Centro Nacional de Memoria Histórica

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

CENTRO NACIONAL DE MEMORIA HISTÓRICA

ENERO 2024

	NOMBRE	CARGO	FECHA
ELABORÓ	Ronal Alexis Martinez Ceron	Profesional Especializado	20/01/2024
REVISÓ	Fabio A Velandia Quecan	Profesional Especializado	20/01/2024
REVISÓ	Ana María Trujillo Coronado	Directora Administrativo y Financiero	23/01/2024
APROBÓ	Comité institucional de Gestión y desempeño	Comité institucional de Gestión y desempeño	xx/01/2024

Contenido

1. INTRODUCCIÓN

En el Centro Nacional de Memoria Histórica (CNMH) de Colombia, reconocemos la información como uno de nuestros activos más valiosos y críticos. Dada su relevancia, es esencial adoptar un enfoque robusto y sistemático para su protección. Este enfoque se centra en la identificación y el tratamiento de riesgos relacionados con la seguridad de la información, entendiendo que una gestión de riesgos eficaz es clave para salvaguardar nuestros datos.

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), siguiendo el ciclo de mejora continua "Planear, Hacer, Verificar y Actuar" (PHVA), constituye la piedra angular de nuestra estrategia para asegurar la confidencialidad, integridad y disponibilidad de la información. Este sistema no solo responde a los requerimientos de seguridad de la información establecidos, sino que también permite una gestión proactiva y adaptativa de los riesgos, garantizando así que el CNMH mantenga y mejore constantemente sus prácticas de seguridad de la información.

El presente Plan de Tratamiento de Riesgos es un componente esencial de nuestro SGSI. Establece el marco mediante el cual identificamos, evaluamos y tratamos los riesgos de seguridad y privacidad de la información, asegurando que nuestras operaciones y la información que gestionamos estén protegidas de manera efectiva contra amenazas y vulnerabilidades.

2. OBJETIVO

Establecer el contexto y la importancia de la gestión de riesgos de seguridad y privacidad de la información en el CNMH, subrayando la relevancia de la información como un activo crítico de la entidad. Este segmento tiene como objetivo proporcionar una visión general de los principios y estrategias que guían la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), destacando el enfoque en el ciclo de mejora continua “Planear, Hacer, Verificar y Actuar”. Además, busca enfatizar el compromiso del CNMH con la protección de la confidencialidad, integridad y disponibilidad de sus datos, estableciendo las bases para el desarrollo detallado del Plan de Tratamiento de Riesgos.

3. ALCANCE

Los procesos determinados en el alcance del SGSI: Difusión de Memoria Histórica; Acuerdos de la Verdad, Investigaciones, Registro – Acopio – Procesamiento, Talento Humano, Gestión de las TIC.

4. DEFINICIONES

- **Activo:** cualquier elemento que tiene valor para la organización y que para Gestión de riesgos de seguridad de la información se consideran los siguientes; información, software, físicos, servicios, personas e intangibles.
- **Amenaza:** causa potencial de un incidente no deseado, el cual puede resultar en daño al sistema o a la Entidad.
- **Confidencialidad:** propiedad de la información que hace que no esté disponible o que sea revelada a individuos no autorizados, entidades o procesos.
- **Disponibilidad:** propiedad de ser accesible y utilizable ante el uso de una entidad autorizada.
- **Importancia del activo:** valor que refleja el nivel de protección requerido por un activo de información frente a las tres propiedades de la seguridad de la información; integridad, confidencialidad y disponibilidad.
- **Integridad:** propiedad de precisión y completitud de la información.
- **Monitoreo:** verificación, supervisión, observación crítica o determinación continua del estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.
- **Parte involucrada:** persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o una actividad. Una persona que toma decisiones puede ser una parte involucrada.
- **Propietario del activo:** persona o cargo que administra, autoriza el uso, regula o gestiona el activo de información. El propietario del activo aprueba el nivel de protección requerido frente a confidencialidad, integridad y disponibilidad.
- **Riesgo:** un riesgo es más que la probabilidad que una amenaza informática se convierta en un evento real que resulte en una pérdida para la Entidad, el efecto de un riesgo es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen, medio ambiente) y se pueden aplicar a niveles diferentes (estratégico, operacional o toda la organización).
- **Vulnerabilidad:** es una debilidad identificada sobre un activo y que puede ser aprovechada por una amenaza para causar una afectación sobre la confidencialidad, integridad y/o

