Dirección TIC

GOBERNACIÓN de BOLIVAR

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Gobernación de Bolívar

Dirección de Tecnologías de la Información y las Comunicaciones

Vía Cartagena - Turbaco, Km 3 Sector Bajo Miranda, El Cortijo
Teléfono: 60 - 5 - 6517444 Ext: 1010 - 1007 - 1006 - 2103
E-mail: contactenos@bolivar.gov.co
www.bolivar.gov.co

FIRMAS Y REVISIONES

TITULO	Plan General para el Tratamiento de Riesgos de Seguridad de la Información.
Autor	Dirección de las Tecnologías de la Información y las Comunicaciones - Gobernación de Bolívar
Tema	Política de Tecnología de Información y Comunicación, Estrategia Gobierno Digital
Fecha de Elaboración	Agosto 2021
Formato	PDF
Versión	4.0
Palabras Relacionadas	Modelo de Gestión TI, Tecnología de Información – TI, Gobierno Digital

CONTROL DE CAMBIOS

Fecha	Autor	Versión	Cambio
28 de diciembre 2018	Dirección TIC	1.0	Versión Inicial
26 de diciembre 2019	Dirección TIC	2.0	Se detalló la evaluación del riesgo asociados la seguridad y privacidad de la información
30 de noviembre 2020	Dirección TIC	3.0	Se definieron de manera general los riesgos, vulnerabilidades y amenazas. Se incluyeron los controles según la norma ISO/IEC 27002:2013
31 de agosto 2021	Dirección TIC	4.0	Se agregan Amenazas del Catálogo de Enisa
06 de diciembre de 2022	Dirección TIC	4.1	Se agregó cronograma de actividades.

TABLA DE CONTENIDO

INTRODUCCIÓN

La revolución digital está obligando a reconocer el protagonismo de la información en los procesos productivos de todas las empresas y la importancia de tener la información adecuadamente identificada y protegida. Por lo anterior, se amerita dar un tratamiento, manejo y clasificación a la información bajo una correcta administración y custodia.

La GOBERNACIÓN DE BOLÍVAR, atendiendo a su política general de seguridad y privacidad de la información, previamente aprobada, ha decidido vincular un modelo de administración de los riesgos de seguridad de la información el logro de los objetivos de mantener la información de la Entidad confidencial, integra y disponible, a través de su ciclo de vida desde su captura, almacenamiento, explotación, hasta su eliminación.

OBJETIVO

Establecer en la GOBERNACIÓN DE BOLIVAR una ruta con enfoque metódico que facilite las pautas necesarias para desarrollar y fortalecer una correcta gestión de los riesgos de seguridad de la información, a través de metodologías que faciliten la determinación del contexto estratégico, la identificación de riesgo y oportunidades, el análisis, la valoración y la generación de políticas.

ALCANCE

La gestión de riesgos será aplicada sobre cualquier proceso de la GOBERNACIÓN DE BOLÍVAR, a través de los principios básicos para la administración de los riesgos de seguridad de la información. Dicha gestión, incluye las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información, análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación.

TERMINOS Y DEFINICIONES

A continuación, se listan algunos términos y definiciones de términos que se utilizarán durante el desarrollo de la gestión de riesgos de seguridad de la información:

Aceptación de un riesgo: Decisión informada de tomar un riesgo particular. La aceptación del riesgo puede ocurrir sin tratamiento de riesgo o durante el proceso de tratamiento de riesgo. Los riesgos aceptados están sujetos a monitoreo y revisión. (International Organization for Standardization, 2016)

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000) (Ministerio de Tecnologías de la Información y las Comunicaciones, 2015b)

Amenaza: Causa potencial de un incidente no deseado, que puede resultar en un daño a un sistema u organización. (International Organization for Standardization, 2016)

Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y para determinar su nivel. El análisis de riesgos proporciona la base para la evaluación del riesgo y las decisiones sobre el tratamiento del riesgo. El análisis de riesgo incluye estimación de riesgo. (International Organization for Standardization, 2016)

Ataque: Intento de destruir, exponer, alterar, inhabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo de información. (International Organization for Standardization, 2016).

Confidencialidad: Propiedad que la información no esté disponible o sea revelada a personas, entidades o procesos no autorizados. (International Organization for Standardization, 2016)

Control: Mecanismo que modifica el valor de un riesgo. Los controles incluyen cualquier proceso, política, dispositivo, práctica u otras acciones que modifiquen el riesgo. Los controles no siempre ejercen el efecto modificador previsto o asumido. (International Organization for Standardization, 2016)

Criterios de riesgos: Términos de referencia con los que se evalúa la importancia del riesgo. Los criterios de riesgo se basan en los objetivos de la organización y en el contexto externo e interno. Los criterios de riesgo pueden derivarse de normas, leyes, políticas y otros requisitos. (International Organization for Standardization, 2016)

Detectar: Descubrir la existencia de algo que no era patente. (Real Academia Española, 2019a)

Disponibilidad: Propiedad de ser accesible y utilizable a petición de una entidad autorizada. (International Organization for Standardization, 2016)

Evaluación del riesgo: Proceso de comparar los resultados del análisis de riesgo con los criterios de riesgo para determinar si es aceptable o tolerable la magnitud del riesgo. La evaluación del riesgo ayuda a la decisión sobre el tratamiento del riesgo. (International Organization for Standardization, 2016)

Evento: Acontecimiento o cambio de un conjunto particular de circunstancias. Un evento puede ser uno o más acontecimientos, y puede tener varias causas. Un evento puede consistir en algo que no sucede. Un evento puede en ocasiones referirse a un “incidente” o un “accidente”. (International Organization for Standardization, 2016)

Evento de seguridad de la información: Acontecimiento identificado en el estado de un sistema, servicio o red que indica una posible violación a la política de seguridad de la información o fallo de los controles o una situación previamente desconocida que puede ser relevante para la seguridad. (International Organization for Standardization, 2016)

Gestión de incidentes de seguridad de la información: Proceso para detectar, informar, evaluar, responder ante los incidentes de seguridad, mitigarlos y aprender de ellos. (International Organization for Standardization, 2016)

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos. (International Organization for Standardization, 2016)

Identificar: Reconocer si una persona o cosa es la misma que se supone o se busca. (Real Academia Española, 2019b)

Identificación del riesgo: Proceso de encontrar, reconocer y describir los riesgos. La identificación del riesgo implica la identificación de fuentes de riesgo, eventos, sus causas y sus potenciales consecuencias. La identificación de riesgos puede incluir datos históricos, análisis teóricos, opiniones informadas y de expertos y necesidades de los interesados. (International Organization for Standardization, 2016)

Incidente de seguridad de la información: Evento o serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer de manera negativa las operaciones de la empresa y amenazar la seguridad de la información. (International Organization for Standardization, 2016)

Integridad: Propiedad de la exactitud y completitud de la información. (International Organization for Standardization, 2016)

Monitoreo: Determinación del estado de un sistema, proceso o una actividad. (International Organization for Standardization, 2016)

Política: Intenciones y directrices de una organización expresada formalmente por su alta dirección. (International Organization for Standardization, 2016)

Proceso de gestión del riesgo: Aplicación sistemática de políticas de gestión, procedimientos y prácticas a las actividades de comunicación, consulta, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, seguimiento y revisión de los riesgos. (International Organization for Standardization, 2016)

Registros de auditoria: Un registro cronológico de las actividades del sistema de información, incluyendo los registros de accesos del sistema y las operaciones realizadas en un período determinado. (National Institute of Standards and Technology, 2014)

Riesgo: Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de lo esperado positiva o negativamente. La incertidumbre es el estado total o parcial de la insuficiencia de la información relacionada con la comprensión o el conocimiento de un evento, su consecuencia o probabilidad. (…). En el contexto de la seguridad de la información, los sistemas de gestión, los riesgos de la seguridad de la información pueden expresarse como efecto de la incertidumbre en los objetivos de la seguridad de la información. El riesgo de seguridad de la información se asocia con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daño a una organización. (International Organization for Standardization, 2016)

Riesgo residual: Riesgo restante después de realizado tratamiento. (International Organization for Standardization, 2016)

Seguridad de la información: Preservación de la confidencialidad, disponibilidad e integridad de la información. (International Organization for Standardization, 2016)

Tratamiento de riesgo: Proceso para modificar el valor del riesgo. El tratamiento del riesgo puede incluir lo siguiente:

- Evitar el riesgo al decidir no iniciar o continuar con la actividad que da lugar al riesgo.
- Tomar o aumentar el riesgo para poder aprovechar una oportunidad.
- Eliminación de la fuente de riesgo.
- Cambiar la probabilidad.
- Modificar las consecuencias.
- Compartir el riesgo con otra parte o partes.
- Asumir el riesgo mediante una elección informada.

