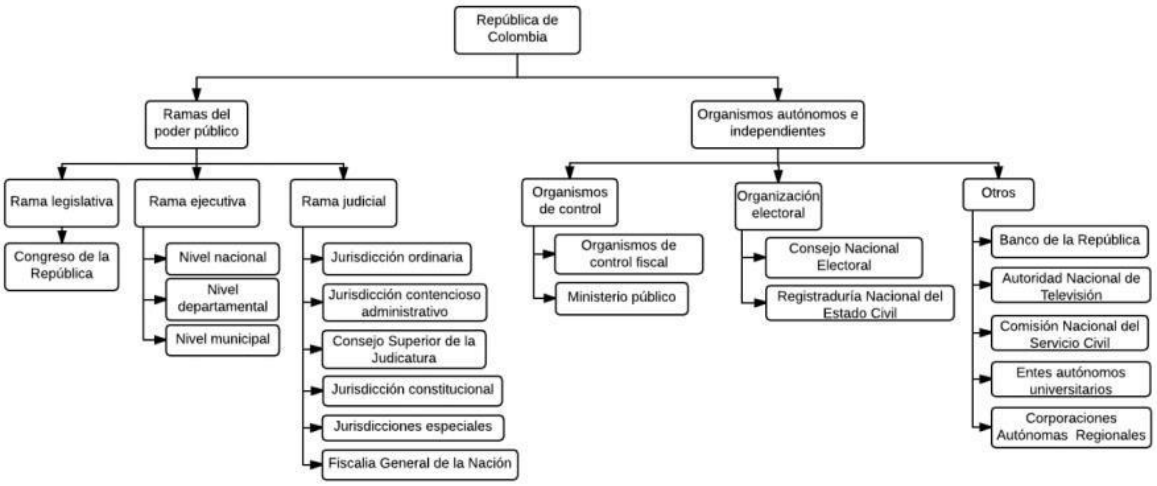
En contexto, el desarrollo del presente proyecto se realiza en términos generales como una guía que puede ser adoptada por entidades del estado, ya sean del orden nacional o del orden territorial. Este diseño de un sistema de gestión de seguridad de la información pretende que sirva como modelo de implementación en la necesidad que tienen las entidades del estado de salvaguardar su información.

En Colombia las entidades del estado están tipificadas a partir de la Constitución Política de 1991, Colombia está organizada de tal forma como República unitaria (Const., 1991, art. 1) por lo tanto, cuenta con un solo orden jurídico válido para todo el territorio nacional y su poder político se ejerce por la estructura central del gobierno.

De acuerdo con lo establecido en el Título V de la Constitución Política, el Estado Colombiano está compuesto por tres ramas del Poder Público (legislativa,

ejecutiva y judicial), y otros órganos, autónomos e independientes, que contribuyen al cumplimiento de las funciones de Estado (Const., 1991, art. 113)[1].

Figura 1. Estructura Orgánica del Estado Colombiano



Fuente: Elaborado a partir del Manual de estructura del Estado Colombiano del Departamento Administrativo de la Función Pública.

5.3 MARCO TEORICO

5.3.1 Seguridad informática. Se define como un área de la informática que se enfoca en proteger la infraestructura tecnológica y de comunicaciones que soportan la operación de una organización, se caracteriza básicamente en la seguridad de todo lo relacionado al hardware y software.

Su análisis de riesgos esta direccionado a vulnerabilidades del hardware o software, y llevar el nivel de riesgo a un nivel aceptable por la organización[2].

5.3.2 Seguridad de la información. Se define como el área de la informática encargada de la protección y privacidad de los datos contra las amenazas y

[1] ORGANIZACIÓN DEL ESTADO COLOMBIANO. Entidades del estado, [en línea]. <http: //enciclopedia.banrepcultural.org/index.php/Organización_del_Estado_colombiano> [citado en 27 de septiembre de 2017]
[2] SEGURIDAD DE LA INFORMACION EN COLOMBIA. Seguridad Informática, [en línea]. <http://seguridadinformacioncolombia.blogspot.com.co/2010/02/seguridad-de-la-informacion-y-seguridad.html.> [citado en 27 de septiembre de 2017]

eventos que atenten con el acceso, uso, divulgación, interrupción y destrucción de forma no autorizada[3].

De acuerdo con la norma ISO 27001, la seguridad de la información busca preservar la confidencialidad, integridad y disponibilidad de los datos mediante el establecimiento de un conjunto coherente de procesos, normas y herramientas para la gestión eficaz de acceso a la información, y la implementación de mecanismos y medidas de seguridad tanto físicas como lógicas, orientadas a la prevención y detección de amenazas internas y externas que puedan atentar contra la seguridad de la organización y la continuidad del negocio.

Por lo tanto, es un proceso de mejora continua que demanda la participación activa de toda la organización y busca preservar, entre otros, los siguientes principios de la información:

- **La confidencialidad:** Este principio tiene como objetivo asegurar que solo las personas debidamente autorizadas tengan acceso a la información.

- **La integridad**: Este principio tiene como objetivo asegurar que la información no sea modificada sin la debida autorización.

- **La disponibilidad:** Este principio tiene como objetivo asegurar que la información esté totalmente disponible para las personas debidamente autorizadas cuando ellos la requieran.

- **La autenticidad:** Este principio tiene como propósito garantizar la identidad de la persona que genera la información. La autenticidad de la información es la capacidad de asegurar que el emisor de la información es quien dice ser y no un tercero que esté intentando suplantarlo.

- **La trazabilidad:** con el objetivo de poder monitorear o rastrear cualquier operación que se realiza sobre la información desde su mismo origen.

- **El no repudio**: con el propósito de conocer exactamente quienes son los actores que participan en una transacción o una comunicación y no puedan negarlo en ningún momento. El no repudio evita que el emisor o el receptor nieguen la transmisión de un mensaje.

5.3.3 Gestión de seguridad de la información. Se define como un proceso continuo que se enfoca en garantizar que los riesgos de la seguridad de la

[3] UNIVERSIDAD LIBRE. Seguridad de la Información, [en línea]. <http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/152-seguridad-de-la-informacion> [citado en 27 de septiembre de 2017]

información sean identificados, valorados, gestionados y tratados por todos los miembros de la organización de una forma documentada, sistemática, estructurada, eficiente y adaptada a los cambios que se produzcan en los riesgos.

La gestión de la seguridad de la información requiere la participación activa de toda la organización con relación a la planeación, definición, identificación e implementación de controles y medidas orientadas a salvaguardar la seguridad de la información, así como el debido control de acceso a los recursos y activos de información[4].

5.3.4 Sistema de gestión de seguridad de la información (SGSI). De acuerdo con la norma ISO 27001, se define como una herramienta de gestión que utiliza una metodología de buenas prácticas para realizar procesos sistemáticos, documentados y conocidos por una organización o entidad. Por lo tanto permite establecer políticas, procedimientos y controles con el objetivo de disminuir los riesgos y preservar la seguridad de la información.

De acuerdo a la norma NTC-ISO-IEC 27001:2013[5], un sistema de gestión de seguridad de la información tiene por finalidad preservar la confidencialidad, integridad y disponibilidad de la información, a través de la aplicación de un proceso de gestión del riesgo.

5.3.5 Normas ISO/IEC 27000. La familia de las normas ISO/IEC 27000, están definidas como un marco de referencia de seguridad a nivel mundial, desarrollado y diseñado por la *International Organization for Standardization - ISO e International Electrotechnical Commission – IEC*, que proporcionan un marco de lineamientos y mejores prácticas para la debida gestión de seguridad de la información en cualquier tipo de organización. Estas normas especifican los requerimientos y procedimientos que deben cumplir las organizaciones para implementar, establecer, poner en funcionamiento, controlar y mejorar continuamente un sistema de gestión de seguridad de la información.

En Colombia, el Instituto Colombiano de Norma Técnicas y Certificaciones, ICONTEC, es el organismo encargado de normalizar este tipo de normas según el Decreto 2269 de 1993.

5.3.6 Norma ISO/IEC 27001. Establece los requisitos y proporciona una metodología para gestionar la seguridad de la información en una organización,

[4] BSI. Norma ISO/IEC 27001 - Gestión de la Seguridad de la Información. [en línea]. <https://www.bsigroup.com/es-ES/Seguridad-de-la-Informacion-ISOIEC-27001/> [citado en 27 de septiembre de 2017]
[5] NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27001:2013, Capitulo Introducción.

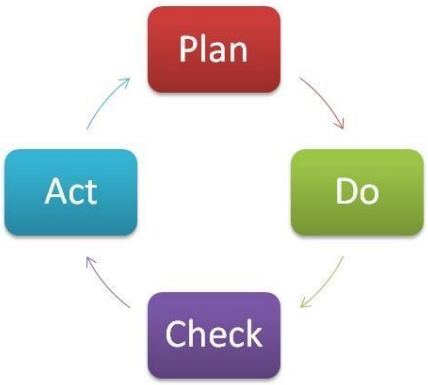
está redactada por los mejores especialistas a nivel mundial en el tema, por lo tanto puede ser implementada en cualquier tipo de organización, sin importar su actividad económica o el tamaño de la misma.

La última versión de esta norma fue publicada a finales del 2013, y corresponde a la principal norma de la serie 27000, adicionalmente esta norma también incluye los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adoptadas a las necesidades de la organización[6].

5.3.7 Ciclo PHVA. Establece los requisitos para la implementación de un sistema de mejora continua, por lo tanto se usa para monitorear y adoptar el proceso de planeación de un sistema de gestión. P.H.V.A. sus siglas en español significan (planear, hacer, verificar y actuar), este ciclo permite planear, tomar acciones, verificar los resultados y actuar sobre los resultados obtenidos.

5.3.8 Ciclo de mejora continua vs norma ISO/IEC 27001:2013. Conocido también como ciclo PDCA (del inglés *plan-do-check-act*) o PHVA (planificar-hacer-verificar-actuar) o Ciclo de Deming por ser Edwards Deming su creador, es uno de los sistemas más usados para la implementación de un sistema de mejora continua, el cual establece los siguientes cuatro pasos o fases esenciales que de forma sistemática las organizaciones deben llevar a cabo para lograr la mejora continua de sus sistemas de gestión.

Figura 2. Ciclo de mejora continua (Ciclo Deming).



Fuente: http://www.pdcahome.com/5202/ciclo-pdca/

[6] NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27001:2013, Pág. 1

El ciclo PHVA consiste básicamente en:

- **Fase Planificar (*Plan*):** En esta etapa del ciclo se establecen los objetivos a lograr y las actividades del proceso susceptibles de mejora, igualmente con los indicadores de medición para controlar y cuantificar los objetivos.
- **Fase Hacer (*Do*):** En esta etapa del ciclo se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.
- **Fase Verificar (*Check*):** En esta etapa del ciclo una vez implementada la mejora, se estipula un periodo de prueba para verificar el perfecto funcionamiento de las acciones implementadas.
- **Fase Actuar (*Act*):** En esta etapa del ciclo se analizan los resultados de las acciones implementadas y si estas por cualquier razón no se cumplen con los objetivos definidos, se analizan las causas de las desviaciones y se generan los respectivos planes de acción.

La siguiente figura muestra la relación entre las fases del ciclo de mejora continua P.H.V.A (Planear, Hacer, Verificar y Actuar) y la estructura de capítulos y numerales de la norma ISO 27001:2013:

Figura 3. Ciclo de mejora continúa alineado a la norma ISO 27001:2013.

Fuente: Elaborada con base en la información publicada en el sitio web http://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la-norma-para-gestionar-la-seguridad-de-la-informacion/

5.3.8.1 Fase PLANEAR. En la norma ISO 27001:2013 En el capítulo 4 - Contexto de la organización[7], se determina la necesidad de realizar un análisis de los factores externos e internos de la organización y de su contexto, con el fin de incluir las necesidades y expectativas de las partes interesadas de la organización en el alcance del Sistema de gestión de seguridad de la información.

En el capítulo 5 - Liderazgo[8], se determinan las responsabilidades y los compromisos de la alta gerencia con respecto al sistema de gestión de seguridad de la información.

En el capítulo 6 - Planeación[9], se proporcionan los lineamientos para la valoración y tratamiento de riesgos y para la definición de objetivos viables de seguridad de la información.

En el capítulo 7 - Soporte[10] se determina que la organización debe asegurar los recursos necesarios para la implementación, establecimiento, y mejora continua del sistema de gestión de seguridad de la información.

5.3.8.2 Fase HACER. En la norma ISO 27001:2013. En el capítulo 8 - Operación[11]. Se establece que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los objetivos de seguridad, y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.

5.3.8.3 Fase VERIFICAR. En la norma ISO 27001:2013. En el capítulo 9 - Evaluación del desempeño[12], se proporcionan los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia de la misma.

5.3.8.4 Fase ACTUAR. En la norma ISO 27001:2013. En el capítulo 10 - Mejora, Se establecen los procesos de mejora continua del sistema de gestión de seguridad de la Información, que a partir de las no-conformidades que sucedan, las organizaciones deben determinar las acciones más efectiva para solucionarlas y así poder evaluar la necesidad de acciones para poder eliminar las causas de la no conformidad con el objetivo de que no vuelvan a ocurrir.

---

[7] NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27001:2013, Pág. 1-2
[8] Ibídem, Pág. 2-3
[9] Ibídem, Pág. 4-6
[10] Ibídem, Pág. 6
[11] Ibídem, Pág. 8-9
[12] Ibídem, Pág. 9-11

5.3.9 MAGERIT. Metodología de análisis y gestión de riesgos, desarrollada por el Consejo Superior de Administración Electrónica de España, ofrece un método de procedimientos sistemáticos para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC), para de esta forma diseñar e implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados[13].

Prácticamente Magerit se basa en analizar el impacto que puede tener para las organizaciones la vulneración de la seguridad, de esta manera busca identificar las amenazas que pueden llegar a poner en riesgo la organización.

Esta metodología está dividida en cuatro etapas:

- Planificación (definir lo que se va a cumplir).
- Análisis de Riesgos.
- Gestión de riesgos.
- Seleccionar las salvaguardas.

Esta metodología de buenas prácticas permite establecer una cuantificación y calcular el valor del activo de acuerdo al nivel de impacto que su daño o perdida pueda provocar en la organización si se materializa. Esta valoración puede realizarse de manera cuantitativa o cualitativa de acuerdo a la siguiente escala:

- Muy Alto (MA)
- Alto (A)
- Medio (M)
- Bajo (b)
- Muy bajo (MB)

Es una metodología robusta, gratuita y que permite a los responsables en sistemas de información realizar un análisis y gestión de riesgos profundo, clasificar los activos, identificar las amenazas asociados a los activos, su nivel de impacto en la organización y seleccionar las salvaguardas más adecuadas para tratar y minimizar los riesgos y amenazas detectados previamente.

5.3.10 EAR / PILAR. Se define como una herramienta que implementa la metodología MAGERIT, la cual soporta el análisis y gestión de riesgos de un sistema de información.

[13] MAGERIT. Metodología práctica para gestionar riesgos, [en línea]. <https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/ > [citado en 28 de septiembre de 2017]

Esta herramienta dispone de una biblioteca estándar de propósito general, y es capaz de realizar calificaciones de seguridad respecto de normas ampliamente conocidas como son[14]:

- COBIT.
- ISO/IEC 27002:2005.
- Esquema Nacional de Seguridad.

5.4 MARCO CONCEPTUAL

De acuerdo con el tema de estudio, se presentan los principales referentes conceptuales relacionados directamente con Sistemas de Gestión de la Seguridad de la Información.

5.4.1 Seguridad informática y de la información. A simple interpretación pareciera que tienen el mismo significado, especialmente si se tiene en cuenta que el auge y avance de la tecnología tiende hacia un modelo de digitalizar y asegurar cualquier tipo de información mediante un sistema informático. Aunque se encuentran destinados a trabajar de forma conjunta, cada una de las áreas de seguridad tiene objetivos y actividades diferentes.

Hoy en día, es común ver en la red el término internet de todo, la forma en cómo están interconectados las cosas, las personas, los dispositivos, los procesos y los datos. La forma en como viaja la información de forma constante de una parte a otra mediante correo electrónico, las transacciones en línea, unidades USB y discos duros externos, todo este avance de las nuevas tecnologías hacen que las organizaciones y entidades tomen mayor conciencia sobre qué mecanismos y procedimientos deben utilizar para salvaguardar y proteger su información.

5.4.1.1 Seguridad Informática. Se considera como el área de la seguridad que establece los procedimientos o técnicas para asegurar la información en formato digital y la estructura tecnológica de cualquier organización.

Para las organizaciones y entidades es importante diseñar y establecer las medidas de seguridad y procedimientos que debe soportar la infraestructura

[14] ANÁLISIS Y GESTIÓN DE RIESGOS. Herramienta EAR / PILAR, [en línea]. <https://www.aec.es/c/document_library/get_file?uuid=b3945e58-17f2-4dc0-88ac-863ae9f998cb&groupId=10128> [citado en 28 de septiembre de 2017]

tecnológica, con el fin de minimizar los riesgos y pérdidas de información, ya que es el activo vital con mayor importancia en una entidad de cualquier tipo.

Para el caso del presente proyecto se pretende que la infraestructura tecnológica de una organización o entidad cuente con las herramientas necesarias que permitan tener información confiable para la misma.

Los procedimientos de seguridad que se establezcan deben contar con políticas y controles que hayan sido definidos de forma profesional, por lo tanto lo que se quiere es que las entidades puedan manejar su información de forma segura, y a su vez que esta no se ponga en riesgo ante situaciones intencionales o no intencionales para los cuales no se haya previsto una política con anterioridad.

5.4.1.2 Seguridad de la información. Se considera la disciplina que tiene como finalidad salvaguardar y proteger toda la información existente (físico, digital u otros), no importando en qué clase de medio se encuentre almacenada.

Para obtener los resultados se apoya en la seguridad informática, por lo tanto, a pesar de ser disciplinas diferentes, la una no puede ir sin la otra. De manera que la seguridad de la información será la encargada de regular y establecer las pautas a seguir para la protección de la información.

Para el caso del presente proyecto, las entidades del estado deben tomar todos los mecanismos para asegurar la información. Ya que la mayoría no la tienen asegurada y están expuestas a todo tipo de riesgos, por lo tanto, el objetivo de este proyecto es preservar la confidencialidad, integridad y disponibilidad de la información con el sistema de gestión de seguridad de la información que sirva como guía para todo tipo de organizaciones.

Para que la información esté asegurada y sea confiable debe cumplir con lo siguiente:

Confidencialidad: Propiedad que la información no esté disponible o pueda ser descubierta por usuarios no autorizados, entidades o procesos.
Integridad: Propiedad de salvaguardar la precisión y completitud de los recursos.
Disponibilidad: Propiedad de ser accesible y usable bajo demanda por una entidad autorizada.

5.4.2 Amenaza. Hoy en día todas las organizaciones y sistemas informáticos están expuestos a imprevistos que puede ser de origen natural o intencionado, las amenazas consisten en una causa potencial de un suceso no deseado, por lo tanto tienen la capacidad de provocar daños y atentar contra la seguridad de la información.

Las amenazas se manifiestan por la existencia de vulnerabilidades, por lo tanto sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.

A continuación clasificación de tipos de amenazas:

- Intencionales: En caso de que a propósito se intente producir un daño, por ejemplo el robo de información aplicando la propagación de código malicioso y las técnicas de ingeniería social.
- No intencionales: En donde se producen hechos u omisiones de acciones que si bien no buscan explotar una vulnerabilidad, ponen en riesgo los activos de información y pueden producir un daño, por ejemplo las amenazas relacionadas con fenómenos naturales.

5.4.3 Vulnerabilidad. En la actualidad es un tema que se escucha frecuentemente en el área de la seguridad de la información, diariamente se observa en diferentes medios, cómo los ataques han aprovechado las vulnerabilidades encontradas en sistemas informáticos para causar daños graves en las organizaciones y entidades a nivel global.

En materia de protección de la información, consiste en una debilidad de cualquier tipo presente en un sistema informático el cual afecta y/o compromete la seguridad de la organización, lo que le permitiría a un atacante explotar y violar la confidencialidad, integridad, disponibilidad de la misma.

Para las organizaciones y entidades es importante determinar que las vulnerabilidades están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño.

5.4.4 Riesgo. En las organizaciones hoy en día, la información sigue siendo el activo más valioso. Es por ello que debe ser protegida de cualquier posibilidad de ocurrencia de eventos de riesgo de seguridad de la información y que pudiese

significar un impacto indeseado generando una consecuencia negativa para el normal funcionamiento de las actividades de las entidades.

El riesgo según la norma ISO/IEC 27001 se define como la situación de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Por lo tanto, puede considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
De igual manera, el objetivo general de dicha norma es gestionar el riesgo para identificar y establecer controles efectivos que garanticen la confidencialidad, integridad y disponibilidad de la información en las organizaciones.

5.4.5 Sistema de gestión de seguridad de la información (SGSI) en entidades. El avance tecnológico que se está presentando en la actualidad en este mundo globalizado trae consigo grandes desafíos que originan inquietudes a los altos directivos de una organización. Prometer un máximo nivel de disponibilidad, integridad y confidencialidad de la información es un aspecto de gran importancia que se procura tener en cuenta dentro de las labores organizacionales hoy en día[15].

En el área de la tecnología las entidades y organizaciones están constantemente expuestas a diferentes amenazas tales como los ataques de ciberdelincuentes en busca de datos confidenciales y de gran interés comercial, sabotajes, modificación de información altamente confidencial, entre otras, que se realizan con algún interés comercial, económico, competitivo o con el objetivo de que el atacante obtenga alguna reputación. Pero esta problemática no solo afecta a las grandes organizaciones con una gran infraestructura para su funcionamiento, hoy en día ni las grandes y pequeñas empresas, ni las entidades del estado o personas del común están exentas, o se encuentran vulnerables ante algún ataque informático.

