TABLA DE CONTENIDO

INTRODUCCIÓN

La meta principal de la Gestión y Evaluación del Riesgo de seguridad de información es proteger a la organización y su habilidad de manejar su misión; los riesgos deben ser estimados en el contexto del negocio, y las interrelaciones con otras funciones de negocios, tales como recursos humanos, planeación, producción, procedimientos, administración, TI, finanzas, entre otros y los clientes deben ser identificados para lograr una imagen general y completa de estos riesgos. Además, el proceso no solo debe de ser manejado como una función técnica generada por los expertos en tecnología que operan y administran los sistemas, sino como una función esencial de administración por parte de toda la organización.

Objetivo del Manual

Establecer la metodología para evaluar y tratar los Riesgos de la Seguridad de Información en el Instituto Nacional Penitenciario y Carcelario INPEC para garantizar la confidencialidad, disponibilidad e integridad de la información, teniendo en cuenta los lineamientos descritos en la Norma Técnica Colombiana NTC-ISO/IEC 27001. Versión Oficial

Objetivos Específicos

- Aplicar técnicas de valoración de Riesgos de la Seguridad de la Información, para identificar los relacionados con la perdida de confidencialidad, integridad y disponibilidad dentro del Sistema de Gestión de Seguridad de la Información.
- Identificar vulnerabilidades que dan origen al riesgo, eliminarlo o modificarlo de tal forma que no se genere en una amenaza para los activos de información del Instituto.

Glosario

- **Administración de Riesgos de la Seguridad de la Información:** es el proceso de identificar, comprender, evaluar y mitigar los riesgos y sus vulnerabilidades subyacentes y el impacto en la información, los sistemas de información y las organizaciones que dependen de la información para sus operaciones.

- **Activo:** con relación con la Seguridad de la Información, se refiere a cualquier información que una organización o empresa considera importante para la misma; ya que puede estar comprendida en; Bases de datos, equipos de red, personas, infraestructura, etc.

- **Amenaza:** es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS).

- **Análisis de Riesgo:** proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

- **Confidencialidad:** es la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados. Asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

- **Control:** cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos.

- **Disponibilidad:** característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. La disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

- **Evaluación de riesgos:** analiza la probabilidad, impacto y efecto de todos los riesgos conocidos que pueden afectar el proyecto, como también las acciones correctivas que deben llevarse a cabo en caso que el riesgo llegara efectivamente a ocurrir.

- **Evento de Seguridad de la Información:** identificación del estado de un sistema, servicio o red, que indica una posible violación de la Política de Seguridad de la Información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

- **Gestión de riesgos:** actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos

- **Identificación del riesgo:** elemento de control que posibilita conocer los eventos potenciales estén o no bajo el control del Instituto, que ponen el riesgo el logro de la misión estableciendo los agentes generadores las causas y los efectos de su ocurrencia. Se puede entender como el proceso que permite determinar qué podría suceder, por qué sucederá y de qué manera se llevara a cabo.

- **Impacto:** resultados y consecuencias de que se materialice un riesgo.

- **Integridad:** propiedad que busca mantener los datos libres de modificaciones no autorizadas.

- **Plan de Tratamiento de Riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

- **Probabilidad:** medida para estimar la ocurrencia del riesgo.

- **Riesgo:** posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

- **Riesgo residual:** riesgo que permanece tras el tratamiento del riesgo.

- **Sistema de Gestión de la Seguridad de la Información (SGSI):** conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de Seguridad de la Información y alcanzar dichos objetivos, basándose en un enfoque de Gestión del Riesgo y de mejora continua.

- **Seguridad de la Información:** preservación de la confidencialidad, la integridad y la disponibilidad de la información.

- **Tratamiento: c**ualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

- **Tratamiento de riesgos:** proceso de modificar el riesgo, mediante la implementación de controles.

- **Valoración del riesgo: p**roceso de análisis y evaluación del riesgo.

- **Vulnerabilidad:** debilidad de un activo o control que puede ser explotada por una o más amenazas.

1. Proceso de Gestión de Riesgo del SGSI

Responde al requisito mínimo de la norma NTC-ISO/IEC 27001: 2013, específicamente en el Capítulo 6, numeral 6.1.2 Valoración de Riesgos de la Seguridad de la Información:

La organización debe definir y aplicar un proceso de Valoración de Riesgos de la Seguridad de la Información que:

a) Seleccionar las opciones apropiadas de tratamiento de Riesgos de la Seguridad de la Información, se deben tener en cuenta los resultados de la Valoración de Riesgos.
b) Producir una declaración de aplicabilidad que contenga los controles necesarios y la justificación de las inclusiones, ya sea que se implementen o no, y la justificación para las exclusiones de los controles del Anexo A.
c) Formular un Plan de Tratamiento de Riesgos de la Seguridad de la Información.
d) Obtener la aprobación del Plan de Tratamiento de Riesgos de la Seguridad de la Información y la aceptación de los riesgos residuales de la Seguridad de la Información
e) La organización debe conservar información documentada sobre el proceso de tratamiento de Riesgos de la Seguridad de la Información

En su capítulo 8, numeral 8.2. Valoración de Riesgos de la Seguridad de la Información:

La organización debe llevar a cabo Valoraciones de Riesgos de la Seguridad de la Información a intervalos planificados o cuando se propagan u ocurran cambios significativos, teniendo en cuenta los criterios establecidos en el numeral 6.1.2 a).
La organización debe conservar información documentada de los resultados de las valoraciones de Riesgos de la Seguridad de la Información.

