POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2024

	NOMBRE	CARGO	FECHA
ELABORÓ	César Augusto Ortiz Barrera	Contratista Gestión de TIC	04/03/2024
REVISÓ	María Camila Pardo Reyes	Oficina Asesora jurídica	13/08/2024
	Ronal Alexis Martínez Cerón	Profesional Especializado	20/08/2024
APROBÓ	Comité Institucional de Gestión y Desempeño	Comité Institucional de Gestión y Desempeño	27/11/2024
APROBÓ	Ana María Trujillo Coronado	Directora Administrativa y Financiera	20/08/2024

TABLA DE CONTENIDO

1. INTRODUCCIÓN 4
1.1. Definiciones 4
2. OBJETIVO 9
3. ALCANCE 9
4. PRINCIPIOS 10
6. CUMPLIMIENTO 12
7. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 15
7.1. Política de estructura organizacional de la seguridad de la información. 15
7.2. Política de seguridad para los recursos humanos. 15
7.3. Política de gestión de activos de Información. 16
7.4. Política de uso de equipos de cómputo. 17
7.5. Política de uso de Internet. 17
7.6. Política de clasificación de la información. 19
7.7. Política de manejo, disposición de información en medios de almacenamiento y equipos. 19
7.8. Política de control de acceso. 20
7.9. Política de establecimiento, uso y protección de claves de acceso. 21
7.10. Política de controles criptográficos. 22
7.11. Política de Gestión de Cambios 25
7.12. Política de escritorio y pantalla limpia 26
7.13. Política de copias de respaldo y restauración de información 27
7.14. Política para la Transferencia de Información 31
7.15. Política de uso de correo electrónico 33
7.17. Política de adquisición, desarrollo y mantenimiento de sistemas de información. 35
7.18. Política de gestión de incidentes. 40
7.19. Política de seguridad del centro de datos y centros de cableado. 40

7.20. Política de seguridad de proveedores. (los proveedores también se encuadran en la categoría de contratistas, ya que prestan un servicio o suministran un bien. Si se hace ésta distinción tendría que definirse la categoría. 41

7.21. Política de cumplimiento de requisitos legales y contractuales. 44

7.22. Política de tratamiento de datos personales. 44

7.23. Política de seguridad física y del entorno. 45

7.24. Política de seguridad en las operaciones. 45

7.25. Política de seguridad de las comunicaciones. 45

8. CONTROLES 46

9. SENSIBILIZACIÓN Y COMUNICACIÓN 46

10. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS 46

11. SANCIONES 46

12. MARCO LEGAL 47

13. REQUISITOS TÉCNICOS 48

14. RESPONSABLE DEL DOCUMENTO 48

1. INTRODUCCIÓN

El Centro Nacional de Memoria Histórica - CNMH, consciente de la importancia de la información como activo intangible clave para el cumplimiento de su misión y el logro de sus objetivos estratégicos, reconoce la necesidad de implementar políticas que permitan gestionar adecuadamente los atributos fundamentales de seguridad de la información como son: la *confidencialidad*, la *integridad* y la *disponibilidad* en su ciclo de vida. Bajo estos principios y con base en los lineamientos de la Política de Gobierno Digital expedida por el MINTIC (Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto número 1078 de 2015[1]), el Modelo de Seguridad y Privacidad de la Información- MSPI y la Norma Técnica Colombiana NTC- ISO-IEC 27001:2013 formuló el Sistema de Gestión de Seguridad de la Información - SGSI que parte de la expedición de las políticas de seguridad y privacidad de la información las cuales deben ser acatadas por los servidores públicos, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con el Centro Nacional de Memoria Histórica – CNMH.

Las Políticas de Seguridad y Privacidad de la Información deben ser actualizadas periódicamente para estar acorde con las buenas prácticas de seguridad de la información, los cambios en la Política de Gobierno Digital, los cambios en el MSPI, los cambios generados en la norma técnica, la legislación de Protección de Datos Personales, Transparencia y Acceso a la Información Pública y aquello que impacte la gestión de la seguridad de la información.

1.1. 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.
- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- **Alerta:** Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.
- **Almacenamiento en la Nube:** Del inglés cloud storage, es un modelo de almacenamiento de datos basado en redes de computadoras que consiste en

[1] Subrogado por el Decreto 1008 de 2018.

guardar archivos en un lugar de Internet. Esos lugares de Internet son aplicaciones o servicios que almacenan o guardan esos archivos.

- **Amenaza:** causa potencial de un incidente no deseado, el cual puede resultar en daño al sistema o a la Entidad.
- **Análisis de riesgos:** A partir del riesgo definido, se define las causas del uso sistemático de la información para identificar fuentes y estimar el riesgo.
- **Auditor:** Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.
- **Auditoría:** Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.
- **Autenticación:** Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.
- **Autenticidad:** Propiedad que garantiza que la identidad de un sujeto o recurso es la que se declara. La autenticidad se aplica a entidades como a usuarios, procesos, sistemas e información.
- **Aplicaciones:** Es todo el software que se utiliza para la gestión de la información. Ejemplo: Ulises, SAIA.
- **Base de datos de gestión de configuraciones (CMDB, Configuration Management DataBase):** Es una base de datos que contiene toda la información acerca de los componentes físicos y lógicos de la infraestructura de TI de una organización y las relaciones entre esos componentes. Una CMDB ofrece una vista organizada de los datos y una forma de examinar los datos desde cualquier perspectiva que desee. En este contexto, los componentes de un sistema de información se conocen como elementos de configuración (CI). Un CI puede ser cualquier elemento imaginable de TI, incluyendo software, hardware, documentación y personal, así como cualquier combinación de ellos. Los procesos de gestión de la configuración tratan de especificar, controlar y realizar seguimiento de elementos de configuración y los cambios introducidos en ellos de manera integral y sistemática.
- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Confiabilidad:** Es la capacidad de un producto de realizar su función de la manera prevista, de otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin

incidentes por un período de tiempo especificado y bajo condiciones indicadas.