Por lo anterior, es de gran importancia para las entidades la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) el cual está desarrollado bajo la norma ISO27001 y establece unos procesos sistemáticos para la protección ante cualquier amenaza que podría llegar afectar la confidencialidad, integridad o disponibilidad de la información. Este sistema proporciona las mejores prácticas y procedimientos que siendo aplicados de manera correcta, suministra una mejora continua y apropiada para evaluar los riegos que se presentan a diario, establecer controles para una mejor protección y defender así el activo más importante dentro de la organización, como lo es la información.

[15] IMPORTANCIA DE IMPLEMENTAR UN SGSI EN NUESTRA ORGANIZACIÓN, [en línea]. < https://www.safesociety.co/importancia-de-implementar-un-sgsi-en-nuestra-organizacion/> [citado en 28 de septiembre de 2017]

En resumidas cuentas, un sistema de gestión de seguridad de la información es una herramienta de gestión que utiliza una metodología sencilla y de buenas prácticas con el objetivo de establecer políticas, procedimientos y controles para disminuir los riesgos de una organización[16].

La implementación de este sistema dentro de las entidades resulta de gran importancia ya que proporciona muchos beneficios como, por ejemplo:

- El acceso a la información tendrá controles de acuerdo con niveles de seguridad y confidencialidad que dificultan la manipulación por parte de personas no autorizadas.
- Garantiza la continuidad del negocio, aspecto importante dentro de la competitividad empresarial.
- Garantiza un alto nivel de confidencialidad, integridad y disponibilidad de la información manejada en las labores diarias en la organización.
- Los funcionarios, contratistas y ciudadanos, obtienen mayor confianza debido a la calidad y confidencialidad que genera la implementación de un SGSI.

5.4.6 Generalidades Norma ISO/IEC 27001:2013. Emitida por la Organización Internacional de Normalización (ISO), establece las herramientas para poder implementar, mantener y mejorar un sistema de gestión de seguridad de la Información en una organización.

Es un estándar para la seguridad de la información que abarca las diferentes directivas que deben utilizar para mantener la red de la organización a salvo. La implementación de estos procedimientos que plantea esta norma ayuda a revisar punto a punto todos los patrones de seguridad que se tienen que cumplir para asegurar el buen funcionamiento de los sistemas de información[17].

Esta norma busca proponer un modelo para la implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI), convirtiéndose en una decisión estratégica para las organizaciones que desean proteger sus activos de los sistemas de información.

Para el presente proyecto se utiliza la norma ISO/IEC 27001:2013 como referencia, ya que para la implementación de un sistema de gestión de seguridad

[16] EL PORTAL DE ISO 27001 EN ESPAÑOL. SGSI, [en línea]. <http://www.iso27000.es/sgsi.html> [citado en 28 de septiembre de 2017]
[17] ISOTOOLS. ISO27001, [en línea]. <https://www.isotools.org/2018/03/05/la-norma-iso-iec-27000-va-a-ser-revisada/> [citado en 28 de septiembre de 2017]

de la información brinda las herramientas suficientes para realizar un trabajo estructurado y enfocado en buenas prácticas que exigen las organizaciones hoy en día.

5.4.7 Política de seguridad de la información. Para la correcta implementación de un sistema de gestión de seguridad de la información las entidades deben definir la formulación de unas políticas de seguridad, las cuales son un elemento fundamental para poder gestionar la seguridad de la misma en una organización.

Estas políticas, son los documentos básicos para respaldar lo que se ha denominado gobierno de seguridad de la información, es decir, todas aquellas responsabilidades y prácticas que ejerce la alta dirección en cuanto a la seguridad[18].

En la actualidad estas políticas son consideradas como un conjunto de documentos y procedimientos, que se encuentran sistematizados e indican las normas, y las actuaciones que se deben cumplir por parte de la organización.

En este sentido, también ayudan en la definición de los lineamientos para determinar la conducta esperada de los funcionarios, contratistas y ciudadanos, a través de la definición de funciones y responsabilidades.

5.4.8 Plan de tratamiento de riesgos. Es considerado por la norma ISO 27001 como el documento donde se establecen las bases para la seguridad del activo de mayor importancia de una organización. Por lo tanto, determina las acciones para gestionar los riesgos de seguridad de la información que no son permitidos y así poder implementar los controles necesarios para proteger la misma.

5.4.9 Declaración de aplicabilidad. Considerado como un requisito de documentación en el estándar ISO/IEC 27001, puede ser utilizado por cualquier organización, como una manera de mantener el registro y control de las medidas de seguridad que son aplicadas.

Este documento tiene como objetivo definir y enumerar cuales son los controles que serán aplicados por el sistema de gestión de seguridad de la información en la

[18] WELIVESECURITY. Beneficios de la aplicación efectiva de políticas de seguridad, [en línea]. <https://www.welivesecurity.com/la-es/2014/07/25/beneficios-aplicacion-efectiva-politicas-de-seguridad/> [citado en 28 de septiembre de 2017]

organización. Por lo tanto, tiene la obligación de aprobar riesgos residuales y aprobar formalmente la implementación de los controles mencionados[19].
Dicho documento hace un listado de los controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001 (un conjunto de 114 controles agrupados en 35 objetivos de control, en la versión de 2013 de esta norma de seguridad).

Para el caso del presente proyecto se realizará el formato y se diligenciará este documento para que sirva como modelo y pueda ser adoptado por la entidad que lo deseen implementar, lo relevante es su contenido, que en general debe incluir los objetivos de control y controles seleccionados del estándar, las razones por las cuales han sido seleccionados y medidas de seguridad adicionales si es el caso.

Finalmente, un documento de esta naturaleza permite tener un panorama amplio de lo que está haciendo una entidad para salvaguardar su información, por lo tanto, es importante que toda entidad que implemente un sistema de gestión de seguridad de la información desarrolle una Declaración de Aplicabilidad, que contribuya a la identificación, organización y registro de las medidas de seguridad que se están implementando y las que se desean poner en marcha.

5.4.10 Plan de continuidad del negocio. De acuerdo con la norma ISO/IEC 27000 es considerado como un plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro[20].

Cuando se habla de continuidad del negocio se refiere a la capacidad de sobrevivir a las “cosas malas” que pueden tener un impacto negativo en la entidad u organización, desde un simple virus informático hasta un brote de virus biológico, y todos los demás peligros como incendios, inundaciones y catástrofes naturales.

Este documento ayuda a las entidades u organizaciones a establecer procedimientos que deberán seguir en caso de un desastre o materialización de un riesgo y reconocer los servicios que como negocio tendrán que restablecerse de manera oportuna para garantizar la operación y atención a los funcionarios, contratistas y ciudadanos de dicha entidad, respondiendo a las siguientes preguntas: ¿Cuándo? ¿Cómo? Y ¿en qué tiempo?

[19] ADVISERA. Declaración de Aplicabilidad, [en línea]. <https://advisera.com/27001academy/es/documentation/declaracion-de-aplicabilidad/> [citado en 28 de septiembre de 2017]

[20] INCIBE. Plan de Contingencia y Continuidad de Negocio, [en línea]. <https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingencia-continuidad-negocio> [citado en 28 de septiembre de 2017]

Por lo tanto, la entidad podrá reducir el impacto de un desastre y fortalecer la respuesta ante un evento de este tipo, garantizando así menores pérdidas que pudieran ser humanas, materiales y económicas.

5.4.11 Ciberseguridad. En la actualidad con el auge y avance de las nuevas tecnologías surgen un sinnúmero de términos informáticos que vienen tomando mayor relevancia cada día, Este término de ciberseguridad hace referencia a la capacidad que tiene el estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética según documento CONPES 3701[21].

5.5 MARCO LEGAL

Las siguientes son las principales leyes o normativas directamente ligadas con un Sistema de Gestión de Seguridad de la Información:

5.5.1 Decreto 1151 de 2008. "¨Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea de la república de Colombia, se reglamenta parcialmente la ley 962 de 2005, y se dictan otras disposiciones"[22]

5.5.2 Ley 1273 de 2009. "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"[23]

[21] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Ciberseguridad, [en línea]. <https://www.mintic.gov.co/portal/604/w3-article-6120.html> [citado en 28 de septiembre de 2017]

[22] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 1151 de 200, [en línea]. <https://www.mintic.gov.co/portal/604/articles-3643_documento.pdf> [citado en 28 de Agosto de 2017]

[23] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Ley 1273 de 2009, [en línea]. <http://www.mintic.gov.co/portal/604/w3-article-3705.html> [citado en 28 de Agosto de 2017]

5.5.3 Ley 1712 de 2014. "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones."[24]

5.5.4 Decreto 2573 de 2014. "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones".[25]
En lo referente a seguridad de la información, la Ley 1341 de 2009 "por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones –TIC- se crea la agencia nacional de espectro y se dictan otras disposiciones", señala en su artículo dos (2), como principios orientadores y aspectos fundamentales para la promoción de la libre competencia y el comercio electrónico, lo siguiente: la protección a los derechos de los usuarios de las TIC, el acceso y uso de las TIC, la garantía de los derechos de los ciudadanos y la masificación del Gobierno en Línea. Adicional a lo expuesto, el Gobierno Nacional, a través del documento CONPES 3701 del 14 de julio de 2011, estableció la Estrategia Nacional de Ciberseguridad y Ciberdefensa, con el fin de desarrollar medidas que aseguren la información de los ciudadanos frente a las amenazas informáticas, estableciendo compromisos a cargo del Ministerio de las TIC, entre otras entidades relacionados con el diseño e implementación de planes, políticas, estrategias, gestión, capacitación y sensibilización en lo referente a seguridad de la información.

Con la expedición del decreto 2618 del 2012, se modifica la estructura del Ministerio de las TIC, se crea la Subdirección de Seguridad y Privacidad de TI, la cual tiene las siguientes funciones:

- Formular y liderar proyectos para identificar fortalezas y debilidades relacionadas con la estructura de la información tales como la innovación, adaptación y obsolescencia tecnológica para garantizar estándares de calidad y seguridad de la información en coordinación con la Subdirección de Gestión Pública de Tecnologías de la Información.
- Promover la investigación, el desarrollo y la innovación del Sector en materia de la ciberseguridad, que proporcione soluciones de tecnologías de la información requeridas por el Estado.
- Promover en la dinámica del Estado una cultura de la ciberresponsabilidad, basada en la concientización y formación continua en ciberseguridad, a través

[24] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Ley 1712 de 201, [en línea]. <http://www.mintic.gov.co/portal/604/w3-article-7147.html> [citado en 28 de Agosto de 2017]
[25] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 2573 de 2014, [en línea]. <http://tic.bogota.gov.co/images/boletines/DECRETO-2573-DEL-12-DE-DICIEMBRE-DE-2014-1.pdf> [citado en 28 de Agosto de 2017]

de planes de estudio que desarrollen teoría práctica aplicable en las organizaciones y provean empleo cualificado.

- Fomentar y reforzar la cooperación internacional en materia de ciberseguridad a través de alianzas multinacionales y bilaterales en la materia.
- Identificar los activos dependientes del ciberespacio, así como su regulación y definir el marco funcional y de responsabilidades en la materia, centrándose en la defensa de las infraestructuras críticas, el tejido empresarial y las libertades y derechos individuales, conforme a la ley vigente.
- Definir los lineamientos de política y estándares de protección de la información pública, para su preservación en situaciones de desastre.
- Elaborar una estrategia de seguridad de la información que soporte un marco normativo específico para las entidades del orden nacional y en coordinación con las entidades del orden territorial respetando la autonomía administrativa.
- Definir, conjuntamente con las autoridades competentes, una estrategia de seguridad y privacidad de la información desde la perspectiva de la tecnología en las dimensiones de la protección de bienes, activos, servicios, derechos y libertades dependientes del Estado y que coordine las agencias y entidades público -privadas relacionadas con este fin.
- Liderar la implementación en el Estado de plataformas con estándares de seguridad y privacidad de la información en coordinación con las autoridades pertinentes.

6. DISEÑO METODOLOGICO

6.1 METODOLOGIA DE INVESTIGACION

El desarrollo del presente proyecto se basa en un enfoque de procesos sistemáticos y documentados, construidos a partir de una herramienta de gestión que permita implementar y salvaguardar la seguridad de la información en una entidad del estado.

En complemento, el tipo de investigación que se implementará en el presente proyecto será descriptiva y aplicada, puesto que la finalidad es estructurar una herramienta de gestión que sirva como guía con recomendaciones apropiadas que puedan ser utilizadas y adoptadas en entidades del estado o por los interesados de manera posterior a su publicación.

Para llevar a cabo todo el proceso de una manera más estructurada, el presente proyecto estará alineado al estándar ISO27001:2013, con el fin de poder implementar el Sistema de Gestión de Seguridad de la Información con los mejores procedimientos y códigos de buenas prácticas de seguridad.

El alcance del proyecto en términos generales depende del nivel de madurez que pueda tener cada entidad, por lo tanto, los procesos y procedimientos que se describen en esta guía de implementación son un punto de referencia inicial, con el fin de proporcionar lineamientos que puedan ser consultados después de su publicación en el repositorio de la UNAD.

Con base en lo anterior, la metodología que se adoptara para el diseño del SGSI para entidades del estado es el ciclo de mejora continua PHVA (planificar-hacer-verificar-actuar).

6.1.1 Población y Muestra. Este proyecto está planteado para que sea adoptado como una guía de implementación, por lo tanto, su población seleccionada para la investigación son todas las personas involucradas directa e indirectamente con una entidad del estado, como son los servidores públicos, contratistas, proveedores, y todas las dependencias donde se realizan las operaciones que hacen parte de la entidad.

El Sistema de Gestión de Seguridad de la Información, se aplicará específicamente a la infraestructura tecnológica de la entidad, a los funcionarios y ciudadanos que hacen parte del capital humano.

6.1.2 Instrumentos de recolección de información. Como instrumentos para realizar la recolección de información para el desarrollo del proyecto se utilizó entrevistas, cuestionarios, herramientas de gestión, listas de chequeo y formatos guías suministrados por el programa gobierno en línea del Ministerio de tecnologías de la información y las comunicaciones (MINTIC).

6.2 METODOLOGIA DE DESARROLLO

Durante el transcurso de la realización del presente proyecto se materializaron una serie de actividades, procedimientos sistémicos y documentados orientados a salvaguardar la seguridad de la información en entidades del estado, el desarrollo de este proyecto de investigación está encaminado a la generación de una guía o modelo de un sistema de gestión de seguridad de la información que pueda ser implementado y adoptado por la entidad que lo desee, para el uso y tratamiento de la privacidad de sus datos.

Con la finalidad de establecer el material suficiente para diseñar el SGSI para entidades del estado y que cumpla con la normatividad y código de buenas prácticas, se realizaron las siguientes actividades de acuerdo con los objetivos del proyecto, por lo tanto, las cuales se desarrollaron en el orden que a continuación se determina.

6.2.1 Objetivo 1. Identificar los activos informáticos comunes que se manejan en las entidades del estado para determinar los dominios del estándar que serán aplicados para el diseño del SGSI.

Uno de los requerimientos principales para poner en funcionamiento un sistema de gestión de seguridad de información es identificar los activos más comunes que se manejan en una entidad del estado, esta es una de las etapas preliminares para dar inicio al proyecto, de este punto se desprenden las condiciones y situaciones que deben evaluarse en todo el proceso.

En esta fase de identificación, se determina que activos posee la entidad, se estable como se deben utilizar, cuáles son las responsabilidades y roles que tienen los funcionarios a esta identificación y el nivel de clasificación de la información que a cada activo debe proporcionársele.

La correcta realización de un inventario y clasificación de activos hace parte de la estructura y guía que desarrolla este proyecto, con respecto a la seguridad de los activos de información de una entidad, por lo tanto, la finalidad es dar cumplimiento a cuatro principales puntos que se describen en el Ítem 8 de la Tabla

A.1. del Anexo A, del estándar ISO/IEC 27001:2013 y que se detallan a continuación:

- **Inventario de activos:** En términos generales la entidad debe elaborar y mantener actualizado un inventario de activos, por lo tanto, todos deben estar plenamente identificados.
- **Propiedad de los activos:** todos los activos de información del inventario deben tener un propietario responsable.
- **Clasificación de la información:** La información se debe clasificar en función de su criticidad, valor, requisitos legales, y la susceptibilidad a su divulgación, modificación sin autorización previa.
- **Etiquetado y manipulado de la información:** En este punto se debe implementar un conjunto adecuado de procedimientos para el etiquetado de la información, conforme al esquema de clasificación adoptado por la organización.

El inventario de activos de información de la entidad debe especificar para cada activo lo siguientes datos mínimos:

- Información básica del activo (nombre, observaciones, proceso, entre otras).
- El nivel de clasificación de la información.
- Información relacionada con su ubicación, tanto física como electrónica.
- Su propietario y su custodio.
- Los usuarios y derechos de acceso.

6.2.2 Objetivo 2. Determinar los factores de amenaza, las vulnerabilidades y riesgos de seguridad informática y de la información que afectan a las entidades del estado.

Esta etapa de identificación es de vital importancia porque se determinan cuáles son los factores que ponen en peligro la integridad, confidencialidad y disponibilidad de la información en una organización, se establece como se deben utilizar y cuáles son los mecanismos para mitigarlos.

A continuación, una breve descripción de la identificación de cada factor que atenta con la seguridad de la información en una Entidad:

- **Identificación del riesgo:** El objetivo de la identificación del riesgo es determinar que podría suceder, que cause una perdida potencial, y llegar a entender el cómo, donde, y por qué motivo podría suceder está perdida de información.

- **Identificación de las amenazas:** Las amenazas pueden ser de origen natural o humano, podrían ser accidentales o deliberadas, es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas.

Una amenaza tiene el potencial de causar daños a activos como información, procesos y sistemas, por lo tanto, a la entidad. Las amenazas se deberían clasificar genéricamente y por tipo, como por ejemplo: Acciones no autorizadas, daño físico, fallas técnicas.

- **Identificación de las vulnerabilidades:** Para gestionar una debida identificación de vulnerabilidades es necesario conocer la lista de inventario de activos, la lista de amenazas comunes, y el listado de controles existentes. Se pueden identificar vulnerabilidades en las siguientes áreas de la entidad:

  - Organización.
  - Procesos y procedimientos.
  - Personal
  - Configuración del sistema de información.
  - Hardware, software y equipos de comunicaciones.
  - Ambiente físico
  - Dependencias

6.2.3 Objetivo 3. Aplicar la metodología de análisis y evaluación de riesgos para determinar el impacto de los riesgos detectados.

Todo sistema de gestión de seguridad de la información debe definir qué metodología utilizará en el proceso. Por lo anterior; para el presente proyecto, en la etapa de análisis y evaluación de riesgos se utilizará la metodología basada en la guía para la administración del riesgo, emitida por el departamento administrativo de la función pública “DAFP”, que proporciona los lineamientos para la gestión del riesgo de seguridad de la información en entidades públicas.

6.2.4 Objetivo 4. Verificar la existencia de controles de seguridad informática y de la información de acuerdo con la norma ISO 27001 en las entidades del estado.

Las actividades por desarrollar en esta etapa buscan determinar que controles de seguridad existen en la organización, la selección de controles se determina en la etapa de planificación y durante la etapa de implementación se ejecutan.

Para el desarrollo de esta actividad, se cuenta con el anexo de controles del estándar ISO 27001:2013.

6.2.5 Objetivo 5. Diseñar las Políticas de Seguridad de la información para las entidades del estado basado en la ISO 27001:2013.

Las Políticas de Seguridad de la Información son elementos fundamentales dentro del sistema de gestión de seguridad de la información puesto que contienen directrices que enmarcan la actuación de todos los funcionarios y contratistas de una entidad del estado.

En el marco del desarrollo del presente proyecto se establecieron las políticas de seguridad que se propusieron y se documentaron, teniendo en cuenta los resultados que se obtuvieron en el análisis de la situación actual y de riesgos de la entidad.

7. IDENTIFICACION DE ACTIVOS

En el caso del presente proyecto, esta guía o modelo de implementación entrega los lineamientos básicos que deben ser utilizados por los responsables de la seguridad de la información, con la finalidad de determinar cuáles son los activos comunes que posee la entidad, cómo deben ser utilizados, cuáles son los roles y responsabilidades que tienen los funcionarios sobre los mismos.

La identificación de activos consiste en determinar qué activos de información van a hacer parte del inventario, para esta tarea debe existir un equipo que realice la gestión de activos de información al interior de la entidad y por medio del líder de cada proceso que ayude en realización de la actividad. Por lo tanto, se realizará empezando por identificar toda la información que se maneja al interior de la entidad, tanto de forma digital como física, analizando cuales son las actividades realizadas y los elementos tecnológicos y físicos utilizados en dicho procedimiento.

Según la norma ISO 27000:2013, un activo es todo aquello que tiene valor para la entidad y que, a su vez, requiere de protección. La identificación de activos se debe llevar acabo con un nivel adecuado de detalle que proporcione información clara y suficiente.

En la siguiente tabla se describen los tipos de activos comunes que se manejan en las entidades del estado los cuales están detallados de la siguiente manera:

Tabla 1. Tipos de Activos

Tipo de Activo	Descripción
Software	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades.
Hardware	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información.
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

.

Tabla 1. (Continuación)

Tipo de Activo	Descripción
Servicios	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por *hardware y software*).
Intangibles	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el *good will*, entre otros.
Componentes de red	Medios necesarios para realizar la conexión de los elementos de *hardware* y *software* en una red, por ejemplo, el cableado estructurado y tarjetas de red, *routers, switches*, entre otros.
Personas	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades.
Instalaciones	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

7.1 Clasificación de Activos

Según la norma ISO27001:2013 establece que debe realizarse una clasificación de los activos, teniendo en cuenta tres características: la disponibilidad, la integridad y la confidencialidad.