disponibilidad de la información

5. METODOLOGÍA

Considerando la Misión y objetivos del CNMH y teniendo en consideración la GUÍA METODOLÓGICA GESTIÓN DE RIESGOS PARA SGSI (G-1101-GTI-01) de la entidad, en la definición del Plan de tratamiento de riesgos de seguridad de la información se realizó la identificación de los controles con sus observaciones para abarcar el tratamiento de riesgos

SECCIÓN	CONTROL	OBSERVACIONES
A.5	**Políticas de Seguridad**	
A.5.1	Orientación de la Dirección para la gestión de la seguridad de la información	
A.5.1.1	Políticas para la seguridad de la información	Se define política (SIP- PC-013 V2 Política de Seguridad y privacidad de la Información- Intranet publicada y aprobada, se comunica a todo el personal del CNMH y se realizaran actualizaciones anuales, se considera el contexto, objetivos misionales y los resultados de Análisis de riesgos
A.5.1.2	Revisión de las políticas para la seguridad de la información	Se define política (SIP- PC-013 V2 Política de Seguridad y privacidad de la Información- Intranet publicada y aprobada, se comunica a todo el personal del CNMH y se realizarán actualizaciones anuales
A.6	**Aspectos Organizativos de la Seguridad de la Información**	
A.6.1	Organización Interna	
A.6.1.1	Roles y Responsabilidades de Seguridad de la Información	Se define política de roles y responsabilidades, adicional a lo anterior se establece un profesional encargado de realizar el seguimiento al S.G.S.I.
A.6.1.2	Separación de deberes	Se define política de control de acceso mediante la cual se asignan o no permisos. Se establece la separación de deberes mediante la aplicación de la política de control de acceso, los deberes se encuentran definidos en el Manual de funciones (GTH-PR-001 V3 Actualización Manual Funciones)
A.6.1.3	Contacto con las autoridades	Se define instructivo GTC-IN-001 V2 para el Contacto con las autoridades
A.6.1.4	Contacto con grupos de interés especial	Se verifico que ya se tiene el GTC-IN-001 V2 Instructivo para el Contacto con las autoridades e igualmente los grupos de interés
A.6.1.5	Seguridad de la información en la gestión de proyectos	En los proyectos se tiene en cuenta la seguridad de la información y cláusulas de confidencialidad en los contratos
A.6.2	Dispositivos móviles y teletrabajo	

