PLAN DE RIESGO DE SEGURIDAD Y CONTINUIDAD DIGITAL

GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN

ELABORADO POR:
PROFESIONAL ESPECIALIZADO

GRUPO ÁREA GESTION SISTEMAS

INSTITUTO NACIONAL DE CANCEROLOGÍA

2025

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Este documento detalla el Plan de Riesgo de Seguridad Digital para el Instituto Nacional de Cancerología (INC), con un enfoque en la cultura preventiva para mitigar el impacto de los riesgos materializados y alcanzar los objetivos institucionales.

El plan de riesgo de Seguridad Digital se basa en una orientación estratégica que busca el desarrollo de una cultura de carácter preventivo en el Instituto Nacional de Cancerología (INC). Su propósito es identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y continuidad de TI con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos institucionales. Esto se realiza en cumplimiento de la normativa establecida por el estado colombiano, como el CONPES 3854 de 2016, el Modelo de Seguridad y Privacidad de MINTIC (MSPI), y adoptando las buenas prácticas y los lineamientos de los estándares de seguridad ISO 27001:2022, ISO 31000:2018, el marco de trabajo de ciberseguridad NIST v2.0 y la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - emitida por el DAFP..

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Establecer las directrices y estrategias que deben seguir todos los procesos del Instituto Nacional de Cancerología para la gestión de riesgo de seguridad digital, integrado con el sistema de gestión de riesgo institucional.

2.2. OBJETIVOS ESPECÍFICOS:

- Propender por la mejora continua generando una cultura de autocontrol y autoevaluación al interior de cada proceso.
- Identificar, analizar, valorar, hacer seguimiento y tratar los riesgos de seguridad digital.

3. ANÁLISIS DE LA SITUACIÓN ACTUAL

La situación actual de gestión de riesgos es cada vez más crítica debido a la creciente cantidad de amenazas de seguridad digital. El instituto enfrenta una gran variedad de riesgos, desde ataques cibernéticos y violaciones de datos hasta desastres naturales y fallas en la infraestructura tecnológica.

3.1. FACTORES EXTERNOS

Algunos aspectos clave que describen la situación actual de gestión de riesgos en el instituto son:

- Amenazas en aumento: Las amenazas de seguridad digital están en constante aumento, con nuevas vulnerabilidades y riesgos emergentes cada día. El instituto debe mantenerse al día con las últimas tendencias y amenazas para garantizar una gestión efectiva de riesgos.
- Cambios en el entorno institucional: El instituto opera en un entorno cada vez más complejo y dinámico con arquitecturas hibridas en la nube, y necesidades de interoperabilidad, lo que aumenta la complejidad de la gestión de riesgos. Los riesgos pueden surgir de fuentes internas y externas, como proveedores, empleados, colaboradores y pacientes.
- Falta de conciencia de riesgos: A menudo, la falta de conciencia de riesgos por parte de los empleados, colaboradores y de los lideres del instituto es un problema crítico en la gestión de riesgos. El instituto debe asegurarse de que todos sus usuarios entiendan los riesgos de seguridad digital y estén comprometidos con la seguridad de la información.

- Enfoque reactivo: El instituto adopta un enfoque reactivo hacia la gestión de riesgos, y debe lograr en su lugar una gestión proactiva. El instituto debe estar preparado para responder a los riesgos en tiempo real y tener un plan de contingencia bien definido en caso de una violación de seguridad.
- Falta de recursos: La gestión efectiva de riesgos requiere una inversión significativa en recursos institucionales, incluyendo personal capacitado, tecnología y herramientas de gestión de riesgos. Y por supuesto el tiempo que debe dedicar todo el personal a la gestión de riesgo.
- **Amenazas Potenciadas por Inteligencia Artificial (IA)**: La evolución rápida de la inteligencia artificial y el aprendizaje automático presenta un nuevo panorama de amenazas. Los ciberdelincuentes están utilizando cada vez más la IA para automatizar y escalar ataques, desarrollando malware más sofisticado capaz de evadir detecciones tradicionales, generar ataques de phishing y spear phishing altamente personalizados y convincentes, y optimizar ataques de fuerza bruta y denegación de servicio. La IA también facilita la creación de "deepfakes" y la manipulación de información, lo que aumenta los riesgos de suplantación de identidad y desinformación dirigida al instituto y sus usuarios. El instituto debe invertir en capacidades de defensa impulsadas por IA y en la capacitación del personal para reconocer y mitigar estas nuevas formas de ataque, así como considerar el riesgo de la IA en su propia infraestructura y sistemas.

A continuación, se presentan algunas de las principales situaciones de riesgo de seguridad digital a las que se ve expuesta el instituto en el entorno actual:

- **Phishing y spear phishing:** el phishing es una técnica de fraude que consiste en enviar correos electrónicos o mensajes de texto que parecen provenir de una entidad legítima, como un banco u otra entidad, para engañar a los usuarios y hacer que revelen información personal o financiera. El phishing es una de las principales causas de materialización de incidentes de seguridad en el Instituto
- **Malware:** el malware es un software malicioso que se utiliza para infectar y dañar sistemas informáticos. Existen varios tipos de malware, como virus, gusanos, troyanos y spyware, y pueden utilizarse para robar información, dañar archivos y sistemas, o controlar remotamente el dispositivo infectado.
- **Ransomware**: el Ransomware es un tipo de malware que se utiliza para secuestrar los archivos de un usuario y pedir un rescate a cambio de la clave para recuperarlos. El Ransomware es una amenaza cada vez más común y se combina con la exfiltración de información para realizar una doble extorsión. En el sector salud cada vez son más frecuentes este tipo de ataques.
- **Malware y Ransomware impulsados por IA:** El malware y el ransomware están evolucionando para incorporar capacidades de IA, lo que les permite adaptarse, aprender del entorno de la víctima y evadir las defensas de seguridad tradicionales de manera más efectiva. Esto incluye la capacidad de propagarse de forma más autónoma, cifrar archivos de manera más sigilosa y negociar rescates de forma automatizada, lo que podría aumentar la frecuencia y el impacto de los incidentes.
- **Ataques de fuerza bruta:** los ataques de fuerza bruta son un método utilizado para intentar adivinar las contraseñas de un sistema o cuenta. Los hackers utilizan programas que prueban diferentes combinaciones de letras y números para descubrir la contraseña correcta.
- **Ataques de denegación de servicio (DoS/DDoS) adaptativos:** los ataques de denegación de servicio (DoS, por sus siglas en inglés) son una técnica utilizada por los ciberdelincuentes para sobrecargar un sitio web, red o servicio en línea, con el objetivo de que éste no pueda atender a las solicitudes legítimas de los usuarios. Estos ataques pueden ser devastadores, ya que impiden el acceso a los usuarios legítimos y pueden causar pérdidas económicas y de reputación. La IA puede ser empleada para orquestar ataques de denegación de servicio más sofisticados y difíciles de mitigar, que se adaptan dinámicamente a las defensas del instituto. Esto podría resultar en interrupciones más prolongadas y severas de los servicios críticos de TI, afectando la disponibilidad y la continuidad operativa.
- **Robo de identidad:** el robo de identidad es cuando un delincuente utiliza la información personal de alguien para cometer fraudes o delitos. Esto puede incluir la obtención de información de tarjetas de crédito, cuentas bancarias, y otros datos personales.

- **Robo de credenciales y suplantación de identidad potenciados por IA**: La IA mejora la capacidad de los atacantes para adivinar contraseñas, descifrar credenciales y generar información personal falsa para suplantar identidades. Esto facilita el acceso no autorizado a sistemas y datos sensibles, incrementando el riesgo de fraude y violación de la privacidad.
- **Vulnerabilidades de seguridad:** las vulnerabilidades de seguridad son situaciones en las que la información de una empresa o de un usuario se ha visto comprometida. Las brechas pueden ocurrir por errores humanos, fallos en la seguridad informática o ataques malintencionados.
- **Explotación de vulnerabilidades automatizada:** Las herramientas de IA pueden ser utilizadas para identificar y explotar vulnerabilidades en sistemas y aplicaciones de forma más rápida y a gran escala de lo que lo harían los atacantes humanos. Esto reduce el tiempo que el instituto tiene para parchear y mitigar vulnerabilidades antes de que sean explotadas, aumentando la superficie de ataque y el riesgo de intrusiones.
- **Intentos de intrusión:** también conocidos como intentos de acceso no autorizado, son actividades malintencionadas en las que un individuo o un grupo de individuos intentan ingresar a los sistemas informáticos del instituto sin autorización. Estos intentos pueden ser llevados a cabo por diferentes motivos, como el robo de información confidencial, la realización de actividades ilegales, la alteración o destrucción de datos, o simplemente por diversión, desafío o reputación del atacante.
- **Fuga de información:** La exfiltración o fuga de información consiste en el intento de robo o filtración de información confidencial del instituto, y es una de las mayores preocupaciones de seguridad digital. Puede ser llevada a cabo por delincuentes cibernéticos, hackers, empleados descontentos o cualquier persona que tenga acceso a la información confidencial.
- **Ataques de Cadena de suministro:** es un tipo de ciberataque que se dirige a la infraestructura y los procesos de una cadena de suministro de una empresa, gobierno o país, con el objetivo de comprometer la seguridad de una o varias entidades a nivel país, o incluso a nivel internacional. Estos ataques son altamente sofisticados y pueden tener graves consecuencias, ya que aprovechan la confianza en los proveedores y terceros que forman parte de la cadena de suministro de la institución.
- **Ataques de ingeniería social avanzados (Deepfakes y Clonación de Voz):** Con el avance de la IA, los ciberdelincuentes pueden crear videos y audios "deepfake" extremadamente realistas, simulando ser ejecutivos, colegas o entidades de confianza del instituto. Estos pueden ser utilizados para engañar a los empleados, colaboradores y líderes, induciéndolos a revelar información confidencial, transferir fondos, instalar malware, etc. haciendo que sea significativamente más difícil distinguir entre comunicaciones legítimas y fraudulentas.
- **Rompimiento de cifrado por computación cuántica**: Aunque aún en fases iniciales, el desarrollo de la computación cuántica representa una amenaza futura significativa para los métodos de cifrado actuales. La capacidad de las computadoras cuánticas para resolver problemas matemáticos complejos a una velocidad sin precedentes podría, eventualmente, romper algoritmos criptográficos ampliamente utilizados para proteger la información sensible. Esto comprometería la confidencialidad de datos históricos y futuros si no se implementan medidas de criptografía post-cuántica a tiempo, lo que afectaría la privacidad de los pacientes y la seguridad de la información institucional a largo plazo.

Por todos esto, la gestión de riesgos se ha vuelto cada vez más crítica en la actualidad debido a las amenazas en aumento y los cambios en el entorno del sector Salud y gobierno. Para gestionar efectivamente los riesgos, el Instituto debe ser proactivo, crear conciencia de riesgos, adoptar un enfoque reactivo, tener un plan de contingencia bien definido y contar con los recursos adecuados.

3.2. FACTORES INTERNOS

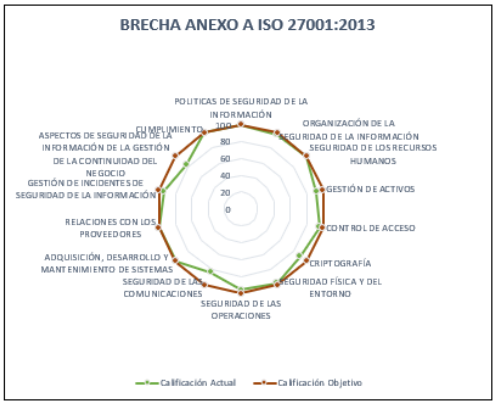
La gestión del riesgo de seguridad digital esta alineada a los principios y valores institucionales del BOTOSS

La identificación de la situación actual de seguridad se realiza mediante el diligenciamiento del instrumento de evaluación del MSPI de MINTIC.