- **La disponibilidad:** Hace referencia a que la información sea accesible y utilizable por solicitud de una entidad autorizada. A partir de esto, las entidades u organizaciones deben desarrollar las estrategias y los instrumentos con los cuales las partes interesadas puedan hacer uso de la información. Esto implica que la documentación pueda ser localizada, recuperada e interpretada, con base en su contexto de producción, manteniendo los vínculos existentes entre los documentos, la secuencia de actividades que les dan origen y las funciones asignadas a la entidad.
- **La integridad:** Hace referencia a la propiedad de salvaguardar la exactitud y estado completo de los activos. Para las entidades públicas toda la producción documental es evidencia del cumplimiento de su objeto social, funciones, procesos y procedimientos, por lo que la totalidad de esa producción debe ser salvaguardada para cumplir estas propiedades.

- **La confidencialidad**: hace referencia a la propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Con base en lo anterior, el artículo 6 de la Ley 1712 de 2014 proporciona a continuación las siguientes definiciones:

- **Información pública:** Es considerada toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.
- **Información pública reservada:** Es considerada aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley.
- **Información pública clasificada:** Es considerada aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley.

En cuanto a la Confidencialidad, la Integridad y la Disponibilidad de cada activo. El método de clasificación definido se basa en la confidencialidad como principio rector. Por lo tanto, contempla el impacto que causaría la pérdida de alguna de estas propiedades. Para cada propiedad se deben proporcionar criterios específicos para el tratamiento adecuado del activo. En el caso del presente proyecto se definieron tres (3) niveles que permiten determinar el valor general del activo en la entidad. A continuación, se muestran las tablas 2 y 3 con los niveles de criterio y clasificación de activos que pueden ser definidos por cada entidad, con el objetivo de identificar qué activos deben ser tratados de manera prioritaria.

Tabla 2. Criterios de Clasificación de Activos

Confidencialidad	Integridad	Disponibilidad
INFORMACION PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACION PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACION PUBLICA NO CLASIFICADA	BAJA (B) NO CLASIFICADA	BAJA (3) NO CLASIFICADA

Fuente: Elaboración realizada por el autor del proyecto.

Tabla 3. Niveles de Clasificación de Activos

Valoración	Descripción
ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Fuente: Elaboración realizada por el autor del proyecto.

7.2 Formato de Identificación y Clasificación de Activos

La identificación y clasificación consiste en establecer que activos hacen parte del inventario, por lo tanto, para esta actividad debe existir un recurso humano que realice el levantamiento de la información. El formato de identificación debe incluir la información básica que hace referencia a aquellas características del activo como son las siguientes:

- Identificador
- Proceso
- Nombre de Activo
- Descripción
- Tipo
- Propietario
- Custodio
- Clasificación
- Criticidad

Para el caso del presente proyecto se realizó la identificación y valoración de activos que puede tener una entidad en términos generales. Por lo tanto es una guía o modelo que puede ser adoptada por las partes interesadas.

En la siguiente tabla que se muestra a continuación se describe la identificación, clasificación y valoración de activos que se realizó y que está enfocado a entidades del estado.

Tabla 4. Identificación y Clasificación de Activos

Espacio para el Logo de la Entidad	Nombre de la entidad Formato inventario de activos de información y clasificación de activos basado en la norma iso 27001:2013 para un sistema de gestión de seguridad de la información.	Versión. 1.0 Fecha de Creación:

Identificación de activos de información								Clasificación de activos			Valoración del activo
								Confidencialidad	Integridad	Disponibilidad	
ID Activo	Nombre del Activo	Proceso	Descripción	Tipo	Ubicación	Propietario	Custodio	Nivel	Nivel	Nivel	Criticidad
1	Sistemas Operativos Microsoft WindowsProfessional 7. Windows 8.1 pro. Windows 10.	Gestión Informática	Software que administra los recursos de las computadoras de uso institucional.	Software	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
2	Sistema Operativo Windows Server	Gestión Informática	Software de administracion de servidores	Software	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	ALTA	ALTA
3	Exchange Server	Gestión Informática	Software de administracion de correo	Software	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	ALTA	ALTA
4	Office Professional	Gestión Informática	Software de ofimatica	Software	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	ALTA	ALTA
5	Kaspersky endpoint security 10	Gestión Informática	Software de antivirus	Software	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	ALTA	ALTA
6	Project Professional	Gestión Informática	Software de proyectos	Software	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	ALTA	ALTA
7	Linux RedHat	Gestión Informática	Software de administracion de servidores	Software	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	ALTA	ALTA
8	Ubuntu Server	Gestión Informática	Software de administracion de servidores	Software	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	ALTA	ALTA
9	Servidores Virtuales	Gestión Informática	Software de administracion de servidores	Software	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	ALTA	ALTA
10	SQL Server	Gestión Informática	Software de bases de datos	Software	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	ALTA	ALTA
11	Oracle	Gestión Informática	Software de bases de datos	Software	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	ALTA	ALTA
12	Visual Studio	Gestión Informática	Software de promación.	Software	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
13	Visual Basic	Gestión Informática	Software de promación.	Software	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA

Fuente: Elaboración realizada por el autor del proyecto

Tabla 4. (Continuación)

Identificación de activos de información								Clasificación de activos			Valoración del activo
								Confidencialidad	Integridad	Disponibilidad	
ID Activo	Nombre del Activo	Proceso	Descripción	Tipo	Ubicación	Propietario	Custodio	Nivel	Nivel	Nivel	Criticidad
14	Visual FoxPro	Gestión Informática	Software de promación de bases de datos.	Software	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
15	Linux Suse	Gestión Informática	Software de administracion de servidores	Software	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
16	Corell Draw	Gestión Informática	Software de diseño grafico.	Software	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
17	Crystal Reports Windows	Gestión Informática	Software de inteligencia empresarial	Software	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
18	Auto CAD Full	Gestión Informática	Software de Diseño	Software	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
19	Kawak - Sistema de Gestión de Calidad	Gestión Informática	Software de Sistema de Gestión de Calidad	Software	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	ALTA	ALTA
20	SIAM (SW de Mantenimiento)	Gestión Informática	Software de mantenimiento	Software	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	ALTA	ALTA
21	Sistema ERP - SEVEN	Gestión Informática	Software ERP	Software	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	ALTA	ALTA
22	Sistema RH - KACTUS	Gestión Informática	Software de Recursos Humanos	Software	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	ALTA	ALTA
23	Orfeo (Software de Gestión Documental)	Gestión Documental y de Activos Fijos	Software de Gestión Documental	Software	Oficina de Sistemas e Informatica	Coordinador de Gestión Documental	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	ALTA	ALTA
24	DataProtector Access License	Gestión Informática	Licencia de Software	Software	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	ALTA	ALTA
25	Impresora, escáner multifuncional	Gestión Financiera	Equipos de Computo	Hardware	Tesoreria	Jefe de la Oficina de Area Admnistrativa	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
26	Impresora a color minolta magicolor 330	Gestión Informática	Equipos de Computo	Hardware	Oficina de Sistemas e Informatica	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
27	Escáner Plano HP	Gestión Informática	Equipos de Computo	Hardware	Oficina de Sistemas e Informatica	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
28	Computadores de Escritorio (Entidad)	Gestión Informática	Equipos de Computo	Hardware	Oficina de Sistemas e Informatica	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
29	Computadores Portatiles (Entidad)	Gestión Informática	Equipos de Computo	Hardware	Oficina de Sistemas e Informatica	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA

Fuente: Elaboración realizada por el autor del proyecto

Tabla 4. (Continuación)

Identificación de activos de información								Clasificación de activos			Valoración del activo
								Confidencialidad	Integridad	Disponibilidad	
ID Activo	Nombre del Activo	Proceso	Descripción	Tipo	Ubicación	Propietario	Custodio	Nivel	Nivel	Nivel	Criticidad
30	Servidor de Aplicaciones	Gestión Informática	Equipos de Computo	Hardware	Centro de Computo	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
31	Servidor de Datos	Gestión Informática	Equipos de Computo	Hardware	Centro de Computo	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	ALTA
32	Servidores blade tipo 1	Gestión Informática	Equipos de Computo	Hardware	Centro de Computo	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
33	Servidores blade tipo 2	Gestión Informática	Equipos de Computo	Hardware	Centro de Computo	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
34	Servidor tipo rack u2 xeon sixcore	Gestión Informática	Equipos de Computo	Hardware	Centro de Computo	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
35	Solución de backup institucional	Gestión Informática	Equipos de Computo	Hardware	Centro de Computo	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
36	Switches Cisco 24 puertos	Gestión Informática	Equipos de Computo	Hardware	Centro de Computo	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
37	Switches Cisco 48 puertos	Gestión Informática	Equipos de Computo	Hardware	Centro de Computo	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
38	Switch Core	Gestión Informática	Equipos de Computo	Hardware	Centro de Computo	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
39	UPS de 30 KVA (Centro de Cómputo)	Gestión Informática	Equipos de Computo	Hardware	Oficina de Sistemas e Informatica	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
40	Ups de 900va regulada	Gestión Informática	Equipos de Computo	Hardware	Centro de Computo	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
41	Sistema de almacenamiento NAS	Gestión Informática	Equipos de Computo	Hardware	Centro de Computo	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
42	Planta telefónica con servidor de voz IP tipo rack	Gestión Informática	Equipos de Computo	Hardware	Centro de Computo	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
43	Controladora Access points inalámbricos	Gestión Informática	Equipos de Computo	Hardware	Centro de Computo	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
44	Access Points Inalámbricos	Gestión Informática	Equipos de Computo	Hardware	Centro de Computo	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA

Fuente: Elaboración realizada por el autor del proyecto

Tabla 4. (Continuación)

Identificación de activos de información								Clasificación de activos			Valoración del activo
								Confidencialidad	Integridad	Disponibilidad	
ID Activo	Nombre del Activo	Proceso	Descripción	Tipo	Ubicación	Propietario	Custodio	Nivel	Nivel	Nivel	Criticidad
45	Estaciones de trabajo mac	Gestión Informática	Equipos de Computo	Hardware	Centro de Computo	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
46	Dispositivos Moviles (Tablets,celulares)	Gestión Informática	Equipos de Computo	Hardware	Oficina de Sistemas e Informatica	Jefe de la Oficina de Sistemas.	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
47	firewall	Gestión Informática	Dispositivo de seguridad de la red	Hardware	Oficina de Sistemas e Informatica	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
48	Servidores web correo electronico	Gestión Informática	servidor de Internet, para prestar servicio de correo electrónico	Servicios	Oficina de Sistemas e Informatica	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
49	Internet	Gestión Informática	Canal de uso interno y externo para los procesos informaicos.	Servicios	Oficina de Sistemas e Informatica	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
50	Pagina Web Institucional	Gestión Informática	Portal Institucional de uso externo y de información.	Servicios	Oficina de Sistemas e Informatica	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
51	Telefonia IP	Gestión Informática	Telefonia para uso interno de la Entidad.	Servicios	Oficina de Sistemas e Informatica	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
52	Correos Eletronicos	Gestión Informática	Correo corporativo de la entidad,	Servicios	Oficina de Sistemas e Informatica	Jefe de la Oficina de Sistemas e Informática	Oficina de Sistemas e Informatica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
53	Certificado de Disponibilidad Presupuestal (CDP)	Gestión Financiera	Refleja la disponiblidad de recursos económicos que tiene la entidad para la adquisición de un bien o un servicio.	Información	ERP SEVEN	Jefe de presupuesto	Jefe de presupuesto	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	ALTA	ALTA
54	Documento Físicos Actos Administrativos, CD's o correo electrónico.	Oficina Asesora Jurídica		Información	Archivo fisico Oficina Juridica.	Jefe de oficina Juridica	Jefe de oficina Juridica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	ALTA	ALTA
55	SECOP (Carga de información para contratos inter-administrativos)	Oficina Asesora Jurídica	Sistema electronico de Contratación publica	Información	WEB Colombia Compra Eficiente	Jefe de oficina Juridica	Jefe de oficina Juridica	INFORMACION PUBLICA	MEDIA	ALTA	MEDIA
56	Actos Administrativos (Físico y magnético)	Oficina Asesora Jurídica	Documentos	Información	Archivo fisico Oficina Juridica. Carpeta Compartida Unidad F en servidor de Datos.	Jefe de oficina Juridica	Jefe de oficina Juridica	INFORMACION PUBLICA	ALTA	MEDIA	MEDIA
57	Registro de Contingencias (Informe mensual demandas a favor o en contra)	Oficina Asesora Jurídica	Documentos de informes	Información	Archivo fisico Oficina Juridica. Carpeta Compartida Unidad F en servidor de Datos.	Jefe de oficina Juridica	Jefe de oficina Juridica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA

Fuente: Elaboración realizada por el autor del proyecto

Tabla 4. (Continuación)

Identificación de activos de información								Clasificación de activos			Valoración del activo
								Confidencialidad	Integridad	Disponibilidad	
ID Activo	Nombre del Activo	Proceso	Descripción	Tipo	Ubicación	Propietario	Custodio	Nivel	Nivel	Nivel	Criticidad
58	Registro Mensual de los procesos disciplinarios	Gestión del Talento Humano	Documentos disciplinarios	Información	Archivo fisico Oficina Juridica. Carpeta Compartida Unidad F en servidor de Datos.	Jefe de oficina Juridica	Jefe de oficina Juridica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
59	Resoluciones	Oficina Asesora Jurídica	Actos administrativos expedidos por la administración.	Información	Archivo fisico Oficina Juridica. Carpeta Compartida Unidad F en servidor de Datos.	Jefe de oficina Juridica	Jefe de oficina Juridica	INFORMACION PUBLICA	ALTA	ALTA	ALTA
60	Procesos contractuales	Oficina Asesora Jurídica	Documentos	Información	Archivo fisico Oficina Juridica. Carpeta Compartida Unidad F en servidor de Datos.	Jefe de oficina Juridica	Jefe de oficina Juridica	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	ALTA	ALTA
61	Contratos Finalizados	Oficina Asesora Jurídica	Documentos	Información	Archivo fisico Oficina Juridica. Carpeta Compartida Unidad F en servidor de Datos.	Jefe de oficina Juridica	Jefe de oficina Juridica	INFORMACION PUBLICA	ALTA	ALTA	ALTA
62	Convenios Interadministrativos	Oficina Asesora Jurídica	Acuerdo suscrito entre dos o mas personas jurídicas de derecho público o entre una o varias entidades públicas .	Información	Archivo fisico Oficina Juridica. Carpeta Compartida Unidad F en servidor de Datos.	Jefe de oficina Juridica	Jefe de oficina Juridica	INFORMACION PUBLICA	ALTA	ALTA	ALTA
63	Base de datos de los informes en Planeación	Gestión de Planeación	Bases de datos	Información	Archivo fisico Oficina de Planeación. Carpeta Compartida Unidad F en servidor de Datos.	Jefe Oficina Asesora de Planeación	Jefe Oficina Asesora de Planeación	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	ALTA	ALTA
64	Informes de contraloria (informe cuenta anual, informe contractual, plan de mejoramiento)	Gestión Administrativa	Documentos de informes	Información	Archivo Oficina Administrativa	Secretaria Administrativa y Financiera	Secretaria Administrativa y Financiera	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	ALTA	ALTA
65	Publicaciones en la página web	Comunicaciones	Documentos	Información	Pagina Web Institucional	Oficina de Sistemas e Informática	Oficina de Sistemas e Informática	INFORMACION PUBLICA	ALTA	MEDIA	MEDIA
66	Plan Anual de Compras	Gestión de Planeación	Documentos de compras	Información	Archivo Oficina Administrativa	Jefe Oficina Asesora de Planeación	Jefe Oficina Asesora de Planeación	INFORMACION PUBLICA	ALTA	ALTA	MEDIA
67	Planos de Infraestructura	Gestión de Planeación	Documentos	Información	Archivo fisico Oficina de Planeación. Carpeta Compartida Unidad F en servidor de Datos.	Jefe Oficina Asesora de Planeación	Jefe Oficina Asesora de Planeación	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
68	Peticiones, quejas, reclamos, sugerencias, felicitaciones y denuncias	Comunicaciones	Documentos	Información	Archivo Oficina Administrativa	Jefe de oficina Juridica	Jefe de oficina Juridica	INFORMACION PUBLICA	MEDIA	MEDIA	MEDIA

Fuente: Elaboración realizada por el autor del proyecto

Tabla 4. (Continuación)

Identificación de activos de información								Clasificación de activos			Valoración del activo
								Confidencialidad	Integridad	Disponibilidad	
ID Activo	Nombre del Activo	Proceso	Descripción	Tipo	Ubicación	Propietario	Custodio	Nivel	Nivel	Nivel	Criticidad
69	Derechos de petición, tutelas, parte administrativa, legal	Oficina Asesora Jurídica	Documentos	Información	Archivo fisico Oficina Juridica. Carpeta Compartida Unidad F en servidor de Datos.	Jefe de oficina Juridica	Jefe de oficina Juridica	INFORMACION PUBLICA	ALTA	MEDIA	MEDIA
70	Informes a Organismo del Estado	Gestión Administrativa	Informes que reportan la gestión que ha adelantado la Entidad .	Información	Archivo Oficina Administrativa	Secretaria Administrativa y Financiera	Secretaria Administrativa y Financiera	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	ALTA	ALTA
71	Estrategías de Comunicación	Comunicaciones	Documentos	Información	Archivo fisico Oficina de Comunicaciones. Carpeta Compartida Unidad F en servidor de Datos.	Oficina de Sistemas e Informática	Oficina de Sistemas e Informática	INFORMACIÓN PUBLICA CLASIFICADA	MEDIA	MEDIA	MEDIA
72	Proyectos de Inversión	Gestión Administrativa	Son todos aquellos proyectos que aportan a la gestión de la entidad.	Información	Archivo fisico Oficina de Planeación. Carpeta Compartida Unidad F en servidor de Datos.	Secretaria Administrativa y Financiera	Secretaria Administrativa y Financiera	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	ALTA	ALTA
73	Plan Anual de Adquisiciones	Gestión Administrativa	Es un documento donde se consolida y discrimina, por rubro presupuestal, los bienes, obras y servicios que deben ser adquiridos.	Información	Archivo Oficina Administrativa	Secretaria Administrativa y Financiera	Secretaria Administrativa y Financiera	INFORMACION PUBLICA	ALTA	ALTA	ALTA
74	Archivos de los proyectos que se radican en el banco de proyectos	Gestión de Planeación	Proyectos	Información	Archivo fisico Oficina de Planeación. Carpeta Compartida Unidad F en servidor de Datos.	Jefe Oficina Asesora de Planeación	Jefe Oficina Asesora de Planeación	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
75	Tesorero	Oficina de area administrativa	Recurso Humano	Personas	Oficina de area administrativa	Jefe de Area Administrativa	Gestión de Desarrollo del Talento Humano	INFORMACION PUBLICA RESERVADA	ALTA	ALTA	ALTA
76	Jefe de la Oficina de Sistemas e Informática	Gestión Informática	Recurso Humano	Personas	Oficina de Sistemas e Informática	Jefe de la Oficina de Sistemas e Informática	Gestión de Desarrollo del Talento Humano	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
77	Jefe de Presupuesto	Oficina de area administrativa	Recurso Humano	Personas	Oficina de area administrativa	Jefe de Presupuesto	Gestión de Desarrollo del Talento Humano	INFORMACION PUBLICA RESERVADA	ALTA	MEDIA	ALTA
78	Secretario de Gobierno	Secretaría de Gobierno	Recurso Humano	Personas	Secretaría de Gobierno	Secretario de Gobierno	Gestión de Desarrollo del Talento Humano	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
79	Secretario de Educación	Secretaría de Educación	Recurso Humano	Personas	Secretaría de Educación	Secretario de Educación	Gestión de Desarrollo del Talento Humano	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA

Fuente: Elaboración realizada por el autor del proyecto

Tabla 4. (Continuación)

Identificación de activos de información								Clasificación de activos			Valoración del activo
								Confidencialidad	Integridad	Disponibilidad	
ID Activo	Nombre del Activo	Proceso	Descripción	Tipo	Ubicación	Propietario	Custodio	Nivel	Nivel	Nivel	Criticidad
80	Jefe de Oficina Juridica	Oficina Asesora Jurídica	Recurso Humano	Personas	Oficina Asesora Jurídica	Jefe de Oficina Juridica	Gestión de Desarrollo del Talento Humano	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
81	Secretario de Planeacion y obras.	Secretaría de Planeacion y obras.	Recurso Humano	Personas	Secretaría de Planeacion y obras.	Secretario de Planeacion y obras.	Gestión de Desarrollo del Talento Humano	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
82	Jefe de Recursos Humanos	Gestión de Desarrollo del Talento Humano	Recurso Humano	Personas	Gestión de Desarrollo del Talento Humano	Jefe de Recursos Humanos	Gestión de Desarrollo del Talento Humano	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
83	Tecnico Administrativo	Secretaría de Planeacion y obras.	Recurso Humano	Personas	Secretaría de Planeacion y obras.	Secretario de Planeacion y obras.	Gestión de Desarrollo del Talento Humano	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
84	Jefe de Control Interno	Oficina de area administrativa	Recurso Humano	Personas	Oficina de area administrativa	Jefe de Control Interno	Gestión de Desarrollo del Talento Humano	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
85	Asesor Juridico	Oficina Asesora Jurídica	Recurso Humano	Personas	Oficina Asesora Jurídica	Jefe de Oficina Juridica	Gestión de Desarrollo del Talento Humano	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
86	Red WIFI	Gestión Informática	Red de Acceso inalambrico, para el uso de empleados y visitantes de la Entidad.	RED	Oficina de Sistemas e Informática	Gestión Informática	Jefe de la Oficina de Sistemas e Informática	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
87	Red LAN	Gestión Informática	Red Interna de uso de los empleados.	RED	Oficina de Sistemas e Informática	Gestión Informática	Jefe de la Oficina de Sistemas e Informática	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
88	INTRANET	Gestión Informática	Portal Institucional de uso interno de la entidad, contiene información de uso exclusivo y interes de los empleados	RED	Oficina de Sistemas e Informática	Gestión Informática	Jefe de la Oficina de Sistemas e Informática	INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA	MEDIA
Elaborado por: Juan Carlos de León Camelo					**Aprobado por: Alcalde**						
Cargo: Jefe de Oficina de Sistemas e Informática					**Cargo: ALCALDE**						
Lugar y fecha: 4 de Marzo de 2019					**Lugar y fecha: 4 de Marzo de 2019**						

Fuente: Elaboración realizada por el autor del proyecto

8. FACTORES DE RIESGOS, AMENAZAS Y VULNERABILIDADES

La información es de vital importancia para cualquier tipo de entidad u organización dentro de la política pública y su relación con los ciudadanos. Por esta razón debe estar asegurada de cualquier posibilidad de ocurrencia de eventos de riesgo de seguridad de la información y que pudiese significar un impacto indeseado generando una consecuencia negativa para el normal funcionamiento de las actividades de la entidad. A través de este proyecto se busca orientar a las entidades a identificar los factores de riesgos, amenazas y vulnerabilidades que afectan la seguridad de la información, basado en los criterios de confidencialidad, integridad y disponibilidad.