- **Confidencialidad:** propiedad de la información que hace que no esté disponible o que sea revelada a individuos no autorizados, entidades o procesos.
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1074 de 2015 Artículo 2.2.2.25.1.3. Definiciones).
- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).
- **Datos Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1074 de 2015 Artículo 2.2.2.25.1.3. Definiciones).
- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el SGSI del CNMH, tras el resultado de los procesos de evaluación y tratamiento de riesgos, además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma.
- **Desastre:** Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.
- **Disponibilidad:** propiedad de ser accesible y utilizable ante el uso de una entidad autorizada.
- **Evaluación de riesgos:** proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo. [ISO27000]
- **FTP: (File Transfer Protocol):** es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar y/o subir archivos a él.

- **Gestión de claves:** Controles referidos a la gestión de claves criptográficas.
- **Gestión de riesgos:** Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización, incluye la valoración de riesgos y el tratamiento de riesgos.
- **Hardware:** Son todos aquellos Equipos electrónicos donde se procesa la información. Ejemplo: Equipos de cómputo, Discos duros externos.
- **Información - Datos:** Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en el CNMH, siendo requeridos para el cumplimiento de su misión y objetivos.
- **Instalaciones:** Son todos los lugares en los que se alojan los sistemas de información. Infraestructura física que soporta el funcionamiento de la Entidad cubriendo los aspectos relacionados con edificios, muebles, servicios y seguridad física.
- **Intangibles:** Aspectos que pueden afectar a la Entidad pero que no se pueden asociar a un elemento físico.
- **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.
- **Inventario de activos:** Lista de todos aquellos recursos (físicos, de información, software, hardware, documentos, servicios, personas, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.
- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.
- **Ley de Transparencia y Acceso a la Información Pública:** se refiere a la Ley Estatutaria 1712 de 2014.
- **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.
- **No repudio:** Capacidad para probar que una acción o evento ha tenido lugar de modo que tal evento o acción, no pueda ser negado posteriormente.
- **Plan de continuidad del negocio (Bussines Continuity Plan):** Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.
- **Plan de tratamiento de riesgos (Risk treatment plan):** Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
- **Política de seguridad:** Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.
- **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.

- **Propietario / Responsable del riesgo**: Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.
- **Privacidad:** Derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la Entidad en el marco de las funciones que a ella le compete realizar y que generan las entidades, de acuerdo con la política de Gobierno Digital, la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- **Redes de Comunicaciones:** Los dispositivos y su interacción que habilitan el servicio de comunicaciones de red en la Entidad.
- **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).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas. [ISO/IEC 27001:2013].
- **Selección de controles:** Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.
- **SGSI Sistema de Gestión de la Seguridad de la Información:** Sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.) [ISO27001:2013].
- **Servicios:** Son tanto los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a clientes y usuarios. Conjunto organizado de actividades cuyo objetivo es responder a un requerimiento específico de un cliente externo o interno de la Entidad. Ejemplo: Solicitud de vacaciones, solicitud de certificación laboral.
- **Software:** Las aplicaciones y sistemas de información que atienden los requerimientos informáticos de la entidad.
- **Tecnología:** Son todos los equipos utilizados para gestionar la información y las comunicaciones. Ejemplo: equipo de cómputo, teléfonos, impresoras.
- **Tratamiento de riesgos:** A partir del riesgo definido, se aplican los controles

con los cuales se busca que el riesgo no se materialice.

- **Trazabilidad:** Propiedad que garantiza que las acciones puedan ser rastreadas de forma permanente.
- **Usuario:** Se refiere a servidores públicos, contratistas y terceros del CNMH, autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red y a quienes se les otorga un nombre de usuario y una clave de acceso.
- **VPN (Virtual Private Network):** es una tecnología de red que permite una extensión segura de la red privada de área local (LAN) sobre una red pública o no controlada como Internet.
- **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.

2. OBJETIVO

Establecer las políticas que regulan la seguridad y privacidad de la información en el Centro Nacional de Memoria Histórica - CNMH que deben conocer, acatar y cumplir todos los servidores públicos, contratistas, personal en comisión, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con el CNMH.

3. ALCANCE

Las Políticas de Seguridad y Privacidad de la Información son aplicables en todo el ciclo de vida de los activos de información para el Centro Nacional de Memoria Histórica - CNMH, incluyendo creación, distribución, almacenamiento y eliminación. Aplica para todos los servidores públicos, contratistas y terceros que realicen alguna labor en la Entidad.

Estas políticas aplican a todos los procesos, aspectos administrativos y de control que ejecutan los servidores públicos, contratistas y terceros que presten servicios o tengan relación con el Centro Nacional de Memoria Histórica – CNMH en cumplimiento de la misión y la ciudadanía en general, teniendo en cuenta los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI que están determinados por las siguientes premisas:

- Minimizar el riesgo de los procesos misionales de la Entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los servidores públicos, contratistas y terceros.

- Apoyar la innovación tecnológica, evitar la obsolescencia.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los servidores públicos y contratistas del Centro Nacional de Memoria Histórica.
- Garantizar la continuidad del cumplimiento misional frente a incidentes.

4. PRINCIPIOS

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento en el 100% de las Políticas.