En su capítulo 8, numeral 8.3. Tratamiento de Riesgos de la Seguridad de la Información. La organización debe implantar el Plan de Tratamiento de Riesgos de la Seguridad de la Información.

La organización debe conservar información documentada de los resultados del Tratamiento de Riesgos de la Seguridad de la Información.

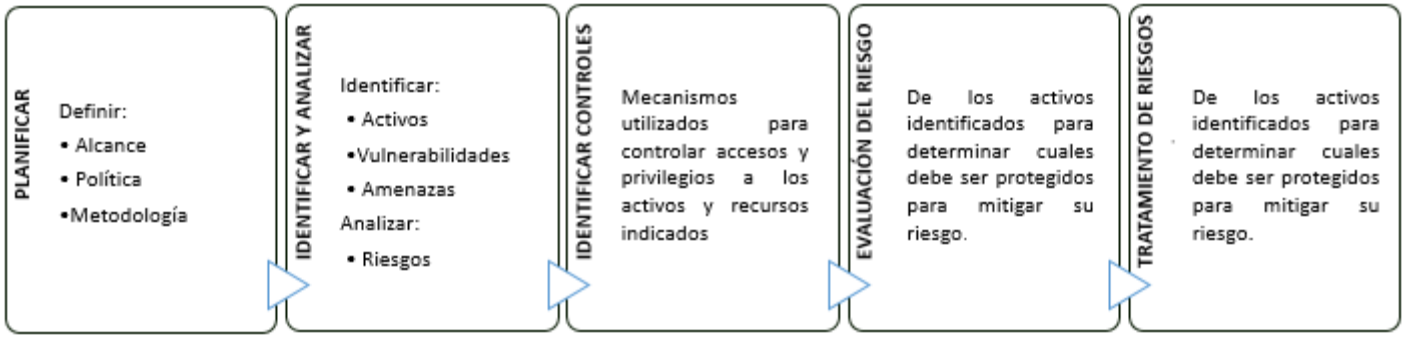

Figura No. 1 Gestión del Riesgo de Seguridad de la Información

1.1. ¿Qué es el Riesgo?

De acuerdo con la norma NTC-ISO/IEC 27000:2014 se define el riesgo como la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. De igual manera el objetivo general de dicha norma es gestionar el riesgo para identificar y establecer controles efectivos que garanticen la confidencialidad, integridad y disponibilidad de la información.

1. 1. 1. Riesgos de la seguridad de la información

Combinación de amenazas y vulnerabilidades en el ambiente digital y dado su naturaleza dinámica incluye también aspectos relacionados con el entorno físico. En la tipificación de dichos riesgos, se encuentran los siguientes:

- Perdida de confidencialidad del activo de información.
    - Divulgación de la información no autorizada.
    - Acceso no autorizado a la información.

- Pérdida de la integridad del activo de información.
    - Inconsistencias en la información
    - Modificación no autorizada

- Pérdida de la disponibilidad del activo de información.

- No disponibilidad de la información debido a fallas técnicas o fallas en el software.
- Pérdida de información.

1. 1. 2. Riesgos de la Privacidad de los datos personales

Afectan a las personas cuyos datos son tratados y que se resume en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización ilícita o fraudulenta de los mismos. Como riesgo se encuentra lo siguiente:

- Inadecuado tratamiento de datos: sobre los afectados (invasión en su vida privada, comunicar datos a terceros sin autorización, no haber realizado un procedimiento adecuado de tratamiento, mantener los datos más tiempo que el estrictamente necesario para la finalidad que se recogieron).
- No cumplir con la legislación de protección de datos, o servicios de la sociedad de la información.

1. 1. 3. Factores de riesgo

Son aquellos que pueden afectar la confidencialidad, la integridad o la disponibilidad de la información del Instituto Nacional Penitenciario y Carcelario (INPEC), en relación con las vulnerabilidades de los activos de información, las causas o amenazas que puedan determinar la materialización de un evento.

Factor de Riesgo	Descripción
Humano	Personas que interactúan día a día con los sistemas de información de la organización y que se encuentran relacionadas con la ejecución de los procesos de forma directa o indirecta.
Procesos	Sucesión e interrelación de pasos, tareas y decisiones, con valor agregado, que se vinculan entre sí para transformar un insumo en un producto o servicio.
Tecnología	Conjunto de activos de hardware y software con capacidad de procesamiento de datos, para la ejecución de los procesos.
Infraestructura	Conjunto de medios técnicos, servicios e instalaciones necesarios para el desarrollo de una actividad o para que un lugar pueda ser utilizado.
Factores Externos	Relación existente entre una organización con empresas de outsourcing que generan prestaciones de servicio, proveedores, clientes, entidades reguladoras y otros.

Tabla No. 1 – Factores de Riesgo.

1. 1. 4. Tipos de Riesgo

Son aquellos asociados con las actividades realizadas diariamente al interior de la organización.