8.1 IDENTIFICACIÓN DEL RIESGO

El riesgo es la posibilidad de sufrir daños o pérdidas, la finalidad de la identificación del riesgo es establecer que podría suceder, que cause una perdida potencial, y llegar a entender el cómo, donde, y por qué motivo podría suceder está perdida de información.

8.2 IDENTIFICACIÓN DE LAS AMENAZAS

En términos generales, las amenazas que afectan a las entidades hoy en día son de dos tipos, estas pueden ser de sucesos naturales o las que son provocadas por la actividad humana, podrían ser accidentales o deliberadas, es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas.

Una amenaza tiene el potencial de causar daños a activos como información, procesos y sistemas, por lo tanto, afecta a la entidad propiamente. Estas se deben identificar genéricamente y por tipo, como, por ejemplo: Acciones no autorizadas, daño físico, fallas técnicas.

En algunos casos las amenazas pueden afectar a más de un activo, pueden causar diferentes impactos dependiendo de los activos que se vean afectados. A continuación, en la tabla número 5 se muestran algunas de las amenazas comunes que pueden afectar a una entidad de gobierno.

Nomenclatura: A= Accidentales, D= Deliberadas, E= Ambientales

Tabla 5. Catálogo de Amenazas Comunes en entidades

Tipo	Amenaza	Origen
Daño físico	Fuego.	A, D, E
	Agua.	A, D, E
	Contaminación.	A, D, E
	Accidente Importante.	A, D, E
	Destrucción del equipo o medios.	A, D, E
	Polvo, corrosión, congelamiento.	A, D, E
Eventos naturales	Fenómenos climáticos.	E
	Fenómenos sísmicos.	E
	Fenómenos volcánicos.	E
	Fenómenos meteorológicos.	E
	Inundación.	E
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado.	E
	Perdida de suministro de energía.	E
	Falla en equipo de telecomunicaciones.	A, D, E
Perturbación debida a la radiación	Radiación electromagnética.	A, D, E
	Radiación térmica.	A, D, E
	Impulsos electromagnéticos.	A, D, E
Compromiso de la información	Interceptación de señales de interferencia comprometida.	A, D
	Espionaje remoto.	
	Escucha encubierta.	A, D
	Hurto de medios o documentos.	A, D
	Hurto de equipo.	A, D
	Recuperación de medios reciclados o desechados.	A, D
	Divulgación.	A, D
	Datos provenientes de fuentes no confiables.	A, D
	Manipulación con hardware.	A, D
	Manipulación con software.	A, D
	Detección de la posición.	A, D
Fallas técnicas	Fallas del equipo.	A, D
	Mal funcionamiento del equipo.	A, D
	Saturación del sistema de información.	A, D
	Mal funcionamiento del software.	A, D
	Incumplimiento en el mantenimiento del sistema de información.	A, D
Acciones no autorizadas	Uso no autorizado del equipo.	D
	Copia fraudulenta del software.	D
	Uso de software falso o copiado.	D
	Corrupción de los datos.	A, D
	Procesamiento ilegal de datos.	D
Compromiso de las funciones.	Error en el uso.	A, D
	Abuso de derechos.	D
	Falsificación de derechos.	D
	Negación de acciones.	D
	Incumplimiento en la disponibilidad del personal.	A, D

Fuente: Elaboración realizada por el autor del proyecto

Se encuentran también las amenazas que son permitidas o causadas por seres humanos, estas pueden ser actos involuntarios o bien acciones intencionales, Es muy importante y recomendable tener mucha atención a las fuentes de amenazas de actividad humana. En la siguiente tabla que se describe a continuación se muestra un catálogo de amenazas específicas dirigidas por el hombre:

Tabla 6. Catálogo de Amenazas de Actividad Humana

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	Reto, Ego, Rebelión, Estatus, Dinero.	Piratería, Ingeniería social, Intrusión, accesos forzados al sistema, Acceso no autorizado.
Criminal de la computación.	Destrucción de la Información. Divulgación ilegal de la información. Ganancia monetaria. Alteración no autorizada de los datos.	Crimen por computador. Acto fraudulento. Soborno de la información. Suplantación de identidad. Intrusión en el sistema.
Terrorismo	Chantaje, Destrucción, Explotación, Venganza, Ganancia política, Cubrimiento de los medios de comunicación.	Bomba/Terrorismo. Guerra de la información. Ataques contra el sistema DDoS. Penetración en el sistema. Manipulación en el sistema.
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses).	Ventaja competitiva. Espionaje económico.	Ventaja de defensa, ventaja política, explotación económica, hurto de información, intrusión en privacidad personal, ingeniería social, penetración en el sistema y acceso no autorizado al sistema.
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad, Ego, Inteligencia, Ganancia monetaria, Venganza, Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación).	Asalto a un empleado, Chantaje, Observar información reservada, Uso inadecuado del computador, fraude, hurto, soborno de información, Ingreso de datos falsos o corruptos, interceptación, Código malicioso, venta de información personal, errores en el sistema, intrusión al sistema y sabotaje del sistema.

Fuente: Elaboración realizada por el autor del proyecto

8.3 IDENTIFICACIÓN DE LAS VULNERABILIDADES

En términos de seguridad de la información, una vulnerabilidad es una debilidad que se encuentra en un activo y que puede ser explotada por una o más amenazas, lo que se convierte en un riesgo de seguridad. Una forma de proteger la información es a través de la identificación de las debilidades en los activos.

Es muy importante tener en cuenta que para realizar una óptima identificación de vulnerabilidades se debe tener conocimiento de un listado de amenazas y el inventario de activos que posee la entidad.

Las vulnerabilidades se pueden identificar en las siguientes áreas:

- Organización.
- Configuración del sistema de información.
- Hardware, software y equipos de comunicaciones.
- Procesos y procedimientos.
- Rutinas de gestión.
- Personal.
- Ambiente físico.
- Dependencia de partes externas.

A continuación, se presentan resaltadas en la tabla No. 7 las vulnerabilidades que se pueden identificar en una entidad, de acuerdo con el tipo de activos.

Tabla 7. Catálogo de Vulnerabilidades Comunes sobre los Activos

Tipo	Vulnerabilidades
Software	Software nuevo o inmaduro
	Ausencia de documentación.
	Interfaz de usuario compleja.
	Asignación errada de los derechos de acceso.
	Ausencia de registros de auditoría.
	Ausencia de terminación de sesión.
	Ausencia o insuficiencia de pruebas de software.
	Fechas incorrectas.
	Ausencia de mecanismos de identificación y autenticación de usuarios.
	Contraseñas sin protección.
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)

Fuente: Elaboración realizada por el autor del proyecto

Tabla 7. (Continuación)

Tipo	Vulnerabilidades
Personal	Ausencia del personal. Entrenamiento insuficiente. Falta de conciencia en seguridad. Ausencia de políticas de uso aceptable. Trabajo no supervisado de personal externo o de limpieza.
Red	Punto único de falla. Ausencia de pruebas de envío o recepción de mensajes. Líneas de comunicación sin protección. Conexión deficiente de cableado. Tráfico sensible sin protección.
Lugar	Uso inadecuado de los controles de acceso al edificio. Áreas susceptibles a inundación. Red eléctrica inestable. Ausencia de protección en puertas o ventanas.
Organización	Ausencia de procedimiento de registro/retiro de usuarios. Ausencia de proceso para supervisión de derechos de acceso. Ausencia de control de los activos que se encuentran fuera de las instalaciones. Ausencia de mecanismos de monitoreo para brechas en la seguridad. Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas).

Fuente: Elaboración realizada por el autor del proyecto

A continuación, en la tabla No. 8 se presentan ejemplos de relación entre vulnerabilidades de acuerdo con el tipo de activos y las amenazas.

Tabla 8. Amenazas y vulnerabilidades en entidades

Tipo de activo	Ejemplo de vulnerabilidades	Ejemplo de amenazas
RED	Ausencia de pruebas de envío o recepción de mensajes.	Negación de acciones
	Líneas de comunicación sin protección.	Escucha encubierta
	Tráfico sensible sin protección.	Escucha encubierta
	Conexión deficiente de los cables.	Fallas del equipo de telecomunicaciones
	Punto único de fallas	Fallas del equipo de telecomunicaciones
	Ausencia de identificación y autentificación de emisor y receptor.	Falsificación de derechos
	Arquitectura insegura de la red.	Espionaje remoto
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento).	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo

Fuente: Elaboración realizada por el autor del proyecto

Tabla 8. (Continuación)

Tipo de activo	Ejemplo de vulnerabilidades	Ejemplo de amenazas
HARDWARE	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o medios.
	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosion y congelamiento.
	Sensibilidad a la radiación electromagnética	Radiación electromagnética.
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurtos medios o documentos.
	Falta de cuidado en la disposición final	Hurtos medios o documentos.
	Copia no controlada	Hurtos medios o documentos.
SOFTWARE	Ausencia o insuficiencia de pruebas de software.	Abuso de los derechos.
	Defectos bien conocidos en el software.	Abuso de los derechos.
	Ausencia de “terminación de sesión” cuando se abandona la estación de trabajo.	Abuso de los derechos.
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado.	Abuso de los derechos.
	Ausencias de registros de auditoria	Abuso de los derechos.
	Asignación errada de los derechos de acceso.	Abuso de los derechos.
	Software ampliamente distribuido.	Corrupción de datos.
	En términos de tiempo utilización de datos errados en los programas de aplicación.	Corrupción de datos.
	Interfaz de usuario compleja.	Error en el uso.
	Ausencia de documentación.	Error en el uso.
	Configuración incorrecta de parámetros.	Error en el uso.
	Fechas incorrectas.	Error en el uso.
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario.	Falsificación de derechos.
	Tablas de contraseñas sin protección.	Falsificación de derechos.
	Gestión deficiente de las contraseñas.	Falsificación de derechos.
	Habilitación de servicios Innecesarios.	Procesamiento ilegal de datos.

Fuente: Elaboración realizada por el autor del proyecto

Tabla 8. (Continuación)

Tipo de activo	Ejemplo de vulnerabilidades	Ejemplo de amenazas
SOFTWARE	Software nuevo o inmaduro.	Mal funcionamiento del Software.
	Especificaciones incompletas o no claras para los desarrolladores.	Mal funcionamiento del Software.
	Ausencia de control de cambios eficaz.	Mal funcionamiento del Software.
	Descarga y uso no controlado de software.	Manipulación con software.
	Ausencia de copias de respaldo.	Manipulación con software.
	Fallas en la producción de informes de gestión.	Uso no autorizado del equipo.
PERSONAL	Ausencia del personal.	Incumplimiento en la disponibilidad del personal.
	Procedimientos inadecuados de contratación.	Destrucción de equipos y Medios.
	Entrenamiento insuficiente en seguridad.	Error en el uso.
	Uso incorrecto de software y hardware.	Error en el uso.
	Falta de conciencia acerca de la seguridad.	Error en el uso.
	Ausencia de mecanismos de monitoreo.	Procesamiento ilegal de los datos.
	Trabajo no supervisado del personal externo o de limpieza.	Hurto de medios o documentos.
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería.	Uso no autorizado del equipo.
LUGAR	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	
	Ubicación en área susceptible de inundación	
	Red energética inestable	
	Ausencia de protección física de la edificación (Puertas y ventanas)	Hurto de medios o documentos.
ORGANIZACIÓN	Ausencia de procedimiento formal para el registro y retiro de usuarios.	Abuso de los derechos
	Ausencia de proceso formal para la revisión de los derechos de acceso.	Abuso de los derechos
	Ausencia de disposición en los contratos con clientes o terceras partes (seguridad).	Abuso de los derechos
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información.	Abuso de los derechos

Fuente: Elaboración realizada por el autor del proyecto

Tabla 8. (Continuación)

Tipo de activo	Ejemplo de vulnerabilidades	Ejemplo de amenazas
	Ausencia de procedimientos de identificación y valoración de riesgos.	Abuso de los derechos
	Ausencia de reportes de fallas en los registros de administradores y operadores.	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio.	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de acuerdos de nivel de servicio o insuficiencia de estos.	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de procedimientos de control de cambios.	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de procedimiento formal para la documentación del SGSI.	Corrupción de datos
	Ausencia de procedimiento formal para la supervisión del registro del SGSI	Corrupción de datos
ORGANIZACIÓN	Ausencia de procedimiento formal para la autorización de la información disponible al público.	Datos provenientes de fuentes no confiables
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información.	Negación de acciones
	Ausencia de planes de continuidad.	Falla del equipo
	Ausencia de políticas sobre el uso de correo electrónico.	Error en el uso
	Ausencia de procedimientos para introducción del software en los sistemas operativos.	Error en el uso
	Ausencia de registros en bitácoras	Error en el uso
	Ausencia de procedimientos para el manejo de información clasificada.	Error en el uso
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos.	Error en el uso
	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información.	Hurto de equipo
	Ausencia de política formal sobre la utilización de computadores portátiles.	Hurto de equipo
	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo

Fuente: Elaboración realizada por el autor del proyecto

Tabla 8. (Continuación)

Tipo de activo	Ejemplo de vulnerabilidades	Ejemplo de amenazas
ORGANIZACIÓN	Ausencia de política sobre limpieza de escritorio y pantalla.	Hurto de medios o documentos.
	Ausencia de autorización de los recursos de procesamiento de información.	Hurto de medios o documentos.
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad.	Hurto de medios o documentos.
	Ausencia de revisiones regulares por parte de la gerencia.	Uso no autorizado de equipo
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad.	Uso no autorizado de equipo

Fuente: Elaboración realizada por el autor del proyecto

9. METODOLOGIA DE ANÁLISIS Y EVALUACIÓN DE RIESGOS EN SEGURIDAD DE LA INFOMACIÓN

En esta etapa del proyecto, para el análisis y evaluación de riesgos se utilizó la metodología basada en la guía para la administración del riesgo, emitida por el departamento administrativo de la función pública "DAFP", que proporciona los lineamientos para la gestión del riesgo de seguridad de la información en entidades públicas[26].

Esta metodología busca orientar a las entidades a gestionar los riesgos de seguridad de la información basada en los criterios de confidencialidad, integridad y disponibilidad.

Para realizar un correcto análisis y evaluación del riesgo en esta etapa del proyecto es importante tener organizado lo siguiente:

- Identificación de los activos de información con su respectiva valoración.
- Identificación de las amenazas y vulnerabilidades que afectan a la entidad.

El análisis, evaluación y valoración del riesgo se introduce en las entidades del gobierno, teniendo en cuenta que todas las organizaciones independientemente de su naturaleza, tamaño y razón de ser están todo el tiempo expuestas a diferentes eventos que pueden poner en peligro la seguridad de la información.

9.1 ANALISIS DEL RIESGO

El análisis del riesgo tiene como finalidad determinar la probabilidad de ocurrencia de este y sus consecuencias, este último aspecto puede orientar la clasificación del riesgo, con el objetivo de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar en la entidad.

El análisis del riesgo depende de la información obtenida en la fase de identificación de riesgos, De esta forma los procedimientos claves en el análisis de riesgos son la probabilidad y el impacto.

---

[26] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PÚBLICA. Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas, Anexo 4. [en línea]. <http://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas++Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b> [citado en 15 de marzo de 2019]

La probabilidad se considera la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia, si se ha materializado (por ejemplo: número de veces en un tiempo determinado), o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque este no se haya materializado.

Por Impacto se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Con base a lo anteriormente expuesto se procede a avanzar en el análisis de riesgo donde se deben considerar como prioritarios los siguientes aspectos:

9.1.1 Calificación del riesgo. Se logra a través de la estimación de la probabilidad de su ocurrencia del riesgo y el impacto que puede causar la materialización del riesgo.

9.1.2 Criterio de Probabilidad. El riesgo se debe medir a partir de las siguientes especificaciones que se describe en la siguiente tabla que presenta 5 niveles para medir la probabilidad de ocurrencia.

Tabla 9. Tabla de probabilidad

Nivel	Descriptor	Descripción	Frecuencia
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos de una vez en los últimos 5 años.
3	Posible	El evento podría ocurrir en algún momento.	Al menos de una vez en los últimos 2 años.
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de una vez en el último año.
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de una vez al año.

Fuente: Elaborado a partir de la Guía de Riesgo del Departamento Administrativo de la Función Pública, Página 28.

9.1.3 Criterio de impacto. En este punto se presentan 5 niveles para lograr medir el impacto, dando las herramientas con las cuales se definen los criterios de riesgo. El riesgo se debe medir a partir de las siguientes especificaciones que se muestran a continuación en la siguiente tabla:

Tabla 10. Tabla de impacto

Nivel	Descriptor	Descripción
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
4	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

Fuente: Elaborado a partir de la Guía de Riesgo del Departamento Administrativo de la Función Pública, Página 28.

Adicionalmente se muestra a continuación la tabla donde se describen los impactos de mayor ocurrencia en las entidades del Estado, en este punto en específico se trata el impacto sobre la confidencialidad de la Información, el cual es uno de los pilares de seguridad de la misma.

Tabla 11. Impacto sobre la Confidencialidad de la Información

Nivel	Concepto
1	Personal
2	Grupo de trabajo
3	Relativa al proceso
4	Institucional
5	Estratégica

Fuente: Elaborado a partir de la Guía de Riesgo del Departamento Administrativo de la Función Pública, Página 29.

9.2 EVALUACIÓN DEL RIESGO

Esta etapa del proceso permite hacer una comparación de los resultados de la calificación del riesgo, con los criterios definidos para establecer el grado de exposición de la entidad en seguridad de la información, de esta forma es posible distinguir entre los riesgos importantes, moderados, tolerables, aceptables, o inaceptables y fijar las prioridades de las acciones requeridas para su tratamiento.

Esta evaluación se realiza de forma cualitativa donde se presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto de este.

A continuación, se presenta la tabla número 12 con una matriz para facilitar la calificación y evaluación de los riesgos.

Tabla 12. Matriz de Calificación, Evaluación y respuesta a los Riesgos

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

B: Zona de riesgo baja: Asumir el riesgo

M: Zona de riesgo moderada: Asumir el riesgo, reducir el riesgo

A: Zona de riesgo Alta: Reducir el riesgo, evitar, compartir o transferir

E: Zona de riesgo extrema: Reducir el riesgo, evitar, compartir o transferir

Fuente: Elaborado a partir de la Guía de Riesgo del Departamento Administrativo de la Función Pública, Página 31.

9.3 APLICACION DE LA METODOLOGIA EN LA ENTIDAD

Para el caso del presente proyecto se realizó el análisis y evaluación de riesgos de seguridad de la información enfocada en términos generales a entidades del estado, De esta forma, es una guía o modelo que puede ser adoptada por las partes interesadas.

En este proceso de análisis y evaluación de riesgos, la entidad debe definir si gestionará los riesgos en todos los activos del inventario o solo en aquellos que tengan un nivel de criticidad alto, esto debe estar debidamente documentando y aprobado por la alta dirección.

En este caso del proyecto, el análisis de riesgo se realizó en términos generales a los activos de información de la entidad que tienen un nivel de criticidad alto.

A continuación, se describe en la siguiente tabla el análisis y la evaluación del riesgo de seguridad de la información de la entidad.

Tabla 13. Análisis de Riesgos y Evaluación de Riesgos

Análisis y Evaluación del Riesgo							
Proceso: Gestión de Seguridad de la Información.							
Objetivo: Brindar Soporte Institucional en Seguridad de la Información							
Tipo de Activo	**Riesgo**	**Causa**	**Calificación**		**Tipo de Impacto**	**Evaluación Zona de Riesgo**	**Medidas de Respuesta**
			Probabilidad	**Impacto**			
Datos / Información.	**Perdida de la información Institucional.**	Falta de conciencia sobre seguridad de la información por parte de los funcionarios y contratistas de la entidad en el manejo de la información. Fuga de Información Acceso no Autorizado Ausencia de asignación adecuada de responsabilidades en seguridad de la información.	4	5	CONFIDENCIALIDAD DE LA INFORMACIÓN	**Extrema**	Reducir el riesgo, evitar, compartir o transferir.
	Pérdida de los activos de información que reposan en el servidor de datos de la entidad.	Uso no autorizado de equipo. Entrenamiento insuficiente en seguridad. Falsificación de derechos.	3	4	CONFIDENCIALIDAD DE LA INFORMACIÓN	**Extrema**	Reducir el riesgo, evitar, compartir o transferir.
	Accesos no autorizados de personal mal intencionado para modificar o robar información.	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario. Uso no autorizado de equipo. Abuso de los derechos. Uso no autorizado de equipo. Vulnerabilidades en los sistemas de seguridad. Fuga de Información	3	5	CONFIDENCIALIDAD DE LA INFORMACIÓN	**Extrema**	Reducir el riesgo, evitar, compartir o transferir.