Los tratamientos de riesgo que se ocupan de las consecuencias negativas se denominan a veces "mitigación del riesgo", "eliminación del riesgo", "prevención del riesgo" y "reducción del riesgo". El tratamiento de riesgos puede crear nuevos riesgos o modificar los riesgos existentes. (International Organization for Standardization, 2016)

Valoración de riesgo: Es el proceso global de la identificación del riesgo, el análisis de riesgo y la evaluación del riesgo. (International Organization for Standardization, 2016)

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (International Organization for Standardization, 2016)

PROCESO DE GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Basados en la norma ISO 27005, la GOBERNACIÓN DE BOLÍVAR, ejecutará el siguiente modelo de gestión de riesgos de la **Guía de Gestión de Riesgos del Mintic**, el cual ayudará a garantizar un tratamiento adecuado de los riesgos de seguridad de la información:

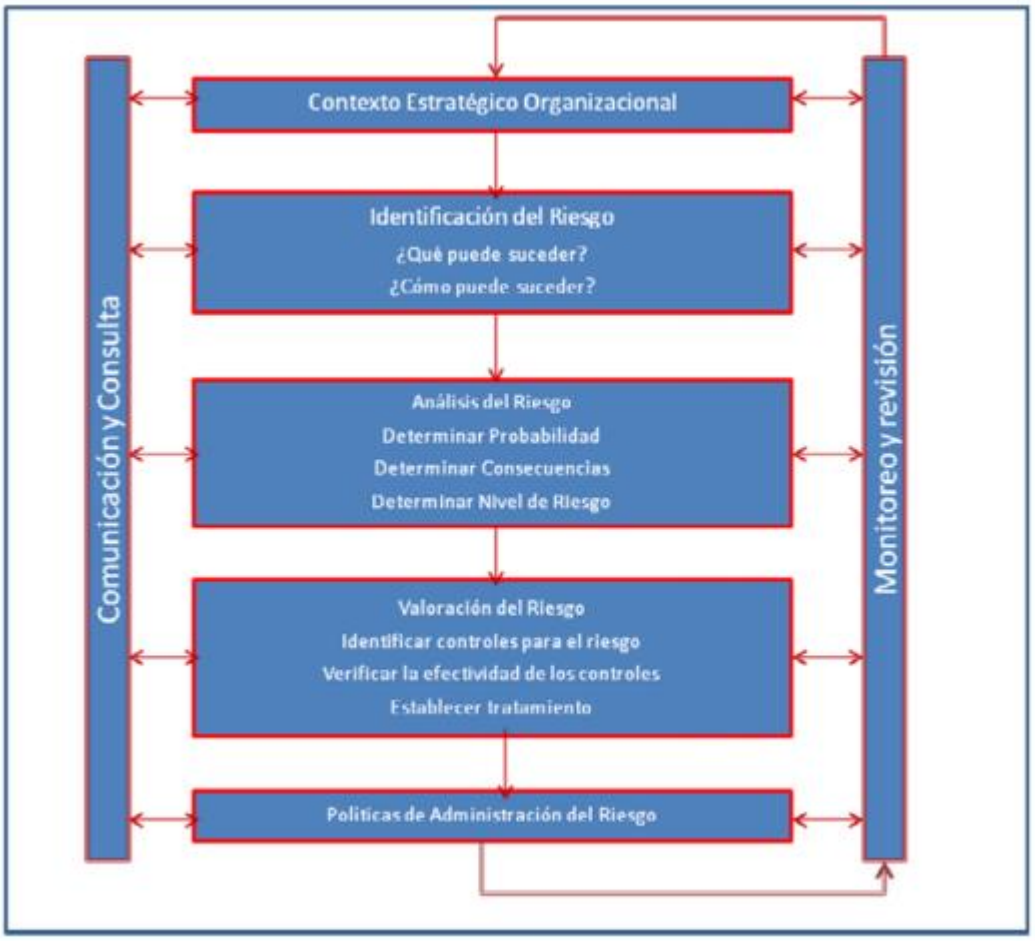


Imagen 1. Tomado de la Cartilla de Administración de Riesgos del DAFP

Modelo de gestión de riesgos de seguridad de la información. NTC/ISO 27005

Metodología de Administración de Riesgos

El proceso consiste en:

Inventario de Activos

La actividad de Inventario de Activos de Información se realiza con base en el documento "**Instructivo Inventario de Activos de TI Gobernación de Bolívar**" y la Matriz "**Inventario de Activos de TI Gobernación de Bolívar**"

Describir Activos

La primera actividad es realizar el Inventario de Activos de TI de la Gobernación de Bolívar, para lo cual se utilizó el Instructivo de Inventario de Activos.

El documento del inventario se encuentra en Custodia del responsable del proceso.

Criticidad Del Activo

La criticidad de los activos estará determinada por la tabla publicada en la **Guía de Gestión de riesgos** del Mintic e indicadas en el Instructivo de Inventario de Activos de TI de la Gobernación de Bolívar.

Identificación de los Riesgos

Esta fase tiene como objetivo conocer los escenarios que pueden producir en la entidad y los efectos que puedan tener sobre los objetivos de esta.

El procedimiento para la gestión de riesgos contiene el reconocimiento de las causas y la procedencia del riesgo que puedan afectar a los objetivos.

Del inventario de Activos de Información de TI de la Gobernación de Bolívar, identificar los activos de información por proceso en evaluación.

Identificar la propiedad de la Información que afecta el riesgo.

- Riesgo de Disponibilidad
- Riesgo de Integridad
- Riesgo de Confidencialidad

Identificar el riesgo correspondiente
Para esta actividad se utiliza la descripción de los riesgos de la **Matriz de Riesgos de Seguridad Digital:**

Riesgos	Descripción
Incumplimiento de las políticas de seguridad y privacidad de la información que atenten contra la disponibilidad, integridad y confidencialidad de la información	Políticas o controles de seguridad y privacidad de la información no aplicados total o parcialmente por desconocimiento o actos intencionales.
Información imprecisa o inexacta en las operaciones	La información podría ser modificada o alterada sin autorización. Se puede dar por alteración o cambios de la información (digital o electrónica) generada, recolectada, procesada o almacenada.
Pérdida en la trazabilidad de las operaciones realizadas	Las operaciones realizadas con la información no pueden rastrearse o no presenta claramente quién y qué se ha realizado con la misma.
Indisponibilidad de la Información oportuna o de los sistemas para las operaciones	La información no se encuentra disponible en el momento que se necesita para cumplir la operación o funciones propias en la Agencia.
Indisponibilidad de la Información oportuna o de los sistemas para las operaciones	La información no se encuentra disponible en el momento que se necesita para cumplir la operación o funciones propias en la Agencia.
Indisponibilidad de la Información oportuna o de los sistemas para las operaciones	La información no se encuentra disponible en el momento que se necesita para cumplir la operación o funciones propias en la Agencia.
Fuga o acceso de información por personal no autorizado	La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.
Fuga o acceso de información por personal no autorizado	La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.