3.2.1 Evaluación de efectividad de controles

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	98	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	100	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	92	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	96	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	90	100	OPTIMIZADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	98	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	96	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	83	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	99	100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	100	100	OPTIMIZADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	94	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	84	100	OPTIMIZADO
A.18	CUMPLIMIENTO	100	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		95	100	OPTIMIZADO



La evaluación de controles de 2024 requirió de hacer una equivalencia entre la norma del instrumento de gobierno, diseñado para evaluar la norma ISO 27001:2013, y los controles y gestión de la norma ISO27001:2022 que implementó el sistema de gestión de seguridad de la informacion del instituto desde 2024. La evaluación de la efectividad de controles equivalente evidencia una calificación de 95% con una mejora de 2 puntos porcentuales con respecto al año anterior, identificando el cierre de brechas en criptografía y el ajuste con la identificación de brecha en continuidad de negocio.

3.2.2. Nivel de Madurez del modelo de seguridad y privacidad de la información

NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

	NIVEL DE CUMPLIMIENTO
Inicial	SUFICIENTE
Repetible	SUFICIENTE
Definido	SUFICIENTE
Administrado	SUFICIENTE
Optimizado	SUFICIENTE

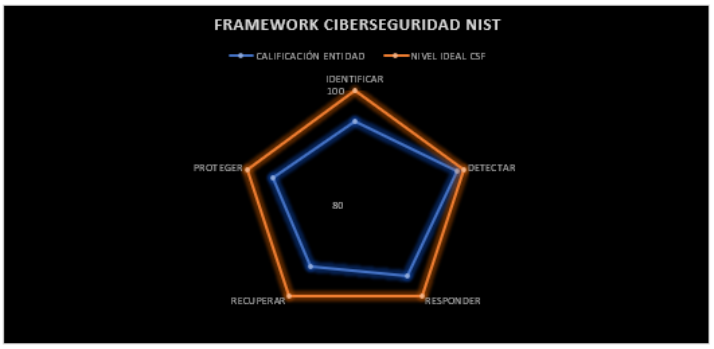
Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorias al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

El nivel de madurez del Sistema de Gestión de Seguridad de la Información SGSI se clasifica en Nivel de tipo Optimizado con cumplimiento suficiente, avanzando dos niveles de cumplimiento con respecto al periodo anterior. Esto significa que la entidad cuenta con una adecuada identificación de activos y gestión de riesgos, los controles están debidamente documentados y se cuentan con métricas, indicadores de seguridad digital, se realizan auditorias periódicas sobre el SGSI, se recolecta información para establecer la efectividad de los controles, y existe un mejoramiento continuo sobre el SGSI.

3.2.3. Calificación frente a mejores prácticas de Ciberseguridad

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	95	100
DETECTAR	99	100
RESPONDER	96	100
RECUPERAR	93	100
PROTEGER	95	100
Promedio	**95,51**	**100,00**



La evaluación de la efectividad de los controles de acuerdo con la NIST para gestión de incidentes de ciberseguridad evidencia una calificación promedio del 95.51%.

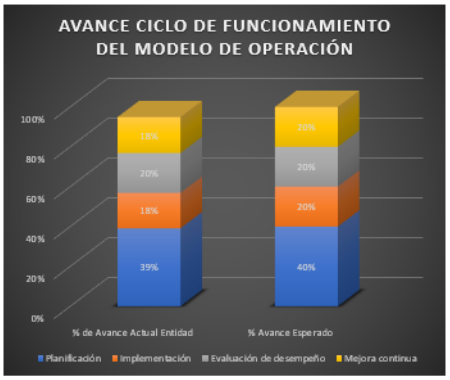
El Instituto Nacional de Cancerología (INC) demuestra una notable fortaleza en las funciones de Detección y Respuesta de su sistema de gestión de seguridad digital, alineándose con los principios del Framework de Ciberseguridad del NIST. Esto se debe a la implementación y despliegue de su arquitectura de Cero Confianza, y al enfoque de la automatización y uso de IA para la gestión de eventos, incidentes y vulnerabilidades.

Aun existen brechas en Criptografía y Aspectos de seguridad de la información de la gestión de la continuidad del negocio que son directamente relevantes para las funciones de Proteger y Recuperar del NIST, respectivamente.

También se identifican brechas en Relación con los proveedores y la gestión de inventarios y obsolescencia tecnológica de los equipos Biomédicos que impacta en la capacidad de Identificar, proteger y recuperar los activos que se comparten o dependen de terceros, un aspecto clave en el marco de seguridad.

3.2.4. Avance del ciclo de funcionamiento del modelo de operación PHVA

AVANCE PHVA		
COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
Planificación	39%	40%
Implementación	18%	20%
Evaluación de desempeño	20%	20%
Mejora continua	18%	20%
TOTAL	95%	100%



El Instituto Nacional de Cancerología ha logrado un 95% de avance actual en el ciclo PHVA (Planificar, Hacer, Verificar, Actuar) de su modelo de operación, frente a un 100% de avance esperado. Esto indica un progreso significativo y un alto nivel de cumplimiento en la implementación de su modelo de gestión.
Los componentes de "Planificación", "Implementación" y "Mejora continua" muestran pequeñas brechas, pero el alto porcentaje general sugiere que el instituto está en camino hacia la optimización de su modelo de operación y, por extensión, de su gestión de riesgos de seguridad digital. En general estas diferencias representan la oportunidad para un enfoque mas intensivo en la continuidad de negocio operacional.

4. DESARROLLO DEL PLAN

4.1 DEFINICIONES

- **Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
- **Amenaza:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).
- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
- **Probabilidad:** es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.
- **Controles:** 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.

4.2 NORMATIVIDAD

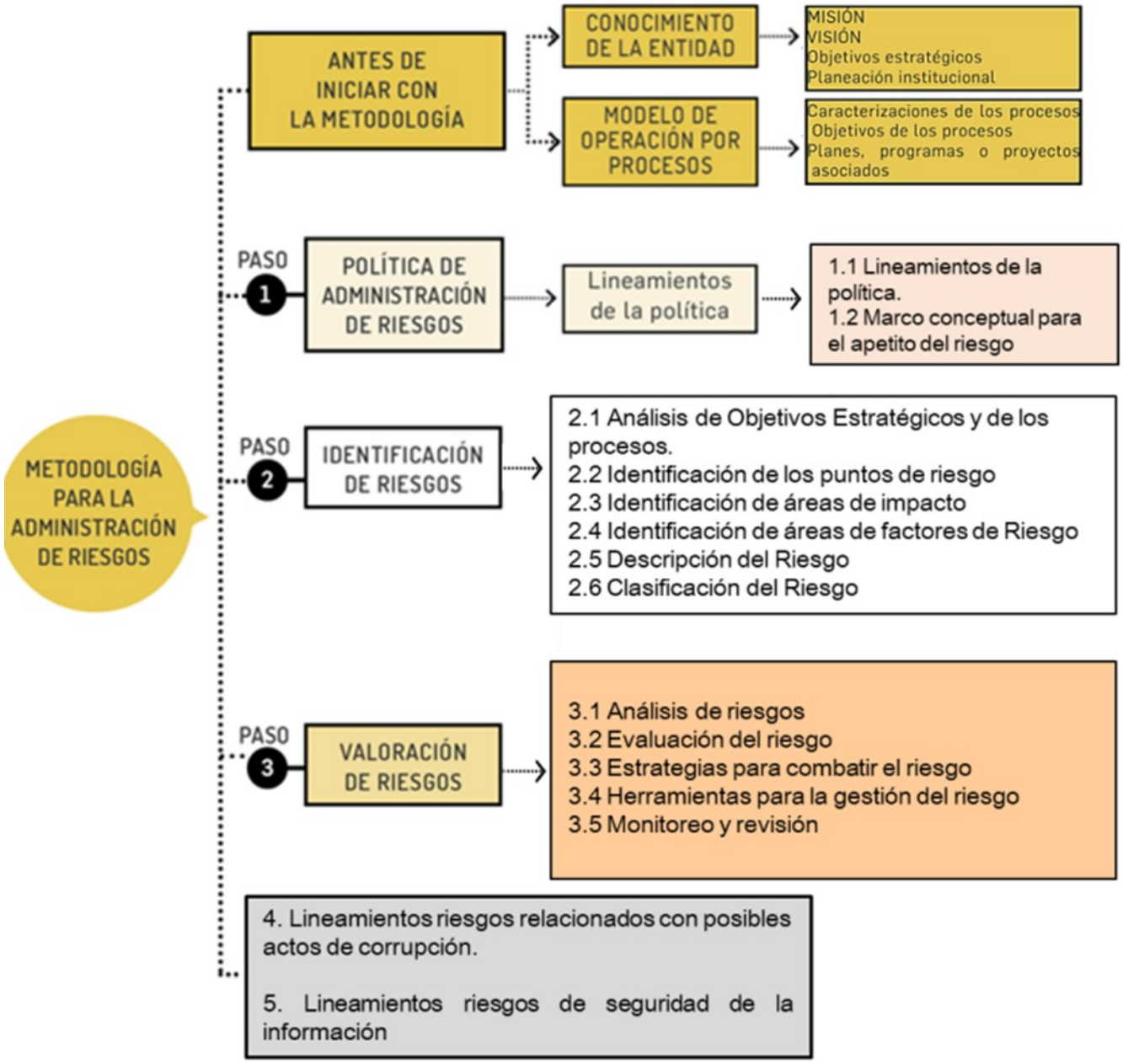
- **ISO/IEC 27001:2022:** La norma ISO 27001 es un estándar internacional emitido por la Organización ISO que define los requisitos en relación en cómo gestionar la seguridad de la información. Esta norma es certificable. Está basada en la creación de un Sistema de Gestión de Seguridad de la Información (SGSI), a partir del cual se articula toda la norma.
- **ISO/IEC 27002:2022:** Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información fue concebida como una guía que detallaba cómo implementar los 114 controles de la norma ISO/IEC 27001. No es certificable. Prioriza el enfoque y protección de los activos de información. Enfatiza el monitoreo al separar los objetivos de algunos controles. Favorece la

priorización al integrar varios controles que se convierten en uno. Se basa en resiliencia, protección, defensa y gestión.

- **ISO 31000:2018**: Gestión del riesgo – Directrices. Esta norma internacional proporciona principios y directrices para la gestión del riesgo. Ofrece un enfoque común para la gestión de cualquier tipo de riesgo y puede ser utilizada por cualquier organización, independientemente de su tamaño, tipo o actividad. Aunque no es certificable, ayuda a las organizaciones a integrar la toma de decisiones basada en el riesgo en sus procesos de gobernanza y operaciones.
- **ISO/IEC 42001:2023** es la norma específica y certificable para la gestión de sistemas de inteligencia artificial, abarcando no solo la seguridad sino también aspectos éticos y de gobernanza clave en el ámbito de la IA.
- **Decreto 338 2022:** Por medio del cual se establecen los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el modelo y las instancias de gobernanza de seguridad digital y se dictan otras disposiciones.
- **Resolución 500 de 2021:** Establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital.
- **Guía para la administración del riesgo y el diseño de controles en entidades públicas** - Versión 6 - 2022 - DAFP
- **Decreto 620 de 2020:** Este decreto establece el marco regulatorio para la ciberseguridad y la protección de datos personales en Colombia. Se establecen lineamientos para la gestión de riesgos de seguridad digital y se establecen las obligaciones de las empresas y las entidades gubernamentales.
- **Ley Estatutaria 1581 de 2012** y Reglamentada Parcialmente por el Decreto Nacional 1377 De 2013: Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Decreto 2609 de 2012:** Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.
- **Ley 1273 de 2009:** Esta ley establece los delitos informáticos y sanciones correspondientes, tales como la interceptación de datos, la violación de datos personales, la falsificación de documentos, entre otros.