SECCIÓN	CONTROL	OBSERVACIONES
A.6.2.1	Política para dispositivos móviles	Se encuentra definida la política de dispositivos móviles
A.7	**Seguridad Ligada a los Recursos Humanos**	
A.7.1	Antes de asumir el empleo	
A.7.1.1	Selección	En el proceso de Adquisición de Bienes y Servicios se cuenta con el Procedimiento de Contratación Directa de Prestación de Servicios Profesionales y de acuerdo a la Gestión. El cual cumple revisando la lista de Chequeo "ABS-FT-007 V11 Lista de Chequeo - Personas Naturales"
A.7.1.2	Términos y condiciones del empleo	Para los Contratos en el "ABS-FT-013 V8 Minuta de Contrato", contiene todas las obligaciones de los contratistas y de la Entidad respecto a lo solicitado.
A.7.2	Durante el empleo	
A.7.2.1	Responsabilidades de la dirección	Se realizan sensibilizaciones periódicas y la Directora General formaliza la implementación del SGSI con un acto administrativo, provee y vela por el cumplimiento de las directrices establecidas.
A.7.2.2	Concienciación sobre la seguridad de la información, la educación y la formación	Se realizan planes de sensibilización y encuestas de seguridad a los funcionarios y colaboradores del CNMH, contando con el apoyo de Talento Humano
A.7.2.3	Proceso disciplinario	Está definido el Proceso disciplinario para registrar, evaluar y sancionar el incumplimiento de las Políticas de Seguridad de la Información
A.7.3	Terminación y cambio de empleo	
A.7.3.1	Terminación o cambio de responsabilidades de empleo	Los contratos contienen este detalle
A.8	**Gestión de Activos**	
A.8.1	Responsabilidad de los activos	
A.8.1.1	Inventario de Activo	Se define un inventario de activos de información que se actualiza anualmente
A.8.1.2	Propietario de los activos	El inventario de activos fue definido incluyendo el Propietario de cada activo.
A.8.1.3	Uso aceptable de los activos	Definido con las políticas y procedimientos del SGSI que determinan el uso aceptable de los activos
A.8.1.4	Devolución de los activos	Está definido un procedimiento a este control
A.8.2	Clasificación de la información	
A.8.2.1	Clasificación de la información	Está definida la metodología de Identificación, clasificación y valoración de los activos de información la cual rige a partir de la formalización del SGSI
A.8.2.2	Etiquetado de la información	Está definido el procedimiento de etiquetado de la información el cual está aprobado por la dirección.

SECCIÓN	CONTROL	OBSERVACIONES
A.8.2.3	Manejo de activos	A partir de la implementación del SGSI el manejo de activos debe llevarse a cabo con la aplicación de las Políticas y Procedimientos que apliquen para cada uno
A.8.3	Manejo de medios	
A.8.3.1	Gestión de medios removibles	Definido en el Procedimiento para la Gestión segura de medios removibles
A.8.3.2	Disposición de los medios	Definido en el Procedimiento para la Gestión segura de medios removibles
A.8.3.3	Transferencia de medios físicos	Definido en la política de manejo, disposición de información, medios y equipos
A.9	**Control de Acceso**	
A.9.1	Requisitos del negocio para el control de acceso	
A.9.1.1	Política de control de acceso	Fue definida la Política de Control de Acceso a la Información que define los criterios para que la protección se cumpla con base en la criticidad de los activos involucrados
A.9.1.2	Acceso a redes y servicios en red	Se definieron las políticas de control de acceso y la política de establecimiento, uso y protección de claves de acceso
A.9.2	Gestión de acceso de usuarios	
A.9.2.1	Registro y cancelación del registro de usuarios	Está definida las políticas de control de acceso y la política de establecimiento, uso y protección de claves de acceso
A.9.2.2	Suministro de acceso de usuarios	Está definida las políticas de control de acceso y la política de establecimiento, uso y protección de claves de acceso
A.9.2.3	Gestión de derechos de acceso privilegiado	Está definida las políticas de control de acceso y la política de establecimiento, uso y protección de claves de acceso
A.9.2.4	Gestión de información de autenticación secreta de usuarios	Está definida las políticas de control de acceso y la política de establecimiento, uso y protección de claves de acceso
A.9.2.5	Revisión de los derechos de acceso de usuarios	Está contemplado este aspecto en el registro de perfiles de usuario
A.9.2.6	Retiro o ajuste de los de derechos de acceso	Está contemplado este aspecto en el registro de perfiles de usuario
A.9.3	Responsabilidades de los usuarios	
A.9.3.1	Uso de información de autenticación secreta	Se realiza control mediante el dominio para exigir a los usuarios con las prácticas de autenticación secreta
A.9.4	Control de acceso al sistema y aplicaciones	
A.9.4.1	Restricciones de acceso a la información	Definido en la política de control de acceso
A.9.4.2	Procedimiento de ingreso seguro	Definido en la política de control de acceso
A.9.4.3	Sistema de gestión de contraseñas	Definido en la política de control de acceso