Tipo de Riesgo	Descripción
Misional	Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
Imagen	Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
Operativos	Comprende los riesgos relacionados tanto con la parte operativa como técnica de la entidad, incluye riesgos provenientes de deficiencias en los sistemas de información, en la definición de los procesos, en la estructura de la entidad, la desarticulación entre dependencias, lo cual conduce a ineficiencias, oportunidades de corrupción e incumplimiento de los compromisos institucionales.
Financieros	Se relacionan con el manejo de los recursos de la entidad que incluye, la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes de cada entidad. De la eficiencia y transparencia en el manejo de los recursos, así como su interacción con las demás áreas dependerá en gran parte el éxito o fracaso de toda entidad
de Cumplimiento	Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
de Tecnología	Se asocian con la capacidad de la Entidad para que la tecnología disponible y proyectada satisfaga las necesidades actuales y futuras de la entidad y soporte el cumplimiento de la misión. (Configuración, compatibilidad, desarrollos, software, hardware, diseños)
de Seguridad	Combinación de amenazas y vulnerabilidades en el ambiente digital y dado su naturaleza dinámica incluye también aspectos relacionados con el entorno físico
Riesgos de Privacidad	Afectan a las personas cuyos datos son tratados y que se concreta en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización ilícita o fraudulenta de los mismos.

Tabla No. 2 – Tipos de Riesgos.

1. 1. 5. ¿Qué es un Control?

Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una Entidad.

TIPOS DE CONTROLES	DESCRIPCIÓN
Físico	Es la implementación de medidas de seguridad en una estructura definida usada para prevenir o detener el acceso no autorizado a material confidencial. Ejemplos de los controles físicos son: • Cámaras de circuito cerrado • Sistemas de alarmas térmicos o de movimiento • Guardias de seguridad • Identificación con fotos • Puertas de acero con seguros especiales • Biométrica (incluye huellas digitales, voz, rostro, iris, escritura a mano y otros métodos automatizados utilizados para reconocer individuos). • Seguridad de oficinas. • Seguridad en el cableado estructurado
Técnico	Los controles técnicos utilizan la tecnología como una base para controlar el acceso y uso de datos confidenciales a través de una estructura física y sobre la red. Los controles técnicos son mucho más extensos en su ámbito e incluyen tecnologías tales como: • Criptografía • Tarjetas inteligentes • Autenticación a nivel de la red • Listas de control de acceso (ACLs) • Software de auditoría de integridad de archivos • Antivirus • Copias de respaldo – respaldo de la información • Protección de la información • Control de software • Licenciamiento de Software • Gestión de seguridad en las redes de datos • Seguridad en los sistemas de información • Gestión de activos (Inventario, identificación de propietarios de los activos.) • Gestión de acceso a los usuarios (Acceso a la red y a servicios de red, autenticación, roles) • Gestión de contraseñas. • Acceso a códigos fuente de programas.
Administrativo	Definen los factores humanos de la seguridad. Incluye todos los niveles del personal dentro de la organización y determina cuáles usuarios tienen acceso a qué recursos e información usando medios tales como: • Entrenamiento y conocimiento

	• Planes de recuperación y preparación para desastres • Estrategias de selección de personal y separación • Registro y contabilidad de personal • Políticas de seguridad. • Responsabilidades de los usuarios

Tabla No.3 – Tipos de Controles.

2. Metodología de Valoración del Activo y Análisis de Riesgos de Seguridad de la Información

La presente metodología de Valoración del Activo y Análisis de Riesgos de la Seguridad de la Información, contribuyen al Sistema Integrado de Gestión abarcando el siguiente aspecto:
Se identifican los activos de información en el flujo de cada proceso, teniendo en cuenta las Tablas de Retención Documental, con el objetivo de valorarlos e identificar los Riesgos de la Seguridad y Privacidad de la Información asociada a los factores.

2.1. ¿Qué son los Activos?

Los activos son los recursos del Sistema de Seguridad de la Información NTC-ISO/IEC 27001:2013, necesarios para que una organización funcione y consiga los objetivos que se ha propuesto la Alta Dirección. Los activos se encuentran relacionados, directa o indirectamente, con las demás entidades según el siguiente esquema:

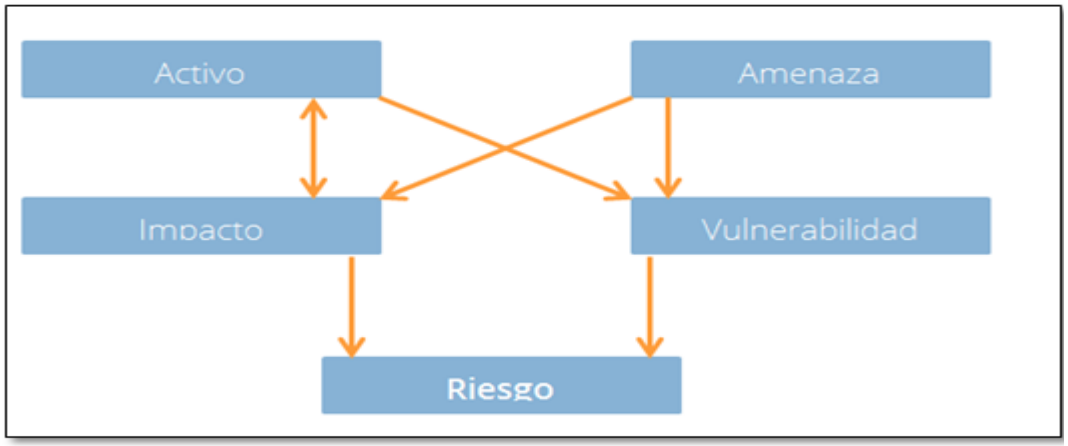

Figura No. 2 – Relación de Activos.