Fuga o acceso de información por personal no autorizado	La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.
Pérdida de la continuidad de los servicios u operaciones de la entidad	La información no se encuentra disponible por ausencia o falla en los activos de información que hacen parte de los procesos u operaciones.
Pérdida de equipos y/o de información contenida en los mismos	Extravío o no disponibilidad de equipos o información debido a un inadecuado tratamiento en el almacenamiento, disposición final, custodia o destrucción segura de los mismos.
Falla en los dispositivos o equipos	Las fallas en los equipos tecnológicos o redes de comunicación debido a agentes externos, ambientales, intencionales o no intencionales afectan la disponibilidad de la información para el desarrollo de las funciones y operaciones
Falla en los dispositivos o equipos	Las fallas en los equipos tecnológicos o redes de comunicación debido a agentes externos, ambientales, intencionales o no intencionales afectan la disponibilidad de la información para el desarrollo de las funciones y operaciones
Pérdida de la continuidad de los servicios u operaciones de la entidad	La información no se encuentra disponible por ausencia o falla en los activos de información que hacen parte de los procesos u operaciones.
Falla en los dispositivos o equipos	Las fallas en los equipos tecnológicos o redes de comunicación debido a agentes externos, ambientales, intencionales o no intencionales afectan la disponibilidad de la información para el desarrollo de las funciones y operaciones
Falla en los dispositivos o equipos	Las fallas en los equipos tecnológicos o redes de comunicación debido a agentes externos, ambientales, intencionales o no intencionales afectan la disponibilidad de la información para el desarrollo de las funciones y operaciones
Pérdida de equipos y/o de información contenida en los mismos	Extravío o no disponibilidad de equipos o información debido a un inadecuado tratamiento en el almacenamiento, disposición final, custodia o destrucción segura de los mismos.
Pérdida de equipos y/o de información contenida en los mismos	Extravío o no disponibilidad de equipos o información debido a un inadecuado tratamiento en el almacenamiento, disposición final, custodia o destrucción segura de los mismos.
Fuga o acceso de información por personal no autorizado	La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.
Indisponibilidad de la Información oportuna o de los sistemas para las operaciones	La información no se encuentra disponible en el momento que se necesita para cumplir la operación o funciones propias en la Agencia.
Fuga o acceso de información por personal no autorizado	La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.
Fuga o acceso de información por personal no autorizado	La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.
Pérdida de la continuidad de los servicios u operaciones de la entidad	La información no se encuentra disponible por ausencia o falla en los activos de información que hacen parte de los procesos u operaciones.

Pérdida de la continuidad de los servicios u operaciones de la entidad	La información no se encuentra disponible por ausencia o falla en los activos de información que hacen parte de los procesos u operaciones.
Elevación de privilegios y acceso no autorizado a la información	Acceso indebido a los sistemas y/o información aprovechando las vulnerabilidades tecnológicas, ambientales y del recurso humano.
Fuga o acceso de información por personal no autorizado	La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.
Fuga o acceso de información por personal no autorizado	La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.
Pérdida de la continuidad de los servicios u operaciones de la entidad	La información no se encuentra disponible por ausencia o falla en los activos de información que hacen parte de los procesos u operaciones.
Fuga o acceso de información por personal no autorizado	La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.
Fallas o deficiencia del software	Las fallas en los sistemas de información, aplicaciones o desarrollos tecnológicos o debido a prácticas inadecuadas del software, actos accidentales, intencionales o no intencionales afectan la disponibilidad de la información para el desarrollo de las funciones y operaciones
Fallas o deficiencia del software	Las fallas en los sistemas de información, aplicaciones o desarrollos tecnológicos o debido a prácticas inadecuadas del software, actos accidentales, intencionales o no intencionales afectan la disponibilidad de la información para el desarrollo de las funciones y operaciones
Fuga o acceso de información por personal no autorizado	La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.
Pérdida de equipos y/o de información contenida en los mismos	Extravío o no disponibilidad de equipos o información debido a un inadecuado tratamiento en el almacenamiento, disposición final, custodia o destrucción segura de los mismos.
Pérdida en la trazabilidad de las operaciones realizadas	Las operaciones realizadas con la información no pueden rastrearse o no presenta claramente quién y qué se ha realizado con la misma.
Elevación de privilegios y acceso no autorizado a la información	Acceso indebido a los sistemas y/o información aprovechando las vulnerabilidades tecnológicas, ambientales y del recurso humano.
Información imprecisa o inexacta en las operaciones	La información podría ser modificada o alterada sin autorización. Se puede dar por alteración o cambios de la información (digital o electrónica) generada, recolectada, procesada o almacenada.
Información imprecisa o inexacta en las operaciones	La información podría ser modificada o alterada sin autorización. Se puede dar por alteración o cambios de la información (digital o electrónica) generada, recolectada, procesada o almacenada.
Información imprecisa o inexacta en las operaciones	La información podría ser modificada o alterada sin autorización. Se puede dar por alteración o cambios de la información (digital o electrónica) generada, recolectada, procesada o almacenada.

Información imprecisa o inexacta en las operaciones	La información podría ser modificada o alterada sin autorización. Se puede dar por alteración o cambios de la información (digital o electrónica) generada, recolectada, procesada o almacenada.
Información imprecisa o inexacta en las operaciones	La información podría ser modificada o alterada sin autorización. Se puede dar por alteración o cambios de la información (digital o electrónica) generada, recolectada, procesada o almacenada.
Información imprecisa o inexacta en las operaciones	La información podría ser modificada o alterada sin autorización. Se puede dar por alteración o cambios de la información (digital o electrónica) generada, recolectada, procesada o almacenada.
Fuga o acceso de información por personal no autorizado	La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.
Elevación de privilegios y acceso no autorizado a la información	Acceso indebido a los sistemas y/o información aprovechando las vulnerabilidades tecnológicas, ambientales y del recurso humano.
Elevación de privilegios y acceso no autorizado a la información	Acceso indebido a los sistemas y/o información aprovechando las vulnerabilidades tecnológicas, ambientales y del recurso humano.
Sanciones legales o económicas	Incumplimiento de legislación aplicable o normatividad interna de la Agencia Nacional Digital.
Información imprecisa o inexacta en las operaciones	La información podría ser modificada o alterada sin autorización. Se puede dar por alteración o cambios de la información (digital o electrónica) generada, recolectada, procesada o almacenada.
Información imprecisa o inexacta en las operaciones	La información podría ser modificada o alterada sin autorización. Se puede dar por alteración o cambios de la información (digital o electrónica) generada, recolectada, procesada o almacenada.
Pérdida de la continuidad de los servicios u operaciones de la entidad	La información no se encuentra disponible por ausencia o falla en los activos de información que hacen parte de los procesos u operaciones.
Elevación de privilegios y acceso no autorizado a la información	Acceso indebido a los sistemas y/o información aprovechando las vulnerabilidades tecnológicas, ambientales y del recurso humano.
Pérdida de la continuidad de los servicios u operaciones de la entidad	La información no se encuentra disponible por ausencia o falla en los activos de información que hacen parte de los procesos u operaciones.
fuga o acceso de información por personal no autorizado	La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.
Información imprecisa o inexacta en las operaciones	La información podría ser modificada o alterada sin autorización. Se puede dar por alteración o cambios de la información (digital o electrónica) generada,

	recolectada, procesada o almacenada.
Pérdida de la continuidad de los servicios u operaciones de la entidad	La información no se encuentra disponible por ausencia o falla en los activos de información que hacen parte de los procesos u operaciones.
Sanciones legales o económicas	Incumplimiento de legislación aplicable o normatividad interna de la Agencia Nacional Digital.
Deficiencias en tratamiento adecuado y seguro de la información	Tratamiento inadecuado de la información por desconocimiento de políticas, controles y buenas prácticas de seguridad y privacidad de la información establecidas por la AND por parte del personal.
Información imprecisa o inexacta en las operaciones	La información podría ser modificada o alterada sin autorización. Se puede dar por alteración o cambios de la información (digital o electrónica) generada, recolectada, procesada o almacenada.
Información imprecisa o inexacta en las operaciones	La información podría ser modificada o alterada sin autorización. Se puede dar por alteración o cambios de la información (digital o electrónica) generada, recolectada, procesada o almacenada.
Pérdida en la trazabilidad de las operaciones realizadas	Las operaciones realizadas con la información no pueden rastrearse o no presenta claramente quién y qué se ha realizado con la misma.
Fuga o acceso de información por personal no autorizado	La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.
Elevación de privilegios y acceso no autorizado a la información	Acceso indebido a los sistemas y/o información aprovechando las vulnerabilidades tecnológicas, ambientales y del recurso humano.
Fuga o acceso de información por personal no autorizado	La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.
Pérdida de la continuidad de los servicios u operaciones de la entidad	La información no se encuentra disponible por ausencia o falla en los activos de información que hacen parte de los procesos u operaciones.
Pérdida de la continuidad de los servicios u operaciones de la entidad	La información no se encuentra disponible por ausencia o falla en los activos de información que hacen parte de los procesos u operaciones.
Fuga o acceso de información por personal no autorizado	La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.
Elevación de privilegios y acceso no autorizado a la información	Acceso indebido a los sistemas y/o información aprovechando las vulnerabilidades tecnológicas, ambientales y del recurso humano.
Elevación de privilegios y acceso no autorizado a la información	Acceso indebido a los sistemas y/o información aprovechando las vulnerabilidades tecnológicas, ambientales y del recurso humano.
Elevación de privilegios y acceso no autorizado a la información	Acceso indebido a los sistemas y/o información aprovechando las vulnerabilidades tecnológicas, ambientales y del recurso humano.
Pérdida en la trazabilidad de las operaciones realizadas	Las operaciones realizadas con la información no pueden rastrearse o no presenta claramente quién y qué se ha realizado con la misma.
Pérdida en la trazabilidad de las operaciones realizadas	Las operaciones realizadas con la información no pueden rastrearse o no presenta claramente quién y qué se ha realizado con la misma.
Pérdida de la continuidad de los servicios u operaciones de la entidad	La información no se encuentra disponible por ausencia o falla en los activos de información que hacen parte de los procesos u operaciones.
Pérdida de la continuidad de los servicios u operaciones de la entidad	La información no se encuentra disponible por ausencia o falla en los activos de información que hacen parte de los procesos u operaciones