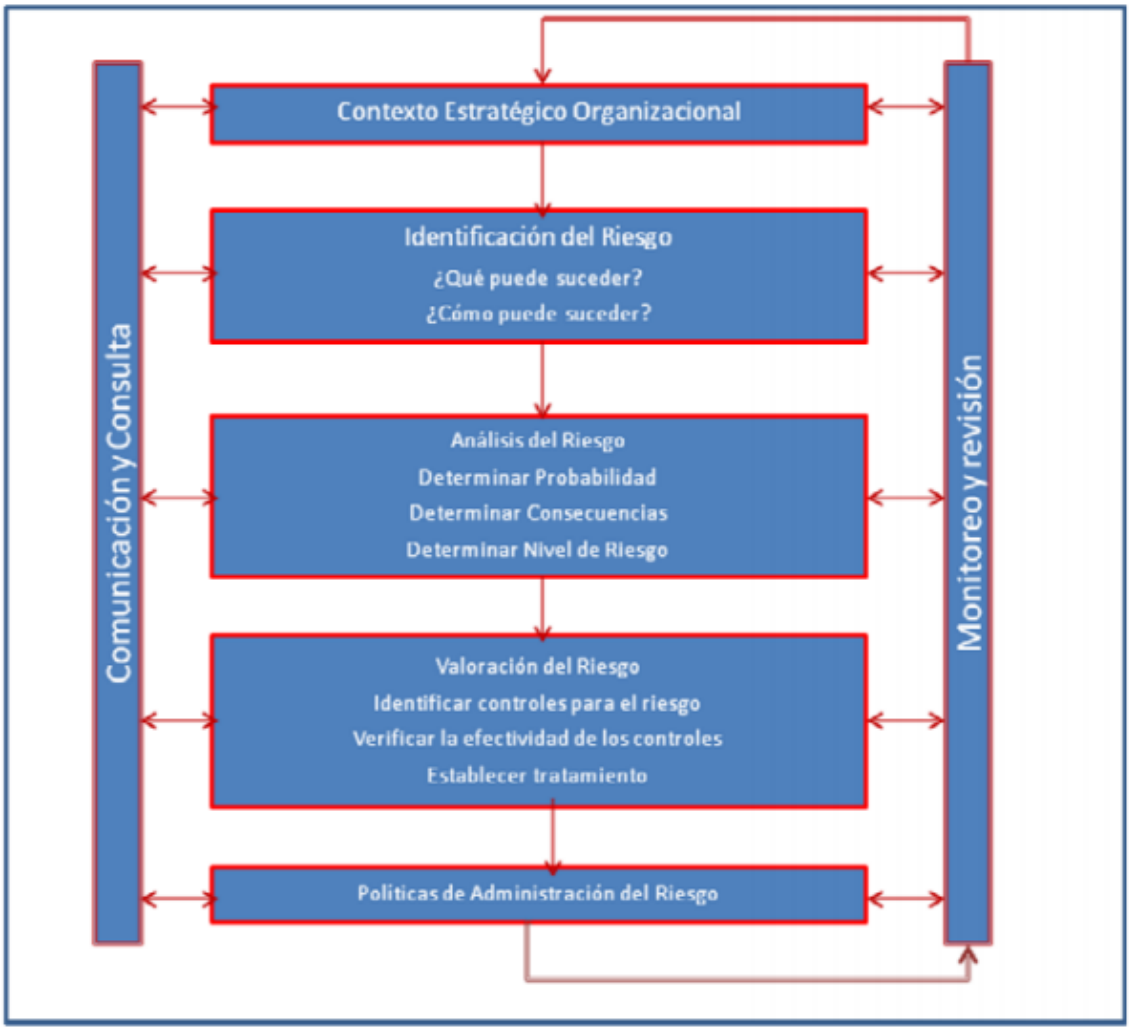
4.3 METODOLOGÍA DE RIESGO DE SEGURIDAD DIGITAL

La metodología para la administración del riesgo de seguridad digital se alinea a la metodología de riesgos institucional, y requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en el instituto, además del conocimiento de esta desde un punto de vista estratégico de la aplicación de las tres (3) fases para su desarrollo y , finalmente, de la definición e implantación y ejecución de estrategias de comunicación transversales a toda la entidad para que su efectividad pueda ser evidenciada. A continuación, se puede observar la estructura de gestión de riesgos completa implementada en el INC con sus desarrollos básicos:



En particular el proceso de gestión de riesgo en la seguridad digital consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento.

La metodología de valoración de riesgos de seguridad y privacidad en INC consta de 5 fases y se describe a continuación:



4.3.1. 1era Fase: Contexto Estratégico Organizacional

El contexto estratégico de seguridad de la información y de riesgo de seguridad digital está definido en los siguientes documentos:

- GTI-P01-PL-01 Plan estratégico de seguridad de la información (PESI)
- Resolución 0820 de 2024, Política de Administración del riesgo institucional
- Resolución 0322 -2024, Política de seguridad y privacidad de la información

El propósito de la gestión de riesgo de seguridad digital es:

- Dar soporte al sistema de gestión de seguridad de la información al interior del instituto
- Cumplimiento legal y regulatorio
- Preparación de contingencias tecnológicas
- Responder a incidentes de seguridad digital

4.3.2 2da Fase: Identificación del riesgo de seguridad digital

Identificación de riesgos de seguridad digital

La identificación del riesgo de seguridad digital relacionado con el proceso se lleva a cabo determinando las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos. Algunas causas externas no controlables por el instituto se podrán evidenciar en el análisis del contexto externo la cuales deben ser tenidas en cuenta en el análisis y valoración del riesgo. A partir de este contexto se identifica el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso o los estratégicos.

El siguiente esquema también puede orientar la identificación del riesgo:

Debido a	Riesgo	Lo que podría generar
(Causas)	(Puede ocurrir que)	(Efectos o consecuencias)

Para definición de riesgo de seguridad Digital desde el proceso, se debe tener en cuenta que:

- Se deben cubrir aspectos relacionados con el ambiente físico, digital y las personas.
- Es necesario que, en la descripción de riesgo de seguridad digital sobre los activos de información, concurran los principales atributos de seguridad digital así: confidencialidad + disponibilidad + integridad de la información.
- Su redacción debe ser transversal y debe aplicar para todos los activos de información identificados en el instituto

Identificación de las amenazas

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la entidad. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas. Las amenazas se deberían identificar genéricamente y por tipo (ej. Acciones no autorizadas, daño físico, fallas técnicas) Algunas amenazas pueden afectar a más de un activo y en tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados. A continuación, se describen una serie de amenazas comunes, que fueron determinadas por el INC dentro de mesas de trabajo con el grupo de cibersegruidad de Minsalud usando metodología de Árbol de Arem:

Categoría	ID	Amenaza	Tipo	Descripción	Conocidos	Latentes (Conocido, pero no hay control)	Focales (organización o sector)	Emergentes
Malware	1	Virus informático /Malware	Incidente	Aplicaciones maliciosas que pueden replicarse de forma automática en una red o se instala en un computador con el fin de realizar actividades no autorizadas como colectar información y enviarla remotamente, dañar la información de negocio o dañar el equipo	X			
	2	Caballos de Troya / Rootkits	Incidente	Aplicaciones maliciosas como spyware, scareware, Ransomware y adware que busca engañar los sistemas de seguridad y funcionales de un equipo o red; pasando inadvertido, enmascarado en una aplicación "inofensiva o autorizada" mientras envía información de forma no autorizada	X			
	3	Cliente BOTNET	Incidente	Robot informático que hace que un equipo infectado haga parte de una red de equipos "zombi"; es decir, equipos que también han sido infectado. Este tipo de ataques permite que un ciberdelincuente pueda llevar a cabo ataques de denegación de servicio, envío de grandes cantidades de spam o infectar sistemas de cómputo adicionales.	X			

Hacking	4	DoS y DDoS	Incidente	Aumento en el número de solicitudes que se hace a un sistema o red, lo cual hace que haya una saturación puesto que el sistema afectado no alcanza a gestionar las peticiones que recibe y se genera la degradación del servicio o se genera indisponibilidad. Estos ataques se realizan de forma automática utilizando robots		X		
	5	Intento de un usuario por usar datos de autenticación validos en sistemas no autorizados	Incidente	Uso no autorizado de credenciales de acceso validas por personal interno malintencionado o terceros para obtener acceso a las aplicaciones de la organización, sistemas de cómputo y redes como resultado de 'robo de identidad'.		X		
	6	Ejecución de pruebas de vulnerabilidades no autorizadas sobre la infraestructura tecnológica	Incidente	Ejecución de pruebas o escaneos sobre dispositivos de red (ej.: enrutadores, switches, firewalls etc.), sistemas de cómputo (ej.: servidores Web, servidores de correo, servidor de archivos etc.) o aplicaciones para obtener información que puede ser utilizado para llevar a cabo ataques más elaborado con el fin de robar información o causar daño a los sistemas tecnológicos		X		

Hacking	7	Interceptación, escucha o alteración de tráfico de red	Incidente	Interceptación no autorizada (conocido como eavesdropping o man in the middle) o modificación de información al transmitirse sobre redes públicas o privadas o entre máquinas mediante el uso de técnicas que permiten obtener o modificar información de forma no autorizada (criptoanálisis)		X		
	8	Secuestro de Sesión - Hijacking	Incidente	Es utilizado para llevar a cabo actividades no autorizadas con las credenciales de usuarios legítimos.	X			
	9	Modificación no autorizada de sitios y servicios web	Incidente	Es la realización de cambios en el contenido de un sitio web de forma no autorizada (website defacement)		X		
	10	Criptojacking	Incidente	Instalación de programas sin autorización de minería de criptomonedas, para utilizar los recursos de máquina de equipos y servidores corporativos para mantener operación de monedas virtuales	X			
	11	Uso de Proxys y programas para violar restricciones de navegación	Incidente	Instalación o uso en la nube de programas como proxyes virtuales, conexiones remotas, vpns, redes alternativas para saltar las restricciones de navegación impuestas por el instituto				

	12	Acceso no autorizado o modificación de datos	Incidente	Acceso, cambio, adición o eliminación de información no autorizada por medio de técnicas como ataques tipo SQL injection, buffer overflows, malware o aprovechando los privilegios de acceso que hayan sido asignados para usarlos de forma incorrecta.		X		
	13	Descifrado no autorizado de información sensible	Incidente	Actividad que realiza un usuario sin autorización para acceder a la información en texto plano, usando métodos como rainbow tables, ataque de fuerza bruta o cracking de llaves de cifrado (determinar las versiones de texto plano de llaves de cifrado como llaves WPA2 en redes inalámbricas).	X			
	14	Acceso no autorizado sobre IOT y hardware biomédico	Incidente	Accesos a dispositivos de IOT biomédicos con el fin de cambiar su configuración, instalación de Botnets o saboteo de funcionamiento.				X
	15	Ransomware	Incidente	Secuestro de la información cifrando activos de Info exigiendo pago por la recuperación o no publicación de esta.	X			
	16	Robo de credenciales de autenticación	Incidente	Obtención de datos de autenticación mediante engaño o keylogger que permite a un atacante o persona inescrupulosa hacerse con los datos de acceso legítimos para poder robar o modificar información suplantando al verdadero dueño de los datos de acceso	X			

	17	Formjacking	Incidente	Ataque de Suplantación de formularios Web de sitios de comercio o transacciones virtuales en el navegador de los usuarios, para hacerse con tarjetas de créditos e información bancaria				X
Cloud	18	Interfaces y API inseguras	Incidente	interfaces pueden presentar vulnerabilidades debidas a una configuración incorrecta, vulnerabilidades de codificación o falta de autenticación y autorización, entre otras cosas. Estos descuidos pueden dejarlos potencialmente vulnerables a la actividad maliciosa.				
	19	Desconfiguración y control de cambios inadecuado		Falta de conocimiento del sistema o de comprensión de los ajustes de seguridad en nube pueden dar lugar a configuraciones erróneas, que se ven magnificados en la nube por su escalabilidad				X
	20	Falta de arquitectura y estrategia de seguridad en la nube		La no adherencia de una estrategia de infraestructura y a unos principios de diseño Cloud causa complejidad frente al manejo de las amenazas emergentes, y problemas de visibilidad y correlación de riesgo				X