2.2. Características de los activos

TIPO DE ACTIVOS	DESCRIPCIÓN
Activos Esenciales	**Datos importantes o vitales para la Administración de la Entidad:** Aquellos que son esenciales, imprescindibles para la continuidad de la entidad; es decir que su carencia o daño afectaría directamente a la entidad, permitiría reconstruir las misiones críticas o que sustancian la naturaleza legal de la organización o de sus usuarios. **Datos de carácter personal:** Cualquier información concerniente a personas físicas identificadas o identificables. Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su intimidad personal y familiar (Ley 1581 de 2012). **Datos Clasificados o Calificados:** Aquellos sometidos a normativa específica de control de acceso y distribución o cuya confidencialidad es tipificada por normativa interna o legislación nacional (Ley 1712 de 2014).
Datos / Información	**Que es almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.** Ejemplo: Copias de Respaldo, Ficheros, Datos de Gestión Interna, Datos de Configuración, Credenciales (Contraseñas), Datos de Validación de Credenciales (Autenticación), Datos de Control de Acceso, Registros de Actividad (Log), Matrices de Roles y Privilegios, Código Fuente, Código Ejecutable, Datos de Prueba.
Hardware / Infraestructura	**Medios físicos, destinados a soportar directa o indirectamente los servicios que presta la entidad, siendo depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.** Ejemplo: Servidores (host), Equipos de Escritorio (Pc), Equipos Portátiles (Laptop), Dispositivos Móviles, Equipos de Respaldo, Periféricos, Dispositivos Criptográficos, Dispositivos Biométricos, Servidores de Impresión, Impresoras, Escáneres, Equipos Virtuales (vhost), Soporte de la Red (Network), Módems, Concentradores, Conmutadores (switch), Encaminadores (router), Pasarelas (bridge), Firewall, Central Telefónica, Telefonía IP, Access Point, Discos Duros removible.
Software / Aplicaciones Informáticas	**Que gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.** Ejemplo: Desarrollo Inhouse, Desarrollo Subcontratado, Estándar, Navegador, Servidor de Presentación (www), Servidor de Aplicaciones (app), Cliente de Correo Electrónico, Servidor de Correo Electrónico, Servidor de Ficheros (file), Sistemas de Gestión de Bases de Datos (dbms), Monitor Transaccional,

	Ofimática, Antivirus, Sistema Operativo (SO), Servidor de Terminales, Sistema de Backup o Respaldo, Gestor de Máquinas Virtuales, Software de Contabilidad, Software Administrativo.
Servicios	**Funciones que permiten suplir una necesidad de los usuarios (del servicio).** Ejemplo: Página Web, Correo Electrónico, Acceso Remoto, almacenamiento de ficheros, transferencia de ficheros, intercambio electrónico de datos, Gestión de Identidades (altas y bajas de usuarios del sistema), Gestión de Privilegios, Intercambio electrónico de datos, PKI (Infraestructura de Clave Pública).
Personas	Usuarios Internos, Usuarios Externos, Operadores, Administradores de Sistemas, Administradores de Comunicaciones, Administradores de Bases de Datos, Administradores de Seguridad, Líder de Proyectos, Programadores, Contratistas, Proveedores. En general, todos aquellos que tengan acceso de una manera u otra a la entidad.
Soportes de Información	**Dispositivos físicos electrónicos o no que permiten almacenar información de forma permanente o durante largos periodos de tiempo.** Ejemplo: Discos, Discos Virtuales, Almacenamiento en Red (san), Memorias USB, CDROM, DVD, Cinta Magnética (tape), Tarjetas de Memoria, Tarjetas Inteligentes, Material Impreso, Microfilmaciones.
Redes de Comunicaciones	**Instalaciones dedicadas como servicios de comunicaciones contratados a terceros o medios de transporte de datos de un sitio a otro.** Ejemplo: Red Telefónica, Red Inalámbrica, Telefonía Móvil, Satelital, Red Local (LAN), Red Metropolitana (MAN), Internet, Radio Comunicaciones, Punto a Punto, ADSL, Red Digital (rdsi).
Claves Criptográficas	**Esenciales para garantizar el funcionamiento de los mecanismos criptográficos.** Ejemplo: Claves de Cifrado, Claves de Firma, Protección de Comunicaciones (Claves de Cifrado de Canal), Cifrado de Soportes de Información, Certificados Digitales, Certificados de Claves, Claves de Autenticación.
Equipos Auxiliares	**Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.** **Ejemplo:** Fuentes de alimentación, generadores eléctricos, equipos de climatización, sistemas de alimentación ininterrumpida (UPS), cableado, cable eléctrico, fibra óptica, equipos de destrucción de soportes de información, mobiliarios, armarios, cajas fuertes.
Instalaciones	Lugares donde albergan los sistemas de información y comunicaciones.

Tabla No. 4 – Tipos de Activos-

2.3. ¿Qué es una Vulnerabilidad?

Las vulnerabilidades de un sistema son las debilidades o puertas abiertas para posibles ataques, de ahí que sea tan importante tenerlas en cuenta; en cualquier momento podrían ser aprovechadas. Podemos clasificar cuatro:

Calificación	Definición
Crítica	Vulnerabilidad que puede permitir la propagación de un virus de Internet sin la acción del usuario.
Importante	Vulnerabilidad que puede poner en peligro la confidencialidad, integridad o disponibilidad de los datos de los usuarios, o bien, la integridad o disponibilidad de los recursos de procesamiento.
Moderada	El impacto se puede reducir en gran medida a partir de factores como configuraciones predeterminadas, auditorías o la dificultad intrínseca en sacar partido a la vulnerabilidad.
Baja	Vulnerabilidad muy difícil de aprovechar o cuyo impacto es mínimo.

Tabla No. 5 – Calificación de Vulnerabilidades.