Se establecen los 12 principios de seguridad que soportan el SGSI del Centro Nacional de Memoria Histórica:

1) El Centro Nacional de Memoria Histórica ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la misionalidad de la Entidad, y a los requerimientos regulatorios que le aplican a su naturaleza.
2) Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los servidores públicos y contratistas.
3) El Centro Nacional de Memoria Histórica protegerá la información recibida, acopiada, generada, procesada, custodiada y preservada por los procesos misionales y de apoyo y activos de información que hacen parte de los procesos.
4) El Centro Nacional de Memoria Histórica protegerá la información recibida, acopiada, generada, procesada, custodiada y preservada por sus procesos misionales y de apoyo, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta, para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
5) El Centro Nacional de Memoria Histórica protegerá su información de las amenazas originadas por parte del personal o cualquier tercero.
6) El Centro Nacional de Memoria Histórica protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
7) El Centro Nacional de Memoria Histórica controlará la operación de sus procesos de misionales y de apoyo garantizando la seguridad de los recursos tecnológicos y las redes de datos.

8) El Centro Nacional de Memoria Histórica implementará control de acceso a la información, sistemas y recursos de red.
9) El Centro Nacional de Memoria Histórica garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
10) El Centro Nacional de Memoria Histórica garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
11) El Centro Nacional de Memoria Histórica garantizará la disponibilidad de sus procesos misionales y de apoyo y la continuidad de su operación, basado en el impacto que pueden generar los eventos.
12) El Centro Nacional de Memoria Histórica garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

NOTA: El incumplimiento a la Política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales aplicables conforme a la normatividad vigente.

5. COMPROMISO

El Centro Nacional de Memoria Histórica - CNMH, entendiendo la importancia de una adecuada gestión de la información que brinde niveles de seguridad y privacidad, se compromete con la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Entidad.

Para el Centro Nacional de Memoria Histórica - CNMH, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la información, acorde con las necesidades de los diferentes grupos de interés identificados.

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración del Centro Nacional de Memoria Histórica - CNMH con respecto a la protección de los activos de información (los servidores públicos, contratistas, terceros, la información, los procesos, uso de hardware y el software), que soportan los procesos de la Entidad y sobre los cuales se basa la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas,

procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

6. CUMPLIMIENTO

El Centro Nacional de Memoria Histórica declara que todos sus servidores públicos y contratistas son responsables de ejecutar estas políticas en el desarrollo de sus actividades comprometiéndose a realizar la planeación y las gestiones tendientes a su puesta en marcha. En caso de violación de las políticas de seguridad y privacidad, ya sea de forma intencional o por negligencia, el CNMH tomará las acciones disciplinarias y legales correspondientes. Las Políticas de Seguridad y privacidad de la Información deben prevenir el incumplimiento de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.

La Entidad velará por el cumplimiento de la legislación vigente respecto a los requisitos establecidos en la seguridad y privacidad de la información, derechos de propiedad intelectual, protección de datos personales, transparencia y del derecho de acceso a la información pública.

Actuaciones que conllevan a la violación de la seguridad de la información establecidas por el CNMH:

1) No firmar los acuerdos de confidencialidad o de entrega de información o de activos de información.
2) No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad y privacidad, cuando se tenga conocimiento de ello.
3) No actualizar la información de los activos de información a su cargo.
4) Clasificar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para este fin.
5) No guardar la información digital, producto del procesamiento de la información perteneciente al CNMH.
6) Dejar información pública reservada, en carpetas compartidas o en lugares distintos al servidor de archivos, obviando las medidas de seguridad.
7) Dejar los computadores encendidos en horas no laborables, sin la debida autorización de la Dirección Administrativa y Financiera – Gestión de TIC.
8) Permitir que personas ajenas al CNMH, deambulen sin acompañamiento, al interior de las instalaciones, en áreas no destinadas al público.
9) Almacenar en los discos duros de los computadores personales de los usuarios, la información de la entidad.
10) Solicitar cambio de contraseña de otro usuario, sin la debida autorización del titular o su jefe inmediato.

11) Hacer uso de la red de datos del CNMH, para obtener, mantener o difundir en los equipos de sistemas, material pornográfico (penalizado por la ley) u ofensivo, cadenas de correos y correos masivos no autorizados.
12) No guardar de forma segura la información (publica reservada, clasificada o relacionada con datos personales de terceros) cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral.
13) Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica de la Entidad.
14) Recibir o enviar información institucional a través de correos electrónicos personales, diferentes a los asignados por la institución.
15) Enviar información pública reservada o información pública clasificada (privada o semiprivada) por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.
16) Utilizar equipos electrónicos o tecnológicos desatendidos o que a través de sistemas de interconexión inalámbrica, sirvan para transmitir, recibir y almacenar datos.
17) Usar dispositivos de almacenamiento externo en los computadores, cuya autorización no haya sido otorgada por la Dirección Administrativa y Financiera – Gestión de TIC del CNMH.
18) Permitir el acceso de servidores públicos a la red de la entidad, sin la autorización de la Dirección Administrativa y Financiera – Gestión de TIC del CNMH
19) Utilización de servicios disponibles a través de internet, como FTP y Telnet, no permitidos por el CNMH o de protocolos y servicios que no se requieran y que puedan generar riesgo para la seguridad.
20) Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias del CNMH.
21) No cumplir con las actividades designadas para la protección de los activos de información del CNMH.
22) Destruir o desechar de forma incorrecta la documentación institucional.
23) Descuidar documentación con información pública reservada o clasificada de la entidad, sin las medidas apropiadas de seguridad que garanticen su protección.
24) Registrar información pública reservada o clasificada, en pos-it, apuntes, agendas, libretas, etc. Sin el debido cuidado.
25) Almacenar información pública reservada o clasificada, en cualquier dispositivo de almacenamiento que no permanezca al CNMH o conectar computadores portátiles u otros sistemas eléctricos o electrónicos personales a la red de datos de CNMH, sin la debida autorización.
26) Archivar información pública reservada o clasificada, sin claves de seguridad o cifrado de datos.