	21	Recursos de terceros cloud vulnerables o no seguros		Los riesgos de terceros existen en todos los productos y servicios que se contratan o consumen. Los servicios cluoud con seguridad débil o son seguridad pueden ser un el eslabón para propagación de software malicioso				X
	22	Falta de control de la infraestructura de la nube limita las opciones de mitigación de los problemas de seguridad de las aplicaciones		limita las opciones de mitigación de los problemas de seguridad de las aplicaciones y la visibilidad de las herramientas de seguridad tradicionales				
	23	Exfiltración de datos en la nube		La exfiltración de datos de almacenamiento en la nube se produce cuando la información sensible, protegida o confidencial es liberada, vista, robada o utilizada por un individuo fuera del entorno operativo de la organización				
Sociales	24	Suplantación de marca	Incidente	Uso no autorizado del nombre, marca o logo de una organización, mediante el registro de dominios en Internet o creando sitios Web falsos (phishing) donde se redireccionan usuarios desprevenidos			X	
	25	Suplantación de identidad	Incidente	Es cuando una persona pretende ser otra persona por medio de engaños o simplemente usando los datos de autenticación previamente robados con el fin de ejecutar acciones no autorizadas para cometer fraude.		X		

	26	Phishing	Incidente	Es un ataque de ingeniería social que por medio del envió de un mail busca que un usuario acceda a un sitio web en el cual solicitará datos personales, de autenticación etc. los cuales serán conocidos por el atacante cibernético permitiéndole robar, estafar etc. Las variantes de phishing incluyen spear phishing (ataques de phishing orientados a individuos específicos o un grupo pequeño de individuos), whaling (ataques de phishing orientado a altos ejecutivos) y vishing (ataques de phishing mediante el uso de VoIP).	X			
	27	Spam	Incidente	Es un ataque orientado al envío de una gran cantidad de mensajes (incluyendo correo electrónico, mensajería instantánea y telefonía) no solicitados (comerciales).	X			
	28	Noticias e informacion falsa, fuentes de información no confiable	Incidente	Noticias falas por redes sociales, sitios de noticias, o descarga de información y estadísticas de sitios no seguros para investigaciones y docencia				X
	29	Hacktivismo	Incidente	Utilización no-violenta de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos				

	30	Ciberterrorismo	Incidente	Uso de medios de tecnologías de información, comunicación, informática, electrónica o similar con el propósito de generar terror o miedo generalizado en una población, clase dirigente o gobierno, causando con ello una violación a la libre voluntad de las personas				
	31	Grupos de amenazas persistentes avanzada APT	Incidente	APT suelen centrar su forma de robar en la adquisición de datos. Estos grupos son estudiados de cerca por grupos de inteligencia de amenazas, que publican informes detallados sobre los métodos y tácticas de los grupos. El informe de la CSA recomienda a las organizaciones que utilicen esos informes para organizar ejercicios de "equipo rojo" con el fin de protegerse mejor de los ataques de las APT, así como realizar ejercicios de caza de amenazas para identificar la presencia de cualquier APT en sus redes.				X

	32	BEC Bussines email compromise	Incidente	Un BEC es una forma de ataque de phishing en el que un delincuente cibernético se hace pasar por un ejecutivo (a menudo el CEO) y trata de conseguir que un empleado, cliente o proveedor transfiera fondos o información confidencial al Atacante. Los criminales cibernéticos escarbaran las bandejas de entrada de correo electrónico comprometidas, estudiarán las noticias recientes de la compañía e investigarán a los empleados en los sitios de medios sociales para hacer que estos ataques por correo electrónico parezcan tan convincentes como sea posible. Este alto nivel de segmentación ayuda a estas estafas por correo electrónico a pasar a través de los filtros de spam y evadir las campañas de listas blancas de correo electrónico.				X
	33	Falta de capacitación y concienciación	Requerimiento	Falta de preparación o de conocimiento del usuario sobre los controles y riesgos en la ejecución de sus procesos, en el manejo de sus activos de información, y en el cumplimiento de las políticas de seguridad del Instituto				
Uso Inadecuado o indebido de recursos	34	Violación de Derechos de Autor, y propiedad intelectual	Incidente	Infracciones a derechos de autor y propiedad intelectual, plagio, descarga y almacenamiento de música, videos libros publicaciones	X			

	35	Modificación no autorizada de privilegios de acceso	Incidente	Cambio deliberado en la configuración de los privilegios asignados a un usuario en un sistema o aplicación (típicamente escalamiento) sin aprobación alguna		X		
	36	Actividad no autorizada en el sistema	Incidente	Uso no autorizado de sistemas de cómputo (usualmente por individuos autorizados) incluyendo: causar de forma intencional comportamiento adverso del sistema / ejecución (ej.: mediante el cambio o adición de software, transacciones, archivos o bases de datos); llevar a cabo fraudes mediante el reenvío de fondos a cuentas no autorizadas; uso de sistemas de cómputo de forma maliciosa o excesiva o utilizando servicios de comunicación no autorizada (ej.: correo electrónico y mensajería instantánea) mediante la ejecución de actividades no autorizadas (ej.: descarga o envío de contenido obsceno, discriminatorio o de acoso).	X			
	37	Robo de software	Incidente	Robo de programas, Licencias, código de computador, código fuente y metodologías	X			

	38	Robo de información en medio físico o digital	Incidente	Robo de listas de clientes, diseños de productos, secretos de marca, propiedad intelectual, información sensible o personal como número de tarjetas de crédito, ID de empleados o registros médicos etc..	X			
	39	Uso indebido de contraseñas	Incidente	Divulgar, compartir o vulnerar las políticas de contraseñas fuertes en el Instituto		X		
	40	Uso indebido de equipos Biomédicos	Incidente	Uso indebido de equipos biométricos y hospitalarios que pueden interrumpir la operación del servicio, de la red, sistemas de información, plataformas o de la infraestructura eléctrica del instituto.				X
	41	Uso de aplicaciones no autorizadas e infracciones de licenciamiento	Incidente	Descarga, instalación y uso de aplicaciones no autorizadas por la organización en los equipos corporativos que pueden causar problemas de funcionamiento, licenciamiento, daño de equipos de cómputo o sistemas tecnológicos. Uso de programas para crakear o romper el sistema de validación de claves para instalación de software.	X			
Físicas	42	Acceso físico no autorizado	Incidente	Ingreso de un individuo a zonas protegidas o a lugares donde se procesa información de negocio, aplicaciones, sistemas de cómputo o redes (ej.: mediante ingreso sin autorización o pretendiendo ser un individuo autorizado).	X			

	43	Robo o pérdida de equipos de computo, moviles o de resguardo de información	Incidente	Robo o pérdida de equipos de cómputo, incluyendo servidores, Workstation, portátiles, ultrabooks, tablets, smartphones y dispositivos de resguardo portátil dentro de las instalaciones del instituto, o en comisión de una labor para el INC.	x			
	44	Perdida o robo de dispositivos móviles o de resguardo	Incidente	Robo o pérdida de equipos de cómputo portátiles (ej.: equipos utilizados por personas en ambientes remotos), como ultrabooks, tablets, smartphones y dispositivos de resguardo portátil.	x			
	45	Robo o pérdida de dispositivos físicos de autenticación	Incidente	Robo o pérdida de dispositivos de autenticación física como tokens o smartcards, carnets y tarjetas de ingreso		x		
	46	Fallo de controles ambientales de datacenter y centros de datos	Incidente	Fallos de Aire acondicionado, sistema de CCTV , sistemas de extinción de incendios, monitores ambientales	x			
	47	Daño físico accidental	Incidente	Daño material no intencionado de sistemas de cómputo, equipos de red o ambiente físico afectando su funcionamiento normal (ej.: fuego, escapes de líquidos, colapso del edificio o aseo).	x			
	48	Daño físico malintencionado o para tratar de forzar equipos de cómputo o redes	Incidente	Actividad premeditada y malintencionada que busca afectar el correcto funcionamiento de sistemas de cómputo o equipos de red.	x			

	49	Fallo de controles de acceso	Incidente	Fallos los sistemas de control de acesso Físico al instituto, incluye CCTV, Biometricos, Sistemas de tarjetas, talanqueras, barreras perimetrales, cerraduras electrónicas, sistemas de aseguramiento tipo bunker	x			
Ambientales y del entorno	50	Eventos terroristas	Incidente	Actividades delictivas realizadas por personas u organizaciones con el fin de generar desestabilización social en la Organización o gobierno que afecta las instalaciones	x			
	51	Eventos sobre infraestructura critica	Incidente	Evento o fallo sobre infraestructura eléctrica interna del instituto, sobre sistemas de protección radiológicos, sistemas de y sobre que pueden ocasionar impacto critico de operación y ambiental			x	
	52	Eventos Naturales	Incidente	Desastres naturales incluyendo tormentas, terremotos, fuego y efectos de clima extremo (ej.: inundaciones o heladas).	x			
	53	Cortes Eléctricos	Incidente	Caídas o fallas temporales del suministro eléctrico debido a proveedor de Servicio	x			
Errores	54	Daño o pérdida de comunicaciones externas	Incidente	Daño o pérdida de los enlaces de comunicación o servicios (ej.: conexiones de Internet, wifi de área network (WAN), local Area networks (LANs), enlaces satelitales o redes inalámbricas).	x			

	55	Interferencia o bloqueo malicioso de comunicaciones inalámbricas	Incidente	Interferencia maliciosa de comunicaciones inalámbricas con el fin de prevenir o impedir que las comunicaciones lleguen a su destinatario.	x			
	56	Errores de usuarios	Incidente	Errores cometidos por personal interno o externo (ej.: consultores, contratistas o empleados de terceros) mediante el uso de aplicaciones (ej.: errores al ingresar datos, operación incorrecta o envío de material a direcciones equivocadas). Sin ánimo de hacer daño o que haya sido una actividad premeditada	x			
	57	Errores del equipo de TI	Incidente	Fallas llevadas a cabo por personas responsables del diseño, desarrollo y mantenimiento de aplicaciones, sistemas de cómputo y redes (ej.: errores al escribir código, configurar sistemas de cómputo o mantener la configuración de los dispositivos de red). Sin ánimo de causar daño o que haya sido una actividad premeditada.	x			
	58	Malfuncionamiento o fallas de servicios (Hardware, software) de seguridad	Incidente	Ejecución incorrecta o fallas de hardware o software detectadas sobre servicios de seguridad como: Wsus, Consola Antivirus, Políticas Active Directory, UTM, Firewall, Antispam, CAserver, Certificados digitales , VPN, Monitores de disponibilidad, etc	x			

	59	Malfuncionamiento o falla de controles de seguridad de sistemas de información y BD	Incidente	Ejecución incorrecta o fallas de controles de seguridad configurados para protección BD, plataformas y sistemas de seguridad como: fallas en sistemas de autenticación, permisos de usuarios, configuración de roles y perfiles, certificados digitales, validaciones de escritura, políticas de directorio activo, políticas de antivirus, políticas de firewall, políticas de antispam etc.	x			
	60	Sobrecarga de sistema (Capacidad)	Incidente	Deficiencia en el correcto funcionamiento de un sistema o aplicación, causado por una configuración errónea sin tener en cuenta las limitantes para su funcionamiento.		x		
	61	Efectos inesperados de los cambios	Incidente	Impacto adverso o daño a la información o a los sistemas de cómputo cuando se aplican cambios significativos a la institución.	x			
	62	Fallos en planes de continuidad	Incidente	Fallos identificados en planeación ejecución de planes de continuidad informática	x			
Privacidad y Confidencialidad	63	Solicitud de Tratamiento de datos personales	Requerimiento	Solicitudes realizadas por el interesado en el tratamiento de su información personal: Acceso, modificación(Actualización) , rectificación limitaciones de finalidad , supresión, borrado parcial, portabilidad, Realizadas por el paciente , proveedor, colaborador o tercero	X			