2.4. ¿Qué es una Amenaza?

Una amenaza es un evento que pueden causar alteraciones a la información de la organización, ocasionándole pérdidas materiales, económicas, de la misma información y de prestigio. Estas son consideradas como ajenas a un sistema cualquiera, debido a que nadie planea un sistema con amenazas, por el contrario, se establecen medidas para protegerse de esas amenazas aunque es prácticamente imposible controlarlas y más aún eliminarlas.

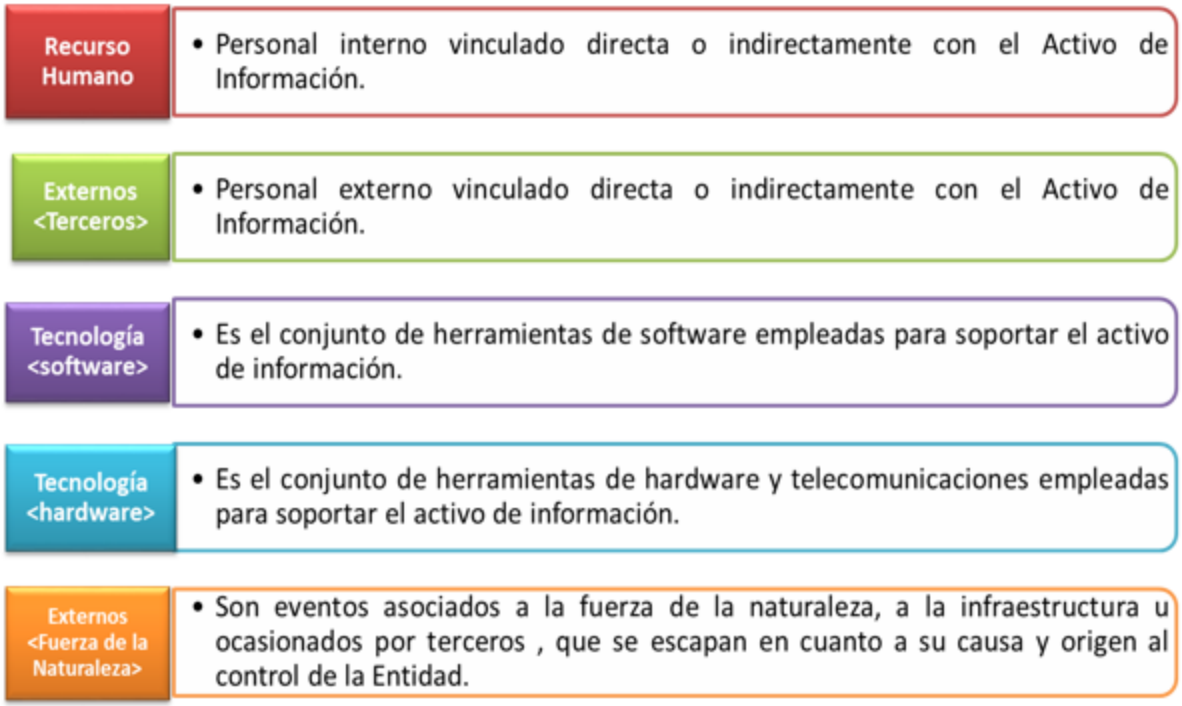

Figura No. 3 Tipos de Amenazas-

2.5. Análisis de Riesgos incluye la identificación de Vulnerabilidades y Amenazas.

Pueden determinar la materialización de un evento, sus posibles consecuencias o afectación, relacionándolos con la identificación del Riesgo de Seguridad o Privacidad de la Información.

TIPO DE ACTIVO	VULNERABILIDADES	AMENAZAS
HARDWARE	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información, virus, fallos del sistema y de las aplicaciones.
	Susceptibilidad a la humedad, falta de ventilación polvo y la suciedad.	Mal funcionamiento de los equipos, dispositivos, pérdida de velocidad, cortos circuitos, bloqueo de equipos, sobrecalentamiento apagado inesperado.
	Incumplimiento de las condiciones técnicas y/o ambientales provistas por el fabricante.	Error en la configuración y/o uso.
	Susceptibilidad a las variaciones de voltaje.	Fallas o pérdida del suministro de energía, sin tener un respaldo.
	Almacenamiento de equipos sin protección.	Hurtos de dispositivos medios o documentos.