Pérdida de la continuidad de los servicios u operaciones de la entidad	La información no se encuentra disponible por ausencia o falla en los activos de información que hacen parte de los procesos u operaciones.
Pérdida de la continuidad de los servicios u operaciones de la entidad	La información no se encuentra disponible por ausencia o falla en los activos de información que hacen parte de los procesos u operaciones.
Pérdida de la continuidad de los servicios u operaciones de la entidad	La información no se encuentra disponible por ausencia o falla en los activos de información que hacen parte de los procesos u operaciones.
Información imprecisa o inexacta en las operaciones	La información podría ser modificada o alterada sin autorización. Se puede dar por alteración o cambios de la información (digital o electrónica) generada, recolectada, procesada o almacenada.
Información imprecisa o inexacta en las operaciones	La información podría ser modificada o alterada sin autorización. Se puede dar por alteración o cambios de la información (digital o electrónica) generada, recolectada, procesada o almacenada.
Fuga o acceso de información por personal no autorizado	La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.
Pérdida en la trazabilidad de las operaciones realizadas	Las operaciones realizadas con la información no pueden rastrearse o no presenta claramente quién y qué se ha realizado con la misma.
Pérdida de la continuidad de los servicios u operaciones de la entidad	La información no se encuentra disponible por ausencia o falla en los activos de información que hacen parte de los procesos u operaciones.
Fuga o acceso de información por personal no autorizado	La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.
Pérdida de la continuidad de los servicios u operaciones de la entidad	La información no se encuentra disponible por ausencia o falla en los activos de información que hacen parte de los procesos u operaciones.
Pérdida en la trazabilidad de las operaciones realizadas	Las operaciones realizadas con la información no pueden rastrearse o no presenta claramente quién y qué se ha realizado con la misma.
Fuga o acceso de información por personal no autorizado	La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.
Elevación de privilegios y acceso no autorizado a la información	Acceso indebido a los sistemas y/o información aprovechando las vulnerabilidades tecnológicas, ambientales y del recurso humano.
Sanciones disciplinarias inadecuadas	Inconsistencia o fallas en el tratamiento de sanciones sobre los incidentes del software

Fuga o acceso de información por personal no autorizado	La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.
Fuga o acceso de información por personal no autorizado	La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.
Fuga o acceso de información por personal no autorizado	La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.
Elevación de privilegios y acceso no autorizado a la información	Acceso indebido a los sistemas y/o información aprovechando las vulnerabilidades tecnológicas, ambientales y del recurso humano.
Fuga o acceso de información por personal no autorizado	La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.
Elevación de privilegios y acceso no autorizado a la información	Acceso indebido a los sistemas y/o información aprovechando las vulnerabilidades tecnológicas, ambientales y del recurso humano.
Elevación de privilegios y acceso no autorizado a la información	Acceso indebido a los sistemas y/o información aprovechando las vulnerabilidades tecnológicas, ambientales y del recurso humano.
Sanciones legales o económicas	Incumplimiento de legislación aplicable o normatividad interna de la Agencia Nacional Digital.

Registrar el responsable de identificar Incidente

En esta actividad se registra la persona que tendrá la responsabilidad de identificar que se ha materializado un riesgo, es decir, se ha producido un incidente.

Identificar las amenazas

En esta actividad se identifican las Amenazas dependiendo de la propiedad que estemos analizando.

Para esta actividad se utilizan las Amenazas de la **Matriz de Riesgos de Seguridad Digital**:

Activo	*Amenazas*
Información	Fallas humanas
	Pérdida de información
	Falla en los sistemas
	Hurto de información
Hardware (Equipos y Redes de Comunicación)	Incumplimiento en el mantenimiento del sistema de información
	Destrucción de equipos o de medios
	Polvo, corrosión, congelamiento

	Radiación electromagnética
	Error en el uso
	Pérdida del suministro de energía
	Fenómenos metereológicos
	Hurto de medios o documentos
	Negociación de acciones
	Escucha encubierta
	Falla del equipo de telecomunicaciones
	Falsificación de derechos
	Espionaje remoto
	Saturación del sistema de información
	Uso no autorizado del equipo
Software	Abuso de los derechos
	Corrupción de datos
	Error en el uso
	Falsificación de derechos
	Procesamiento ilegal de datos
	Mal funcionamiento del software
	Manipulación con software
	Hurto de medios o documentos
	Uso no autorizado del equipo
Recurso Humano	Incumplimiento en la disciplina del personal
	Destrucción de equipos o medios
	Error en el uso
	Procesamiento ilegal de datos
	Hurto de medios o documentos
	Uso no autorizado del equipo
Infraestructura Física	Destrucción de equipo o medios
	Inundación
	Pérdida del suministro de energía
	Hurto de equipo
Organizacionales	Abuso de los derechos
	Incumplimiento en el mantenimiento del sistema de información
	Corrupción de datos
	Datos provenientes de fuentes no confiables
	Negación de acciones

	Falla del equipo
	Error en el uso
	Hurto de equipo
	Hurto de medios o documentos
	Uso no autorizado del equipo
	Uso de software falso o copiado

En algunos casos puede ser necesario realizar la identificación de amenazas con un nivel más especializado, en estos casos se utilizará el **Reference Incident Classification Taxonomy** de la **Enisa Threat Taxonomy**:

Incidentes y Amenazas Enisa			
Integra los datos de Enisa Threat Taxonomy con la Reference Incident Classification Taxonomy.			
Amenaza de alto nivel	**Amenaza**	**Detalle de amenaza**	**Incidente**
Ataque físico (deliberado / intencional)	Fraude	Fraude por empleados	Fraude
	Sabotaje		Incidente de disponibilidad
	Vandalismo		Incidente de disponibilidad
	Robo (dispositivos, medios de almacenamiento y documentos)	Robo de dispositivos móviles (teléfonos inteligentes / tabletas)	Incidente de disponibilidad
		Robo de hardware fijo	Incidente de disponibilidad
		Robo de documentos	Incidente de disponibilidad
		Robo de copias de seguridad	Incidente de disponibilidad
	Fuga de información / compartir		Incidente de Seguridad del contenido de la información
	Acceso físico no autorizado / Entrada no autorizada a las instalaciones		Intrusión
	Coacción, extorsión o corrupción		Otro
	Daños por guerra		Otro
	Ataque terrorista		Otro
Daño / pérdida involuntaria de información o activos de TI	Fuga / intercambio de información debido a un error humano	Fugas accidentales / intercambio de datos por parte de los empleados	Incidente por Vulnerabilidad
		Fugas de datos a través de aplicaciones móviles	Incidente por Vulnerabilidad
		Fugas de datos a través de aplicaciones web	Incidente por Vulnerabilidad