SECCIÓN	CONTROL	OBSERVACIONES
A.9.4.4	Uso de programas utilitarios privilegiados	Definido en la política de control de acceso
A.9.4.5	Control de acceso a códigos fuente de programas	Se restringe el acceso al código fuente de todas las aplicaciones excepto aquellas que son intervenidas por el CNMH, para lo cual se tiene un profesional especializado
A.10	**Cifrado**	
A.10.1	Controles criptográficos	
A.10.1.1	Política de uso de controles criptográficos	Definido en la política de controles criptográficos
A.10.1.2	Gestión de llaves	Definido mediante la política de controles criptográficos
A.11	**Seguridad Física y Ambiental**	
A.11.1	Áreas seguras	
A.11.1.1	Perímetro de seguridad física	Establecida en la logística para la seguridad perimetral
A.11.1.2	Controles de acceso físicos	Se define control de acceso físico
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Se define procedimiento de Trabajo en Áreas Seguras
A.11.1.4	Protección contra las amenazas externas y ambientales	Se define procedimiento de Trabajo en Áreas Seguras
A.11.1.5	Trabajo en áreas seguras	Se define procedimiento de Trabajo en Áreas Seguras
A.11.1.6	Áreas de despacho y carga	Se definen los aspectos y alcance de este control
A.11.2	Equipos	
A.11.2.1	Ubicación y protección de equipos	Se define control mediante la política de seguridad del centro de datos y centros de cableado
A.11.2.2	Servicios de suministro	Se define control mediante la política de seguridad del centro de datos y centros de cableado
A.11.2.3	Seguridad del cableado	Se define control mediante la política de seguridad del centro de datos y centros de cableado
A.11.2.4	Mantenimiento de los equipos	Se definen los aspectos de este control por medio del plan de mantenimiento
A.11.2.5	Retiro de activos	Se define la política de Manejo y disposición de información medios y equipos
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Se define el alcance de este control
A.11.2.7	Disposición segura o reutilización de equipos	Se define el alcance de este control
A.11.2.8	Equipo de usuario desatendido	Control definido en la Política de Escritorio y Pantallas limpias
A.11.2.9	Política de escritorio limpio y pantalla limpia	Control definido en la Política de Escritorio y Pantallas limpias
A.12	**Seguridad en la Operativa**	
A.12.1	Procedimientos operacionales y responsabilidades	

SECCIÓN	CONTROL	OBSERVACIONES
A.12.1.1	Procedimientos de operación documentados	Los procedimientos se encuentran en el SIG Procesos de tecnología de la Información y las Comunicaciones
A.12.1.2	Gestión de cambios	Se encuentra definido el proceso de Gestion de Cambios
A.12.1.3	Gestión de la capacidad	Se realiza seguimiento periódico de capacidad de procesamiento y almacenamiento
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Los sistemas que experimentan ajustes y cuentan con ambientes de pruebas
A.12.2	Protección contra códigos maliciosos	
A.12.2.1	Controles contra códigos maliciosos	Este aspecto fue contemplado en el desarrollo de las Políticas complementarias.
A.12.3	Copias de respaldo	
A.12.3.1	Respaldo de la información	Definido en la Política de Generación de Copias de respaldo
A.12.4	Registro y seguimiento	
A.12.4.1	Registro de eventos	El alcance de este control fue definido en el protocolo
A.12.4.2	Protección de la información de registro	El alcance de este control fue definido en el protocolo
A.12.4.3	Registros del administrador y del operador	El alcance de este control fue definido en el protocolo
A.12.4.4	Sincronización de relojes	El alcance de este control fue definido en el protocolo
A.12.5	Control de software operacional	
A.12.5.1	Instalación de software en sistemas operativos	Está definido el procedimiento para autorización de instalación de software
A.12.6	Gestión de la vulnerabilidad técnica	
A.12.6.1	Gestión de las vulnerabilidades técnicas	El alcance de este control se definió mediante análisis de software
A.12.6.2	Restricciones sobre la instalación de software	Está definido el Procedimiento para Autorización de instalación de software
A.12.7	Consideraciones sobre auditorías de sistemas de información	
A.12.7.1	Controles sobre auditorías de sistemas de información	
A.13	**Seguridad en las comunicaciones**	
A.13.1	Gestión de la seguridad de las redes	
A.13.1.1	Controles de redes	Se deben aplicar las recomendaciones del documento de Arquitectura de Seguridad
A.13.1.2	Seguridad de los servicios de red	Se deben aplicar las recomendaciones del documento de Arquitectura de Seguridad
A.13.1.3	Separación en las redes	Se deben aplicar las recomendaciones del documento de Arquitectura de Seguridad
A.13.2	Transferencia de información	
A.13.2.1	Políticas y procedimientos de transferencia de información	Se aplica la política definida para la transferencia de información