Fuente: Elaboración realizada por el autor del proyecto

Tabla 13. (Continuación)

Análisis y Evaluación del Riesgo							
Proceso: Gestión de Seguridad de la Información.							
Objetivo: Brindar Soporte Institucional en Seguridad de la Información							
Tipo de Activo	**Riesgo**	**Causa**	**Calificación**		**Tipo de Impacto**	**Evaluación Zona de Riesgo**	**Medidas de Respuesta**
			Probabilidad	**Impacto**			
Software y/o Aplicaciones.	**Uso ilegal de sistemas o Activos de Software.**	Falta de conciencia acerca de la seguridad.	3	4	CONFIDENCIALIDAD DE LA INFORMACIÓN	**Extrema**	Reducir el riesgo, evitar, compartir o transferir.
		Instalación indiscriminada de productos o activos de software en los equipos por los usuarios.					
		Deficiente seguimiento y control a las condiciones de uso, vigencia y cantidad de los productos de software adquiridos.					
		No formalización de la cesión de los derechos patrimoniales de autor en productos de software desarrollados internamente o donados a la entidad.					
	Pérdida, alteración, divulgación indebida o indisponibilidad de información sensible procesada a través del software que maneja la entidad.	Uso no autorizado de equipo.	2	4	CONFIDENCIALIDAD DE LA INFORMACIÓN	**Alta**	Reducir el riesgo, evitar, compartir o transferir.
		Entrenamiento insuficiente en seguridad.					
		Amenazas y vulnerabilidades sobre la plataforma tecnológica					
		Software nuevo o inmaduro.					
		Mal funcionamiento del software.					
		Uso no autorizado de equipo.					
		Virus Informático.					
Red	**Afectación e indisponibilidad de la plataforma tecnológica de canales, Internet, servidores y correo electrónico.**	Indisponibilidad de las redes (WAN, LAN, WIFI), Servidores y correo electrónico.	4	4	CONFIDENCIALIDAD DE LA INFORMACIÓN	**Extrema**	Reducir el riesgo, evitar, compartir o transferir.
		Arquitectura insegura de la red.					
		Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)					

Fuente: Elaboración realizada por el autor del proyecto

Tabla 13. (Continuación)

Análisis y Evaluación del Riesgo							
Proceso: Gestión de Seguridad de la Información.							
Objetivo: Brindar Soporte Institucional en Seguridad de la Información							
Tipo de Activo	**Riesgo**	**Causa**	**Calificación**		**Tipo de Impacto**	**Evaluación Zona de Riesgo**	**Medidas de Respuesta**
			Probabilidad	**Impacto**			
Hardware	**Falla técnica en Servidor o Equipos de Cómputo.**	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento. Incumplimiento en el mantenimiento del sistema de información. Susceptibilidad a la humedad, el polvo y la suciedad. Pérdida del suministro de Energía. Fallas del equipo.	4	3	CONFIDENCIALIDAD DE LA INFORMACIÓN	**Alta**	Reducir el riesgo, evitar, compartir o transferir.
	Perdida, hurto o daño accidental en equipos tecnológicos.	Inadecuadas condiciones y medidas de seguridad. Mala manipulación y accidentes Uso no autorizado de equipo. Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información. Ausencia de protección física de la edificación, puertas y ventanas	2	4	CONFIDENCIALIDAD DE LA INFORMACIÓN	**Alta**	Reducir el riesgo, evitar, compartir o transferir.
Personas	**Falta de personal debidamente autorizado y capacitado para la realización de las actividades de los procesos institucionales.**	Uso incorrecto de software y hardware. Falta de conciencia acerca de la seguridad.	3	3	CONFIDENCIALIDAD DE LA INFORMACIÓN	**Alta**	Reducir el riesgo, evitar, compartir o transferir.
Servicios	**Falta completa de Continuidad en el negocio, interrupción en el servicio de la entidad.**	Eventos catastróficos, Inundaciones, incendios, terremotos.	1	5	CONFIDENCIALIDAD DE LA INFORMACIÓN	**Alta**	Reducir el riesgo, evitar, compartir o transferir.

Fuente: Elaboración realizada por el autor del proyecto

10. CONTROLES DE REFERENCIA PARA LA MITIGACION DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En esta fase del proyecto después de realizar el análisis y evaluación de riesgos, el siguiente paso debe ser verificar la existencia de controles de seguridad en la entidad, esto con el fin de que la entidad pueda mitigar y tratar los riesgos de seguridad de la información.

En la realización de esta actividad se tuvo en cuenta los objetivos de control y controles de referencia, basados en la norma ISO/IEC 27001:2013 en su Anexo A, como un insumo base para mitigar los riesgos de seguridad de la información[27], sin embargo, la entidad en cualquier caso puede implementar nuevos controles de seguridad que no estén incluidos dentro del Anexo, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo.

Para el caso de este proyecto aplicado se realizó la Declaración de Aplicabilidad en términos generales y enfocado a las entidades del estado que deseen adoptar esta guía o modelo, con el fin de mitigar y tratar los riesgos de seguridad de la información, se emplearon los siguientes controles que se describen en la tabla No. 15 Declaración de Aplicabilidad, tomados del Anexo A del estándar ISO/IEC 27001:2013 y los dominios a los que pertenecen, siempre y cuando se ajusten al análisis de riesgos.

Tabla 14. Razones de Aplicabilidad

Nomenclatura	Nombre
RL	Requerimientos Legales
OC	Obligación Contractual
RN/BP	Requerimiento del negocio/Mejores prácticas adoptadas
RAR	Resultado de la evaluación de riesgos

Fuente: Elaboración realizada por el autor del proyecto

El contenido de la tabla No. 15 Declaración de Aplicabilidad se puede interpretar de la siguiente manera:

A.X – Dominio
A.X.X – Objetivo de Control
A.X.X.X - Controles

[27] NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27001:2013, Pág. 13

Tabla 15. Declaración de Aplicabilidad

Objetivos de Control	Controles ISO 27001:2013	Aplicabilidad	Razones para la selección de controles	Justificación
A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN				
A.5.1 Directrices establecidas por la dirección para la seguridad de la información	A.5.1.1 Políticas para la seguridad de la información.	SI	RAR	La entidad identifica los riesgos que afectan la seguridad que hay dentro de la misma, es importante establecer una política de seguridad de la información para su respectiva divulgación a todos los funcionarios y contratistas, para así concientizarlos de los riesgos a los que está expuesto la entidad y dar a conocer los controles implementados para minimizar y mitigar los riesgos detectados.
	A.5.1.2 Revisión de las políticas para seguridad de la información.	SI	RAR	La política de seguridad de la información de la entidad deberá ser planificada y revisada con frecuencia para asegurar su idoneidad, efectividad y eficacia. Está política permitirá que la entidad trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales a los cuales esté obligada a cumplir la entidad.
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN				
A.6.1 Organización interna	A.6.1.1 Roles y responsabilidades para la seguridad de información.	SI	RN/BP	La entidad a través de una resolución establece la creación del comité de seguridad de la información donde establece los roles, responsabilidades y funciones. Con el fin de determinar compromisos institucionales para su cumplimiento.
	A.6.1.2 Separación de deberes.	SI	RN/BP	Como principio de seguridad, la entidad define y separa los roles y responsabilidades en las áreas críticas para evitar y reducir el acceso no autorizado y el uso indebido de los activos de información.
	A.6.1.3 Contacto con las Autoridades.	SI	RL	La entidad realiza el contacto con las autoridades pertinentes como la Policía Nacional y la Fiscalía dependiendo del incidente presentado.
	A.6.1.4 Contacto con grupos de interés especial.	SI	RN/BP	La entidad a través de los funcionarios encargados, serán los indicados para reportar cualquier incidente de Seguridad de la información que pueda poner en peligro la confidencialidad, integridad, y disponibilidad de la información. Se debe mantener contacto permanente con grupos de interés especial para de esta manera mantenerse al tanto en amenazas, incidentes y soluciones.

Fuente: Elaboración realizada por el autor del proyecto apoyado en la norma ISO/IEC 27001:2013 en su Anexo A

Tabla 15. (Continuación)

Objetivos de Control	Controles ISO 27001:2013	Aplicabilidad	Razones para la selección de controles	Justificación
	A.6.1.5 Seguridad de la información en la gestión de proyectos.	SI	RN/BP	La Entidad deberá aplicar todas y cada una de las políticas establecidas, para todos los proyectos que se desarrollen, independientemente del tipo y la clase de proyecto, con la finalidad de garantizar la confidencialidad, integridad, disponibilidad de la información que se utilice o se genere como producto del desarrollo de dichos proyectos.
A.6.2 Dispositivos móviles y teletrabajo	A.6.2.1 Política para dispositivos móviles.	SI	OC	Como principio de seguridad, la entidad deberá adoptar una política de seguridad de la información para gestionar los riesgos introducidos por el uso de dispositivos móviles.
	A.6.2.2 Teletrabajo.	SI	OC	Como principio de seguridad, la entidad deberá adoptar y proporcionar una política de seguridad para salvaguardar la información a la que se tiene acceso, que es procesada o almacenada en los lugares donde realiza el teletrabajo.
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS				
A.7.1 Antes de asumir el empleo	A.7.1.1 Selección.	SI	OC	La entidad a través del departamento de gestión humana o quien haga las veces en los procesos de selección de personal, tienen la obligación de verificar los datos que reposan en la hoja de vida del aspirante, para verificar el cumplimiento del perfil, así como la verificación de los respectivos antecedentes disciplinarios.
	A.7.1.2 Términos y condiciones del empleo.	SI	OC	Como principio de seguridad, la entidad debe exigir en los contratos que se firman con funcionarios y contratistas que haya unos términos y condiciones donde se establezcan responsabilidades acerca de la confidencialidad y seguridad de la información.
A.7.2 Durante la ejecución del empleo	A.7.2.1 Responsabilidades de la dirección.	SI	OC	La entidad a través de la alta dirección deberá exigir a los funcionarios y contratistas el estricto cumplimiento y su respectiva aplicación de la seguridad de la información conforme a las políticas y procedimientos establecidos por la entidad.
	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	SI	OC	La entidad en su deber institucional deberá capacitar y formar a todos los funcionarios y contratistas en la importancia de la seguridad de información, para que tengan conciencia apropiada de los roles, políticas y lineamientos pertinentes a su cargo.

Fuente: Elaboración realizada por el autor del proyecto apoyado en la norma ISO/IEC 27001:2013 en su Anexo A

Tabla 15. (Continuación)

Objetivos de Control	Controles ISO 27001:2013	Aplicabilidad	Razones para la selección de controles	Justificación
	A.7.2.3 Proceso disciplinario.	SI	OC	La entidad dentro de sus deberes y obligaciones debería tener un reglamento o proceso disciplinario establecido, el cual debe ser divulgado para todos los funcionarios y contratistas que incurran en incidentes de violación de la seguridad de la información, con el fin de emprender las acciones pertinentes.
A.7.3 Terminación o cambio de empleo	A.7.3.1 Terminación o cambio de responsabilidades de empleo.	SI	OC	La entidad debería establecer en los términos y condiciones contractuales las responsabilidades y deberes con respecto a la seguridad de la información para cuando un funcionario termine su vinculación laboral, estas deben ser definidas comunicadas por la alta dirección y respectivamente se deben hacer cumplir.
A.8 GESTIÓN DE ACTIVOS				
A.8.1 Responsabilidad por los activos	A.8.1.1 Inventario de activos.	SI	RN/BP	La entidad como obligación debe tener todos sus activos de información plenamente identificados, por lo tanto, debe realizar y mantener un inventario de estos activos.
	A.8.1.2 Propiedad de los activos.	SI	RN/BP	Los activos identificados y organizados en el inventario deberían tener un propietario responsable, es su deber proteger y mantener la confidencialidad, integridad y disponibilidad de los activos de información.
	A.8.1.3 Uso aceptable de los Activos.	SI	RN/BP	Todos los funcionarios y contratistas que hagan uso de los activos de la entidad tienen la responsabilidad de dar cumplimiento a las reglas establecidas para el uso aceptable de los activos, entendiendo que el uso no adecuado de los recursos pone en peligro el objetivo institucional y genera sanciones de acuerdo con las normas y legislación vigentes.
	A.8.1.4 Devolución de activos.	SI	RN/BP	Todos los funcionarios y contratistas que hagan uso de activos de la entidad tienen la responsabilidad de entregar y devolver los que tienen asignados a su cargo al momento de la terminación de su vinculación laboral. Esto con el fin de dar el visto bueno de su jefe inmediato y su correspondiente paz y salvo.
A.8.2 Clasificación de la información	A.8.2.1 Clasificación de la Información.	SI	RN/BP	La entidad debería clasificar la información física o digital en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada por parte de funcionarios y contratistas.

Fuente: Elaboración realizada por el autor del proyecto apoyado en la norma ISO/IEC 27001:2013 en su Anexo A

Tabla 15. (Continuación)

Objetivos de Control	Controles ISO 27001:2013	Aplicabilidad	Razones para la selección de controles	Justificación
	A.8.2.2 Etiquetado de Información.	SI	RAR	La entidad a través de los responsables de la seguridad de la información debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, dependiendo del esquema de clasificación adoptado por la entidad, por cada definición, deben elaborarse lineamientos a seguir para realizar el copiado, la impresión, el almacenamiento, la transmisión electrónica, el intercambio físico y su destrucción.
	A.8.2.3 Manejo de activos.	SI	RN/BP	La entidad a través de los responsables de la seguridad de la información debería desarrollar e implementar procedimientos para el manejo de activos, dependiendo del esquema de clasificación adoptado por la misma, cada funcionario o contratista será responsable por el uso indebido que se les dé a los activos de información.
A.8.3 Manejo de Medios	A.8.3.1 Gestión de medios removibles.	SI	RN/BP	La entidad a través de los responsables de la seguridad de la información debería implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la misma.
	A.8.3.2 Disposición de los Medios.	SI	RN/BP	La entidad a través de los responsables de la seguridad de la información definirá procedimientos y lineamientos para la eliminación segura de los medios de información respetando la normatividad vigente.
	A.8.3.3 Transferencia de medios físicos.	SI	RN/BP	La entidad debe establecer los controles de seguridad necesarios para proteger los medios que contienen información institucional, contra el acceso no autorizado, uso indebido o corrupción durante el transporte.
A.9 CONTROL DE ACCESO				
A.9.1 Requisitos del negocio para control de acceso	A.9.1.1 Política de control de Acceso.	SI	RN/BP	La entidad debería establecer y documentar medidas de control de acceso a nivel de red, sistema operativo, sistemas de información y servicios de TI. Los controles de acceso deben ser conocidos por todos los servidores públicos de la entidad y limitar el acceso hacia los activos de información de acuerdo con lo establecido por el perfil del cargo. Los controles de acceso deberán contemplar requerimientos de seguridad y definir los perfiles o privilegios de acceso de los usuarios de acuerdo con su perfil de cargo en la entidad.

Fuente: Elaboración realizada por el autor del proyecto apoyado en la norma ISO/IEC 27001:2013 en su Anexo A

Tabla 15. (Continuación)

Objetivos de Control	Controles ISO 27001:2013	Aplicabilidad	Razones para la selección de controles	Justificación
	A.9.1.2 Política sobre el uso de los servicios de red.	SI	RN/BP	Como principio de seguridad, la entidad deberá adoptar una política de seguridad de la información para permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2 Gestión de acceso de usuarios	A.9.2.1 Registro y cancelación del registro de usuarios.	SI	RN/BP	La entidad a través de los responsables de la seguridad de la información debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso. Con el fin de evitar el acceso no autorizado.
	A.9.2.2 Suministro de acceso de usuarios.	SI	RN/BP	La entidad a través de los responsables de la seguridad de la información debería implementar un protocolo de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios de la entidad.
	A.9.2.3 Gestión de derechos de acceso privilegiado.	SI	RN/BP	La asignación y uso de derechos de acceso privilegiado en la entidad debe ser restringida y controlada por parte de los responsables de la seguridad de la información, esto formalizado bajo una política de control de acceso con privilegios altos y autorizados.
	A.9.2.4 Gestión de información de autenticación secreta de usuarios.	SI	RN/BP	La entidad debería establecer, documentar y revisar una política de control de acceso donde la asignación de la información secreta se debería controlar por medio de un proceso de gestión formal, revisado y autorizado por la alta gerencia.
	A.9.2.5 Revisión de los derechos de acceso de usuarios.	SI	RN/BP	La entidad a través de los propietarios de los activos de información debería establecer un esquema sistémico que les permita revisar frecuentemente los derechos de acceso de los usuarios, con el fin de mantener un control eficiente y eficaz del acceso a los datos y servicios de información de la entidad.
	A.9.2.6 Retiro o ajuste de los derechos de acceso.	SI	RN/BP	La entidad a través del departamento de Gestión Humana o quien haga sus veces deberá notificar al funcionario o contratista que sus derechos de acceso a las instalaciones y los sistemas de información serán retirados al finalizar su vinculación laboral, Con el fin de entregar todos los pendientes de su cargo a la fecha y su respectivo paz y salvo.

Fuente: Elaboración realizada por el autor del proyecto apoyado en la norma ISO/IEC 27001:2013 en su Anexo A

Tabla 15. (Continuación)

Objetivos de Control	Controles ISO 27001:2013	Aplicabilidad	Razones para la selección de controles	Justificación
A.9.3 Responsabilidades de los usuarios	A.9.3.1 Uso de la información de autenticación secreta.	SI	OC	La entidad debería exigir a los funcionarios y contratistas que sigan y cumplan las buenas prácticas de la entidad para el uso de información de autenticación secreta. Se recomienda que se utilicen contraseñas seguras para la correcta validación y autenticación de la identidad.
A.9.4 Control de acceso a sistemas y aplicaciones	A.9.4.1 Restricción de acceso Información.	SI	OC	La entidad a través de los responsables de la seguridad de la información debería restringir el acceso a la información y a las funciones de los sistemas de las aplicaciones a los funcionarios y contratistas no autorizados bajo unas estrictas medidas y políticas de control de acceso.
	A.9.4.2 Procedimiento de ingreso seguro.	SI	OC	La entidad implementará un procedimiento de acceso a los sistemas y a las aplicaciones, con el fin de minimizar la oportunidad de acceso no autorizado a los mismos. Esto apoyado bajo la política de control de acceso para controlar un proceso de ingreso seguro.
	A.9.4.3 Sistema de gestión de contraseñas.	SI	OC	La entidad a través de los responsables de la seguridad de la información determina que los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas. Los funcionarios y contratistas podrán acceder al servicio de contraseña informática mediante la validación de esta, la cual es exclusividad de su propietario.
	A.9.4.4 Uso de programas utilitarios privilegiados	SI	RN/BP	La entidad a través de los responsables de la seguridad de la información debería establecer procedimientos de control para restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones. Es importante que su uso sea estrictamente limitado y controlado con el fin de evitar que funcionarios y contratistas con acceso estándar puedan instalar software que puedan poner en riesgo la seguridad de la información.
	A.9.4.5 Control de acceso a códigos fuente de programas	SI	OC	La entidad a través de los responsables de la seguridad de la información debería restringir el acceso no autorizado a los códigos fuente de los programas. Esto apoyado bajo la política de control de acceso para controlar un proceso de ingreso seguro.

Fuente: Elaboración realizada por el autor del proyecto apoyado en la norma ISO/IEC 27001:2013 en su Anexo A

Tabla 15. (Continuación)

Objetivos de Control	Controles ISO 27001:2013	Aplicabilidad	Razones para la selección de controles	Justificación
A.10 CRIPTOGRAFÍA				
A.10.1 Controles criptográficos	A.10.1.1 Política sobre el uso de controles criptográficos	SI	RN/BP	La entidad a través de los responsables de la seguridad de la información serán los encargados de definir los mecanismos de cifrado de información más apropiados frente a las necesidades de la entidad. El uso de herramientas de cifrado será autorizado conforme a los roles y responsabilidades de los funcionarios y contratistas de la entidad.
	A.10.1.2 Gestión de llaves	SI	RN/BP	Las diferentes dependencias de la entidad son las encargadas de realizar la respectiva adquisición, creación, activación, distribución de dispositivos de control criptográfico (token) para sus respectivas dependencias.
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO				
A.11.1 Áreas seguras	A.11.1.1 Perímetro de seguridad física	SI	OC	La entidad debe contar con perímetros de seguridad en las áreas donde se encuentren instalados los centros de procesamiento de la Información, Suministro de Energía Eléctrica, de Aire Acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los Sistemas de Información de la entidad. Los perímetros de seguridad deben estar delimitados por una barrera, por ejemplo, una pared, una puerta de acceso controlado por dispositivo de autenticación u oficina de recepción atendidos por personas para controles de acceso físico.
	A.11.1.2 Controles físicos de entrada	SI	OC	Todas las áreas destinadas al procesamiento o almacenamiento de información confidencial y secreta, así como aquellas en las que se encuentren los equipos y demás infraestructura que soporte a los sistemas de información y comunicaciones debe ser protegida con medidas de control de acceso físico tales como: • Los Centros de Cómputo deben contar con mecanismos de control de acceso tales como puertas de seguridad, cerradura, sistemas de control con tarjetas inteligentes, sistema de alarmas o controles biométricos. • Todos los funcionarios, Contratistas o Terceros deben portar el carné que los acredite que prestan sus servicios a la entidad, no deben intentar ingresar a las áreas donde no tengan la debida autorización.