	Falta de capacidad de almacenamiento.	Perdida de información, mal funcionamiento y rendimiento de los dispositivos.
	Falta de conciencia respecto a la seguridad de la información.	Sabotaje Interno.
SOFTWARE	Asignación errada de los derechos de acceso.	Abuso de los derechos.
	Ausencia de mecanismos de identificación y validación , de usuario.	Falsificación de derechos.
	Software ilegal.	Uso de software falso o copia/Manipulación con software, virus, problemas legales y sanciones económicas.
	Descarga y uso no controlado de software.	Manipulación con software.
	Ausencia de copias de respaldo.	Manipulación con software, pérdida de información.
	Desactualización del Antivirus.	Infección de software malicioso, pérdida de datos, lentitud, robo de identidad, fraude.
	Desactualización de los Gestores de Base de Datos.	Cifrado información del servidor, solicitud de un rescate - ransomware- uso de sistemas como plataforma de ataque hacia otros sistemas.
	Falta de conciencia respecto a la seguridad de la información.	Sabotaje Interno, fraude, robo de información.
INFORMACIÓN	Acceso no controlado a la información sensible.	Robo/perdida/mal uso de la información.
	Afectación de la integridad, de los datos.	Alteración de la Información/Destrucción de Información/Modificación de los permisos y privilegios de acceso.
	Información insuficiente o desactualizada.	Incumplimiento de procedimientos y/o tareas internas/ Información negativa que afecte la imagen de la entidad ante la opinión pública/personal no calificada para el tratamiento de la información.
	Ausencia o insuficiencia de políticas, procedimientos, y directrices de seguridad.	Ataques desde el interior de la Institución/Sabotaje interno/vandalismo.
RED	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento).	Saturación del sistema de información.
	Arquitectura insegura de la red.	Saturación, peticiones, virus, colisiones en el envió y recibo de datos.
	Conexiones de red pública sin protección.	Uso no autorizado del equipo, virus.
	Conexión deficiente de los cables.	Fallas del equipo de telecomunicaciones.
	Transferencia de contraseñas en claro.	Espionaje remoto.
	Ausencia de identificación y autentificación de emisor y receptor.	Falsificación de derechos.
	Punto único de fallas.	Fallas del equipo de telecomunicaciones.
RECURSO HUMANO	Entrenamiento insuficiente en seguridad de la información.	Sabotaje Interno/fuga interna de información/daño de activos.
	Falta de políticas / normas / procedimientos de seguridad de la información.	Sabotaje Interno/fuga interna de información/daño de activos.

	Uso incorrecto de software y hardware.	Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)/Almacenamiento Inapropiado de la Información/daños físicos de equipos/conocimiento inapropiado para el manejo de los mismos.
	Trabajo no supervisado del personal externo o de limpieza.	Hurto de medios o documentos.
	Ausencia del personal.	Retraso en tareas y metas,/personal sin perfil/Falta de continuidad en los procesos/exceso de trabajo/trabajo bajo estrés.
	Procedimientos inadecuados de la contratación.	Destrucción de equipos o medios.
	Falta de conciencia acerca de la seguridad de la información.	Robo de la Información/Robo de activos/fraude.
SERVICIOS	Denegación del servicio.	Servicio o recurso no disponible para los usuarios. Pérdida de la conectividad de la red o sobrecarga de los recursos informáticos del sistema del usuario./colapso total o parcialmente en los servidores para que éste no pueda dar respuesta a los comandos solicitados.
	Eventos catastróficos, inundaciones, incendios, terremotos.	Interrupción completa de los servicios ofrecidos por la organización.
	Inadecuado control de acceso lógico y/o físico a los activos de información.	Falla en el Software-Aplicación.
	Ausencia de registros de log - bitácoras.	Error en el uso/falta de evidencia frente a un vandalismo o catástrofe natural.
	Falta de conciencia acerca de la seguridad dela información.	Robo de la Información/Robo de activos/fraude.
INSTALACIONES LUGAR	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.	Destrucción de equipos o medios, sustracción de activos.
	Ubicación en un área susceptible de inundación.	Inundación.
	Red eléctrica inestable.	Pérdida de suministro de energía.
	Ausencia de protección física de la edificación puertas y ventanas.	Hurto de activos de información.
ORGANIZACIÓN	Ausencia de procedimiento formal para el registro y retiro de usuarios.	Abuso de derechos.
	Ausencia de proceso formal para la revisión de los derechos de acceso.	Abuso de los derechos.
	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con clientes o terceras partes.	Abuso de los derechos.
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de información.	Abuso de los derechos.
	Ausencia de auditorías (supervisiones) regulares.	Abuso de los derechos.

	Ausencia de planes de continuidad.	Falla del equipo.
	Ausencia de políticas sobre el uso de correo electrónico.	Error en el uso.
	Ausencia de procedimientos para el manejo de información clasificada.	Error en el uso.
	Ausencia de responsabilidades en seguridad de la información en la descripción de los cargos	Error en el uso.
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.	Uso de software falsificado o copiado.

Tabla No. 6 –Análisis de Vulnerabilidades y Amenazas por tipos de activos.

2.6. Valoración del Activo de Información

Se realiza mediante la identificación del impacto en el Instituto Nacional Penitenciario y Carcelario por la pérdida de las propiedades, principios o fundamentos de la Seguridad de la Información, teniendo en cuenta la siguiente tabla de criterios:

Criterio	Valor	Descripción
INSIGNIFICANTE	**= 0 y < 1**	Información que ha sido calificada como de conocimiento público. Esta información puede ser entregada o publicada con ciertas restricciones dadas por el propietario del activo a los funcionarios o a cualquier persona sin que implique daños a terceros ni a las actividades y procesos del INPEC. El conocimiento o divulgación no autorizado de la información que gestiona este activo no tiene ningún impacto negativo en los procesos del Instituto.
MODERADO	**= 1 y < 3**	Información manejada por los funcionarios del INPEC para realizar sus labores en los procesos y que no puede ser conocida, manipulada, alterada por terceros sin autorización del propietario del activo. El conocimiento, divulgación o indisponibilidad no autorizada de la información que gestiona este activo impacta negativamente al Instituto.
ALTO	**= 3 y < 5**	Información manejada por los funcionarios del INPEC para realizar sus labores en los procesos y que no puede ser conocida, manipulada, alterada por terceros sin autorización del propietario del activo. El conocimiento, divulgación o indisponibilidad no autorizada de la información que gestiona este activo impacta negativamente al Instituto.
EXTREMO	**5**	Existencia de información vital o esencial a nivel de pérdida de confidencialidad, integridad y disponibilidad por consiguiente debe tener una mayor protección. El conocimiento, divulgación o indisponibilidad no autorizada de la información que gestiona este activo impacta negativamente al Instituto.