SECCIÓN	CONTROL	OBSERVACIONES
A.13.2.2	Acuerdos sobre transferencia de información	Se aplica la política definida para la transferencia de información
A.13.2.3	Mensajería electrónica	Los aspectos relacionados con este control fueron definidos en la política
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Los aspectos relacionados con este control fueron definidos en la política
A.14	**Adquisición, Desarrollo y Mantenimiento de Sistemas de Información**	
A.14.1	Requisitos de seguridad de los sistemas de información	
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Contemplado en la Política de desarrollo seguro de software
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Contemplado en la Política de desarrollo seguro de software
A.14.1.3	Protección de las transacciones de los servicios de las aplicaciones	Contemplado en la Política de desarrollo seguro de software
A.14.2	Seguridad en los procesos de desarrollo y de soporte	
A.14.2.1	Política de desarrollo seguro	Contemplado en la Política de desarrollo seguro de software
A.14.2.2	Procedimientos de control de cambios en sistemas	Definido en el procedimiento de control de cambios
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Se definió política para tal fin
A.14.2.4	Restricciones en los cambios a los paquetes de software	Contemplado en la Política de desarrollo seguro de software.
A.14.2.5	Principios de construcción de los sistemas seguros	Se definieron las respectivas políticas
A.14.2.6	Ambiente de desarrollo seguro	Se definieron las respectivas políticas
A.14.2.7	Desarrollo contratado externamente	Contemplado en la Política de desarrollo seguro de software
A.14.2.8	Pruebas de seguridad de sistemas	N/A
A.14.2.9	Pruebas de aceptación de sistemas	Los aspectos relacionados con este control fueron definidos
A.14.3	Datos de prueba	
A.14.3.1	Protección de los datos de prueba	Los aspectos relacionados con este control fueron definidos
A.15	**Relaciones con los proveedores**	
A.15.1	Seguridad de la información en las relaciones con proveedores	

SECCIÓN	CONTROL	OBSERVACIONES
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Está definido en la política de seguridad proveedores
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Está definido en la política de seguridad proveedores
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	
A.15.2	Gestión de la prestación de servicios de proveedores	
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Los aspectos relacionados con este control fueron definidos
A.15.2.2	Gestión de cambios en los servicios de los proveedores	Los aspectos relacionados con este control fueron definidos
A.16	**Gestión de incidentes de seguridad de la información**	
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	
A.16.1.1	Responsabilidades y procedimientos	Los aspectos relacionados con este control fueron definidos
A.16.1.2	Reporte de eventos de seguridad de la información	Los aspectos relacionados con este control fueron definidos
A.16.1.3	Reporte de debilidades de seguridad de la información	Los aspectos relacionados con este control fueron definidos
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los aspectos relacionados con este control fueron definidos
A.16.1.5	Respuesta a incidentes de seguridad de la información	Los aspectos relacionados con este control fueron definidos
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Los aspectos relacionados con este control fueron definidos
A.16.1.7	Recopilación de evidencia	Los aspectos relacionados con este control fueron definidos
A.17	**Aspectos de la seguridad de la información de la gestión de continuidad de negocio**	
A.17.1	Continuidad de seguridad de la información	
A.17.1.1	Planificación de la continuidad de la seguridad de la información	Está definido en el Procedimiento para la Continuidad del negocio
A.17.1.2	Implantación de la continuidad de la seguridad de la información	Está definido un Procedimiento para la Continuidad de la Seguridad de la Información
A.17.1.3	Verificación, revisión y evaluación de la continuidad	Está definido el Procedimiento para la Continuidad de la Seguridad de la Información