		Fugas de información transferidas por la red	Incidente por Vulnerabilidad
	Uso o administración errónea de dispositivos y sistemas	Pérdida de información debido a errores de mantenimiento / operadores	Incidente de Disponibilidad
		Pérdida de información debido a error de configuración / instalación	Incidente de Disponibilidad
		Aumentando el tiempo de recuperación	Incidente de Disponibilidad
		Pérdida de información debido a errores del usuario	Incidente de Disponibilidad
	Usar información de una fuente no confiable		Otro
	Cambio involuntario de datos en un sistema de información		Seguridad del contenido de la información
	Diseño y planificación inadecuados o adaptación inadecuada		Otro
	Daño causado por un tercero	Fallo de seguridad por parte de un tercero	Incidente por Vulnerabilidad
	Daños resultantes de las pruebas de penetración		Incidente por Prueba
	Pérdida de información en la nube		Incidente de Disponibilidad
	Pérdida de (integridad de) información sensible	Pérdida de integridad de los certificados	Incidente de Disponibilidad
	Pérdida de dispositivos, medios de almacenamiento y documentos	Pérdida de dispositivos / dispositivos móviles	Incidente de Disponibilidad
		Pérdida de medios de almacenamiento	Incidente de Disponibilidad
		Pérdida de documentación de infraestructura de TI	Incidente de Disponibilidad
	Destrucción de registros	Infección de medios extraíbles	Código malicioso
		Abuso de almacenamiento	Incidente de Disponibilidad
Escuchando / interceptando / secuestrando	Búsqueda de redes inalámbricas War driving		Recopilación de información
	Interceptar emisiones comprometidas		Incidente de seguridad del Contenido de la Información
	Intercepción de información	Espionaje corporativo	Incidente de seguridad del Contenido de la Información
		Estado nacional de espionaje	Incidente de seguridad del Contenido de la Información
		Fuga de información debido a Wi-Fi no seguro, puntos de acceso maliciosos	Incidente de seguridad del Contenido de la Información
	Radiación interferente		Otro
	Reproducción de mensajes		Incidente de seguridad del Contenido de la Información

	Reconocimiento de red, manipulación del tráfico de red y recopilación de información		Recopilación de información
	Hombre en el medio / secuestro de la sesión		Incidente de seguridad del Contenido de la Información
Actividad maliciosa/ Abuso	Robo de identidad (fraude / cuenta de identidad)	Robo de credenciales usando troyanos	Código malicioso
	Recibir correo electrónico no solicitado	SPAM	Contenido abusivo
		Correos electrónicos infectados no solicitados	Contenido abusivo
	Negación de servicio	Servicio de denegación de red distribuida (DDoS) (ataque de capa de red, es decir, explotación de protocolo / paquetes malformados / inundación / suplantación)	Incidente de Disponibilidad
		Servicio distribuido de denegación de aplicación (DDoS) (ataque de la capa de aplicación, es decir, Ping of Death / XDoS / WinNuke / HTTP Floods)	Incidente de Disponibilidad
		Distributed DoS (DDoS) a los servicios de red y de aplicaciones (métodos de amplificación / reflexión, es decir, NTP / DNS / ... / BitTorrent)	Incidente de Disponibilidad
	Código malicioso / software / actividad	Abuso de recursos	Código malicioso
		Envenenamiento de motor de búsqueda	Código malicioso
		Explotación de la confianza falsa de las redes sociales	Contenido abusivo
		Gusanos / Troyanos	Código malicioso
		Rootkits	Código malicioso
		Malware móvil	Código malicioso
		Aplicaciones móviles de confianza infectadas	Código malicioso
		Elevación de privilegios	Intentos de intrusión
		Ataques de aplicación web / inyección (Inyección de código: SQL, XSS)	Incidente de seguridad del Contenido de la Información
		Spyware o adware engañoso	Código malicioso
		Virus	Código malicioso
		Software de seguridad no confiable/ Rogueware/ Scareware	Código malicioso
		Exploits/Exploit Kits	Código malicioso
	Ingeniería social	Ataques de phishing	Recopilación de información
		Ataques Spear phishing	Recopilación de información

	Abuso de fuga de información	Fuga que afecta la privacidad de los dispositivos móviles y las aplicaciones móviles	Incidente de seguridad del Contenido de la Información
		Fuga que afecta la privacidad de la web y las aplicaciones web	Incidente de seguridad del Contenido de la Información
		Fuga que afecta el tráfico de la red	Incidente de seguridad del Contenido de la Información
		Fuga que afecta la computación en la nube	Incidente de seguridad del Contenido de la Información
	Generación y uso de certificados maliciosos	Pérdida de (integridad de) información sensible	Incidente de seguridad del Contenido de la Información
		Hombre en el medio / secuestro de la sesión	Incidente de seguridad del Contenido de la Información
		Ingeniería social / malware firmado (por ejemplo, instalación de actualizaciones falsas de sistemas operativos de confianza: malware firmado)	Recopilación de información
		Certificados SSL falsos	Incidente de seguridad del Contenido de la Información
	Manipulación de hardware y software	Proxies anónimos	Fraude
		Abuso del poder de computación de la nube para lanzar ataques (ciberdelincuencia como servicio)	Incidente de Disponibilidad
		Abuso de vulnerabilidades, vulnerabilidades de día 0	Incidente por Vulnerabilidad
		Acceso de sitios web a través de cadenas de proxies HTTP (Ofuscación)	Fraude
		Acceso al software del dispositivo	Incidente de seguridad del Contenido de la Información
		Alternancia de software	Incidente de seguridad del Contenido de la Información
		Hardware Malicioso	Código malicioso
	Manipulación de información	Repudio de acciones	Fraude
		Dirección de secuestro de espacio (prefijos de IP) Manipulación de tabla de enrutamiento	Incidente de seguridad del Contenido de la Información
		Envenenamiento DNS / DNS spoofing / Manipulación DNS	Incidente de seguridad del Contenido de la Información
		Falsificación de registro	Fraude
		Secuestro de sistema autónomo	Intrusión
		Manipulación de sistema autónomo	Intrusión
		Falsificación de configuraciones	Intrusión
	Mal uso de soluciones de auditoría		Incidente por Prueba
	Mal uso de los sistemas de información / información (incluidas las aplicaciones móviles)		Fraude

	Actividades no autorizadas	Uso no autorizado o administración de dispositivos y sistemas	Fraude
		Uso no autorizado del software	Fraude
		Acceso no autorizado a los sistemas / redes de información (Protocolo IMPI / Secuestro de DNS)	Intrusión
		Intrusión de red	Intrusión
		Cambios no autorizados de registros	Incidente de seguridad del Contenido de la Información
	Instalación no autorizada de software	Ataques basados en la web (descargas en Drive-by / URL maliciosas / ataques basados en navegador)	Intentos de intrusión
	Compromiso de información confidencial (violaciones de datos)		Incidente de seguridad del Contenido de la Información
	Hoax Farsa	Falso rumor y / o una advertencia falsa	Contenido abusivo
	Actividad remota (ejecución)	Ejecución remota de comandos	Intrusión
		Instrumento de acceso remoto (RAT)	Intrusión
		Botnets / actividad remota	Intrusión
	Ataques dirigidos (APTs etc.)	Malware móvil	Código malicioso
		Ataques de spear phishing	Recopilación de información
		Instalación de malware sofisticado y específico	Intentos de intrusión
		Ataques de Agujero de riego	Recopilación de información
	Fuerza bruta		Intentos de intrusión
	Abuso de autorizaciones		Fraude
	Violación de leyes o regulaciones / Violación de la legislación		Fraude
Legal	Incumplimiento de los requisitos contractuales	Incumplimiento de los requisitos contractuales por parte de un tercero	Fraude
	Uso no autorizado de recursos protegidos por derechos de propiedad intelectual	Uso ilegal de servicios de uso compartido de archivos	Fraude
	Abuso de datos personales		Fraude
	Decisiones judiciales / órdenes judiciales		Fraude
	Decisiones judiciales / órdenes judiciales		Fraude

Identificar las vulnerabilidades

En esta actividad se identifican las vulnerabilidades que permiten que se materialice ese riesgo específico de cada uno los activos de información.