	64	Adulteración de datos personales	Incidente	Modificación intencionada o accidental de la informacion personal de Pacientes, usuarios terceros en bases de datos, sistemas de informacion, compartidas y archivo físico, que afecten la integridad de la data recolectada, o que causen destrucción y/u ocultamiento de información.	x			
	65	Perdida/ Fuga de BD datos personales	Incidente	Perdida intencionada o accidental, sustracción de la informacion personal de Pacientes, usuarios terceros en bases de datos, sistemas de informacion, compartidas y archivo físico	x			
	66	Acceso no autorizado a datos personales	Incidente	Acceso no autorizado a los datos personales, debido a elevación de permisos, o permisos mal configurados que causen utilización indebida de los datos personales de los interesados.	x			
	67	Transferencia de datos a terceros	Incidente	Solicitud de transferencia de base de datos, archivos planos, información en físico o archivos no estructurados que requiera aprobación, tratamiento	x			
	68	Indisponibilidad de canales de Comunicación de Habeas Data	Incidente	Indisponibilidad de canales de atención establecidos para la recepción, atención y solución de eventos de Habas data, establecidos en la política de datos personales. (Correo electrónicos, radicación de documentos)	x			

AMENAZAS IA	69	Publicación o exposición no autorizada de información	Incidente	Publicación no autorizada (accidental o deliberada) de información confidencial del instituto e infracciones al deber de secreto (ej.: proyectos, nombres de clientes, registros médicos, hojas de vida, arquitecturas de red y seguridad, números de tarjetas de crédito) o credenciales de acceso de usuarios (ej.: identificadores únicos y autenticadores), los cuales deben ser confidenciales.		X		
	70	Ataques de Ingeniería Social con Deepfakes y Clonación de Voz	Incidente	Utilización de IA para generar contenido audiovisual (deepfakes) o de voz (clonación de voz) ultra-realista para suplantar identidades de confianza (ej. directivos, colegas) con el fin de manipular a individuos y obtener información sensible, transferir fondos o facilitar la instalación de malware. La sofisticación hace extremadamente difícil distinguir lo real de lo falso.				X

	71	Malware Polimórfico y Adaptativo impulsado por IA	Incidente	Desarrollo de variantes de malware y ransomware que utilizan capacidades de IA para aprender del entorno de la víctima, evadir las defensas de seguridad tradicionales (antivirus, EDR), modificar su propio código de forma autónoma (polimorfismo) y adaptarse a nuevas contramedidas en tiempo real, dificultando su detección y erradicación.				X
	72	Explotación Automatizada de Vulnerabilidades (AI-driven Exploit Kits)	Incidente	Uso de la IA para escanear, identificar y explotar vulnerabilidades en sistemas y aplicaciones de forma masiva y a gran velocidad. Estas herramientas pueden priorizar vulnerabilidades, diseñar ataques a medida y ejecutar secuencias de explotación complejas sin intervención humana, reduciendo drásticamente el tiempo de reacción de las defensas.				X

	73	Ataques de Denegación de Servicio (DoS/DDoS) Adaptativos e Impulsados por IA	Incidente	Orquestación de ataques de denegación de servicio que emplean IA para analizar las defensas de la víctima y ajustar dinámicamente sus patrones de ataque (ej. volumen, tipo de tráfico, origen) con el fin de sobrecargar o eludir las contramedidas. Esto puede resultar en interrupciones más prolongadas y severas de los servicios críticos de TI.				X
	74	Ataques Cuánticos a Cifrados (Post-Quantum Cryptography Threat)	Incidente	La capacidad emergente de la computación cuántica para resolver problemas matemáticos complejos a una velocidad sin precedentes podría, en el futuro, romper algoritmos criptográficos ampliamente utilizados para proteger la información sensible (ej. RSA, ECC). Esto comprometería la confidencialidad de datos históricos y futuros, requiriendo la adopción de criptografía post-cuántica.				X

	75	Envenenamiento de Datos (Data Poisoning) en Modelos de IA	Incidente	Inserción deliberada de datos corruptos o sesgados en los conjuntos de entrenamiento utilizados para desarrollar modelos de IA. Esto puede llevar a que el sistema de IA tome decisiones incorrectas, genere resultados erróneos o incluso sea explotado para fines maliciosos (ej. clasificar erróneamente un ciberataque como tráfico legítimo).			X	X
	76	Ataques de Evasión (Adversarial Attacks) contra Sistemas de IA	Incidente	Creación de entradas de datos sutilmente modificadas (imperceptibles para un humano) que engañan a un modelo de IA para que clasifique incorrectamente la información. Esto puede ser utilizado para evadir sistemas de seguridad basados en IA (ej. reconocimiento facial, detección de intrusiones) o manipular decisiones automatizadas.				X

4.3.3. 3era Fase: Análisis de riesgos

4.3.3.1 Análisis de riesgos de seguridad digital

En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

Aspectos para tener en cuenta:

- Tabla para determinar probabilidad
- Tablas (s) para determinar el impacto o consecuencias (de acuerdo con la política de riesgos institucional).
- Matriz de evaluación de riesgos de acuerdo con la metodología a utilizar

Estimación del nivel del riesgo inicial – RIESGO INHERENTE
Se logra a través de la determinación de la probabilidad y el impacto que puede causar la materialización del riesgo, teniendo en cuenta las tablas establecidas en cada caso.

Determinar probabilidad:

Es la posibilidad de ocurrencia del riesgo, esta se mide con criterios de frecuencia o factibilidad. Factibilidad (teniendo en cuenta los factores internos y externos que podrían propiciar el riesgo, aunque este no se hubiera materializado), o de frecuencia (si el riesgo se ha materializado o no en un tiempo determinado).

Escoger factibilidad si nunca se ha presentado el riesgo en el INC, en este caso se califica bajo el criterio de experiencia o experticia de quienes participan en las mesas de trabajo.

Diligenciamiento bajo Criterio de Factibilidad
Se analiza la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que se dé.

Nivel	Escalas	Factibilidad	Aplicación
1	RARA VEZ	Excepcionalmente ocurriría.	Nada común o frecuente, escaso.
2	IMPROBABLE	Alguna vez podría ocurrir.	Difícil o poco probable que ocurra.
3	POSIBLE	Existe una posibilidad media que suceda.	Existe la posibilidad de ocurrencia.
4	PROBABLE	Existe una alta posibilidad que suceda.	Muy probable que ocurra.
5	CASI SEGURO	Es seguro que suceda.	Es muy seguro que se presente.

Escoger frecuencia cuando hace referencia a la oportunidad de que algo sucedió, medido o determinado por datos y hechos históricos, o bajo criterio de experiencia o experticia de quien la realiza.

Diligenciamiento bajo Criterio de Frecuencia
Se analizan el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo.

Bajo el Criterio de FRECUENCIA		
Se analizan el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo.		
Nivel	**Escalas**	**Frecuencia**
5	CASI SEGURO	Más de una vez al año.
4	PROBABLE	Una vez en el último año.
3	POSIBLE	Una vez en los últimos 2 años.
2	IMPROBABLE	Una vez en los últimos 5 años.
1	RARA VEZ	Nunca o no se ha presentado en los últimos 5 años.

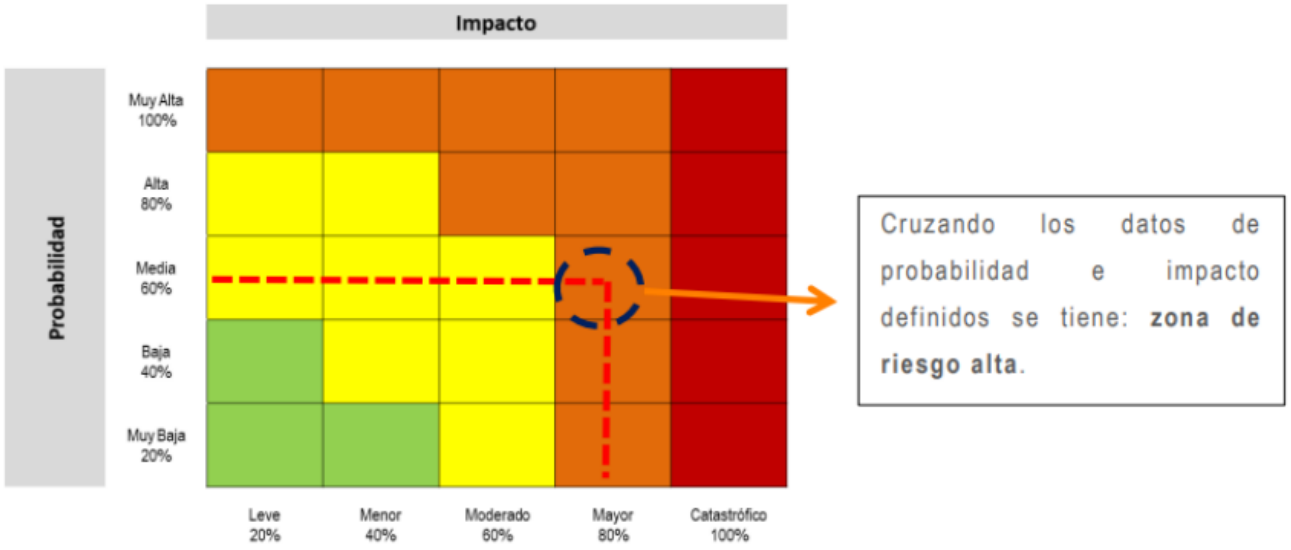
Determinar consecuencias o nivel de impacto
Se entiende que son las consecuencias que puede ocasionar al instituto la materialización del riesgo. Se tienen en cuenta las consecuencias potenciales que se describieron en la identificación del riesgo. Para su determinación se utiliza la tabla de niveles de impacto según el enfoque a determinar (gestión de proceso, de corrupción y de seguridad digital).

Determinación de consecuencias o nivel de impacto con Enfoque de Gestión de Riesgos de Seguridad Digital

Nivel	Escala	Descripción
CATASTRÓFICO	**CONFIDENCIALIDAD**	Divulgación o utilización indebida de información confidencial que impacta negativamente la operación, generando pérdidas económicas e imagen negativa del instituto.
	DISPONIBILIDAD	La información crítica para el desarrollo de los procesos no está disponible, no se pueda recuperar y afecta la operación del negocio. Interrupción de las operaciones por más de 2 días.
	INTEGRIDAD	Cambios que afecten la exactitud y completitud de la información, impactando de forma critica la operación o prestación del servicio.
MAYOR	**CONFIDENCIALIDAD**	Divulgación o utilización indebida de información interna que impacta negativamente la operación, generando pérdidas económicas y requerimientos al instituto.
	DISPONIBILIDAD	La información para el desarrollo de los procesos no está disponible, adicionalmente no se recupera de forma total y genera interrupción de las operaciones entre 1 y 2 días.
	INTEGRIDAD	Cambios que afectan la exactitud y completitud de la información ocasionando errores en la ejecución de los procesos y la toma de decisiones.
MODERADO	**CONFIDENCIALIDAD**	Utilización indebida de información interna que puede llegar a afectar la operación del instituto.
	DISPONIBILIDAD	La información para el desarrollo de los procesos no está disponible y afecta parcialmente al instituto, generando interrupción de las operaciones entre 8 y 24 horas.
	INTEGRIDAD	Cambios que afectan la exactitud y completitud de la información de uso interno ocasionando retrasos o incumplimientos en la operación.
MENOR	**CONFIDENCIALIDAD**	Se divulga información, y afecta algunos procesos del instituto.
	DISPONIBILIDAD	La información para el desarrollo de los procesos no está disponible y afecta algunos procesos de la entidad, generando Interrupción de las operaciones menor a 8 horas.
	INTEGRIDAD	Cambios que afectan la exactitud y completitud de la información de uso interno que afectan parcialmente la ejecución de los procesos.
INSIGNIFICANTE	**CONFIDENCIALIDAD**	Se divulga información, y no altera el funcionamiento de las áreas receptoras y procesadoras de información.
	DISPONIBILIDAD	La información para el desarrollo de los procesos no está disponible y no afecta la operación del instituto
	INTEGRIDAD	Cambios que no afectan la exactitud y completitud de la información y en consecuencia no se afecta la ejecución de los procesos.