SECCIÓN	CONTROL	OBSERVACIONES
	de la seguridad de la información	
A.17.2	Redundancias	
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	Está definido un Procedimiento para la Continuidad de la Seguridad de la Información
A.18	**Cumplimiento**	
A.18.1	Cumplimiento de requisitos legales y contractuales	
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Está definidos en la Política de cumplimiento de requisitos legales y contractuales
A.18.1.2	Derechos de propiedad intelectual (DPI)	El alcance de este control está definido en la Política de cumplimiento de requisitos legales y contractuales. Los usuarios no pueden instalar software. Hay inventario de software
A.18.1.3	Protección de registros	El alcance de este control está definido en la Política de cumplimiento de requisitos legales y contractuales y se cuenta con TRD
A.18.1.4	Privacidad y protección de información de datos personales	Definida en la Política de tratamiento de datos personales, Política de protección de datos personales y política de tratamiento de la información y datos personales
A.18.1.5	Reglamentación de controles criptográficos	
A.18.2	Revisiones de seguridad de la información	
A.18.2.1	Revisión independiente de la seguridad de la información	Se realizan auditorias esporádicas o dependiendo de la necesidad. Planificadas por Control interno o contraloría
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	El centro de cómputo se revisa periódicamente. A los sistemas de información se les monitorea regularmente la seguridad
A.18.2.3	Revisión del cumplimiento técnico	Los aspectos de este control fueron definidos

6. Identificación de Riesgos:

Esta fase del plan tiene como objetivo analizar y valorar los riesgos identificados, para comprender su magnitud y establecer prioridades en el tratamiento. Esto implica evaluar tanto la probabilidad de que cada riesgo se materialice como el impacto que tendría en la entidad si ocurriera.

Evaluación de la Probabilidad:

- Estimar la frecuencia con la que se espera que ocurra cada riesgo. Esto puede basarse en datos históricos, tendencias del sector, evaluaciones expertas, entre otros.
- Clasificar la probabilidad en categorías, por ejemplo, muy baja, baja, moderada, alta y muy alta.

Evaluación del Impacto:

- Determinar el grado de afectación que tendría el riesgo en la entidad. El impacto puede ser en términos de pérdida financiera, daño a la reputación, interrupción de operaciones, entre otros.
- Clasificar el impacto en categorías como mínimo, bajo, moderado, alto y muy alto.

Análisis Cualitativo y Cuantitativo:

- Realizar un análisis cualitativo para obtener una visión general de la naturaleza y el efecto potencial de los riesgos.
- Complementar con un análisis cuantitativo cuando sea posible, utilizando datos numéricos para estimar probabilidades e impactos.

Resultados del Análisis y la Valoración:

- Crear una matriz de riesgos que cruce la probabilidad con el impacto para cada riesgo identificado, lo que permite visualizar y priorizar los riesgos.
- Identificar los riesgos que requieren atención inmediata (alta probabilidad y alto impacto) y aquellos que pueden ser monitoreados o tratados de manera diferente.

7. Estrategia de Tratamiento de Riesgos

El propósito de esta sección es definir las estrategias para abordar los riesgos de seguridad y privacidad de la información identificados en el CNMH. Esto implica determinar la mejor manera de manejar cada riesgo, con el objetivo de reducir su probabilidad de ocurrencia o minimizar su impacto en la entidad.

Opciones Generales de Tratamiento:

- **Evitar:** Implementar medidas para prevenir completamente el riesgo o retirarse de la actividad que lo genera.
- **Transferir:** Delegar la responsabilidad del riesgo a terceros, como a través de seguros o acuerdos contractuales.
- **Mitigar:** Aplicar controles y medidas para reducir la probabilidad o impacto del riesgo. Esto puede incluir cambios en procesos, políticas, tecnologías, etc.
- **Aceptar:** Reconocer que el riesgo existe y decidir no tomar medidas específicas, generalmente debido a que el costo de tratar el riesgo es mayor que el impacto potencial.