Se utilizará el catálogo de vulnerabilidades de la **Matriz de Riesgos de Seguridad Digital**:

Tipos	Vulnerabilidades
Información	Desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información
	Manejo manual de la información
	Ausencia de validación de autenticación de la información
	Ausencia de copias de respaldo o backups de la información
	Retraso en la salida de información de los sistemas
	Retraso en la entrega de información por parte del personal
	Información sensible sin cifrado
	Ausencia o deficiencia en los sistemas de autenticación de los aplicativos
	Deficiencia en la autorización de permisos de la información
Hardware (Equipos y Redes de Comunicación)	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento
	Ausencia de esquemas de reemplazo periódico
	Susceptibilidad a la humedad, el polvo y la suciedad
	Sensibilidad a la radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración
	Susceptibilidad a la variaciones de voltaje
	Susceptibilidad a las variaciones de temperatura
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Tráfico sensible sin protección
	Conexión deficiente de los cables
	Punto único de falla

	Ausencia de identificación y autenticación de emisor y receptor
	Arquitectura insegura de la red
	Transferencia de contraseñas en claro
	Gestión inadecuada de la red (Tolrancia a fallas en el enrutamiento)
	Conexiones de red pública sin protección
Software	Ausencia o insuficiencia de pruebas de software
	Defectos bien conocidos en el software
	Ausencia de terminación de la sesión cuando se abandona la estación de trabajo
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado
	Ausencia de pistas de audotoría
	Asignación errada de los derechos de acceso
	Software ampliamente distribuido
	En términos de tiempo utilización de datos errados en los programas de aplicación
	Interfaz de usuario compleja
	Ausencia de documentación
	Configuración incorrecta de parámetros
	Fechas incorrectas
	Ausencia de mecanismo de identificación y autenticación, como la autenticación de usuario
	Tablas de contraseñas sin protección
	Gestión deficiente de las contraseñas
	Habilitación de servicios innecesarios
	Software nuevo o inmaduro
	Especificaciones incompletas o no claras para los desarrolladores
	Ausencia de control de cambios eficaz
	Descarga y uso no controlados de software
	Ausencia de copias de respaldo
	Ausencia de protección física de la edificación, puertas y ventanas
	Falla en la producción de informes de gestión
Recurso Humano	Ausencia del personal
	Procedimientos inadecuados de contratación
	Entrenamiento insuficiente en seguridad
	Uso incorrecto de software y hardware
	Falla de conciencia acerca de la seguridad
	Ausencia de mecanismos de monitoreo
	Trabajo o supervisado del personal externo o de limpieza
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería
Infraestructura Física	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos
	Ubicación en un área susceptible de inundación

	Red energética Inestable
	Ausencia de protección física de la edificación, puertas y ventanas
Organizacionales	Ausencia de procedimeinto formal para el registro y retiro de usuarios
	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso
	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes
	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información
	Ausencia de auditorías (supervisiones) regulares
	Ausencia de procedimientos de identificación y valoración de riesgos
	Ausencia de reportes de fallas en los registros de administradores y operadores
	Respuesta inadecuada de mantenimiento de servicio
	Ausencia de acuerdos de nivel de servicio, o insuficiencia en los mismos
	Ausencia de procedimiento de control de cambios
	Ausencia de procedimiento formal para el control de la documentación del SGSI
	Ausencia de procedimiento formal para la supervisión del registro del SGSI
	Ausencia de procedimiento formal para la autorización de la información disponible al público
	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información
	Ausencia de planes de continuidad
	Ausencia de políticas sobre el uso del correo electrónico
	Ausencia de procedimientos para la introducción del software en los sistemas operativos
	Ausencia de registros en las bitácoras (logs) de administrador operario
	Ausencia de procedimientos para el manejo de información clasificada
	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos
	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información
	Ausencia de política formal sobre la utilización de computadores portátiles
	Ausencia de control de los activos que se encuentra fuera de las instalaciones
	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla
	Ausencia de autorización de los recursos de procesamiento de la información
	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad
	Ausencia de revisiones regulares por parte de la gerencia
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad
	Ausencia de procedimientos del cumplimeinto de las disposiciones con los derechos intelectuales

Análisis del Riesgo Inherente

Identificar la Probabilidad

En esta actividad se identifica la Probabilidad de materialización de un Incidente.

La Dirección TIC determina que la mejor manera de establecer la Probabilidad de ocurrencia de un incidente es por Factibilidad, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

En la **Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5** de la Función Pública se obtiene:

Tabla 4 Criterios para definir el nivel de probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Facilitando la actividad utilizaremos estas opciones:

Frecuencia de la actividad	Probabilidad	Calificación
Dos veces al año	Muy baja	1
Dos veces al mes	Baja	2
Dos veces a la semana	Media	3
Dos veces al día	Alta	4
Varias veces al día	Muy alta	5

Identificar el Impacto

En esta actividad se identifica el mayor nivel de daño posible en el caso que se materialice dicho incidente.

Para esta actividad En la se utilizará la **Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5** de la Función Pública se obtiene: Tabla 9. Criterios para calificar el impacto – Riesgos de Gestión:

NIVEL	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
CATASTRÓFICO	- Impacto que afecte la ejecución presupuestal en un valor ≥50%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
MAYOR	- Impacto que afecte la ejecución presupuestal en un valor ≥20%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.
MODERADO	- Impacto que afecte la ejecución presupuestal en un valor ≥5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.

MENOR	- Impacto que afecte la ejecución presupuestal en un valor ≥1%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por algunas horas. - Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
INSIGNIFICANTE	- Impacto que afecte la ejecución presupuestal en un valor ≥0,5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad.	- No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, Versión 4, Dirección de Gestión y Desempeño Institucional, octubre 2018, Departamento Administrativo de Función Pública – DAFP-, Pág. No. 42.

Zona de Riesgo

Una vez se identifican la Probabilidad y el Impacto de los posibles escenarios, se hará un cálculo automático de la Zona de Riesgo.

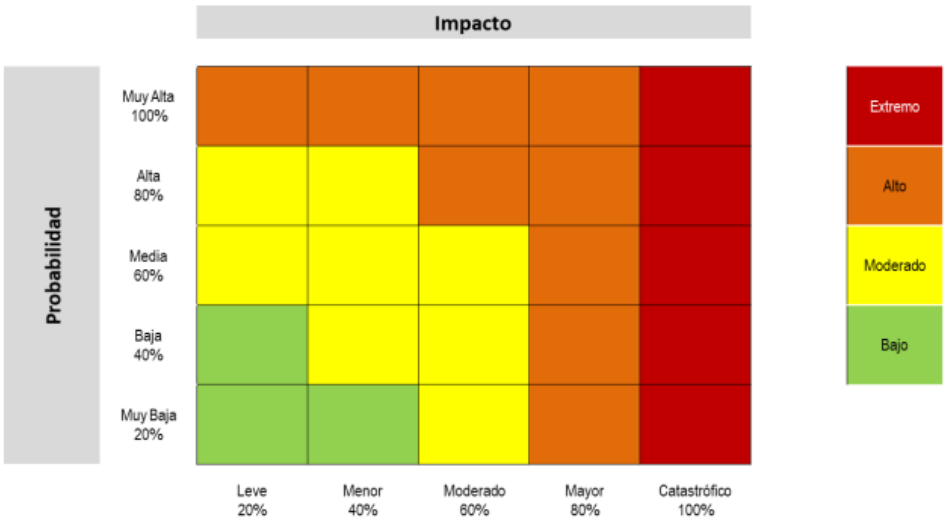
Zona De Riesgo = Probabilidad * Impacto

La Zona de Riesgo permite determinar la severidad de un Incidente a partir del impacto y la probabilidad de su ocurrencia, así como también determinar el riesgo inherente de cada activo.

Este análisis se realiza sin tener presente los controles actuales al materializarse, por lo que debe tomarse el peor de los escenarios posibles.

En la **Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5** de la Función Pública se obtiene:

Figura 14 Matriz de calor (niveles de severidad del riesgo)



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Identificación de Controles

Opciones de Manejo de Riesgo

En esta actividad se identifica la forma de abordar el riesgo, teniendo las siguientes opciones:

- **Asumir el riesgo**, asumir que el riesgo existe y aceptar que puede ocurrir mediante una elección informada.
- **Reducir el Riesgo**, modificar la Probabilidad o el Impacto en caso de ocurrencia de la materialización del Riesgo.
- **Evitar el riesgo,** decidir no iniciar o continuar con la actividad que da lugar al riesgo.
- **Compartir el riesgo,** con otra parte o partes como una aseguradora.

El manejo es como se indica seguidamente:

- Para la Zona de Riesgo Baja se Asume el Riesgo.
- Para la Zona de Riesgo Moderada se Asume o se Reduce el Riesgo.
- Para las Zonas de Riesgo Alta y Extrema se Reduce, se Evita, se Comparte o Se Transfiere el Riesgo.