27) Uso de los recursos tecnológicos del CNMH para beneficio personal y/o promoción y/o mantenimiento de negocios personales.
28) Acceder sin autorización a todo o parte del sistema informático que se mantenga dentro del mismo en contra de la voluntad del CNMH.
29) El que impida u obstruya el funcionamiento o el acceso normal al sistema informático, los datos informáticos o las redes de telecomunicaciones del CNMH, sin estar autorizado.
30) El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de información del CNMH.
31) El que distribuya, envíe, introduzca software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica del CNMH.
32) El que viole datos personales de las bases de datos del CNMH.
33) El que superando las medidas de seguridad informática suplante un usuario ante los sistemas de autenticación y autorización establecidos por el CNMH.
34) No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información del CNMH o permitir que otras personas accedan con el usuario y clave del titular a éstos.
35) Permitir el acceso u otorgar privilegios de acceso a las redes de datos del CNMH a personas no autorizadas.
36) Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a cualquier computador o de terceros del CNMH.
37) Ejecutar acciones tendientes a eludir o variar los controles establecidos por el CNMH.
38) Retirar de las instalaciones de la institución, estaciones de trabajo o computadores portátiles que contengan información institucional sin la autorización pertinente.
39) Sustraer de las instalaciones del CNMH, documentos con información institucional calificada como información pública reservada o clasificada, o abandonarlos en lugares públicos o de fácil acceso.
40) Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas o entidades no autorizadas.
41) Ejecución de cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala imagen del CNMH o de alguno de sus servidores públicos.
42) Realizar cambios no autorizados en la plataforma tecnológica del CNMH.
43) Acceder, almacenar o distribuir pornografía infantil.

7. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

7.1. Política de estructura organizacional de la seguridad de la información.

El Centro Nacional de Memoria Histórica crea un esquema de seguridad de la información definiendo y estableciendo roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad de la información, en cumplimiento de las funciones del Comité Institucional de Gestión y Desempeño, establecidas en la Resolución 038 del 31 de enero de 2018 y en la Resolución 163 del 15 de junio de 2023

La estructura organizacional del Centro Nacional de Memoria Histórica – CNMH se encuentra definida en el Decreto 4803 de 2011 "Por el cual se establece la estructura del Centro de Memoria Histórica". En cuanto a los roles y responsabilidades requeridos para el Sistema de Gestión de Seguridad de la Información, es importante entender que, para todos los cargos existentes, se establecen nuevas responsabilidades que serán asumidas formalmente a partir de la expedición de Resolución 206 de 2018 "Por la cual se adopta la Política de Seguridad de la Información del Centro Nacional de Memoria Histórica". El CNMH contará con un profesional encargado de la Seguridad de la Información o quien haga sus veces para el cumplimiento de sus funciones.

7.2. Política de seguridad para los recursos humanos.

El Centro Nacional de Memoria Histórica – CNMH, implementa acciones para asegurar que los servidores públicos, contratistas y demás colaboradores de la Entidad, entiendan sus responsabilidades, como usuarios y responsables de los roles asignados, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información y de las instalaciones, para lo cual deberán:

Diligenciar y firmar el formato compromiso y reserva "GTH-FT-040 V1 Compromiso de confidencialidad y protección de información" mediante el cual afirma su conocimiento y aceptación de las políticas definidas para el sistema de seguridad de la información y buen uso de los activos de información; y mediante el cual se compromete a realizar un adecuado uso de estos.

Se debe capacitar y sensibilizar a los servidores públicos durante la inducción sobre las políticas de seguridad y privacidad de la información.

7.3. Política de gestión de activos de Información.

El Centro Nacional de Memoria Histórica es el dueño de la propiedad intelectual y de los avances intelectuales realizados por los servidores públicos y los contratistas del CNMH, derivados del cumplimiento de funciones y de las obligaciones contratadas respectivamente, así como las necesarias para el cumplimiento del objeto del contrato.

El Centro Nacional de Memoria Histórica es propietario de los activos de información, para lo cual los servidores públicos designados serán los administradores de estos activos siendo responsables por la información de los procesos a su cargo, así como del uso de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de Tecnología y Sistemas de Información (TIC).

Los servidores públicos y contratistas, están autorizados para hacer uso de los activos de información dispuestos por el CNMH únicamente para ejecución de las funciones asignadas (servidores públicos) y de las obligaciones establecidas en cada contrato. Adicional a lo anterior la Entidad identificará, clasificará y gestionará su inventario de activos conforme a los manuales y procedimientos de Gestión de Activos formalizados. (Definir cuáles son o renombrarlos como estén el SIG -Sistema Integrado de Gestión- o en su defecto colocar el link)

El CNMH deberá mantener un inventario actualizado de sus activos de información, quedando bajo la responsabilidad de cada propietario de la información dicha actualización, el cual se publicará en la intranet de la Entidad. Como guía se cuenta con la "(I) SIP-MA-002 Manual sistema gestión seguridad información".

La Entidad debe realizar el tratamiento de información documental de acuerdo a lo establecido en el proceso de gestión documental "GDC-PO Gestión Documental".

Los activos tecnológicos se deben mantener en una base de datos bajo la responsabilidad de la Dirección Administrativa y Financiera – Gestión de TIC. (CMDB - Base de datos de gestión de configuraciones / Configuration Management Database).

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

7.4. Política de uso de equipos de cómputo.

El Centro Nacional de Memoria Histórica, establece reglas que permitan orientar la correcta utilización de equipos de cómputo por los usuarios, que contribuyan a mantener la seguridad de los activos de información, para lo cual se define:

- El acceso a la cuenta en los equipos de cómputo personal es exclusivo del usuario al que fue asignado. La excepción a esta regla aplica para los servidores públicos y contratistas de la Dirección Administrativa y Financiera – Gestión de TIC para los casos en los que se requiere su intervención para la ejecución de actividades de soporte técnico.

- Solamente deben ser instalados en los equipos de cómputo, aplicaciones tipo cliente, en ningún caso es aceptable que asuma funcionalidad de servidor.