Estrategias Específicas para Cada Riesgo Identificado:

- Basado en los resultados del análisis y valoración de riesgos, se seleccionará la opción más adecuada para cada riesgo.
- Se detallará la estrategia específica para cada riesgo, describiendo las acciones y controles que se implementarán.

Consideraciones para la Selección de Estrategias:

- La elección de la estrategia debe estar alineada con la tolerancia al riesgo de la entidad y los objetivos generales del CNMH.
- Se deben tener en cuenta factores como el costo, la eficacia, la factibilidad y el impacto en las operaciones al seleccionar las estrategias de tratamiento.

Documentación y Planificación:

- Cada estrategia de tratamiento de riesgo será documentada detalladamente, incluyendo la justificación para la elección de la estrategia y los pasos específicos a seguir.
- Se integrará esta información en el Plan de Acción general del SGSI, asegurando una coherencia y una gestión efectiva de riesgos.

8. Roles y Responsabilidades

Esta sección del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del CNMH tiene como objetivo definir y asignar roles y responsabilidades específicos para la gestión efectiva de los riesgos. Esto asegura que todas las tareas relacionadas con la gestión de riesgos estén claramente distribuidas y que haya un entendimiento común de las obligaciones de cada parte involucrada.

Estructura Organizativa:

Alta Dirección:

- Responsable de establecer la visión y el compromiso con la gestión de riesgos.
- Asegurar la asignación de recursos necesarios para la implementación del plan.

Oficial de Seguridad de la Información (OSI):

- Liderar la implementación y supervisión del SGSI.
- Coordinar las actividades de gestión de riesgos y reportar a la alta dirección.

Gestores de Área/Departamento:

- Asegurar que las políticas y procedimientos de seguridad de la información sean seguidos por su equipo.
- Identificar y reportar riesgos específicos de su área.

Personal de TI y Seguridad:

- Implementar medidas técnicas para la mitigación de riesgos.
- Mantener y actualizar los sistemas de seguridad.

Empleados:

- Cumplir con las políticas y procedimientos establecidos.

- Reportar cualquier incidente o actividad sospechosa relacionada con la seguridad de la información.

Responsabilidades Específicas:

- Cada rol tendrá responsabilidades específicas detalladas en el plan, alineadas con sus capacidades y ámbito de acción.
- Se incluirá la responsabilidad de participar en la capacitación y concientización sobre seguridad de la información.

Revisión y Ajuste de Roles:

- Los roles y responsabilidades serán revisados periódicamente para asegurar su relevancia y efectividad en la gestión de riesgos.
- Se harán ajustes conforme a cambios en la estructura organizativa o en los requisitos de seguridad de la información.

9. Mecanismos de Monitoreo y Revisión

Esta sección del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del CNMH está dedicada a establecer mecanismos eficientes para el monitoreo continuo y la revisión periódica del plan. Estos mecanismos son esenciales para garantizar la efectividad del plan a lo largo del tiempo, permitiendo adaptaciones en respuesta a cambios en el entorno interno y externo.

Procesos de Monitoreo:

Seguimiento Continuo:

- Implementar procedimientos para el monitoreo constante de los riesgos de seguridad y privacidad de la información.
- Utilizar herramientas y sistemas para detectar cambios o incidencias que puedan afectar el perfil de riesgo del CNMH.

Indicadores de Rendimiento:

- Establecer indicadores clave de rendimiento (KPIs) para evaluar la efectividad de las estrategias de tratamiento de riesgos.
- Estos indicadores pueden incluir la frecuencia de incidentes de seguridad, el tiempo de respuesta a incidentes, y el grado de cumplimiento de las políticas de seguridad.