Ilustración 7. Revisión de Controles

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: Guía de Riegos DAFP, adecuación Autor

Descripción de Controles

En esta actividad se identifican y escogen los controles que van a ser utilizados y propuestos a la dirección para su implementación, con base en el Anexo A:

Número	
1	**Objeto y campo de aplicación**
	Seleccionar los controles dentro del proceso de implementación del Sistema de Gestión de Seguridad de la Información - SGSI
2	**Referencias normativas**
	La ISO/IEC 27000, es referenciada parcial o totalmente en el documento y es indispensable para su aplicación.
3	**Términos y definiciones**
	Para los propósitos de este documento se aplican los términos y definiciones presentados en la norma ISO/IEC 27000.
4	**Estructura de la norma**
	La norma ISO/IEC 27000, contiene 14 numérales de control de seguridad de la información que en su conjunto contienen más de 35 categorías de seguridad principales y 114 controles.
5	**POLITICAS DE SEGURIDAD**
5.1	**Orientación de la dirección para la gestión de la seguridad de la información**
	Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes
5.1.1	**Políticas para la seguridad de la información**
	Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
5.1.2	**Revisión de las políticas para la seguridad de la información**
	Control: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.
6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**
6.1	**Organización interna**
	Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.
6.1.1	**Roles y responsabilidades para la seguridad de información**
	Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.
6.1.2	**Separación de deberes**
	Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.

6.1.3	**Contacto con las autoridades**
	Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes.
6.1.4	**Contacto con grupos de interés especial**
	Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
6.1.5	**Seguridad de la información en la gestión de proyectos**
	Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.
6.2	**Dispositivos móviles y teletrabajo**
	Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.
6.2.1	**Política para dispositivos móviles**
	Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
6.2.2	**Teletrabajo**
	Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
7	**SEGURIDAD DE LOS RECURSOS HUMANOS**
7.1	**Antes de asumir el empleo**
	Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.
7.1.1	**Selección**
	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
7.1.2	**Términos y condiciones del empleo**
	Control: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
7.2	**Durante la ejecución del empleo**
	Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.
7.2.1	**Responsabilidades de la dirección**
	Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
7.2.2	**Toma de conciencia, educación y formación en la seguridad y privacidad de la información.**
	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.

7.2.3	**Proceso disciplinario**
	Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
7.3	**Terminación o cambio de empleo**
	Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato
7.3.1	**Terminación o cambio de responsabilidades de empleo**
	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir
8	**GESTIÓN DE ACTIVOS**
8.1	**Responsabilidad sobre los activos**
	Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
8.1.1	**Inventario de activos**
	Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.
8.1.2	**Propiedad de los activos**
	Control: Los activos mantenidos en el inventario deberían tener un propietario.
8.1.3	**Uso aceptable de los activos**
	Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
8.1.4	**Devolución de activos**
	Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
8.2	**Clasificación de la Información**
	Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.
8.2.1	**Clasificación de la información**
	Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
8.2.2	**Etiquetado de la información**
	Control: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
8.2.3	**Manejo de activos**
	Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
8.3	**Manejo de medios**

8.3.1	**Gestión de medios removibles**
	Control: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
8.3.2	**Disposición de los medios**
	Control: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
8.3.3	**Transferencia de medios físicos**
	Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
9	**CONTROL DE ACCESO**
9.1	**Requisitos de negocio para el control de acceso**
	Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.
9.1.1	**Política de control de acceso**
	Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
9.1.2	**Acceso a las redes y servicios en red**
	Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
9.2	**Gestión de acceso de usuarios**
	Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.
9.2.1	**Registro y cancelación del registro de usuarios**
	Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
9.2.2	**Suministro de acceso de usuarios**
	Control: Se debería implementar un proceso 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.
9.2.3	**Gestión de derechos de acceso privilegiado**
	Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.
9.2.4	**Gestión de información de autenticación secreta de usuarios**
	Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.
9.2.5	**Revisión de los derechos de acceso de los usuarios**
	Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.
9.2.6	**Retiro o ajuste de los derechos de acceso**
	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.

9.3	**Responsabilidades de los usuarios**
	Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.
9.3.1	**Uso de la información de autenticación secreta**
	Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
9.4	**Control de acceso a sistemas y aplicaciones**
	Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.
9.4.1	**Restricción del acceso a la información**
	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.
9.4.2	**Procedimiento de ingreso seguro**
	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
9.4.3	**Sistema de gestión de contraseñas**
	Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas
9.4.4	**Uso de programas utilitarios privilegiados**
	Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
9.4.5	**Control de acceso al código fuente de los programas**
	Control: Se debería restringir el acceso a los códigos fuente de los programas.
10	**CRIPTOGRAFÍA**
10.1	**Controles criptográficos**
	Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.
10.1.1	**Política sobre el uso de controles criptográficos**
	Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
10.1.2	**Gestión de llaves**
	Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
11	**SEGURIDAD FÍSICA Y DEL ENTORNO**
11.1	**Áreas Seguras**
	Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.
11.1.1	**Perímetro de seguridad física**
	Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.
11.1.2	**Controles físicos de entrada**
	Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.

11.1.3	**Seguridad de oficinas, recintos e instalaciones**
	Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
11.1.4	**Protección contra las amenazas externas y ambientales**
	Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
11.1.5	**Trabajo en áreas seguras**
	Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.
11.1.6	**Áreas de despacho y carga**
	Control: Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
11.2	**Equipos**
	Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.
11.2.1	**Ubicación y protección de los equipos**
	Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.
11.2.2	**Servicios de suministro**
	Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
11.2.3	**Seguridad del cableado**
	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño
11.2.4	**Mantenimiento de los equipos**
	Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.
11.2.5	**Retiro de activos**
	Control: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.
11.2.6	**Seguridad de equipos y activos fuera de las instalaciones**
	Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
11.2.7	**Disposición segura o reutilización de equipos**
	Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
11.2.8	**Equipos de usuario desatendidos**
	Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.
11.2.9	**Política de escritorio limpio y pantalla limpia**

	Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
12	**SEGURIDAD DE LAS OPERACIONES**
12.1	**Procedimientos operacionales y responsabilidades**
	Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información
12.1.1	**Procedimientos de operación documentados**
	Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
12.1.2	**Gestión de cambios**
	Control: Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información
12.1.3	**Gestión de capacidad**
	Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura
12.1.4	**Separación de los ambientes de desarrollo, pruebas y operación**
	Control: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
12.2	**Protección contra código malicioso**
	Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
12.2.1	**Controles contra el código malicioso.**
	Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
12.3	**Copias de seguridad**
	Objetivo: Proteger contra la perdida de datos.
12.3.1	**Copias de seguridad de la información**
	Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
12.4	**Registro y seguimiento**
	Objetivo: Registrar eventos y generar evidencia.
12.4.1	**Registro de eventos**
	Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
12.4.2	**Protección de la información de registro**
	Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.
12.4.3	**Registros del administrador y del operador**
	Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.
12.4.4	**Sincronización de relojes**

	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.
12.5	**Control de software operacional**
	Objetivo: Asegurar la integridad de los sistemas operacionales.
12.5.1	**Instalación de software en sistemas operativos**
	Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.
12.6	**Gestión de la vulnerabilidad técnica**
	Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.
12.6.1	**Gestión de las vulnerabilidades técnicas**
	Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
12.6.2	**Restricciones sobre la instalación de software**
	Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.
12.7	**Consideraciones sobre auditorias de sistemas de información**
	Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.
12.7.1	**Controles de auditorías de sistemas de información**
	Control: 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.
13	**SEGURIDAD EN LAS TELECOMUNICACIONES**
13.1	**Gestión de la seguridad en las redes**
	Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.
13.1.1	**Controles de red**
	Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.
13.1.2	**Seguridad de los servicios de red.**
	Control: Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
13.1.3	**Segregación de redes**
	Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.
13.2	**Transferencia de información**
	Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.
13.2.1	**Políticas y procedimientos de intercambio de información**
	Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.
13.2.2	**Acuerdos sobre transferencia de información**

	Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.
13.2.3	**Mensajería electrónica**
	Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.
13.2.4	**Acuerdos de confidencialidad o de no divulgación**
	Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN**
14.1	**Requisitos de seguridad de los sistemas de información**
	Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.
14.1.1	**Análisis y especificación de requisitos de seguridad de la información**
	Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
14.1.2	**Seguridad de servicios de las aplicaciones en redes públicas**
	Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
14.1.3	**Protección de transacciones de los servicios de las aplicaciones**
	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
14.2	**Seguridad en los procesos de desarrollo y soporte**
	Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
14.2.1	**Política de desarrollo seguro**
	Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.
14.2.2	**Procedimientos de control de cambios en sistemas**
	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.
14.2.3	**Revisión técnica de las aplicaciones después de cambios en la plataforma de operación**
	Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
14.2.4	**Restricciones en los cambios a los paquetes de software**
	Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.
14.2.5	**Principios de construcción de sistemas seguros**
	Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
14.2.6	**Ambiente de desarrollo seguro**

	Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
14.2.7	**Desarrollo contratado externamente**
	Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
14.2.8	**Pruebas de seguridad de sistemas**
	Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.
14.2.9	**Pruebas de aceptación de sistemas**
	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.
14.3	**Datos de prueba**
	Objetivo: Asegurar la protección de los datos usados para pruebas.
14.3.1	**Protección de datos de prueba**
	Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.
15	**RELACIÓN CON PROVEEDORES**
15.1	**Seguridad de la información en las relaciones con los proveedores**
	Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.
15.1.1	**Política de seguridad de la información para las relaciones con proveedores**
	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.
15.1.2	**Tratamiento de la seguridad dentro de los acuerdos con proveedores**
	Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
15.1.3	**Cadena de suministro de tecnología de información y comunicación**
	Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
15.2	**Gestión de la prestación de servicios con los proveedores**
	Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.
15.2.1	**Seguimiento y revisión de los servicios de los proveedores**
	Control: Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
15.2.2	**Gestión de cambios en los servicios de proveedores**
	Control: Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.
16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**
16.1	**Gestión de incidentes y mejoras en la seguridad de la información**

	Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
16.1.1	**Responsabilidad y procedimientos**
	Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
16.1.2	**Reporte de eventos de seguridad de la información**
	Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.
16.1.3	**Reporte de debilidades de seguridad de la información**
	Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
16.1.4	**Evaluación de eventos de seguridad de la información y decisiones sobre ellos**
	Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.
16.1.5	**Respuesta a incidentes de seguridad de la información**
	Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
16.1.6	**Aprendizaje obtenido de los incidentes de seguridad de la información**
	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.
16.1.7	**Recolección de evidencia**
	Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO**
17.1	**Continuidad de seguridad de la información**
	Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.
17.1.1	**Planificación de la continuidad de la seguridad de la información**
	Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
17.1.2	**Implementación de la continuidad de la seguridad de la información**
	Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
17.1.3	**Verificación, revisión y evaluación de la continuidad de la seguridad de la información**
	Control: La organización debería verificar a intervalos regulares 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.
17.2	**Redundancias**
	Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información
17.2.1	**Disponibilidad de instalaciones de procesamiento de información.**
	Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
18	**CUMPLIMIENTO**

18.1	**Cumplimiento de requisitos legales y contractuales**
	Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.
18.1.1	**Identificación de la legislación aplicable y de los requisitos contractuales**
	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
18.1.2	**Derechos de propiedad intelectual**
	Control: Se deberían 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.
18.1.3	**Protección de registros**
	Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
18.1.4	**Privacidad y protección de datos personales**
	Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.
18.1.5	**Reglamentación de controles criptográficos**
	Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
18.2	**Revisiones de seguridad de la información**
	Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.
18.2.1	**Revisión independiente de la seguridad de la información**
	Control: El enfoque de la organización 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) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
18.2.2	**Cumplimiento con las políticas y normas de seguridad**
	Control: Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad
18.2.3	**Revisión del cumplimiento técnico**
	Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Controles - ISO/IEC 27002:2013

Responsable de Ejecutar el Control

En esta actividad se identifica la persona o dependencia que tiene la responsabilidad de implementar el control.

Riesgo Residual

El ciclo PHVA establece que es necesario evaluar el proceso para determinar si han sido efectivos los controles, por lo tanto, se evalúan los controles con los indicadores, lo cual reinicia el proceso.

Realimentación del Proceso

Luego de realizado el proceso, se realiza un análisis de indicadores de los controles establecidos para evaluar la efectividad de los mismos y se realimenta el sistema.

Plan De Sensibilización

Finalmente se debe establecer un plan de Sensibilización en riesgos de tal manera que podamos incorporar a los usuarios en el sistema.

Se realizará una capacitación anual.

Plan De Tratamiento De Riesgos

Este es el Plan propuesto para el Tratamiento de Riesgos del año 2023:

Plan de actividades de Inventario, Análisis de Riesgos de Seguridad Digital e Implementación de Controles 2023					
Cronograma de Actividades					
Actividad	**Descripción**	**Responsable**	**Fecha de inicio**	**Fecha de finalización**	**Días dedicados**
Invitación a líderes	Dirección TIC invitará a los líderes de las diferentes dependencias a realizar el proceso de "**Inventario e Identificación de riesgos de Seguridad Digital**"	Dirección TIC	01/02/23	10/03/23	28
Aceptación	Los líderes de las dependencias informan de la aceptación a la Dirección TIC	Secretarios, Directores, Jefes	13/03/23	17/03/23	5
Programación de reuniones	Dirección TIC programará reuniones	Dirección TIC	21/03/23	24/03/23	4
Reuniones "Sensibilización definiciones Seguridad de la Información"	Dirección TIC realiza entrenamiento "**Sensibilización definiciones Seguridad de la Información**"	Dirección TIC, Secretarios, Directores, Jefes	27/03/23	14/04/23	10
Identificación de Activos	Los líderes deben realizar el proceso de identificación de activos	Secretarios, Directores, Jefes	17/04/23	28/04/23	10

Recibo de información identificación de activos	Líderes entregan información de activos, Dirección TIC consolida información	Dirección TIC, Secretarios, Directores, Jefes	28/04/23	28/04/23	1
Reuniones "Riesgo de Seguridad Digital"	Dirección TIC realiza entrenamiento Identificación Riesgos, Amenazas, Vulnerabilidades	Dirección TIC, Secretarios, Directores, Jefes	02/05/23	12/05/23	9
Identificación de riesgos	Líderes aplican la metodología de identificación de los riesgos asociados a los activos de información.	Secretarios, Directores, Jefes	15/05/23	26/05/23	9
Recibo de información Identificación de riesgos	Líderes entregan información de Riesgos a la Dirección TIC, Dirección TIC consolida información	Dirección TIC, Secretarios, Directores, Jefes	26/05/23	26/05/23	1
Reuniones de "Matriz de Riesgo Seguridad Digital"	Dirección TIC realiza entrenamiento "**Matriz de Riesgo Seguridad Digital**"	Dirección TIC, Secretarios, Directores, Jefes	29/05/23	09/06/23	10
Diligenciamiento "Matriz de Riesgos de Seguridad Digital"	Líderes diligencian la **"Matriz de Riesgos de Seguridad Digital"**	Secretarios, Directores, Jefes	13/06/23	23/06/23	8
Recibo de información Medición	Líderes entregan información a la Dirección TIC, Dirección TIC consolida información	Dirección TIC, Secretarios, Directores, Jefes	23/06/23	23/06/23	1

Reuniones de control	Dirección TIC realiza entrenamiento "**Identificación e Implementación de Controles**"	Dirección TIC, Secretarios, Directores, Jefes	26/06/23	07/07/23	9
Control	Líderes identifican acciones que se deben tomar para controlar o mitigar los riesgos a que se ven expuestos los activos de información con el fin de disminuir la posibilidad o las consecuencias de su materialización. Deben ser suficientes, efectivos y oportunos, identificar si son manuales, automáticos, discrecionales, obligatorios, preventivos o correctivos.	Secretarios, Directores, Jefes	10/07/23	21/07/23	9
Implementación de Controles	Secretarios, Directores, Jefes deben proveer los recursos para establecer los controles de sus dependencias respectivas	Secretarios, Directores, Jefes	24/07/23	31/10/23	69
Recibo de información Control	Líderes entregan información de Controles a la Dirección TIC, Dirección TIC	Dirección TIC, Secretarios, Directores, Jefes	31/10/23	31/10/23	1

	consolida información				
Reuniones de monitoreo	Dirección TIC realiza entrenamiento de "**Monitoreo**"	Secretarios, Directores, Jefes, Dirección TIC	01/11/23	17/11/23	11
Diseño y consolidación de información de Monitoreo	Líderes, Secretarios, Directores, Jefes, Dirección TIC contemplan un proceso de seguimiento efectivo que facilite la rápida detección y corrección de las deficiencias en la administración de los riesgos identificados. Líderes, Secretarios, Directores, Jefes establecen indicadores que evidencien la efectividad del sistema de administración de riesgos adoptado. Dirección TIC asegura que los controles estén funcionando en forma oportuna, efectiva y eficiente. Líderes, Secretarios, Directores, Jefes aseguran que los	Secretarios, Directores, Jefes, Dirección TIC	20/11/23	30/11/23	9

	riesgos residuales se encuentren en los niveles de aceptación establecidos. Dirección TIC Lleva un registro de incidentes que contemple: Bases de datos y datos comprometidos, titulares, fecha del incidente y de descubrimiento, acciones correctivas realizadas y responsables.				
Preparación y Entrega de informe	Preparación y Entrega de informe de los resultados del proceso y controles establecidos	Dirección TIC	01/12/23	31/12/23	19