Mapa de calor

Se denomina también Matriz de criticidad de 5x5 significa que para ubicar el nivel de riesgo se cuenta con 5 niveles en probabilidad y 5 niveles en impacto.



Se toma la calificación de probabilidad y de impacto resultante y el riesgo se ubicará así: la calificación de probabilidad en la fila y la de impacto en las columnas correspondientes, el punto de intersección de las dos corresponde al nivel de riesgo, así se podrá determinar el RIESGO INHERENTE.

ZONA DE RIESGO	
	EXTREMA O CATASTRÓFICA
	ALTA O MAYOR
	MODERADA
	BAJA

4.3.4. 4ta Fase: Evaluación de riesgo de seguridad digital

Los criterios de evaluación y tratamiento de riesgo, criterios de impacto y criterios de aceptación del riesgo del Instituto Nacional de Cancerología están definidos en manual GSI-P07-M-02 MANUAL PARA LA GESTIÓN DEL RIESGO INSTITUCIONAL.

Esta etapa busca establecer la zona en que se ubicarán los riesgos identificados, después de aplicar los controles y confrontar los resultados del análisis de riesgo inicial – RIESGO INHERENTE frente a los controles establecidos, con el fin de determinar el riesgo no cubierto por los controles establecidos y la zona de riesgo final denominada RIESGO RESIDUAL.

Determinación de los controles:

Se trata de establecer un control para que mitigue de manera adecuada el riesgo. Este debe estar correctamente diseñado y valorado. Los controles corresponden a herramientas o prácticas que se disponen en la actualidad para reducir la probabilidad de ocurrencia (preventivos) o el impacto (detectivos o correctivos) que deben establecerse y redactarse en términos de actividad.

Para seguridad digital se deben seleccionar los controles para el riesgo de seguridad digital, teniendo como base los controles descritos en el anexo A de la norma ISO 27001y la norma ISO27002. Con base en los riesgos identificados, los requisitos legales y reglamentarios y los requisitos de negocio, se pueden seleccionar los controles de seguridad adecuados. Esto puede incluir medidas técnicas, organizativas, legales o físicas, o una combinación de ellas. En total lel Anexo A tiene un total de 94 controles

ISO/IEC 27001:2022(Español)

Anexo A
(normativo)

Referencia de controles de seguridad de la información

Los controles de seguridad de la información enumerados en la Tabla A.1 se derivan directamente y están alineados con los enumerados en ISO/IEC 27002:2022(1), Cláusulas 5 a 8, y se utilizarán en contexto con 6.1.3.

Cuadro A.1. Controles de seguridad de la información

5	Controles organizativos	
5.1	Políticas de seguridad de la información	**Control** La política de seguridad de la información y las políticas específicas del tema serán definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos.
5.2	Funciones y responsabilidades de seguridad de la información	**Control** Los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización.
5.3	Separación de funciones	**Control** Las funciones conflictivas y los ámbitos de responsabilidad conflictivos se separarán.
5.4	Responsabilidades de gestión	**Control** La gerencia requerirá que todo el personal aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y procedimientos específicos del tema de la organización.
5.5	Contacto con las autoridades	**Control** La organización debe establecer y mantener contacto con las autoridades pertinentes.
5.6	Contacto con grupos de interés especial	**Control** La organización debe establecer y mantener contacto con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.

Grafica. Ejemplos de Controles de Anexo A

Los controles de seguridad digital aplicables para el instituto, y sus excepciones con la debida justificación se declaran e el formato GTI-P01-F-20 Declaración de Aplicabilidad de Controles.

	INSTITUTO NACIONAL DE CANCEROLOGÍA ESE	CÓDIGO:	GTI-P01-F-20
	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	VERSIÓN:	1
	DECLARACION DE APLICABILIDAD	VIGENCIA:	18-12-2020
		Página 1 de 1	

SECCION ANEXO A ISO 27001:2013
A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

A.5.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información.

Objetivo: Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
5.1.1	Políticas para la Seguridad de la Información.	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	Política general de seguridad de la información Resolución 0238 de 2020.	Implementado			X	
5.1.2	Revisión de las Política de Seguridad de la Información.	Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.	Actualización anual de Política registrada en el PSPI.	Implementado			X	

Justificación de exclusión
Comentarios/ Observaciones / Descripción General del Control
5.1.1 Política general de seguridad de la información en actualizacion en 2023 para alinearla a la ISO27001:2022

SECCION ANEXO A ISO 27001:2013
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

A.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.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.6.1.1	Seguridad de la Información Roles y Responsabilidades.	Se deben definir y asignar todas las responsabilidades de la seguridad de la información	El INC define la asignación de roles y responsabilidades a través de las siguientes acciones: *. Política de seguridad de la información * Comité de seguridad de la información. (MIPG) *. Revisión anual de Definición de roles de Seguridad en el PSPI. *Construccion de Matrices de roles y perfiles de SAP, Incompra y AD	Implementado			X	

Algunos ejemplos de Controles de Seguridad digital:

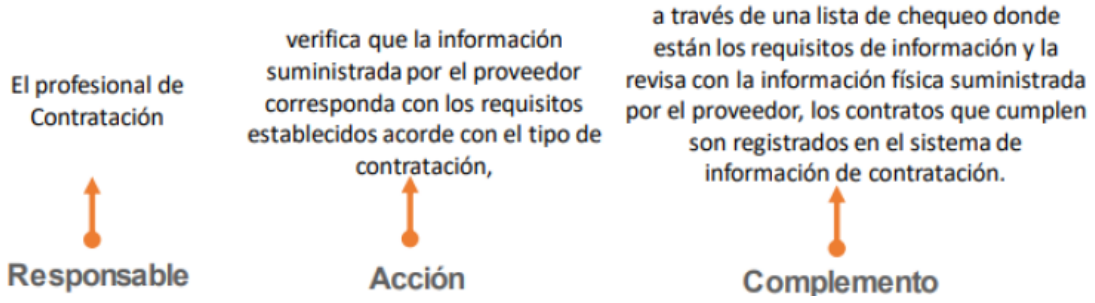
• Controles de acceso lógico y físico.
• Controles y restricciones de Navegación
• Protección de perdida de datos (DLP)
• IPS (Detección contra Intrusos)
• Segmentación de Redes
• Control de Aplicaciones
• WAF (Controle de firewall de acceso web)
• DDOS (Controles para denegación de servicio)
• Antispam
• Antivirus con Learning Machine
• Certificados digitales SSL
• Cifrado de información.
• Aseguramiento de la plataforma tecnológica.
• Ejecución de auditorías internas o externas
• Puesta en marcha de planes de contingencia
• Ejecución de backups o respaldos de información

Estructura para la descripción del control:
Para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

• Responsable de ejecutar el control: identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.

• Acción: se determina mediante verbos que indican la acción que deben realizar como parte del control.

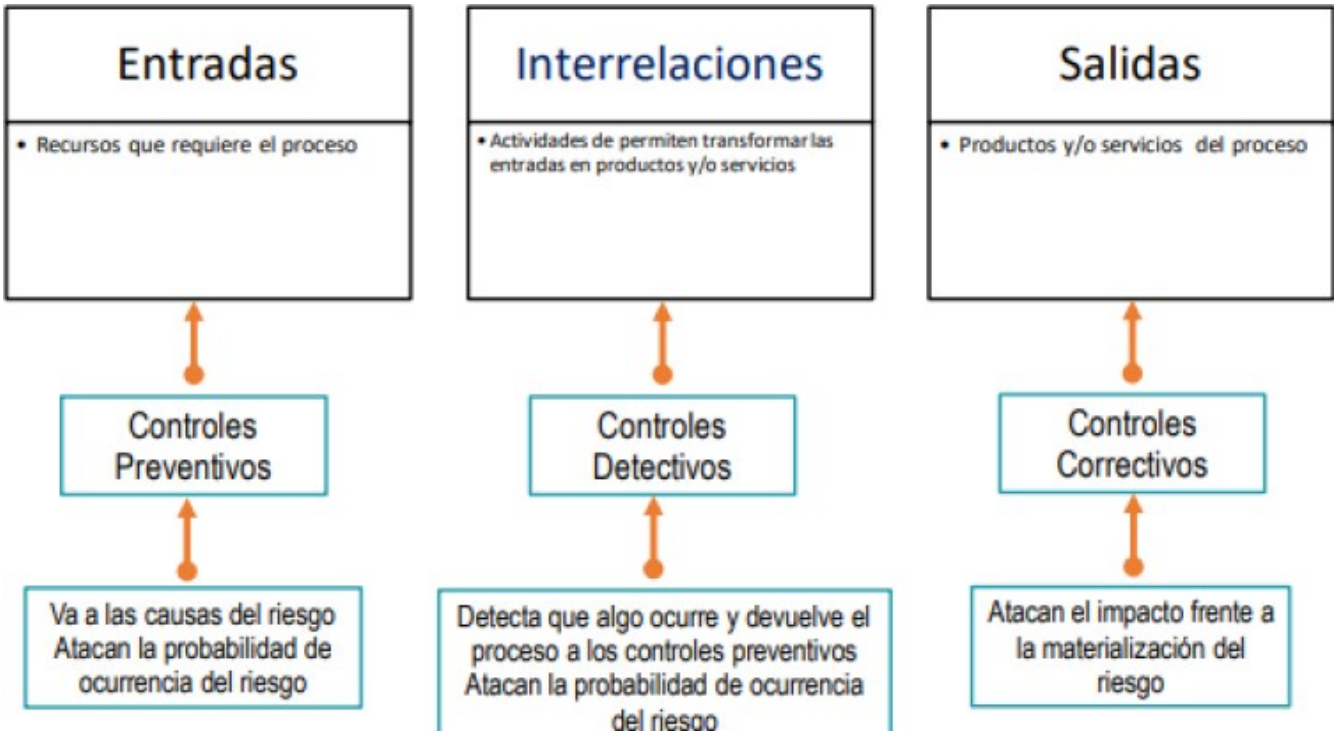
• Complemento: corresponde a los detalles que permiten identificar claramente el objeto del control.



Ejemplo: Fuente Guía administración del riesgo DAFP

Nota: la existencia de controles frente a la probabilidad o impacto dependerá del escenario de riesgo de seguridad digital en particular

Tipología de controles y los procesos: a través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión. Para comprender esta estructura conceptual, se consideran 3 fases globales del ciclo de un proceso así:



Fuente: Guía para la Administración del Riesgo DAFP Versión 6.