Fuente: Elaboración realizada por el autor del proyecto apoyado en la norma ISO/IEC 27001:2013 en su Anexo A

Tabla 15. (Continuación)

Objetivos de Control	Controles ISO 27001:2013	Aplicabilidad	Razones para la selección de controles	Justificación
	A.11.1.3 Seguridad de oficinas, recintos e instalaciones	SI	OC	La entidad dentro de sus políticas y lineamientos define: • Los escritorios o puestos de trabajo de los servidores públicos deben mantenerse limpios y sin documentos fuera del horario de trabajo o en ausencia prolongada del sitio, esto para evitar el acceso no autorizado a la información. • Los Servidores Públicos deben poner las pantallas de sus computadores en una posición en la que se evite que personal no autorizado pueda ver la información que se encuentre desplegada en ellas. • Las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a las oficinas solo deben ser utilizados por los funcionarios autorizados y, salvo situaciones de Emergencia, estos no deben ser transferidos a otros funcionarios de la Entidad, Contratista o Terceros con su debida autorización. • No dejar abandonada en las impresoras información Confidencial y Secreta, una vez se haya impreso.
	A.11.1.4 Protección contra amenazas externas y ambientales	SI	OC	La entidad dentro de sus políticas y lineamientos define: • Las Oficinas e instalaciones donde se procesa y/o almacena la información confidencial o secreta debe contar con sistemas de alarmas y cámaras de seguridad, sistema de detección y extinción automáticas de incendios. • Se debe mantener buena ubicación de los equipos, aislado de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros. • Los equipos del Centro de Cómputo deben tener control de los niveles de temperatura y humedad, estos deben ser mantenidos dentro de los límites requeridos por la infraestructura de cómputo allí instalada.
	A.11.1.5 Trabajo en áreas seguras	SI	OC	La entidad dentro de sus políticas y lineamientos define: • La responsabilidad del ingreso a áreas denominadas como seguras será exclusiva del responsable de dicha área y el responsable del área segura o a quien éste designe debe supervisar los trabajos realizados por terceros en el área segura a su cargo.

Fuente: Elaboración realizada por el autor del proyecto apoyado en la norma ISO/IEC 27001:2013 en su Anexo A

Tabla 15. (Continuación)

Objetivos de Control	Controles ISO 27001:2013	Aplicabilidad	Razones para la selección de controles	Justificación
	A.11.1.6 Áreas de despacho y carga.	SI	OC	La entidad para evitar el acceso no autorizado debe controlar los puntos de acceso tales como áreas de despacho y de carga, Inspeccionar y registrar las cargas antes de entrar al edificio para evitar potenciales amenazas. Las zonas de carga, despacho y acceso al público deben ser zonas incomunicadas con las zonas seguras, para evitar el acceso a personal no autorizado.
A.11.2 Equipos	A.11.2.1 Ubicación y protección de los equipos.	SI	RN/BP	La entidad para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la entidad que se encuentran dentro o fuera de sus instalaciones, provee los recursos que garantizan la mitigación de riesgos sobre dicha plataforma tecnológica.
	A.11.2.2 Servicios de suministro.	SI	RN/BP	Dentro de la entidad existen servicios de suministro que soportan todo el procesamiento de información como son el servicio de energía, respaldo con UPS, equipos de comunicación entre otros. Para ello es necesario que estos servicios se estén monitoreando y realizando mantenimiento preventivo para identificar fallas y corregirlas, y así mitigar los impactos que la no prestación de estos servicios pudiera ocasionar en los servicios de procesamiento con los cuales hoy cuenta la entidad.
	A.11.2.3 Seguridad del cableado.	SI	RN/BP	El cableado estructurado de la entidad debe estar diseñado de tal forma que soporte los servicios tecnológicos y de comunicaciones que requiere, Este debe estar certificado con la categoría de cable exigida para mayor seguridad en la integridad de los datos que soporta.
	A.11.2.4 Mantenimiento de equipos.	SI	RN/BP	La entidad debe implementar el mantenimiento preventivo y correctivo de equipos de cómputo de una forma periódica para asegurar su disponibilidad e integridad continuas. De tal manera que los procesos normales de la entidad no se vean afectados por fallas en los equipos de cómputo.
	A.11.2.5 Retiro de activos	SI	RN/BP	Los funcionarios y contratistas que necesiten retirar activos de información hardware y software deben contar con la autorización de los responsables de la seguridad de la información quien controla los inventarios dentro de la entidad.

Fuente: Elaboración realizada por el autor del proyecto apoyado en la norma ISO/IEC 27001:2013 en su Anexo A

Tabla 15. (Continuación)

Objetivos de Control	Controles ISO 27001:2013	Aplicabilidad	Razones para la selección de controles	Justificación
	A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones	SI	RN/BP	Los funcionarios y contratistas que tienen equipos de cómputo y activos de información a su cargo deben responder dentro y fuera de las instalaciones, teniendo en cuenta los riesgos a los que están sometidos por estar fuera de las instalaciones de la entidad. Para estos procedimientos se deben aplicar las políticas y procedimientos establecidos por la entidad.
	A.11.2.7 Disposición segura o reutilización de equipos	SI	RN/BP	Como principio de seguridad la entidad antes de dar de baja un equipo o reasignarlo, se debe eliminar la información sensible que este contenga, con el fin de evitar la pérdida de la información y recuperación de información no autorizada, igualmente se debe desinstalar cualquier software, de tal forma que se evite tener problemas de licenciamiento.
	A.11.2.8 Equipos de usuarios desatendidos.	SI	RN/BP	Los usuarios de los equipos deben asegurarse de que tengan la protección necesaria cuando estén desatendidos, para mayor seguridad todos los equipos de cómputo que posee la entidad sean los instalados en los puestos de trabajo o los ubicados en el centro de procesamiento de los datos, requieren protección específica frente al acceso no autorizado.
	A.11.2.9 Política de escritorio limpio y pantalla limpia.	SI	RN/BP	La entidad adoptara una política de escritorio limpio para los equipos y medios de almacenamiento removibles (memorias USB, SD, microSD, Discos duros externos, CD, DVD…), y una política de pantalla limpia en las instalaciones de la entidad donde se realicen procesos de información. Con la finalidad de minimizar los riesgos de acceso no autorizado, pérdida y daño de la información.
A.12 SEGURIDAD DE LAS OPERACIONES				
A.12.1 Procedimientos operacionales y responsabilidades	A.12.1.1 Procedimientos de operación documentados.	SI	RN/BP	La entidad a través de los responsables de la seguridad de la información documentará y actualizará los procedimientos de operación, esta debe ser comunicada y divulgada a todos los funcionarios y contratistas de la entidad que la soliciten.
	A.12.1.2 Gestión de cambios	SI	RN/BP	Todo cambio que se realice en la entidad deberá ser evaluado previamente en aspectos técnicos y de seguridad de la información.

Fuente: Elaboración realizada por el autor del proyecto apoyado en la norma ISO/IEC 27001:2013 en su Anexo A

Tabla 15. (Continuación)

Objetivos de Control	Controles ISO 27001:2013	Aplicabilidad	Razones para la selección de controles	Justificación
	A.12.1.3 Gestión de capacidad.	SI	RN/BP	La entidad a través de los responsables de la seguridad de la información realizará monitoreo y análisis permanente a toda la infraestructura tecnológica de procesamiento de información, con el fin de identificar el estado y la utilización de todos los recursos. De esta forma hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
	A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación.	SI	OC	La entidad a través de los responsables de la seguridad de la información deberá separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación. En su mayoría El software que utiliza la entidad es desarrollado, actualizado e implementado por terceros.
A.12.2 Protección contra códigos maliciosos	A.12.2.1 Controles contra códigos maliciosos.	SI	RAR	La entidad a través de los responsables de la seguridad de la información implementa controles de detección y prevención, así mismo los funcionarios y contratistas deben estar concientizados y apropiados para proteger la información contra software malicioso.
A.12.3 Copias de respaldo	A.12.3.1 Respaldo de información.	SI	RN/BP	Le entidad a través de sus políticas de seguridad realiza respaldo de la información y del software frecuentemente. Con el fin de proteger la información institucional y minimizar los riesgos de perdida de información por actos accidentales, malintencionados o por fallas de los equipos y redes.
A.12.4 Registro y seguimiento	A.12.4.1 Registro de eventos	SI	RN/BP	La entidad debería elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
	A.12.4.2 Protección de la información de registro.	SI	RAR	Las instalaciones y la información de registro de la entidad se deberían proteger contra alteración y acceso no autorizado.
	A.12.4.3 Registros del administrador y del operador	SI	RN/BP	Entre los roles y responsabilidades del administrador y operador del sistema es documentar y registrar todas las actividades y eventos que afecten la seguridad de las operaciones, por lo tanto, los registros se deben proteger y revisar con frecuencia.

Fuente: Elaboración realizada por el autor del proyecto apoyado en la norma ISO/IEC 27001:2013 en su Anexo A

Tabla 15. (Continuación)

Objetivos de Control	Controles ISO 27001:2013	Aplicabilidad	Razones para la selección de controles	Justificación
	A.12.4.4 sincronización de relojes.	SI	RN/BP	En la entidad todos los relojes de todos los sistemas de procesamiento de información están sincronizados con la hora legal colombiana tomado de la página de la superintendencia de industria y comercio www.sic.gov.co/hora-legal-colombiana.
A.12.5 Control de software operacional	A.12.5.1 Instalación de software en sistemas operativos.	SI	OC	La instalación, desinstalación, actualización y/o modificación de software en sistemas operativos de la entidad, deberá ser realizado únicamente por el personal autorizado que tenga esos roles y responsabilidades, ningún funcionario o contratista está autorizado para realizar ninguna de los anteriores procedimientos sobre el software.
A.12.6 Gestión de la vulnerabilidad técnica	A.12.6.1 Gestión de las vulnerabilidades técnicas	SI	RN/BP	La entidad a través de los responsables de la seguridad de la información debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen, evaluar la exposición a la que está sometida la entidad sobre estas vulnerabilidades, y tomar los controles pertinentes para tratar y minimizar el riesgo asociado.
	A.12.6.2 Restricciones sobre la instalación de software.	SI	RAR	La entidad tiene definidos unas reglas, roles y responsabilidades para la instalación de software, cualquier tipo de instalación debe estar autorizada por los responsables de la seguridad de la información de la entidad.
A.12.7 Consideraciones sobre auditorias de sistemas de información	A.12.7.1 Información controles de auditoría de sistemas.	SI	RAR	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio. Esto implica una planificación de los requerimientos y tareas, a fin de minimizar el riesgo de interrupción en las operaciones de las áreas involucradas en la auditoría.
A.13 SEGURIDAD DE LAS COMUNICACIONES				
A.13.1 Gestión de la seguridad de las redes	A.13.1.1 Controles de redes	SI	OC	La entidad a través de los responsables de la seguridad de la información definirá e implementará controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la entidad, contra el acceso no autorizado en sistemas y aplicaciones.

Fuente: Elaboración realizada por el autor del proyecto apoyado en la norma ISO/IEC 27001:2013 en su Anexo A

Tabla 15. (Continuación)

Objetivos de Control	Controles ISO 27001:2013	Aplicabilidad	Razones para la selección de controles	Justificación
	A.13.1.2 Seguridad de los servicios de red.	SI	OC	La entidad a través de los responsables de la seguridad de la información definirá los controles y procedimientos para garantizar la seguridad de los servicios de red de esta, se deben documentar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
	A.13.1.3 Separación en las redes.	SI	OC	La entidad a través de los responsables de la seguridad de la información debería separar en las redes los grupos de servicios, usuarios y sistemas de información, se podrán dividir en dominios lógicos o VLAN independientes. Para esto se definirán y documentarán los perímetros de seguridad que sean convenientes.
A.13.2 Transferencia de información	A.13.2.1 Políticas y procedimientos de transferencia de información.	SI	RN/BP	Proteger la información transferida al interior y exterior de la entidad. El Área de Tecnologías y Sistemas de Información, realiza el control del uso de sistemas de transferencia de archivos vía FTP a terceros. Las directrices para transferencia de información se encuentran definidas y documentadas en procedimientos y lineamientos para acuerdos de transferencia de información.
	A.13.2.2 Acuerdos sobre transferencia de información.	SI	RN/BP	Los acuerdos están definidos a través de un documento de políticas y lineamientos, este acuerdo debería tener en cuenta la transferencia segura de información del negocio entre la entidad y las partes externas.
	A.13.2.3 Mensajería electrónica.	SI	RN/BP	La entidad a través de los responsables de la seguridad de la información protegerá, definirá y documentará lineamientos y procedimientos claros con respecto al uso de la mensajería electrónica.
	A.13.2.4 Acuerdos de confidencialidad o de no divulgación.	SI	RL	La entidad como principio de seguridad deberá identificar, revisar periódicamente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación, estos acuerdos son obligatorios y de estricto cumplimiento por parte de la entidad, esto con el fin de proteger la confidencialidad e integridad de la información.

Fuente: Elaboración realizada por el autor del proyecto apoyado en la norma ISO/IEC 27001:2013 en su Anexo A

Tabla 15. (Continuación)

Objetivos de Control	Controles ISO 27001:2013	Aplicabilidad	Razones para la selección de controles	Justificación
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTOS DE SISTEMAS				
A.14.1 Requisitos de seguridad de los sistemas de información	A.14.1.1 Análisis y especificación de requisitos de seguridad de la información.	SI	RN/BP	Esta política aplica los requisitos relacionados con la seguridad de información de la entidad, para incorporar controles de seguridad a los sistemas adquiridos por terceros, al igual que para las mejoras o actualizaciones que se realicen a los sistemas ya existentes.
	A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas.	SI	RN/BP	La entidad a través de los responsables de la seguridad de la información entre sus roles y responsabilidades esta la protección de la información involucrada en los servicios de aplicaciones que pasan sobre redes públicas con el fin de salvaguardarlas de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
	A.14.1.3 Protección de transacciones de los servicios de las aplicaciones	SI	RN/BP	La entidad a través de los responsables de la seguridad de la información deberá establecer e implementar una política de seguridad que proteja la información involucrada en las transacciones de los servicios de las aplicaciones. Con la finalidad de evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizados.
A.14.2 Seguridad en los procesos de desarrollo y soporte.	A.14.2.1 Política de desarrollo seguro.	SI	RL	La entidad deberá establecer e implementar una política de seguridad para que el desarrollo externo de los sistemas de información cumpla con los requisitos de seguridad de alto nivel, donde se cumpla con metodologías de buenas prácticas para desarrollo seguro de aplicativos, así como para la realización de pruebas de aceptación y seguridad al software. Adicionalmente es importante que el desarrollo del software tenga el soporte exigido por la entidad.
	A.14.2.2 Procedimientos de control de cambios en sistemas.	SI	RN/BP	La entidad a través de los responsables de la seguridad de la información deberá establecer e implementar una política con lineamientos formales de control de cambios en los sistemas de información de la entidad, con la finalidad de minimizar los riesgos de alteraciones a los sistemas de información, estos procedimientos deben ser controlados y verificados con acceso autorizado.

Fuente: Elaboración realizada por el autor del proyecto apoyado en la norma ISO/IEC 27001:2013 en su Anexo A

Tabla 15. (Continuación)

Objetivos de Control	Controles ISO 27001:2013	Aplicabilidad	Razones para la selección de controles	Justificación
	A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación.	SI	RN/BP	Cuando en la entidad se realicen cambios en el software como sistemas operativos o aplicaciones, el área de sistemas debe revisar cuales son los más críticos para el funcionamiento institucional, y ponerlos a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la entidad.
	A.14.2.4 Restricciones en los cambios a los paquetes de software.	SI	RN/BP	Cuando en la entidad se realicen cambios en el software como sistemas operativos o aplicaciones, el área de sistemas o los que tengan el rol y la responsabilidad, deberán desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente bajo las políticas y lineamientos definidos por la entidad.
	A.14.2.5 Principios de construcción de sistemas seguros.	SI	RN/BP	La entidad a través de los responsables de la seguridad de la información aplicará los principios de sistemas seguros, documentando y aplicando procesos seguros en la implementación de cualquier sistema de información.
	A.14.2.6 Ambiente de desarrollo seguro.	SI	RN/BP	La entidad debería establecer y proteger adecuadamente bajo políticas y lineamientos establecidos, los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas de información que comprendan todo el ciclo de vida de desarrollo de software.
	A.14.2.7 Desarrollo contratado externamente.	SI	RN/BP	La entidad en los casos de desarrollo de software externo supervisa y realiza seguimiento a través de un funcionario delegado de las actividades de desarrollo de sistemas contratados externamente.
	A.14.2.8 Pruebas de seguridad de sistemas.	SI	RN/BP	La entidad deberá exigir durante el desarrollo de software y aplicaciones las pruebas de funcionalidad necesarias y pertinentes de la seguridad. Esto bajo la supervisión del funcionario o el área designada por la entidad.
	A.14.2.9 Prueba de aceptación de sistemas.	SI	RN/BP	La entidad a través de los responsables de la seguridad de la información o el área de sistemas deberá establecer las políticas y lineamientos para la aceptación de sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas y mecanismos de prueba para aceptación y criterios de aceptación relacionados. Bajo la supervisión de los delegados designados por la entidad.

Fuente: Elaboración realizada por el autor del proyecto apoyado en la norma ISO/IEC 27001:2013 en su Anexo A

Tabla 15. (Continuación)

Objetivos de Control	Controles ISO 27001:2013	Aplicabilidad	Razones para la selección de controles	Justificación
A.14.3 Datos de prueba	A.14.3.1 Protección de datos de prueba.	SI	RAR	La entidad a través del área de sistemas deberá asegurar por intermedio de procedimientos y lineamientos definidos, que los datos de prueba se deberían seleccionar, proteger y controlar cuidadosamente. Con el fin de minimizar y evitar la fuga de información.
A.15 RELACIÓN CON LOS PROVEEDORES				
A.15.1 Seguridad de la información en las relaciones con los proveedores	A.15.1.1 Política de seguridad de la información para las relaciones con proveedores.	SI	RN/BP	Este procedimiento está relacionado con la protección de los activos de la entidad a los cuales los proveedores o terceros tienen acceso. Aquí se establecen los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la entidad, estos se deben acordar de mutuo acuerdo y quedar documentados.
	A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores.	SI	RN/BP	Este procedimiento debe indicar como la entidad establece, acuerda, aprueba y divulga los requerimientos y obligaciones relacionados con la seguridad de la información con los proveedores, (es decir algún intermediario). Dichos acuerdos deben tener características como: Aspectos legales, descripción de la información a la que ambas partes tendrán acceso, reglas de uso aceptable e inaceptable de la información, requerimientos en gestión de incidentes, resolución de conflictos, informes periódicos por parte del proveedor, auditorías al servicio y gestión de cambios.
	A.15.1.3 Cadena de suministro de tecnología de información y comunicación.	SI	RN/BP	Este procedimiento debe indicar como la entidad establece, acuerda, aprueba y divulga los requerimientos y obligaciones relacionados con la seguridad de la información con la cadena de suministro de tecnología de información y comunicación que estos tengan. Dichos acuerdos deben tener características como: Aspectos legales, descripción de la información a la que ambas partes tendrán acceso, reglas de uso aceptable e inaceptable de la información, requerimientos en gestión de incidentes, resolución de conflictos, informes periódicos por parte del proveedor, auditorías al servicio y gestión de cambios.

Fuente: Elaboración realizada por el autor del proyecto apoyado en la norma ISO/IEC 27001:2013 en su Anexo A

Tabla 15. (Continuación)

Objetivos de Control	Controles ISO 27001:2013	Aplicabilidad	Razones para la selección de controles	Justificación
A.15.2 Gestión de la prestación de servicios con los proveedores	A.15.2.1 Seguimiento y revisión de los servicios de los proveedores.	SI	RN/BP	Este procedimiento lo debe realizar la entidad bajo unos controles establecidos donde hace seguimiento, revisión y auditoria con regularidad, con el fin de que la prestación de servicios de los proveedores sea asegurada y minimizar riesgos de seguridad de la información.
	A.15.2.2 Gestión de cambios en los servicios de proveedores.	SI	RN/BP	Cualquier cambio o modificación en los servicios por terceras partes, deberá estar debidamente sustentado y autorizado por la entidad, siguiendo las políticas internas de la misma, teniendo como referencia lo establecido en los objetivos 12.1.2 Gestión de cambios y 14.2.2 Procedimientos de control de cambios en los sistemas.
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN				
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información	A.16.1.1 Responsabilidad y Procedimientos.	SI	RN/BP	De acuerdo con las políticas de seguridad de la información todos los funcionarios, terceros y contratistas que tengan acceso a los activos de información de la entidad deben adoptar roles y responsabilidades asociados a los procedimientos de gestión. Con el fin de asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
	A.16.1.2 Reporte de eventos de seguridad de la información.	SI	RN/BP	Los funcionarios, contratistas o terceros deben reportar los eventos de seguridad de la información que afecte alguno de los 3 servicios fundamentales de la información: Disponibilidad, Integridad o confidencialidad. Se debe informar a través de los canales de gestión apropiados, tan pronto como sea posible.
	A.16.1.3 Reporte de debilidades de seguridad de la información.	SI	RN/BP	La entidad debe exigir a todos los funcionarios y contratistas que usan los servicios y sistemas de información de la entidad, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios. Con el fin de mitigar los riesgos de seguridad de la información que afectan los objetivos institucionales.

Fuente: Elaboración realizada por el autor del proyecto apoyado en la norma ISO/IEC 27001:2013 en su Anexo A

Tabla 15. (Continuación)

Objetivos de Control	Controles ISO 27001:2013	Aplicabilidad	Razones para la selección de controles	Justificación
	A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	SI	RN/BP	La entidad a través del área de sistemas deberá definir los lineamientos para la evaluación de eventos de seguridad de la información y la decisión tomada sobre los mismos, los eventos de seguridad de la información se deben evaluar y decidir si se van a clasificar como incidentes de seguridad de la información.
	A.16.1.5 Respuesta a incidentes de seguridad de la información.	SI	RN/BP	La entidad a través del área de sistemas deberá dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos, lineamientos documentados y establecidos por la entidad.
	A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información.	SI	RN/BP	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o e impacto de incidentes futuros.
	A.16.1.7 Recolección de evidencia.	SI	RN/BP	La entidad a través del área de sistemas deberá definir y aplicar los procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A. 17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO				
A.17.1 Continuidad de seguridad de la información	A.17.1.1 Planificación de la continuidad de la seguridad de la información.	SI	RN/BP	La entidad debería determinar los requisitos para la Seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre.
	A.17.1.2 Implementación de la continuidad de la seguridad de la información.	SI	RN/BP	La entidad debería establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el mantenimiento del nivel de continuidad necesario para la seguridad de la información durante situaciones adversas.
	A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	SI	RN/BP	La entidad deberá verificar periódicamente los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas. Estos controles están delimitados en el plan de continuidad del Negocio de la entidad.
A.17.2 Redundancias	A.17.2.1 Disponibilidad de instalaciones de procesamiento de información.	SI	RN/BP	La entidad tendrá asegurada la existencia de una plataforma tecnológica redundante que cumpla y satisfaga los requerimientos de disponibilidad aceptables para cumplir los requisitos de la misma.