- El software instalado en los equipos de cómputo debe estar explícitamente autorizado por la Dirección correspondiente y la Dirección Administrativa y Financiera.

- Los cambios de configuración, instalación, desinstalación, modificación en las carpetas del sistema operativo no pueden ser ejecutados por el usuario; estos requerimientos solo pueden ser atendidos por el personal de la Dirección Administrativa y Financiera – Gestión de TIC, previa solicitud formalizada.

- Los bienes y recursos de cómputo institucionales se emplearán de manera exclusiva por el funcionario al cual han sido asignados y únicamente para el correcto desempeño de su empleo, cargo o función; por lo tanto, no pueden ser utilizados con fines personales o por terceros no autorizados.

7.5. Política de uso de Internet.

La Entidad permite el acceso al servicio de internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas,

modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.

- Solo se debe establecer conexión a Internet teniendo habilitado el sistema de antimalware provisto por el CNMH.

- Cuando en el uso de internet se identifique una situación anormal debe reportarse a Soporte TIC (aplicación instalada en el escritorio de cada equipo de cómputo), registrando fecha, hora y acción ejecutada.

- La conexión a internet que utilice la infraestructura de red del CNMH, se debe realizar desde los equipos autorizados.

- A los equipos autorizados por el CNMH, no les es permitido una conexión a Internet por un modem, celular o dispositivos diferentes a los provistos por el CNMH, salvo autorización del líder del proceso donde labora el usuario y la aprobación de la Dirección Administrativa y Financiera.

- No está permitido el descargar archivos sin la inspección del sistema antimalware autorizado por el CNMH.

- No está permitido llevar a cabo instalaciones, ni actualizaciones desde sitios de Internet, por parte del usuario.

- Los cambios en la configuración del acceso a Internet solo pueden ser realizados por el administrador del sistema en custodia de la Dirección Administrativa y Financiera – Gestión cde TIC.

- Es responsabilidad de los usuarios reportar comportamientos anormales en sesiones de Internet como por ejemplo instalaciones no solicitadas, ejecución de programas no reconocidos, aparición de íconos, entre otros; estos deben ser reportado inmediatamente a Soporte TIC (aplicación instalada en el escritorio de cada equipo de cómputo).

- Todas las conexiones a Internet deben tener una justificación laboral.

- El usuario es responsable por los daños causados debido a la omisión de las normas descritas. El internet es un recurso valioso para el desempeño de las labores de todos los servidores públicos y, por lo tanto, se definen los siguientes lineamientos para su uso adecuado:

- Estará limitado el acceso a portales de: Juegos, pornografía, drogas, terrorismo, segregación racial, hacking, malware, software gratuito o ilegal y/o cualquier otra página que vaya en contra de las leyes vigentes.

- Se restringirá el acceso a portales de nube e intercambio de información masiva (exceptuando a la nube corporativa o institucional).

- La Dirección Administrativa y Financiera – Gestión de TIC podrá verificar los logs o registros de navegación cuando así se solicite o se requiera para las investigaciones o requerimientos que puedan generarse, con la autorización correspondiente.

- Cada usuario será responsable por cualquier afectación no deseada que provoque al intentar visitar algún sitio no permitido o bien, instalar un programa no autorizado ni licenciado.

7.6. Política de clasificación de la información.

El Centro Nacional de Memoria Histórica, consciente de la necesidad de asegurar que la información reciba el nivel de protección apropiado de acuerdo con el tipo de clasificación establecido por la ley y el CNMH, define reglas de cómo clasificar la información, definición liderada por el proceso de Gestión Documental de la Entidad.

Los niveles de clasificación de la información valiosa que se ha establecido en el CNMH se encuentran en la intranet en el documento "(I) Documento General - Metodología Clasificación de activos SGSI".

7.7. Política de manejo, disposición de información en medios de almacenamiento y equipos.

El Centro Nacional de Memoria Histórica, establece actividades para evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados por el CNMH, velando por la disponibilidad y confidencialidad de la información.

Los medios y equipos donde se almacena procesan o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.

El servicio de acceso a internet, intranet, sistemas de información, medio de almacenamiento, aplicaciones (Software), cuentas de red, navegadores y

equipos de cómputo son propiedad de la Entidad y deben ser usados únicamente para el cumplimiento de la misión de la Entidad.

Una vez el servidor público se retira de la Entidad, se realizará una copia de la información almacenada en todos los medios y/o dispositivos proporcionados por el CNMH, copia que deberá ser ubicará en un repositorio centralizado de propiedad de la Entidad para posteriormente proceder a realizar el borrado seguro de la información almacenada en dichos medios y/o dispositivos.

Está restringida la copia de archivos en medios removibles de almacenamiento, por lo cual se deshabilita la opción de escritura en dispositivos USB, unidades ópticas de grabación en todos los equipos de cómputo institucionales, para evitar las pérdidas de datos de la Entidad.

7.8. Política de control de acceso.

El Centro Nacional de Memoria Histórica, define las reglas para asegurar un acceso controlado, físico y/o lógico, a la información y plataforma informática del CNMH, considerándolas como importantes para el SGSI. La conexión remota a la red de área local del CNMH debe realizarse a través de una conexión VPN segura suministrada por la Entidad, la cual debe ser aprobada, registrada y auditada por la Dirección Administrativa y Financiera – Gestión de TIC.

- Los servicios prestados en la Red del CNMH tienen como requisito indispensable la asignación de una cuenta de usuario de uso exclusivo e intransferible, para cada funcionario y contratista, por parte de la Dirección Administrativa y Financiera – Gestión de TIC.

- El uso de la cuenta asignada para acceder a los servicios tecnológicos que se prestan, tienen como mecanismo de acceso un Usuario y su correspondiente contraseña, que son de total responsabilidad del funcionario o contratista a quien se le autoriza el acceso.