Valoración de los controles

Corresponde valorar los controles y de acuerdo con las respuestas se aplicará puntaje evaluando el nivel de solidez en los siguientes criterios:

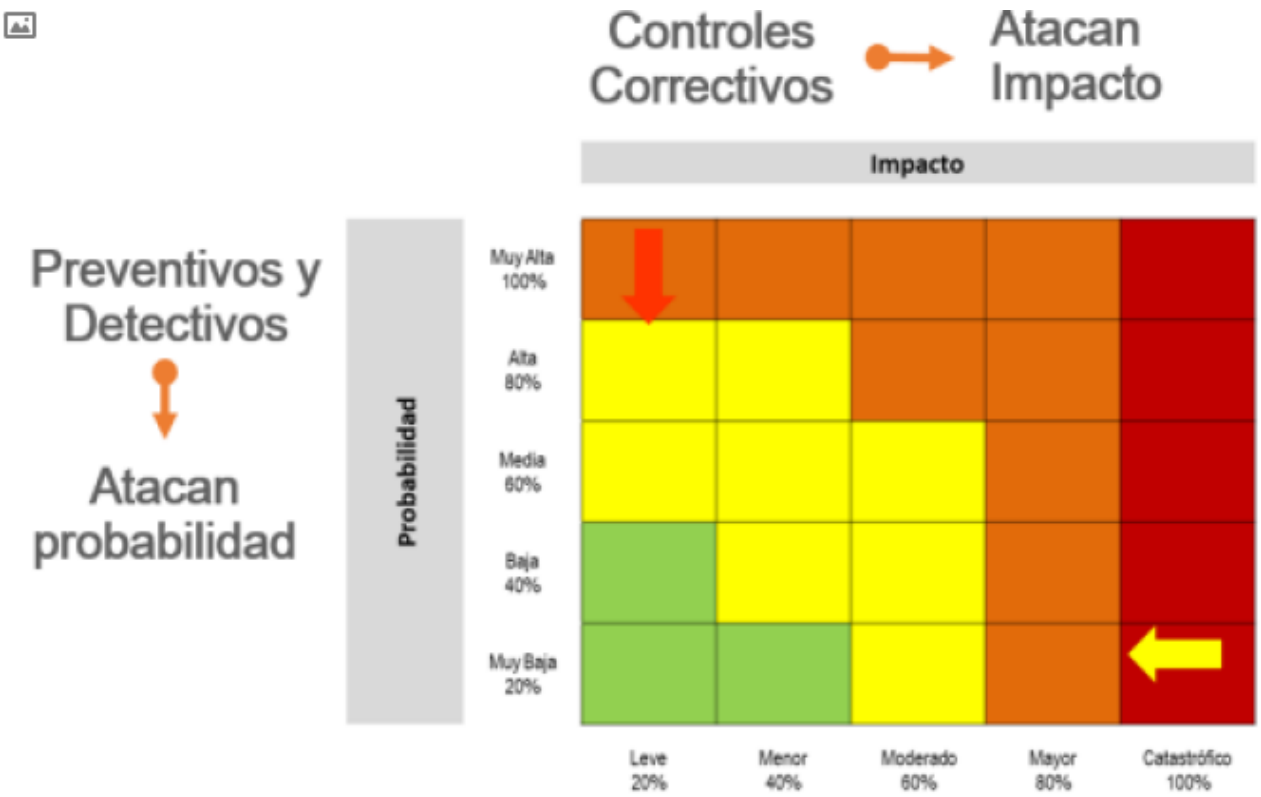
- **Control preventivo:** control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
- **Control detectivo:** control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- **Control correctivo**: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos. Así mismo, de acuerdo con la forma como se ejecutan tenemos:
- **Control manual:** controles que son ejecutados por personas.
- **Control automático:** son ejecutados por un sistema.

De acuerdo con la sumatoria obtenida se determina el rango aplicable al diseño y se determina el rango de calificación del criterio de la ejecución, la cual busca determinar la rigurosidad con la que se ejecuta el control.

Análisis y evaluación de los controles – Atributos: a continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la siguiente tabla se puede observar la descripción y peso asociados a cada uno así:

Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad. Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor que corresponde al movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.



Fuente: Guía para la Administración del Riesgo DAFP Versión 6.

Priorización de Riesgos

Con base en la ubicación de los riesgos dentro de la matriz de valoración – mapa de calor, se determinan los riesgos que requieren acciones de tratamiento a riesgos, bajo el enfoque de criticidad de la zona en que se encuentran e impacto en la materialización de estos, dando prioridad a las calificaciones más altas y determinando la acción requerida asociada a la eliminación de las causas y a el fortalecimiento de los controles existentes (priorizando los riesgos a tratar). Lo anterior está determinado de la siguiente manera para el INC:

ZONA DE RIESGO	DESCRIPCIÓN
EXTREMA	Se requiere una acción inmediata
ALTA	Se requiere una pronta atención
MODERADA	Se administra con procedimientos normales de control
BAJA	Genera menores efectos que pueden ser fácilmente remediados

Niveles de aceptación y tratamiento de los riesgos

La tolerancia o aceptación es el nivel del riesgo que puede o está dispuesta a soportar el INC en relación con la consecución de sus objetivos, está sujeto al tratamiento, manejo y seguimiento a los riesgos que afectan el logro de los objetivos institucionales y son considerados para cada uno de los procesos. Por lo anterior el INC determina:

• Tolerar o acepta los riesgos de seguridad digital que se encuentren en zona residual BAJA y MODERADA, los riesgos calificados en estas zonas de criticidad cumplen con los criterios de aceptación de riesgo, no es necesario poner controles adicionales y este puede ser aceptado, están sujetos a monitoreo permanente, para ellos se establecen acciones de control preventivas que permitan reducir la probabilidad de ocurrencia del riesgo.

• Los riesgos de seguridad digital que el INC prioriza son los que posterior a la etapa de valoración se ubiquen en zona de riesgo residual ALTA o EXTREMA, estos riesgos se deben incluir en el matriz de riesgo Institucional y a ellos se les establece controles o acciones de control preventivas que permitan mitigar la materialización del riesgo y se debe hacer seguimiento.

• En los riegos de seguridad digital valorados en zona de riesgo residual ALTA o EXTREMA, se consolidará el plan de tratamiento de riesgos de Seguridad de la Información. Para los riesgos que se consideren en zona BAJA y MODERADA, se deben continuar monitoreando la operación de los controles.

Tratamiento de los riesgos de seguridad digital

Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos de seguridad digital.

Las opciones existentes en materia de tratamiento del riesgo la definen los lideres de proceso o procedimiento en conjunto con el oficial de seguridad de la información, quienes deberán tener en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre el instituto, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento. El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

• **Evitar el riesgo:** cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades. Desde el punto de vista de los responsables de la toma de decisiones, este tratamiento es simple, la menos arriesgada y costosa, pero es un obstáculo para el desarrollo de las actividades del INC y, por lo tanto, hay situaciones donde no es una opción.

• **Reducir o mitigar el riesgo:** el nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para el INC. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo. Deberían seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

• **Aceptar el riesgo:** aceptar un riesgo es una decisión informada de asumir las consecuencias y la probabilidad de un riesgo en particular, generalmente se admite la existencia del riesgo debido a que se encuentra en una zona de riesgo “Baja” o “Moderada”; el responsable puede aceptar las posibles consecuencias, si estas no afectan el logro de los objetivos del proceso.

• **Trasferir el riesgo:** es entregar la responsabilidad a otra persona u entidad para que se encargue de prevenirlo, eliminarlo o asumir el costo financiero en caso de que el evento o riesgo negativo ocurra. Con la transferencia, el problema pasa a ser de esa otra entidad o persona a la que se le entrega la responsabilidad. En el INC es una alternativa casi nula ya que la gestión de riesgo digital es siempre compartida con el tercero, proveedor o entidad.

Se podrá establecer plan o acciones de tratamiento (diferente a los controles) a los riesgos identificados por proceso, teniendo en cuenta el enfoque hacia el control y la mitigación de las causas identificadas.

4.3.5. 5ta Fase: Monitoreo y revisión

Los controles de seguridad digital deben monitorearse y evaluarse regularmente para garantizar su efectividad y mejorarlos continuamente. Esto incluye la revisión de políticas y procedimientos de seguridad.

El seguimiento a la actualización de las matrices de riesgo y de la gestión del riesgo, acorde con las líneas de defensa del Modelo Integrado de Planeación y Gestión – MIPG- la segunda línea de defensa a cargo de la oficina de Planeación y Sistemas quien realizará verificación de monitoreo de riesgos por parte de la primera línea de defensa, además presentará de manera anual informe de la gestión integral del riesgo.

El Líder del Proceso de TI, en conjunto con sus equipos de trabajo deben monitorear y revisar cada 3 meses como mínimo los riesgos de su proceso y la efectividad de los controles establecidos y de ser necesario ajustarlos.

El Líder del Proceso de TI, en conjunto con su equipo de trabajo y Oficial de seguridad de la información monitorear y revisar mensualmente la materialización de riesgo de seguridad digital, generando los respectivos indicadores y análisis en la herramienta institucional de Gobierno riesgo y cumplimiento (GRC) .

En el evento de materializarse un riesgo, es necesario que el líder realice los ajustes necesarios con acciones, tales como:

- Informar de la ocurrencia del hecho
- Si se trata de corrupción realizar la denuncia del posible acto y tomar medidas.
- Revisar el Mapa de Riesgos, en particular las causas, factores de riesgo y controles.
- Realizar análisis causal del evento y adoptar las medidas o acciones necesarias
- Realizar un monitoreo permanente.
- Reportar en el indicador de riesgos materializados por proceso y realizar su respectivo análisis.

Cuando se trate de materialización de riesgos de seguridad digital, estos se deben tratar según el Manual de Gestión de Incidentes de Seguridad de la Información (o norma que la modifique, adicione o sustituya), el cual define la metodología de tratamiento, medidas de contención, erradicación y recuperación y las actividades que deben realizarse pos incidente.

Anualmente se debe diligenciar el Instrumento de Evaluación MSPI del ministerio de tecnologías de la información y las comunicaciones MINTIC. Esta herramienta permite identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, incluyendo la gestión de riesgos, la madurez de controles de seguridad digital, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior del instituto

Seguimiento

- **Oficina de Planeación y lideres de subsistemas de riesgos**

El seguimiento a la actualización de las matrices de riesgo y de la gestión del riesgo, acorde con las líneas de defensa del Modelo Integrado de Planeación y Gestión – MIPG- la segunda línea de defensa a cargo de la oficina de Planeación y Sistemas quien realizará verificación de monitoreo de riesgos por parte de la primera línea de defensa, además presentará de manera anual informe de la gestión integral del riesgo, incluido seguridad digital.

- **Oficina de Control interno**

De conformidad con la normatividad vigente, entre otras, el Manual Operativo de MIPG, la Oficina de Control Interno ejecuta la evaluación Independiente con periodicidad anual o semestral, realizando evaluación y seguimiento del Sistema de Gestión de Riesgos de seguridad digital, revisión de la aplicación y efectividad de los

controles de acuerdo con el Instrumento de Evaluación MSPI de MINTIC, así como los planes de mejora de tratamiento a riesgos de seguridad digital que se suscriban. Lo anterior de acuerdo con los niveles de riesgo residual. Se incluirá el resultado de esta revisión dentro de los informes de control interno.

Actualización De Mapa de Riesgos de seguridad digital.

La revisión al contenido de la matriz de riesgos de seguridad digital se realizará como mínimo una vez al año o cuando las circunstancias lo ameriten, a partir de modificaciones, cambios sustanciales en el contexto o cualquier hecho sobreviviente externo o interno que afecte la operación del proceso o de la entidad

4.3.6 Política de administración de riesgo (Articulación)

La política de administración de riesgo de seguridad digital se encuentra integrada a la Política de Administración de Riesgo del INC. Esta política se encuentra publicada en el portal web institucional mediante la Resolución 0820 de 2024- Política de administración de riesgo.

4.3.7. Comunicación y consulta

La comunicación y sensibilización de los riesgos incluidos los riesgos de seguridad digital son componentes esenciales del plan de sensibilización y capacitación en seguridad de la información del instituto: GTI-P01-PL-03 PLAN DE CAPACITACION Y SENSIBILIZACION EN SEGURIDAD DE LA INFORMACIÓN.