Tabla No. 7 Valoración del Activo

2.7. Escalas de niveles de Probabilidad e Impacto

a) Probabilidad: posibilidad de ocurrencia del riesgo.

Se establece los niveles de probabilidad de ocurrencia para cada Riesgo de la Seguridad de la Información teniendo en cuenta los siguientes criterios de valoración:

Nivel		Descripción	Frecuencia
1	Rara vez	Evento que ocurre solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.
2	Improbable	El evento podría ocurrir en algún momento.	Al menos una vez en los últimos 5 años.
3	Moderado	El evento puede ocurrir en algún momento.	Al menos una vez en los últimos 2 años.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos una vez en el último año.
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de una vez al año.

Tabla No. 8- Niveles de probabilidad

b) Impacto: las consecuencias que puede ocasionar a la organización la materialización del Riesgo de Seguridad de la Información, se personaliza con la representación de los siguientes niveles:

Nivel	Descriptor	Descripción	Seguridad y Privacidad de la Información
5	Catastrófico	Si el hecho llegara a presentarse tendría desastrosas consecuencias o efectos sobre la organización.	Afecta toda la organización. Multas por incumplimiento de la Legislación. Suspensión de las actividades misionales de la organización.
4	Mayor	Si el hecho llegara a presentarse tendría altas consecuencias o efectos sobre la organización.	Afecta varios conjuntos de datos personales o procesos de la organización.
3	Moderado	Si el hecho llegara a presentarse tendría medianas consecuencias o efectos sobre la organización.	Afecta un conjunto de datos personales o el proceso.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la organización.	Afecta a un grupo de trabajo, a una persona, grupo de personas o algunas actividades del proceso.
1	Insignificante	Si el hecho llegara a presentarse tendría consecuencias o efectos mínimos sobre la organización	Afecta a una actividad del proceso.

Tabla No. 9- Niveles de Impacto

Con base en la determinación de la probabilidad y la valoración del impacto, se establecen los niveles de Riesgos de la Seguridad y Privacidad de la Información:

RESULTADOS DE LA CALIFICACIÓN DEL RIESGO						
PROBABILIDAD	**VALOR**	**ZONA DE RIESGO RESIDUAL**				
Casi seguro	5	Alto	Alto	Extremo	Extremo	Extremo
Probable	4	Moderado	Alto	Alto	Extremo	Extrema
Moderado	3	Inferior	Moderado	Alto	Alto	Extrema
Improbable	2	Inferior	Inferior	Moderado	Alto	Alto
Rara vez	1	Inferior	Inferior	Moderado	Moderado	Alto
		Insignificante	**Menor**	**Moderado**	**Mayor**	**Catástrofico**
		1	2	3	4	5

Tabla No. 10 Resultado de la Calificación del Riesgo.

Nivel del riesgo

EXTREMO	Se requiere de acciones inmediatas.
ALTO	Se requiere de acciones a corto plazo.
MODERADO	Se requiere de acciones a mediano plazo.
INFERIOR	Se requiere de acciones a largo plazo.

TABLA No. 11 Nivel del Riesgo.

DIMENSIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN	ACCIÓN
I: Zona de riesgo insignificante asumir el riesgo.	Permite a la entidad asumirlo. Es decir, el riesgo se encuentra en un nivel que puede aceptarlo sin necesidad de tomar otras medidas de control diferentes a las que se poseen.

M: zona de riesgo moderada, asumir el riesgo y reducir el riesgo.	Si el riesgo se sitúa en cualquiera de las otras zonas (riesgo, moderada o alta), se deben tomar medidas para llevar en lo posible los riesgos a la zona moderada o baja. Siempre que el riesgo sea calificado con impacto catastrófico, la entidad debe diseñar planes de contingencia, para protegerse en caso de su ocurrencia.
A: zona de riesgo alta, reducir el riesgo, compartir o transferir	Si el riesgo se sitúa en cualquiera de las otras zonas (riesgo, moderada o alta), se deben tomar medidas para llevar en lo posible los riesgos a la zona moderada o baja. Siempre que el riesgo sea calificado con impacto catastrófico, la entidad debe diseñar planes de contingencia, para protegerse en caso de su ocurrencia.
E: zona de riesgo extrema, evitar el riesgo, reducir el riesgo, compartir o transferir.	Es aconsejable eliminar la actividad que genera el riesgo en la medida que sea posible. De lo contrario, se deben implementar controles de prevención para evitar la probabilidad del riesgo, de protección para disminuir el impacto o compartir o transferir el riesgo si es posible a través de pólizas de seguros u otras opciones que estén disponibles.

Tabla No 12 - Interpretación del Riesgo

ADMINISTRACIÓN DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	DESCRIPCIÓN
APLICAR CONTROLES	De seguridad obtenidos del Anexo A de la norma 27001 con el objetivo de minimizar la probabilidad de que ocurra el riesgo.
TRANSFERIR EL RIESGO	A otras personas, es decir, comprando un seguro con una compañía aseguradora, al realizarse de esta manera el riesgo que se transfiere es económico. Más sin embargo el riesgo material no se traslada.
EVITAR EL RIESGO	Tomar las medidas encaminadas a prevenir su materialización, al detener la ejecución de la actividad que genera un elevado riesgo, o al hacerla de forma diferente.
ACEPTAR EL RIESGO	Opción para aquellos casos en lo que el costo de eliminar el riesgo es mayor que el daño que causará. En este caso el responsable deberá decidir si acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

Tabla No. 13. – Opciones de Manejo del Riesgo

3. Roles y responsabilidades.

Esta sección describe los roles y responsabilidades claves del personal requerido para soportar y participar en los procesos de Gestión y Evaluación del Riesgo de la Seguridad y Privacidad de la Información.