Fuente: Elaboración realizada por el autor del proyecto apoyado en la norma ISO/IEC 27001:2013 en su Anexo A

Tabla 15. (Continuación)

Objetivos de Control	Controles ISO 27001:2013	Aplicabilidad	Razones para la selección de controles	Justificación
A. 18 CUMPLIMIENTO				
A.18.1 Cumplimiento de requisitos legales y contractuales	A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales.	SI	LR	La Entidad está obligada a cumplir la normatividad vigente que rige para la seguridad y privacidad de la información, en consecuencia, todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de esta, se debe identificar la legislación aplicable y documentarla explícitamente. Con el fin de mantenerlos actualizados para cada sistema de información.
	A.18.1.2 Derechos de propiedad intelectual.	SI	LR	La entidad como principio de seguridad deberá implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. Cualquier cambio que afecte los activos de software (actualización, instalación o desinstalación), debe ser solicitado por los funcionarios o contratistas al área de sistemas, quienes por roles y responsabilidades son los únicos autorizados para ejecutar los mismos.
	A.18.1.3 Protección de registros.	SI	LR	La entidad como principio de seguridad y como obligación de estricto cumplimiento deberá proteger los registros contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y objetivos institucionales.
	A.18.1.4 Privacidad y protección de datos personales.	SI	LR	Todos los funcionarios y contratistas se deben ajustar a la normatividad vigente, deberán firmar una cláusula de confidencialidad, con la cual se hace responsable de la privacidad y protección de datos personales. que genere durante sus labores en la entidad, así mismo, se hará responsable de cualquier daño o perjuicio causado derivado del incumplimiento doloso o culposo de dicha obligación. Con el fin de asegurar cuando sea aplicable la privacidad y la protección de la información de datos personales, como exige la ley y las reglamentaciones pertinentes.

Fuente: Elaboración realizada por el autor del proyecto apoyado en la norma ISO/IEC 27001:2013 en su Anexo A

Tabla 15. (Continuación)

Objetivos de Control	Controles ISO 27001:2013	Aplicabilidad	Razones para la selección de controles	Justificación
	A.18.1.5 Reglamentación de controles criptográficos.	SI	LR	La entidad como principio de seguridad deberá implementar, gestionar y usar controles criptográficos, en cumplimiento de todos los acuerdos y la legislación vigente. Por ejemplo: • Firmas Digitales. • Uso de Token de seguridad en el área Financiera. • Herramientas de software para cifrar la información de los correos electrónicos. • Cifrar para las transacciones web críticas. • El cifrado que se encuentran en las conexiones externas de la entidad.
A.18.2 Revisiones de seguridad de la información	A.18.2.1 Revisión independiente de la seguridad de la información	SI	RN/BP	Se debería analizar y revisar independientemente todo el enfoque de la entidad para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) esto se debe realizar a intervalos planificados o cuando ocurran cambios significativos.
	A.18.2.2 Cumplimiento con las políticas y normas de seguridad.	SI	LR	La entidad a través de la alta gerencia y los responsables de la seguridad de la información deberían revisar con frecuencia el cumplimiento de los procesos, políticas y normas de seguridad de información de cada área de responsabilidad de la entidad, y cualquier otro requisito de seguridad establecido que cumpla con la normatividad vigente.
	A.18.2.3 Revisión del cumplimiento técnico.	SI	RN/BP	La entidad a través de la alta gerencia y los responsables de la seguridad de la información deberá revisar Los sistemas de información periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información. Las verificaciones, supervisiones, y auditoria de cumplimiento técnico sólo serán realizadas por personal autorizado que cumple con el rol y la responsabilidad.

Fuente: Elaboración realizada por el autor del proyecto apoyado en la norma ISO/IEC 27001:2013 en su Anexo A

11. POLITICAS DE SEGURIDAD DE LA INFORMACION PARA ENTIDADES DEL ESTADO

Para las entidades del estado es importante establecer y determinar las políticas de seguridad con que se cuenta, ya que son estas quienes guiaran el comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la misma, así mismo las políticas permitirán que se trabaje bajo las mejores prácticas y lineamientos de seguridad de la información y cumpla con los requisitos legales vigentes a los cuales esté obligada a cumplir la entidad.

11.1 OBJETIVO DE LAS POLITICAS DE SEGURIDAD

Establecer las políticas que regulan la seguridad de la información en la entidad y presentar en forma clara y coherente los elementos que conforman la política de seguridad que deben conocer, acatar y cumplir todos los funcionarios, contratistas, personal en comisión administrativa, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la misma, bajo el liderazgo del Área de Tecnologías y Sistemas de Información.

11.2 ALCANCE

Las políticas de seguridad de la información cubren todos los aspectos que deben ser acatados por directivos, funcionarios, contratistas y terceros que laboren o tengan relación con la entidad, en busca de mantener la confidencialidad, integridad y disponibilidad de la información.

11.3 POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

En este documento se presentan algunas recomendaciones en términos generales de políticas de seguridad de la información para la protección y privacidad de la Información para las entidades del estado que deseen adoptar esta guía como modelo de implementación. Este conjunto de recomendaciones no es exhaustivo, se aconseja que cada Entidad genere sus documentaciones propias dependiendo de sus características particulares, sus activos de información, sus procesos y los servicios de información que pueda prestar. A continuación, se agruparán las políticas con el objetivo de hacer una implementación transversal de Seguridad de la Información en la Entidad.

11.3.1 Política de estructura organizacional de seguridad digital. La entidad con el fin de cumplir con el compromiso y los estándares del sistema de gestión de seguridad de la información determina unos parámetros de seguridad, definiendo y estableciendo roles y responsabilidades que involucran las actividades de gestión, operación y administración de la seguridad de la información, así como la creación del comité y el administrador de seguridad de la información.

El área de tecnologías y sistemas de información será la encargada de establecer los roles, funciones y responsabilidades de operación y administración de los sistemas de información de la entidad, estas directrices, deberán estar debidamente documentadas y distribuidas.

11.3.2 Política para uso de dispositivos móviles. La entidad con el fin de garantizar la confidencialidad de la información institucional establece los parámetros de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes, tabletas), entre otros, suministrados por la entidad y personales que hagan uso de los servicios de información de esta.

La entidad debe contar con routers avanzados, firewall y otros equipos complementarios de seguridad perimetral para la configuración y respectivo bloqueo de aplicaciones no autorizadas. A excepción de los funcionarios que tengan privilegios altos se autoriza el uso de mensajería instantánea como WhatsApp únicamente en dispositivos suministrados por la entidad, está prohibido por esta aplicación, el envío de fotografías, audios, y videos y cualquier otro tipo de archivo clasificados como información pública reservada o información pública clasificada (privada o semiprivada).

Los funcionarios y contratistas no están autorizados a cambiar la configuración, a desinstalar software, formatear o restaurar de fábrica los equipos móviles institucionales, cuando se encuentran a su cargo, únicamente se deben aceptar y aplicar las actualizaciones.

11.3.3 Política de seguridad del personal. La entidad reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales y, con el interés de contar con el personal mejor calificado, garantiza que la vinculación de nuevos funcionarios se realiza siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual está orientado a las funciones y roles que deben desempeñar los funcionarios en sus cargos. Con el fin de proteger la información y garantizar que los acuerdos y/o cláusulas de confidencialidad y aceptación de políticas de seguridad de la información se cumplan.

11.3.4 Política aplicable durante la ejecución del empleo. La entidad a través de la alta directiva en su interés de proteger la información, establece y fomenta la cultura de seguridad digital y la gestión de riesgos durante el desarrollo de las actividades de los funcionarios y contratistas, realizando periódicamente jornadas de capacitación, sensibilización y divulgación de la presente política.

Todos los funcionarios y contratistas deben procurar no divulgar información confidencial en lugares públicos, que pongan en riesgo la seguridad de la información y la reputación de la Entidad.

11.3.5 Política de gestión de activos de Información. La entidad como propietario de la información física y digital generada, procesada, almacenada y transmitida con su plataforma tecnológica, establecerá responsabilidad a las áreas o dependencias sobre sus activos de información, verificando el cumplimiento de los parámetros que regulan el uso adecuado de la misma.

Los activos de información, físicos, digitales, los servicios y los equipos (ej. equipos portátiles, estaciones de trabajo, impresoras, redes de comunicaciones, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos, entre otros) son activos de propiedad de la entidad y se proporcionan a los funcionarios, contratistas y terceros autorizados, para cumplir con la misión y objetivos institucionales.

Toda la información sensible de la entidad, así como los activos donde ésta se almacena y se procesa, deben ser asignados a un responsable, inventariados y clasificados, de acuerdo con los requisitos y los criterios que defina el área de tecnologías y sistemas de información. Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

11.3.6 Política de uso de los activos. La Entidad, como principio de seguridad implementa los lineamientos para lograr y mantener la protección adecuada y uso de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo con sus roles, funciones y responsabilidades.

Los usuarios no están autorizados para mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música, y fotos de cualquier tipo de archivo que no sean de carácter institucional.

11.3.7 Política de clasificación y manejo de la información. La entidad, definirá los procedimientos más adecuados para clasificar su información de acuerdo con su sensibilidad, y proporcionará un formato de clasificación de la información para

que los propietarios de la misma la cataloguen y determinen los controles requeridos para su protección.

Toda la información de la entidad debe ser identificada, clasificada y documentada de acuerdo con el formato de clasificación establecido por la misma, una vez clasificada la información, la entidad proporcionará los recursos necesarios para la aplicación de controles en busca de preservar la confidencialidad, integridad y disponibilidad de esta, con el fin de promover el uso adecuado por parte de los funcionarios y contratistas que requieran de ella para la ejecución de sus actividades.

11.3.8 Política de uso de periféricos y medios de almacenamiento. La entidad en busca de garantizar el uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica de la misma establece los mecanismos y lineamientos conjuntamente con el área de tecnologías y sistemas de información, considerando las labores realizadas por los funcionarios y su necesidad de uso. Con el fin de evitar la divulgación y modificación no autorizada de información almacenada en los medios proporcionados por la entidad.

11.3.9 Políticas de control de acceso. La entidad en busca de garantizar un adecuado control de acceso a sus activos de información definirá las políticas para respaldar un apropiado control de acceso a los sistemas, para ello se implementan procedimientos de control para acceder a la red, sistemas operativos, bases de datos, sistemas de información y en general a todo elemento que de alguna forma acceda a información de carácter público reservado o publico clasificado, cuyo origen sea de la entidad. De igual manera, implementa procedimientos para la asignación de privilegios de acceso a los sistemas.

El acceso a los sistemas de información está establecido por el principio de mínimo privilegio necesario para el cumplimiento de las labores asignadas a funcionarios, contratistas y terceros. El acceso a la información contempla el establecimiento de permisos específicos para leer, escribir, modificar, borrar o ejecutar utilidades que procesen información institucional.

11.3.10 Política de acceso a redes y recursos de red. El área de tecnologías y sistemas de información de la entidad, como responsable de las redes de datos y los recursos de red, proporciona los recursos para que dichas redes sean debidamente aseguradas contra accesos no autorizados a través de mecanismos de control de acceso lógico y físicos monitoreados y con capacidad de generar alertas.

11.3.11 Política de administración de acceso de usuarios. La entidad establecerá y determinará privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información. De este modo, brindará las garantías para que los funcionarios, contratistas y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

11.3.12 Política de responsabilidades de acceso de los usuarios. Los usuarios de los recursos tecnológicos y los sistemas de información de la entidad realizan un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

11.3.13 Política de teletrabajo. La entidad garantizará la seguridad de la información cuando se haga uso de los recursos tecnológicos y activos de información, autorizadas por la misma, el desarrollo de las actividades de teletrabajo será realizadas según lo contemplado en el artículo 2 de la Ley 1221 de 2008.

La entidad realiza un análisis de riesgos que permite identificar, proteger y proporcionar los mecanismos de control adecuados para la protección de sus activos de información cuando se autorizan actividades de Teletrabajo. Antes de realizar cualquier actividad de este tipo, la entidad define con los Líderes del proceso el alcance de las actividades a desarrollar, estableciendo como mínimo, el horario, los activos de información a acceder, los sistemas de información y los servicios requeridos para el desarrollo de las actividades de teletrabajo.

11.3.14 Política de controles criptográficos. La entidad proporcionara los recursos necesarios para que la información de la entidad, calificada como clasificada y reservada, sea cifrada al momento de transferirse y/o transmitirse por cualquier medio. La entidad establece e implementa procedimientos para salvaguardar activos de información clasificada, reforzando la confidencialidad, disponibilidad e integridad, mediante el uso de herramientas criptográficas.

11.3.15 Política de seguridad física y medioambiental. La entidad proporcionara la implementación y garantizará la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus sedes. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas. Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así

como aquellas en las que se encuentren equipos de cómputo e infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

11.3.16 Política de seguridad para los equipos institucionales. Con el fin de evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la entidad que se encuentren dentro o fuera de sus instalaciones, se proporcionaran los mecanismos necesarios que garanticen la seguridad para mitigar los riesgos sobre la plataforma tecnológica.

11.3.17 Política de soporte y mantenimiento a equipos de infraestructura critica (U.P.S., Firewall). La entidad establecerá los procedimientos y proveerá los recursos que garantizan el soporte y mantenimiento de hardware crítico, y que deberá desarrollarse siguiendo las normas y estándares para este fin, permitiendo la seguridad del recurso tecnológico. De la misma manera, deberá asegurar el servicio, la protección de la información y de los equipos.

11.3.18 Políticas de seguridad en las operaciones. La entidad, garantizará la protección de operaciones y el procesamiento de la información, esto incluye la instalación de software en sistemas operativos, gestión de vulnerabilidades técnicas, restricción sobre la instalación de software, protección de la información de registro, registro del administrador y operadores, sincronización de relojes, gestión de capacidad, gestión de cambios, controles contra código malicioso, respaldo de la información, registro de eventos, y controles de auditorías de sistemas de información.

La seguridad en las operaciones en la entidad se debe encontrar documentada y con las responsabilidades asignadas.

11.3.19 Política de escritorio y pantalla limpia. Determinar los parámetros generales para minimizar y reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los usuarios. Los funcionarios, contratistas y terceros que tienen algún vínculo con la entidad deben conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

Los usuarios de los sistemas de información y comunicaciones de la entidad deben cerrar las aplicaciones y servicios de red cuando ya no los necesite.

Los usuarios de los sistemas de información y comunicaciones de la entidad deben bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.

Al imprimir documentos con información pública reservada y/o pública clasificada (semiprivada o privada), deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

11.3.20 Política de protección frente a software malicioso. La entidad proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por software malicioso. Además, establecerá los mecanismos para generar una cultura de seguridad entre sus funcionarios, contratistas y terceros frente a los ataques de software malicioso.

11.3.21 Políticas de copias de respaldo de la información. La entidad certificará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos para la realización de estas actividades. Las áreas propietarias de la información, con el apoyo del área de tecnologías y sistemas de información, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

Así mismo, se garantizará que los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El lugar externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

11.3.22 Política de registro de eventos y monitoreo de los recursos tecnológicos y los sistemas de información. La entidad realiza revisión constante del uso que dan los funcionarios, contratistas y terceros a los recursos de la plataforma tecnológica y los sistemas de información de esta. Además, responde por la custodia de los registros de auditoria cumpliendo con los períodos de retención establecidos para dichos registros.

La supervisión genera una definición de los registros de auditoria sobre los aplicativos donde se opera los procesos misionales de la entidad y análisis de los logs de auditoria para establecer posibles anomalías.

Los logs de los eventos generados por los componentes informáticos capturan y retiene con base en criticidad de los sistemas y el valor de los datos, aspecto relevante para la revisión periódica en beneficio de identificar posibles anomalías, generar alertas tempranas conducentes a reconstruir operaciones sensibles y tomar acciones en lo pertinente a la gestión de riesgos en la entidad.

11.3.23 Política de control al software operativo. La entidad, a través del área de tecnología y sistemas de información, designará responsables y establecerá procedimientos para controlar la instalación de software operativo, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo es actualizado.

11.3.24 Política de gestión de vulnerabilidades. La entidad, a través del área de tecnología y sistemas de información, revisa la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de pruebas periódicas de vulnerabilidades, con el fin de realizar la corrección sobre los hallazgos arrojados por dichas pruebas, de acuerdo con los criterios establecidos.

11.3.25 Políticas de seguridad en las comunicaciones. Con el fin de evitar accesos no autorizados, la entidad proporciona los lineamientos para soportar, gestionar y controlar las redes y los servicios de comunicaciones. La información transmitida o transferida mediante redes públicas se salvaguarda a través de controles para prevenir la pérdida de confidencialidad, integridad y la pérdida de disponibilidad de estos. La conexión de equipo o estaciones de trabajo a las redes de la entidad será controlada y supervisada para asegurar la información.

11.3.26 Política de gestión y aseguramiento de las redes de datos. La entidad establece los mecanismos de control necesarios para proporcionar la disponibilidad de las redes de datos y de los servicios que dependen de ellas, así mismo, garantiza por que se establezcan los mecanismos de seguridad que aseguren la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos. De igual manera, se inclina por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información clasificada y reservada de la entidad.

11.3.27 Política de uso del correo electrónico. La entidad, teniendo en cuenta la importancia del correo electrónico como herramienta para facilitar la comunicación entre funcionarios, contratistas y terceros, proporciona un servicio adecuado y seguro para la ejecución de las actividades laborales que requieran el

uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad, autenticidad y privacidad de quienes realizan las comunicaciones a través de este medio.

11.3.28 Política de uso adecuado del internet. La entidad consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporciona los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad.

11.3.29 Política de intercambio de información. La entidad con el fin de salvaguardar la protección de la información transferida o transmitida con entidades externas y procesos internos establece los procedimientos y controles implementados para el intercambio de datos. Se cuenta con acuerdos de confidencialidad con terceros con quienes interactúen con la información.

La información recibida de terceras partes se conserva por un período de tiempo equivalente al de retención de las bases de datos con información personal sobre las cuales se efectúen actualizaciones, cambios, supresiones con la información fuente, o el tiempo establecido por los requisitos legales aplicables a la entidad.

11.3.30 Políticas de adquisición, desarrollo y mantenimiento de sistemas de información. La adquisición, desarrollo y mantenimiento de sistemas de información comprende procedimientos y lineamientos de buenas prácticas de seguridad durante todo el ciclo de vida, los requisitos relacionados con la seguridad de la información son incorporados a los sistemas de información tanto nuevos como ya existentes. Los servicios asociados a transacciones electrónicas se protegen para evitar transmisión incompleta, alteración o divulgación no autorizada.

11.3.31 Política para el establecimiento de requisitos de seguridad. La entidad asegura que el software adquirido y desarrollado tanto al interior de la entidad, como por terceras partes, cumpla con los requisitos de seguridad y calidad establecidos. Las áreas propietarias de sistemas de información, el área de tecnología y sistemas de información incluyen requisitos de seguridad en la definición de requerimientos y, posteriormente se aseguran de que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido. Todos los sistemas de información o desarrollos de software deben tener un área propietaria dentro de la entidad formalmente asignada.

11.3.32 Política de desarrollo seguro, realización de pruebas y soporte de los sistemas. La entidad, garantizará porque el desarrollo interno o externo de los sistemas de información cumpla con los requisitos de seguridad establecida, basado en buenas prácticas para el desarrollo seguro de software, así como con lineamientos para la realización de pruebas de aceptación y seguridad. Se proporcionarán los mecanismos para asegurar que todo el software desarrollado o adquirido, interna o externamente cuente con el nivel de soporte requerido.

11.3.33 Política para la protección de los datos de prueba. La entidad protege los datos de prueba que se entregan a los desarrolladores, asegurando que no revelan información calificada como clasificada y reservada de los ambientes de producción.

11.3.34 Políticas de relación con proveedores. La entidad, proporciona los mecanismos de control en sus relaciones con proveedores, con el objetivo de asegurar que la información a la que tengan acceso cumpla con las políticas, normas y procedimientos de seguridad de la información.

11.3.35 Política de gestión de la prestación de servicios con proveedores. La entidad, garantiza por mantener los niveles acordados de seguridad de la información y de prestación de los servicios de los proveedores, en concordancia con los acuerdos establecidos con éstos. Así mismo, propende por la adecuada gestión de cambios en la prestación de servicios de dichos proveedores.

11.3.36 Política de gestión de incidentes de seguridad. La entidad, asegura la gestión de incidentes de seguridad de la información incluyendo la comunicación interna y autoridades competentes de ser necesarias. Se tienen definidas las responsabilidades a través de procedimientos de gestión de incidentes para asegurar una respuesta eficaz y oportuna.

11.3.37 Política para el reporte y tratamiento de incidentes de seguridad. La entidad promueve entre los funcionarios, contratistas y terceros el reporte de incidentes de seguridad de la información en sus medios de procesamiento, medio de almacenamiento, la plataforma tecnológica, los sistemas de información y las personas.