Dichas sensibilizaciones permiten desplegar y mantener la metodología de riesgo, y actualizar a los usuarios del INC acerca de las amenazas digitales actuales y potenciales, así como de las mejores prácticas de ciberseguridad. A través de campañas de concienciación, así como la difusión de casos de estudio y ejemplos concretos, se busca crear una cultura de seguridad y riesgo sólida. Esto empodera los colaboradores para que tomen medidas proactivas para proteger la información, y fomenta la colaboración y la responsabilidad compartida en la protección de los activos digitales de la organización.

5. Metas (Criterios de evaluación)

Los criterios de evaluación que se definen en el instituto para evaluar la gestión de riesgos de seguridad digital son los siguientes:

- Identificar los riesgos de seguridad digital y de continuidad informática
- Evaluar la gravedad de los riesgos
- Desarrollar estrategias para mitigar los riesgos
- Monitorear y revisar la gestión de riesgos

6. INDICADORES

ID	Criterios de Evaluación	Nombre de indicador	Descripción
1	-Identificar los riesgos de seguridad digital y de continuidad informática -Evaluar la gravedad de los riesgos	Actualización del mapa de riesgos del proceso GTI	Fórmula: Mapa de riesgos del proceso GTI actualizado Frecuencia: Anual Responsable de cargue: Profesional de riesgo - Oficina de Planeación Eje de acreditación: Gestión del riesgo Tipo de proceso: Procesos Estratégicos Misión: Atención y cuidado de pacientes Visión: Reducción de la incidencia

			Principios BOTOSS: Seguridad Fuente: SIAPINC. POA
2	-Identificar los riesgos de seguridad digital y de continuidad informática -Evaluar la gravedad de los riesgos	Documento BIA-TI actualizado	Fórmula: Documento BIATI actualizado Frecuencia: Anual Responsable de cargue: Coordinador Gestión Ti / Oficial de seguridad de la información. Eje de acreditación: Gestión de la tecnología Tipo de proceso: Procesos de Apoyo Misión: Atención y cuidado de pacientes Visión: Innovación y tecnología Principios BOTOSS: Seguridad Fuente: SIAPINC. POA
3	Desarrollar estrategias para mitigar los riesgos	Documento plan de riesgos de seguridad digital y continuidad actualizado	Fórmula: Documento Plan de la seguridad y privacidad de la información actualizado. Frecuencia: Anual Tendencia: Ascendente Valor meta: 1.00 Responsable de cargue: Arquitecto Ti /Oficial de seguridad de la información. Eje de acreditación: Gestión de Riesgo Tipo de proceso: Procesos Estratégicos Misión: Atención y cuidado de pacientes Visión: Reducción de la incidencia Principios BOTOSS: Orientación a resultados Fuente: SIAPINC. POA
4	Desarrollar estrategias para mitigar los riesgos	Documento Plan Estratégico de seguridad de la información actualizado	Fórmula: Documento Plan de la seguridad y privacidad de la información actualizado. Frecuencia: Anual Tendencia: Ascendente Valor meta: 1.00 Responsable de cargue: Arquitecto Ti /Oficial de seguridad de la información. Eje de acreditación: Gestión de la tecnología Tipo de proceso: Procesos Estratégicos Misión: Atención y cuidado de pacientes Visión: Innovación y tecnología Principios BOTOSS: Orientación a resultados Fuente: SIAPINC. POA
5	Monitorear y revisar la gestión de riesgos	Porcentaje de ejecución del plan estratégico de seguridad de la información	Fórmula: {Número actividades ejecutadas del plan de seguridad y privacidad de la información} / {Total actividades programadas del plan de seguridad y privacidad de la información} * 100 Unidad: Porcentaje (%) Frecuencia: Trimestral Valor meta: 100.00

			Responsable de cargue: Coordinador Grupo Area Gestión TI Eje de acreditación: Gestión de la tecnología Tipo de proceso: Procesos de Apoyo Misión: Atención y cuidado de pacientes Visión: Innovación y tecnología Principios BOTOSS: Orientación a resultados Fuente: SIAPINC. POA
6	Monitorear y revisar la gestión de riesgos de seguridad digital y continuidad informática	Porcentaje de cumplimiento de monitoreo y seguimiento de riesgos proceso GTI	Fórmula: {Número de criterios de evaluación cumplidos de la lista de seguimiento y monitoreo proceso GTI}/{Número total de criterios evaluados lista de seguimiento y monitoreo para el periodo del proceso GTI} * 100 Unidad: Porcentaje (%) Frecuencia: Trimestral Tendencia: Ascendente Valor meta: 100.00 Responsable de cargue: Diana Patricia Martínez Malaver Responsable de Análisis: Diana Patricia Martínez Malaver Eje de acreditación: Gestión del riesgo Tipo de proceso: Procesos Estratégicos Misión: Atención y cuidado de pacientes Visión: Reducción de la incidencia Principios BOTOSS: Orientación a resultados Fuente: SIAPINC. POA
7	Monitorear y revisar la gestión de riesgos de seguridad digital y continuidad informática	Porcentaje de riesgos materializados proceso GTI	Fórmula: {Número de riesgos materializados en el periodo proceso GTI}|{Total de riesgos identificados proceso GTI} * 100 Unidad: Porcentaje (%) Frecuencia: Mensual Responsable de cargue: Coordinador Grupo Gestión TI Eje de acreditación: Gestión del riesgo Tipo de proceso: Procesos Estratégicos Misión: Atención y cuidado de pacientes Visión: Reducción de la incidencia Principios BOTOSS: Orientación a resultados Fuente: SIAPINC.PROCESO

7. CRONOGRAMA

Se presenta cronograma de actividades, de acuerdo con los componentes y actividades del SGSI, y la norma iso27001:2022

Nombre del componete en SGSI	Nombre de la actividad	Nombre de la tarea	Comienzo	Fin	Nombre de los recursos
Liderazgo del SGSI	**Políticas**	Actualización de política de riesgos en su componente de seguridad digital y continuidad informática	01/06/2025	30/09/2025	Profesional de riesgo, CISO, Oficina de planeación
Evaluación rendimiento del SGSI	**Seguimiento, medición, análisis y evaluación**	Aplicar instrumento de medición de desempeño de SGSI del MSPI, SO27001 y NIST	01/10/2025	31/10/2025	CISO; Coordinador Grupo Area Sistemas; Líder Gestión Documental;
Operación del SGSI	**Planificación y control operativo**	Proceso contratación herramienta gestión de riesgos GRC	15/01/2025	30/03/2025	Profesional de riesgo; CISO
		Implementación de cambios herramienta GRC	20/05/2025	30/08/2025	CISO;Oficina Asesora Jurídica contractual;Profesional de Riesgos;Lider Oficina planeación y Sistemas;Asesora de Calidad; Proveedor de GRC
		Elaboración y publicación Plan de Riesgos de Seguridad Digital y continuidad informática	01/05/2025	31/06/2025	CISO; Coordinador grupo Area TI; Profesional de Riesgo; Profesional de OyM
	Evaluación y Tratamiento de riesgos para la seguridad de la información	Actualización de análisis y Matriz de Riesgo GTI	01/11/2025	31/12/2025	CISO;Profesional de Riesgos
		Actualización de análisis y Matriz de Riesgo Continuidad	20/05/2025	31/12/2025	CISO; Líder de Continuidad Operativa; Consultor de continuidad de Negocio
		Actualización de declaración de	01/08/2025	31/10/2025	CISO;Direccion General;Coordinador Grupo

		Aplicabilidad de Controles			Aplicaciones;Coordinador Grupo Area Sistemas;Coordinador Grupo Hardware y Redes
		Actualización de BIA TI	15/07/2025	31/10/2025	CISO;Lider de PlaneaciónCISO;Lider de Continuidad Operativa; Consultor de continuidad de Negocio

8. RECURSOS

La estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad digital identificados en el instituto, corresponderá al dueño del riesgo, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos en el plan de tratamiento

Presupuesto: Valor: $136.000.000 COP

El proyecto de inversión y presupuesto de funcionamiento de este plan incluye actividades y recursos de tecnologías de la información, y se encuentra relacionado en el documentó GTI-P01-PL-01 Plan Estratégico de seguridad de la informacion, sección 5.13. PRESUPUESTO

También se identifican recursos generales que participan en la ejecución del plan:

Tipo de recursos (talento humano, materiales, infraestructura)	Nombre recurso	Variable
Talento Humano	Oficial de seguridad de la información	Responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad digital y contingencia informática, lo cual contribuye a la mejora continua
Talento Humano	Profesional de riesgo - planeación	Responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la gestión de riesgo
Talento Humano	Lideres de Procesos	Primera línea de defensa en la gestión de riesgo
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías	Plan de capacitación y sensibilización en segruidad de la información. Plan de auditorías - Control interno

9. EVALUACIÓN DE RESULTADOS

El seguimiento a los resultados de los indicadores definidos se realiza a traves de la oficina de riesgo, la oficina control interno, y el comité integrado de gestión institucional (MIPG). Todos los indicadores se registran en el sistema de gestión de calidad SIAPINC.

10. APROBACIÓN

El presente Plan se encuentra aprobado mediante acta institucional No. 05 de 23 de mayo de 2025 por el Comité Institucional de Gestión y Desempeño - MIPG

Lía Margarita Álvarez P.
Subdirectora de la Gestión Administrativa y Financiera

Luis Eduardo Martinez
Coordinador Grupo Área Gestión Sistemas

11. BIBLIOGRAFÍA

- Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 6
- Guía 10 - Continuidad de Negocio -Modelo de seguridad y privacidad de la información MINTIC
- Guía 7 - Gestión de Riesgos - Modelo de seguridad y privacidad de la información MINTIC
- Guía 8 - Controles de Seguridad de la Información - Modelo de seguridad y privacidad de la información MINTIC

VERSIÓN	FECHA DE ACTUALIZACIÓN	DESCRIPCIÓN DE ACTUALIZACIÓN	RESPONSABLE OYM
1	28-12-2023	Versión inicial del documento	Diego Andres Paez Gomez
2	20-06-2025	Se revisa el documento y se realizan los siguientes ajustes: Se ajusta la vigencia del plan. 2.Se ajusta la enumeración y estructura del documento. 3. se ajusta titulo del plan como plan de riesgo de seguridad digital. 4. En el ítem 3.2 FACTORES INTERNO se cambia la imagen del BOTOSS por el COTOSS.5 Se adiciona dos nuevos ítem de calificación frente a mejores practicas de ciberseguridad y avance del ciclo de funcionamiento del modelo de operación PHVA. 5. En el ítem 4.3.2 Identificación del riesgo de seguridad digital en la tabla se adiciona 7 amenazas de ciber seguridad. 6. En el ítem 4.3.3.1 Análisis de riesgo de seguridad digital se ajusta el contenido explicando los criterios, consecuencias e impactos de los riesgos de seguridad digital. 7. En el ítem 4.3.4 Evaluación de riesgo de seguridad digital se cambia el instructivo GSI-P07-I-01 por el manual GSI-P07-M-02, se adiciona temas relacionados con la determinación de controles, estructura para la descripción del control, Tipologia de controles y procesos, valoración de controles, priorización de riesgos, niveles de aceptación y tratamiento de riesgos. 8. En el ítem 4.3.5 Fase de Monitoreo y revisión se adiciona el seguimiento que se realiza desde la oficina de planeación, control interno, actualización de mapa de riesgos.	Laura Catherin Rodriguez Galan

ELABORÓ		REVISÓ		APROBÓ	
Cargo:	Profesional Universitario	Cargo:	Coordinador	Cargo:	Coordinador
Dependencia:	Oficina Asesora de Planeación y Sistemas	Dependencia.	Grupo Área Gestión de Tecnologías de Información	Dependencia:	Grupo Área Gestión de Tecnologías de Información
Fecha:	20-06-2025	Fecha:	20-06-2025	Fecha:	20-06-2025