- **La Dirección General** es responsable de apoyar el proceso en su totalidad, asegura la disponibilidad de los recursos necesarios para el logro de los objetivos , incorpora los resultados de la evaluación de riesgos en el proceso de toma de decisiones.
- **La Gestión y Evaluación de Riesgos de Seguridad de Información** debe ser compromiso de cada uno de los integrantes de la entidad, no obstante, la Gestión es responsabilidad de los dueños de proceso, los cuales son los propietarios de los riesgos.
- **Oficial Jefe de Seguridad de la Información (CISO)**: es responsable de velar por que los procesos de seguridad como la Gestión del Riesgo, los controles para mejorar el sistema y mitigar los riesgos sean implementados y mantenidos. Por lo tanto, juega un rol líder en la introducción de una apropiada y estructurada metodología para ayudar a identificar, evaluar y minimizar los riesgos de los sistemas de TI que soportan la misión de la entidad.
- **Propietarios de sistemas y activos de información**: los propietarios (funcionario y/o contratistas) son responsables por clasificar la información a su cargo y asegurar que los controles apropiados están definidos y funcionan en orden a garantizar la integridad, confidencialidad y disponibilidad de los sistemas de TI y de sus datos. Típicamente los propietarios son los responsables por aprobar y autorizar los cambios en sus sistemas, razón por la cual, deben entender el rol que juegan en la Gestión del Riesgo.
- **Administradores Funcionales y de Negocio**: son los administradores responsables (directivos) por las operaciones del Instituto. Estas personas tienen la autoridad y responsabilidad por adoptar o excluir decisiones claves para el logro de los objetivos del negocio. Su participación en la Gestión del Riesgo radica en la consecución de la seguridad apropiada de los sistemas de TI, que si se maneja apropiadamente, proveerá efectividad en el alcance de la misión sin sobrecostos en el uso de los recursos.
- **Dueños de Infraestructura de TI**: Los dueños de la infraestructura de TI (administradores de redes, bases de datos, aplicaciones, especialistas en computadores, analistas de seguridad, custodios y consultores de seguridad) son responsables por la apropiada implementación de los requerimientos de seguridad en los sistemas de TI. A medida que los cambios ocurren (expansión en la conectividad de las redes, cambios en la infraestructura existente y en las políticas, introducción de nuevas tecnologías), los administradores de infraestructura deben soportar la gestión del riesgo para identificar y valorar nuevos riesgos potenciales e implementar nuevas medidas de seguridad requeridas para salvaguardar los sistemas de TI.

4. Matriz de Valoración de Activos y Análisis de Riesgos de la Seguridad de la Información.

Los registros de activos de información, su valoración en cuanto a las dimensiones de Confidencialidad, Integridad, Disponibilidad y el análisis de probabilidad e impacto de los riesgos de seguridad y privacidad de la información, se realiza utilizando el formato Matriz de Valoración de Activos y Análisis de Riesgos de la Seguridad de la Información, adjunto.

Aspectos a tener en cuenta durante el diligenciamiento del formato Matriz de Valoración de Activos y Análisis de Riesgos de la Seguridad de la Información.

1. Diligenciar correctamente los diferentes campos del formato, sin omitir alguno.
2. Consultar las diferentes tablas de ayuda del formato para el respectivo diligenciamiento.

Bibliografía

- Instituto Colombiano de Normas Técnicas y Certificación (INCOTEC). NTC-ISO-IEC COLOMBIANA 27001:2013, capítulos 6.1.2, 6.1.3, 8.2, y 8.3
- Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia MINITC, Guía No. 7 - Guía de gestión de riesgos, Versión 3.0.0 del 01/04/2016
- Departamento Nacional de Planeación DNP. Guía para la Administración en Seguridad de la Información.
- Departamento Administrativo de la Función Pública (DAFP). Guía para la administración del riesgo.
- Departamento Nacional de Planeación, Política Nacional de Seguridad Digital – CONPES 3854. Disponible en web www.dnp.gov.co
- Instituto Nacional Penitenciario y Carcelario INPEC. Política de Seguridad de la Información. Código: PA-TI-PL01.

Anexo

• PA-TI-M01-F01 V01 Matriz de Valoración de Activos y Análisis de Riesgos de la Seguridad de la Información.

Lista de Versiones

Versión	Fecha de Emisión	Motivo de la Modificación	Modificaciones
1	10/Ago/2018	Creación del documento	N.A

Elaboró	Revisó	Aprobó
Nombre: Maria Cristina Reyes Castillo **Cargo:** Auxiliar Adminstrativo **Fecha:** 27/Ago/2018	**Nombre:** Juan Manuel Riaño Vargas **Cargo:** Jefe Oficina Asesora de Planeación **Fecha:** 05/Sep/2018 **Nombre:** Angelica María Patiño García **Cargo:** Profesional Especializado **Fecha:** 27/Ago/2018 **Nombre:** Angelica María Patiño García **Cargo:** Profesional Especializado **Fecha:** 05/Sep/2018	**Nombre:** Adriana Cetina Hernández **Cargo:** Jefe Oficina Sistemas de Información **Fecha:** 05/Sep/2018