Reportes y Análisis:

- Generar reportes periódicos sobre el estado de los riesgos y la eficacia de los controles implementados.
- Analizar estos reportes para identificar tendencias o áreas que requieren atención adicional.

Revisión del Plan:

Revisión Programada:

- Establecer un calendario para la revisión periódica del plan de tratamiento de riesgos, al menos anualmente o después de eventos significativos.
- Estas revisiones deben evaluar la adecuación del plan y hacer ajustes según sea necesario.

Revisión Basada en Eventos:

- Además de las revisiones programadas, realizar revisiones adicionales en respuesta a cambios significativos en el entorno operativo, como nuevos riesgos emergentes, incidentes de seguridad importantes o cambios en la legislación.

Participación de las Partes Interesadas:

- Involucrar a las partes interesadas clave en el proceso de revisión, incluyendo la alta dirección, el personal de TI, los usuarios de la información y, cuando sea relevante, expertos externos.

Documentación y Comunicación:

- Documentar todas las actividades de monitoreo y revisión, incluyendo los hallazgos y las acciones tomadas.
- Comunicar los resultados de las revisiones a todas las partes interesadas, asegurando transparencia y conciencia sobre el estado del plan de tratamiento de riesgos.

10.MARCO LEGAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data.
- Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor.
- Ley 527 de 1999, por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 1032 de 2006, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1266 de 2007, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
- Ley 1581 de 2012, "Protección de Datos personales".
- Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012.
- Decreto 4155: Artículo 13 - promover la aplicación de buenas prácticas y principios para el manejo y custodia de la información institucional, siguiendo lineamientos y directrices del gobierno nacional. Artículo 14 - Liderar la gestión de la información del sector de la inclusión social y la reconciliación, velando por la interoperabilidad de los Sistemas de información, y la calidad, oportunidad e integridad de los datos e información. Artículo 24 - Proponer e implementar políticas de seguridad informática y planes de contingencia de la plataforma tecnológica.

- Decreto 2573 de 2014. Artículo 4. Principios y fundamentos de la Estrategia de Gobierno en línea.
- Ley 1581 de 2012, protección de datos personales.
- Ley 1712 de 2014, "De transparencia y del derecho de acceso a la información pública nacional".
- Ley 962 de 2005. "Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de entidades públicas;"
- Ley 1150 de 2007. "Seguridad de la información electrónica en contratación en línea".
- Ley 1341 de 2009. "Tecnologías de la Información y aplicación de seguridad".
- Decreto 886 de 2014. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012".
- Decreto 1083 de 2015. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012".
- CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016 Política Nacional de Seguridad digital.
- Ley 1078 del 2015 "Por medio del cual se expide el Decreto Único Reglamentario Del Sector De Tecnologías De La Información y Las Comunicaciones".
- Decreto 1008 de 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"
- Decreto 767 de 2022, actualización de la Política de Gobierno digital 2022.

11. REQUISITOS TÉCNICOS

- Norma Técnica ISO 27000: Tecnología de la información, técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Visión general y vocabulario.
- Norma técnica ISO 27001. Tecnología de la Información, técnicas de seguridad, sistemas de gestión de seguridad de la Información (SGSI) Requisitos.
- Norma Técnica ISO 27002. Tecnología de la información. Técnicas de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información.
- Norma Técnica ISO 27003. Tecnología de la información. Técnicas de seguridad. Directrices para la implementación de un sistema de gestión de la seguridad de la información.

- Norma Técnica ISO 27004. Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la información.
- Medición Norma Técnica ISO 27005. Tecnología de la información. Técnicas de seguridad. Gestión del riesgo de seguridad de la información

12. RESPONSABLE DEL DOCUMENTO

Dirección Administrativa y Financiera – Gestión de TIC.

CONTROL DE CAMBIOS			
ACTIVIDADES QUE SUFRIERON CAMBIOS	**CAMBIOS EFECTUADOS**	**FECHA DE CAMBIO**	**VERSIÓN**
Creación del documento	Creación del Documento	20/01/2024	001