- La responsabilidad del uso de la cuenta asignada al funcionario o contratista en cualquier plataforma es exclusiva del mismo, no existe justificación para que estos datos sean compartidos con otras personas.

- El funcionario debe reportar inmediatamente a Soporte TIC, los usos no autorizados detectados con la cuenta asignada en cualquiera de los servicios informáticos proporcionados por la Entidad.

- Para la protección de los activos de información, se establecerán procedimientos y opciones de configuración para el control de acceso a la red, sistemas de información e infraestructura física (Instalaciones). Con el fin de mitigar los riesgos asociados al acceso no autorizado de la información.

- Todos los usuarios deberán asumir la responsabilidad sobre la información física y/o digital a la cual que accedan y procesen dando un uso adecuado con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información.

7.9. Política de establecimiento, uso y protección de claves de acceso.

Como política de control de acceso, ningún usuario deberá acceder a la red o a los servicios TIC del CNMH utilizando una cuenta de usuario o clave de otro usuario. El CNMH suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.

- El máximo periodo de vigencia de una contraseña es de 45 días, plazo en el cual el usuario debe proceder con su cambio, evitando repetir valores usados en los 10 últimos periodos.

- Las claves o contraseñas deben tener mínimo ocho (8) caracteres

- A cada funcionario o contratista que requiera acceso a sistemas de información o correo electrónico del CNMH, se le deberá asignar un usuario y contraseña.

- Las credenciales son personales e intransferibles.

- Deben utilizarse esquemas de seguridad para la creación de contraseñas (uso de Mayúsculas, Minúsculas, Caracteres, Números).

- El CNMH debe garantizar, en las plataformas de tecnología de la Entidad, que el ingreso a la administración en lo posible se realice con la

vinculación directamente de las credenciales de los usuarios de directorio activo.

- Las contraseñas referentes a las cuentas "predefinidas" incluidas en los sistemas o aplicaciones adquiridas deben ser desactivadas, de no ser posible su desactivación, las contraseñas deben ser cambiadas después de la instalación del producto.

- El personal de la Dirección Administrativa y Financiera – Gestión TIC, no debe dar a conocer a terceros su clave de usuario de los sistemas de información, sin previa autorización de la Dirección Administrativa y Financiera.

.

7.10. Política de controles criptográficos.

El CNMH implementará herramientas de cifrado, con el fin de proteger la confidencialidad, disponibilidad e integridad de sus activos de información. Así mismo, la Dirección Administrativa y Financiera – Gestión de TIC determinará las unidades, discos duros o unidades extraíbles a los cuales se les deberán instalar controles criptográficos adicionales cuando así se requiera.

Todas las llaves que sean utilizadas por los algoritmos criptográficos aceptados por el CNMH deben manejarse cumpliendo con los puntos descritos en esta política:

Uso

Las llaves criptográficas pueden pertenecer a dos tipos de Criptografía:

- **Simétrica**: Utiliza la misma llave para el proceso de cifrado como para el de descifrado. En este caso la llave debe ser compartida por los usuarios autorizados para acceder a los datos cifrados.

- **Asimétrica**: Utiliza una llave para el proceso de cifrado que se denomina "pública" y otra para el proceso de descifrado que se denomina "privada". En este caso se comparte la llave pública con todos los usuarios que requieran enviar información protegida a un destino determinado y la llave privada es manejada exclusivamente por dicho usuario o Entidad destino.

La asignación de las llaves debe corresponder a los propietarios de los activos cuya clasificación exija el uso de algoritmos criptográficos.

Ciclo de Vida

- **Generación**: Es la selección del valor que se va a utilizar por parte de un algoritmo criptográfico específico. El usuario puede ser un emisor y receptor, un dominio, una aplicación, un dispositivo o un objeto de datos. La llave debe ser elegida de tal manera que no sea previsible y que evite que se presenten accesos no autorizados. La llave debe ser producto de un algoritmo de selección aleatoria donde se usen rutinas cuya entrada puede ser el movimiento del mouse o la velocidad con que se digite en el teclado, este tipo de herramientas dificulta las opciones de criptoanálisis para lograr un acceso no autorizado. En el CNMH se exigirá que la llave sea generada aleatoriamente sin que exista la opción para un ingreso manual.

- **Distribució**n: Es el proceso de traslado de una llave desde el punto de su generación hasta el punto donde va a ser usada, siendo la mayor exigencia en los algoritmos simétricos, donde es necesario la protección en este proceso, considerando que la llave para el cifrado es la misma para el descifrado. En el CNMH se exigirá que el uso de un cifrado de dicha llave y el establecimiento de vigencias o periodos, mantengan el riesgo de acceso no autorizado por debajo del NRA (Nivel de Riesgo Aceptable).

- **Instalación**: El proceso de almacenamiento de la llave en el dispositivo o proceso que se va a usar debe mantener en todo momento la protección para evitar el acceso no autorizado. El proceso de instalación en el CNMH debe contar siempre con el cifrado del valor de la llave correspondiente.

- **Almacenamiento**: Las llaves sólo pueden almacenarse en forma cifrada utilizando una llave exclusiva para este propósito. El sistema debe contar con mecanismos que eviten manipulación, referenciados como "Anti Tampering" que consiste en que en el momento que se detecte un intento de acceso no autorizado las llaves son autodestruidas automáticamente.

- **Cambio**: Establece la vigencia de una llave, poniendo fin a un valor que se viene usando y empezando con uno diferente, esto se determina por un convenio o protocolo, a mayor tiempo de vigencia de una llave, mayor será la probabilidad de acceso no autorizado, considerando las opciones de criptoanálisis. Para el CNMH este periodo será definido en cada caso particular, pero el máximo permitido sería el de 1 año que únicamente se justifica para los certificados digitales, para los otros tipos de llaves el tiempo

debe ser menor y se debe definir con base en que el nivel de riesgo este por debajo del NRA. El cambio de una llave debe considerar la parte de revocación que se aborda más adelante.