De igual manera, asigna responsables para el tratamiento de los incidentes de seguridad de la información, quienes tienen la responsabilidad de aislar, investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

La Entidad a través de los responsables de la seguridad de la información o la alta directiva, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades, así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

11.3.38 Política de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad digital. La entidad responde ante eventos de contingencia, y proporciona los recursos suficientes para dar una respuesta efectiva y así continuar la operación de procesos críticos, preservando los niveles de seguridad equivalente a los proporcionados en situación normal. La entidad mantiene canales de comunicación adecuados hacia funcionarios y contratistas ante un incidente de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad de la información.

11.3.39 Política de recuperación frente a desastres DRP (*Disaster Recovery Plan*). La entidad establece un conjunto de mecanismos activando planes de contingencia, y proporciona los recursos para dar una respuesta oportuna y efectiva de los servicios y procesos informáticos críticos, tanto como misionales como administrativos de la entidad frente un desastre, minimizando el impacto de este.

11.3.40 Política de redundancia. La entidad, proporciona los mecanismos necesarios por la existencia de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para la misma.

11.3.41 Políticas de cumplimiento. La entidad, velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

11.3.42 Política de cumplimiento de derecho de propiedad intelectual y uso de software patentado. La entidad como principio de seguridad procura porque el software instalado y en uso en los recursos de la plataforma tecnológica de la entidad cumpla con los requerimientos legales y de licenciamiento aplicables. En el procedimiento de Inventario de software y hardware y control de software legal se cumple con los requisitos legislativos relacionados con los derechos de propiedad intelectual y uso de software patentados.

11.3.43 Política de privacidad y protección de datos personales. Con el fin de dar estricto cumplimiento de la Ley 1581 de 2012, la entidad propende por la protección de los datos personales de sus funcionarios, contratistas y terceros de los cuales reciba y administre información. Se adoptan las medidas administrativas, técnicas y de procesos para salvaguardar la privacidad y proteger los datos durante la captura, almacenamiento y procesamiento en las operaciones. Se establecen los procedimientos y lineamientos de protección de datos personales de acuerdo con los parámetros de ley.

11.3.44 Política de cumplimiento de ley de transparencia. La entidad garantiza el derecho de acceso a la información pública a través de los canales habilitados por la entidad excluyendo solo aquella que está sujeta a las excepciones constitucionales, legales y bajo el cumplimiento de los requisitos establecidos en Ley 1712 de Transparencia.

11.3.45 Política de servicios de computación en la nube. La entidad propende por mantener la seguridad de los activos de información de esta, cuando se autoriza el uso de servicios de computación en la nube a fin de garantizar la disponibilidad, privacidad, confidencialidad, integridad y cumplimiento de los requisitos legales en materia de protección de información personal. Esta política se aplica a los servicios de computación en nube que sean utilizados o contratados por la entidad, así como a los procesos que hagan uso de dichos servicios.

12. DIVULGACION

La divulgación del presente proyecto se realizará posterior a su publicación por los medios autorizados y dispuestos por La Universidad Nacional Abierta y a Distancia (UNAD), con la finalidad de presentar el desarrollo final a las partes interesadas y a las entidades que deseen adoptarlas como guía o modelo de implementación.

En la actualidad La Universidad Nacional Abierta y a Distancia (UNAD) cuenta con un sitio web, repositorios, E-portafolio, UNAD Social, Bibliotecas, Radio UNAD Virtual, los cuales son plataformas tecnológicas que pueden ser utilizados para dicha divulgación.

CONCLUSIONES

Se realiza la identificación de activos de información apoyado con el dominio 8 gestión de activos del anexo A de la norma ISO27001:2013, lo cual permitió identificar en términos generales los posibles activos informáticos para entidades del estado, de cómo deben ser utilizados, los roles y responsabilidades que tienen los funcionarios sobre los mismos, y reconociendo el nivel de clasificación de la información que a cada activo debe dársele. Esta fase del proyecto comprende las etapas para el registro de los activos de información, inicia con la identificación, clasificación y valoración, y termina con la publicación del inventario de activos de la entidad.

Se determinaron los riesgos, amenazas y vulnerabilidades comunes que afectan a la entidad, está fase de identificación se logró a partir del inventario de activos que posee la misma, lo cual permitió evidenciar cuales son los factores que ponen en peligro la integridad, confidencialidad y disponibilidad de la información en una organización, se establece como se deben utilizar y cuáles son los mecanismos para mitigarlos.

La aplicación de la metodología basada en la guía para la administración del riesgo, emitida por el departamento administrativo de la función pública “DAFP”, que proporciona los lineamientos para la gestión del riesgo de seguridad de la información en entidades públicas, permitió analizar, evaluar y gestionar los posibles riesgos asociados a la seguridad de la información para entidades del estado, basados en los criterios de confidencialidad, integridad y disponibilidad. Adicionalmente evidenció los posibles activos críticos de la misma, el impacto que puede generar y proporcionó las medidas oportunas para mantener y minimizar los riesgos bajo control.

Se realiza la verificación de controles de seguridad de la información en la entidad, posterior de realizar el análisis y evaluación de riesgos, se tuvo en cuenta los objetivos de control y controles de referencia, basados en la norma ISO/IEC 27001:2013 en su Anexo A, como un insumo base para mitigar los riesgos de seguridad de la información, lo cual permitió evidenciar en términos generales cuales son los controles efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo.

Se definieron directrices para la construcción de las políticas de seguridad de la información en términos generales para la entidad, lo que permite que se trabaje bajo las mejores prácticas y lineamientos de seguridad de la información y proporcione todos los mecanismos y aspectos que deben ser acatados por directivos, funcionarios, contratistas y terceros que laboren o tengan relación con la entidad, en busca de mantener la confidencialidad, integridad y disponibilidad de la información.

RECOMENDACIONES

Como autor del proyecto, El primer elemento que se debe considerar es el respaldo de la alta dirección con respecto a las actividades de seguridad de la información. Un sistema de gestión de la información sólo será eficaz y eficiente con el apoyo pleno y activo de la alta gerencia.

Se recomienda capacitación y concienciación, ya que es uno de los principales motivos de fracaso de los proyectos de Seguridad de la Información en las organizaciones.

La implementación del Sistema de Gestión de Seguridad de la Información no es un paso más, sino que se debe realizar un mantenimiento de forma permanente, revisión y actualización para así conseguir que sea efectivo.

Para mayor soporte y complemento a este proyecto, se recomienda revisar los lineamientos y procedimientos del Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).

BIBLIOGRAFIA

CONGRESO DE COLOMBIA. Código Penal De Colombia Ley 599 de 2000. [En línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388> [citado en 12 de abril de 2017]

--------. Código Procedimiento Penal De Colombia Ley 906 de 2009. [En línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=14787> [citado en 19 de mayo de 2017]

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA (DAFP), Anexo 4 Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas. [En línea]. <http://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba> [citado en 15 de marzo de 2019]

--------. Guía para la administración del riesgo. [En línea]. <http://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba> [citado en 15 de marzo de 2019]

ISO/IEC 27002:2013, *Information Technology. Security Techniques. Code of Practice for Information Security Controls.*

GTC-ISO/IEC 27003:2012, Tecnología de la información. Técnicas de seguridad. Guía de implementación de un sistema de gestión de la seguridad de la información.

ISO/IEC 27004:2009, *Information Technology. Security Techniques. Information Security Management. Measurement.*

ISO/IEC 27005:2011, *Information Technology. Security Techniques. Information Security Risk Management.*

ISO/IEC 27000, *Information Technology. Security Techniques. Information Security Management Systems. Overview and Vocabulary.*

ISO2700.es, ¿Qué es un SGSI? [En línea]. <http://www.iso27000.es/sgsi.html> [citado en 15 de Octubre de 2017]

--------. Sistema de Gestión de la Seguridad de la Información. [En línea]. <http://www.iso27000.es/doc_sgsi_all.htm> [citado en 15 de Octubre de 2017]

ISO 27001, La Seguridad de la Información en la Gestión de la Continuidad de Negocio. [en línea]. <http://www.pmg-ssi.com/2014/11/iso-27001-la-seguridad-de-la-informacion-en-la-gestion-de-la-continuidad-de-negocio/> [citado en 15 de Septiembre de 2017]

ICONTEC. Compendio tesis y otros trabajos de grado. Quinta Actualización. Instituto Colombiano de Normas Técnicas y Certificación – ICONTEC, Bogotá D.C., Colombia, 2006.

--------.Norma técnica NTC-ISO/IEC colombiana 27001. [En línea]. <http://www.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf> [citado en 10 de Octubre de 2017]

MINTIC, Ciberseguridad. [En línea]. <https://www.mintic.gov.co/portal/604/w3-article-6120.html> [citado en 28 de septiembre de 2017]

--------. Controles de Seguridad y Privacidad de la Información. [En línea]. <https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf> [citado en 28 de septiembre de 2017]

--------.Guía de gestión de riesgos. [En línea]. <https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf> [citado en 28 de septiembre de 2017]

--------. Guía para la gestión y clasificación de activos de información. [En línea]. <https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf> [citado en 26 de agosto de 2017]

--------. Modelo de Seguridad y Privacidad de la Información. [En línea]. <https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf> [citado en 28 de septiembre de 2017]

NTC-ISO 31000:2011, Gestión del riesgo. Principios y directrices.

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

NTC-ISO/IEC 27005, Tecnología de la información. Código de práctica para la gestión de la seguridad de la información.

ANEXOS

Anexo A. Formato de Identificación y Clasificación de Activos

Espacio para el Logo de la Entidad	NOMBRE DE LA ENTIDAD FORMATO INVENTARIO DE ACTIVOS DE INFORMACIÓN Y CLASIFICACIÓN DE ACTIVOS BASADO EN LA NORMA ISO 27001:2013 PARA UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Versión. 1.0 Fecha de Creación:

IDENTIFICACION DE ACTIVOS DE INFORMACIÓN								CLASIFICACION DE ACTIVOS			VALORACION DEL ACTIVO
								CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	
ID Activo	Nombre del Activo	Proceso	Descripción	Tipo	Ubicación	Propietario	Custodio	Nivel	Nivel	Nivel	Criticidad

Elaborado por:	**Aprobado por:**
Cargo:	**Cargo:**
Lugar y fecha:	**Lugar y fecha:**

Anexo B. Formato Análisis y Evaluación de Riesgos

Espacio para el Logo de la Entidad	NOMBRE DE LA ENTIDAD FORMATO ANÁLISIS Y EVALUACIÓN DEL RIESGO PARA UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA METODOLOGIA DE LA GUIA PARA LA ADMINISTRACIÓN DEL RIESGO “DAFP”	Versión. 1.0 Fecha de Creación:

Análisis y Evaluación del Riesgo

Proceso:

Objetivo:

Tipo de Activo	Riesgo	Causa	Calificación		Tipo de Impacto	Evaluación Zona de Riesgo	Medidas de Respuesta
			Probabilidad	Impacto			

Elaborado por:	**Aprobado por:**
Cargo:	**Cargo:**
Lugar y fecha:	**Lugar y fecha:**

Anexo C. Formato Declaración de Aplicabilidad

Espacio para el Logo de la Entidad	NOMBRE DE LA ENTIDAD FORMATO DECLARACION DE APLICABILIDAD PARA UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013	Versión. 1.0 Fecha de Creación:

Objetivos de Control	**Controles ISO 27001:2013**	**Aplicabilidad**	**Razones para la selección de controles**	**Justificación**
Elaborado por:			**Aprobado por:**	
Cargo:			**Cargo:**	
Lugar y fecha:			**Lugar y fecha:**	

Anexo D. Resumen Analítico Especializado - RAE

RESUMEN ANALÍTICO ESPECIALIZADO - RAE

1. Información General	
Título:	DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO/IEC 27001 PARA ENTIDADES DEL ESTADO
Autor:	JUAN CARLOS DE LEON CAMELO
Director:	Esp. DANIEL FELIPE PALOMO LUNA
Fuentes bibliográficas:	En el proyecto aplicado se referencia 22 fuentes bibliográficas, algunas que mencionan la temática principal son: DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA (DAFP), Anexo 4 Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas. [En línea]. <http://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a1 59-2d8f-41aa-8182-eb99e8c4f3ba> [citado en 15 de marzo de 2019] GTC-ISO/IEC 27003:2012, Tecnología de la información. Técnicas de seguridad. Guía de implementación de un sistema de gestión de la seguridad de la información. ISO2700.es, Sistema de Gestión de la Seguridad de la Información. [En línea]. <http://www.iso27000.es/doc_sgsi_all.htm> [citado en 15 de Octubre de 2017] MINTIC, Modelo de Seguridad y Privacidad de la Información. [En línea]. <https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf> [citado en 28 de septiembre de 2017] NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos
Año:	2019
Resumen:	El presente documento se basó en la realización y diseño de una guía de buenas prácticas y procedimientos sistémicos, que consisten en minimizar los riesgos y salvaguardar la protección de la información, específicamente en organizaciones y entidades del estado, con la finalidad de preservar la confidencialidad, integridad y disponibilidad de la misma, a través de una herramienta de gestión relacionada con la seguridad y privacidad de los datos. Es por ello que surgió la necesidad de desarrollar un sistema de gestión de seguridad de la información (SGSI) tomando como referencia la metodología que define la norma ISO/IEC 27001. Con el fin de ponerlo a disposición de las entidades del gobierno y que sea utilizado como guía para definir sus políticas de seguridad de la información. De esta manera el presente documento busca proporcionar los lineamientos básicos y de forma general sobre cómo empezar a diseñar y dimensionar el alcance para realizar la implementación de un Sistema de Gestión de Seguridad de la Información en una organización del estado colombiano.
Palabras claves:	Activo, Amenaza, Confidencialidad, Controles, Declaración de Aplicabilidad Disponibilidad, Información, Integridad, Iso27001, Política, Privacidad, Riesgo, Seguridad, Vulnerabilidad.

Contenidos:	TITULO. DEFINICIÓN DEL PROBLEMA. PLANTEAMIENTO DEL PROBLEMA. FORMULACIÓN DEL PROBLEMA. JUSTIFICACIÓN. OBJETIVOS DEL PROYECTO. OBJETIVO GENERAL. OBJETIVOS ESPECÍFICOS. MARCO DE REFERENCIA. ANTECEDENTES. MARCO CONTEXTUAL. MARCO TEORICO. MARCO CONCEPTUAL. MARCO LEGAL. DISEÑO METODOLOGICO. METODOLOGIA DE DESARROLLO. Objetivo 1. Objetivo 2. Objetivo 3. Objetivo 4. Objetivo 5. CONCLUSIONES.

2. Problema de Investigación (Descripción)
En un mundo conectado y globalizado, como el existente en la actualidad, y con el creciente uso de las tecnologías de la información y las comunicaciones (TIC), la seguridad de la información se ha considerado un aspecto esencial en las organizaciones de cualquier tamaño y tipo, específicamente en entidades del gobierno. Lo anterior, se refiere a un aspecto que tiene que ver con la protección de los datos contra accesos no autorizados y para salvaguardarlos de una posible corrupción durante todo su ciclo de vida. Las entidades hoy en día dependen cada vez más de sus sistemas de información y de los datos que estos administran, es por ello por lo que la información se ha convertido en un activo nuevo y de gran valor, sin embargo, muchas entidades no la tienen asegurada, y algunas ni siquiera saben cuál es el valor de sus activos intangibles. Tendencias recientes han demostrado que los riesgos y amenazas están aumentando en frecuencia y en gravedad. Cada día las entidades están expuestas a todo tipo de ataques informáticos, accesos no autorizados, secuestro de información, vulnerabilidades, desastres naturales, siniestros y accidentes, etc. En su gran mayoría las entidades del gobierno no tienen delineadas sus políticas de seguridad de la información, esto conduce a resultados negativos en la protección de los datos y recursos de la Entidad, de esta manera incurren constantemente en fallas del servicio y comprometen los activos más críticos, la continuidad del negocio, el capital intelectual y la información confidencial de la organización. En términos generales, se ve afectada la seguridad de los datos en las entidades del gobierno, por lo tanto, no se puede asegurar la integridad, disponibilidad y confiabilidad, al no contar en su mayoría con herramientas de gestión o políticas de seguridad definidas para el manejo de protección de la información.

3. Objetivos
Objetivo General: Diseñar un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC 27001 que permita preservar la integridad, confidencialidad y disponibilidad de la información en las entidades del estado.

Objetivos Específicos:

- Identificar los activos informáticos comunes que se manejan en las entidades del estado para determinar los dominios del estándar que serán aplicados para el diseño del SGSI.

- Determinar los factores de amenaza, las vulnerabilidades y riesgos de seguridad informática y de la información que afectan a las entidades del estado.

- Aplicar la metodología de análisis y evaluación de riesgos para determinar el impacto de los riesgos detectados.

- Verificar la existencia de controles de seguridad informática y de la información de acuerdo a la norma ISO 27001:2013 en las entidades del estado

- Diseñar las Políticas de Seguridad de la información para las entidades del estado basado en la ISO 27001:2013.

4. Metodología

La metodología que se adoptó para el diseño del Sistema de Gestión de Seguridad de la Información para entidades del estado es el ciclo de mejora continua PHVA (planificar-hacer-verificar-actuar), alineado y apoyado en la Norma Técnica Colombiana NTC-ISO-IEC 27001:2013.

En la etapa de análisis y evaluación de riesgos se utilizó la metodología basada en la guía para la administración del riesgo, emitida por el departamento administrativo de la función pública "DAFP", que proporciona los lineamientos para la gestión del riesgo de seguridad de la información en entidades públicas.

5. Referentes Teóricos

De acuerdo con el tema de estudio, se presentan los principales referentes teóricos relacionados directamente con Sistemas de Gestión de la Seguridad de la Información: Activos de Información, Seguridad informática, Seguridad de la información, Sistema de gestión de seguridad de la información (SGSI), Norma ISO/IEC 27001, Ciclo PHVA.

6. Referentes Conceptuales

De acuerdo con el tema de estudio, se presentan los principales referentes conceptuales relacionados directamente con Sistemas de Gestión de la Seguridad de la Información:

Seguridad de la información. Se considera la disciplina que tiene como finalidad salvaguardar y proteger toda la información existente (físico, digital u otros), no importando en qué clase de medio se encuentre almacenada.

Amenaza. Hoy en día todas las organizaciones y sistemas informáticos están expuestos a imprevistos que puede ser de origen natural o intencionado, las amenazas consisten en una causa potencial de un suceso no deseado, por lo tanto tienen la capacidad de provocar daños y atentar contra la seguridad de la información.

Vulnerabilidad. En materia de protección de la información, consiste en una debilidad de cualquier tipo presente en un sistema informático el cual afecta y/o compromete la seguridad de la organización, lo que le permitiría a un atacante explotar y violar la confidencialidad, integridad, disponibilidad de la misma.

Riesgo. Se considera como la situación de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Por lo tanto, puede considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Política de seguridad de la información. Para la correcta implementación de un SGSI, las entidades deben definir la formulación de unas políticas de seguridad, las cuales son un elemento fundamental para poder gestionar la seguridad de la misma en una organización.

Declaración de aplicabilidad. Considerado como un requisito de documentación en el estándar ISO/IEC 27001, puede ser utilizado por cualquier organización, como una manera de mantener el registro y control de las medidas de seguridad que son aplicadas.

7. Resultados

Como resultado se obtiene una guía o manual de implementación que puede ser adoptada por las entidades y las partes interesadas posterior a su publicación. Adicionalmente:

- Se identificaron los activos de información más críticos y su importancia para la entidad.
- Se identificaron los riesgos, amenazas y vulnerabilidades, se establece como se deben utilizar y cuáles son los mecanismos para mitigarlos.
- Se obtiene concienciación por parte de Directivos, Funcionarios y Contratistas sobre la necesidad de implementar, revisar y mantener actualizada un SGSI.
- A partir de las políticas de seguridad los funcionarios y contratistas conocen sus roles y responsabilidades.

8. Conclusiones

Se realiza la identificación de activos de información apoyado con el dominio 8 gestión de activos del anexo A de la norma ISO27001:2013, lo cual permitió identificar en términos generales los posibles activos informáticos para entidades del estado, de cómo deben ser utilizados, los roles y responsabilidades que tienen los funcionarios sobre los mismos, y reconociendo el nivel de clasificación de la información que a cada activo debe dársele. Esta fase del proyecto comprende las etapas para el registro de los activos de información, inicia con la identificación, clasificación y valoración, y termina con la publicación del inventario de activos de la entidad.

Se determinaron los riesgos, amenazas y vulnerabilidades comunes que afectan a la entidad, está fase de identificación se logró a partir del inventario de activos que posee la misma, lo cual permitió evidenciar cuales son los factores que ponen en peligro la integridad, confidencialidad y disponibilidad de la información en una organización, se establece como se deben utilizar y cuáles son los mecanismos para mitigarlos.

La aplicación de la metodología basada en la guía para la administración del riesgo, emitida por el departamento administrativo de la función pública “DAFP”, que proporciona los lineamientos para la gestión del riesgo de seguridad de la información en entidades públicas, permitió analizar, evaluar y gestionar los posibles riesgos asociados a la seguridad de la información para entidades del estado, basados en los criterios de confidencialidad, integridad y disponibilidad. Adicionalmente evidenció los posibles activos críticos de la misma, el impacto que puede generar y proporcionó las medidas oportunas para mantener y minimizar los riesgos bajo control.

Se realiza la verificación de controles de seguridad de la información en la entidad, posterior de realizar el análisis y evaluación de riesgos, se tuvo en cuenta los objetivos de control y controles de referencia, basados en la norma ISO/IEC 27001:2013 en su Anexo A, como un insumo base para mitigar los riesgos de seguridad de la información, lo cual permitió evidenciar en términos generales cuales son los controles efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo.

Se definieron las políticas de seguridad de la información en términos generales para la entidad, lo que permite que se trabaje bajo las mejores prácticas y lineamientos de seguridad de la información y proporcione todos los mecanismos y aspectos que deben ser acatados por directivos, funcionarios, contratistas y terceros que laboren o tengan relación con la entidad, en busca de mantener la confidencialidad, integridad y disponibilidad de la información.