- **Control**: Es la capacidad de ejercer una dirección o influencia restrictiva sobre el uso o acceso al contenido de las llaves. Este control será ejercido en el CNMH a través del registro que señale fecha, hora y usuario al que le es asignada una llave determinada y de la misma forma el registro con los mismos datos para cuando esta sea usada. Todas las llaves estarán protegidas a su vez con mecanismo de cifrado en tránsito almacenamiento y procesamiento, el usuario responsable manejará al final la clave de acceso a las llaves que le sean asignadas.

- **Eliminación**: Las llaves deben ser eliminadas para evitar su divulgación, esto aplica para los valores de las llaves que por algún momento puedan encontrarse en forma limpia o sin cifrado en algún medio de almacenamiento.

Protección

Para la protección de las llaves de Cifrado se establece que los mecanismos de cifrado utilizados son a su vez los algoritmos criptográficos aceptados por el CNMH tal como lo establece el Procedimiento de Cifrado.

Al final existirá un valor del que el usuario se hace responsable y es el correspondiente a la clave de acceso para la llave de cifrado, este deberá manejarse bajo los principios de definición de contraseña establecidos en el CNMH.

Revocación

Esto es definir la invalidez de una llave antes de que se cumpla el periodo de vigencia establecido y el responsable de esta acción es el usuario al que le fue asignada la llave correspondiente.

Las razones por las cuales un usuario debe solicitar la revocación de una llave son las siguientes:

- Pérdida del dispositivo en el cual se encuentra almacenada la llave.
- Se evidencia alguna circunstancia bajo la cual se haya dado acceso no autorizado a la llave.
- Reporte de ataques informáticos o acción de algún tipo de malware.

7.11. Política de Gestión de Cambios

Todos los cambios que afecten la Gestión de Seguridad de la Información deben cumplir con las directrices establecidas en esta política.

Un cambio que afecte la Gestión de Seguridad de la Información debe estar respaldado por una necesidad evidente de la Entidad para ajustar sus procesos, instalaciones o los sistemas de procesamiento de información.

Activos Afectados

Se debe identificar dentro del SGSI cuáles son los activos que se verán afectados por el cambio propuesto o si es el caso definir los activos de información que ingresen para ser considerados en el proceso de gestión y autorizaciones.

- Documento metodología de activos
- Mirar caracterización de los procesos
- Mirar árbol de dependencias

Amenazas

Si los activos de información son nuevos se debe proceder con la identificación de amenazas tal como se describe en el documento "SIP-PR-007 v6 Administración de riesgos". Para los activos existentes, se debe verificar cómo el cambio afecta las amenazas consideradas inicialmente.

Vulnerabilidades

Verificar si los cambios en el activo generan nuevas vulnerabilidades o si de alguna manera afecta los controles existentes.

Para los activos de información nuevos se debe proceder con la identificación de vulnerabilidades tal como describe en el documento "SIP-PR-007 Administración de riesgos.".

Riesgos

Determinar bajo el nuevo panorama de amenazas y vulnerabilidades los nuevos riesgos para la seguridad de la información y determinar el "(I) SIP-PL-003 Plan de tratamientos de Riesgos", esta tarea la encabezarán el

profesional encargado de la Seguridad de la Información, el propietario del activo y el responsable del riesgo.

Pruebas

Se debe seguir el protocolo de pruebas definido para los procesos y/o activos afectados, verificando que se cumplan los requerimientos de confidencialidad, integridad y disponibilidad.

Pruebas de ethical hacking – ingeniería social – probar los requerimientos de seguridad de la información.

Autorización

Los cambios deben estar autorizados por el propietario del activo y a su vez por los responsables de los riesgos correspondientes.

Documentación

Todos los puntos descritos deben quedar documentados y si el cambio se aprueba debe llevarse a cabo el registro correspondiente en la documentación aprobada en el SGSI.

7.12. Política de escritorio y pantalla limpia

Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los usuarios.

Se ha definido una línea base para ser aplicada en forma general a toda la Entidad en cuanto a la disposición del Escritorio y el acceso visual a la Pantalla de cada equipo de cómputo, los cuales se describen a continuación:

ESCRITORIO

Los activos de información deben recibir su tratamiento con base en la clasificación recibida aplicando la Metodología descrita en el "Documento General - Metodología Clasificación de activos SGSI", acogido por la Entidad para la implementación del SGSI. Teniendo en cuenta que los activos de información pueden ser documentos impresos, su protección debe aplicarse para que estos no se encuentren sin custodia o restricción de acceso en algún

momento, por esto cada funcionario del CNMH debe aplicar las siguientes reglas sobre el uso de su escritorio de Trabajo:

- No deberán dejarse documentos críticos en el "Escritorio" tanto físico como el Escritorio virtual (se denomina "Escritorio" al espacio digital en los equipos de cómputo).
- Los documentos impresos que correspondan a activos de información catalogados como reservados o clasificados no pueden encontrarse encima del escritorio, salvo que estén siendo consultados por el funcionario autorizado.
- En ausencia del funcionario responsable, el escritorio debe permanecer despejado sin ningún tipo de documento impreso.
- Mantener en estricto orden y limpieza el puesto de trabajo.
- Aunque está permitido el consumo de bebidas en el puesto de trabajo, se recomienda todas las medidas preventivas, considerando que el verter líquidos puede causar daños en los equipos electrónicos y esto será responsabilidad del funcionario o contratista.
- Cada vez que los servidores públicos se retiren del lugar de trabajo deben bloquear los equipos de cómputo.
- Emplear las cajoneras o archivos para el almacenamiento de la información sensible o crítica.

PROTECTOR DE PANTALLA

El funcionario debe mantener habilitado el protector de pantalla y que se active cuando el puesto se encuentre sin custodia. El protector de pantalla será provisto por el CNMH y no se admite el uso de software diferente a este.

7.13. Política de copias de respaldo y restauración de información

Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla, garantizando que la información y la infraestructura de software crítica de la Entidad, sean respaldadas y puedan ser restauradas en caso de una falla y/o desastre.

La recuperación efectiva de datos es obligatoria y no opcional, por lo tanto, se deben implementar soluciones que van a depender de múltiples factores,

donde los más importantes son las directrices establecidas en la presente política.

La protección proviene de la capacidad de recuperación efectiva ante un desastre, una crisis o un incidente mayor, con la menor pérdida de datos y el menor tiempo de inactividad posible, para esto se define una estrategia de recuperación donde la más común es la copia de seguridad de datos, que resulta aplicable en los siguientes casos:

- Restaurar los datos en caso de un desastre, crisis o incidente.
- Recuperar un archivo en caso de supresión o la corrupción del mismo.
- Almacenar los datos históricos.
- Cumplimiento de los estándares y mejores prácticas.
- Cumplimiento del marco legal y regulatorio.

FACTORES

- **Tiempo objetivo de recuperación (RTO)**

En caso de contingencia, corresponde al tiempo máximo de inactividad tolerable por la Entidad a partir de la declaración del evento adverso.

Con base en el RTO debe definirse la estrategia de la Copia de respaldo.

- **Punto objetivo de Recuperación (RPO)**

En caso de contingencia, define la máxima cantidad de datos que una Entidad tolera perder en la ocurrencia de un evento adverso.

Esta variable define exactamente el intervalo que debe cubrir una copia de respaldo y define también la estrategia de la Copia de respaldo.

Actualmente el CNMH ha definido un RPO para todos sus sistemas de información en una semana.

- **Disponibilidad**

Este es uno de los 3 objetivos del SGSI y para cada activo de información se debe establecer el requerimiento correspondiente que establece cual es el porcentaje de disponibilidad requerido considerando la criticidad del proceso que atiende. Esto se define con base en los tiempos límite exigidos para cada una de las actividades donde está involucrado el activo de información.

- **Presupuesto**

Estará definido con base en la criticidad de los activos de información involucrados, con lo cual se dispondrá de mayores recursos para aquellos que lo justifiquen. En cuanto a una copia de respaldo esto se verá reflejado en una mayor frecuencia en los siguientes aspectos:

- Tecnología utilizada.
- Frecuencia de la copia de respaldo (definida por el RPO)
- Pruebas

SOLUCIONES

Estas son las opciones disponibles que serán elegidas con base en los requerimientos del activo de información involucrado.

Cintas de Respaldo ó Tape Backup: Ha sido el medio tradicional utilizado para las copias de respaldo y actualmente es la tecnología mas utilizada para este propósito.

Fortalezas

- Es la solución menos costosa.
- Solución portable que facilita su traslado fuera del edificio.
- Modo de operación muy conocido.

Debilidades

- Informes de la industria indican que la cinta puede fallar hasta un 40% que no incluye las copias de seguridad incompletas.
- Carece de la flexibilidad y simplicidad.
- Considerando que los volúmenes de datos siguen en aumento, las copias de seguridad en cinta están tomando cada vez mas tiempo.
- Impacto sobre el procesamiento, por lo cual deben ser ejecutados en horas de receso o bajo procesamiento.
- Compatibilidad con las soluciones considerando los cambios en software y hardware.

En línea: Es un sistema que maneja una infraestructura con el único propósito de realizar copias de respaldo con múltiples opciones de acuerdo con los requerimientos existentes

Fortalezas

- Soluciones de copia y restauración de fácil uso.
- Trazabilidad sobre todas las operaciones.

- Permite una copia incremental, optimizando el tiempo y los recursos requeridos.
- Cifrado de datos para protección de la Confidencialidad.
- Confiabilidad.

Debilidades

- Mayor costo

En línea Remoto: Permite a la Entidad realizar una copia sin contar con la infraestructura local, la copia se realiza utilizando el servicio de Internet.

Fortalezas
- Reducción en el Costo de Propiedad considerando que no es necesario invertir en infraestructura local.
- Operaciones de copia y restauración de fácil uso.

Debilidades
- Carencia de cláusulas de seguridad en la contratación.
- El cumplimiento de los requerimientos de seguridad se torna costoso: cifrado, verificación de integridad y opciones de auditoría y registro.

Disco a Disco: Esta solución esta desplazando a la opción de los Tape Backup, considerando que supera los problemas mas comúnes de esta tecnología.

Fortalezas
- Fácil Uso.
- Confiabilidad.

Debilidades
- Mayor Costo

Redundancia: Consiste en la duplicidad de los componentes para guardar una copia de los datos en forma simultanea en el momento en que se están procesando.

Fortalezas
- Mayor Confiabilidad.
- Considerando que la copia es simultanea satisface cualquier RPO y RTO.
- Mantiene los requerimientos de seguridad frente a confidencialidad e integridad.

Debilidades

- La solución más costosa

De-Duplicación de datos: Se ha demostrado que los procedimientos de copia de respaldo, desperdician tiempo y recursos con datos duplicados. Es necesario implementar una solución que aplique este procedimiento previo a la ejecución de la copia.

Considerando las opciones planteadas y acorde con los requerimientos de seguridad de los activos de información más críticos la solución que más se adapta es la de Copia en línea local y es la que debe ser usada para las copias de respaldo.

PRUEBAS

Las copias de respaldo deben ser probadas para corroborar que los datos efectivamente fueron almacenados correctamente y llegarán a ser la solución cuando los originales sufran un evento adverso.

Las pruebas deben realizarse cumpliendo con el siguiente protocolo:

- Deben ejecutarse trimestralmente.
- Realizar la restauración sobre un ambiente de pruebas.
- Llevar a cabo actividades que se realizan normalmente sobre los datos en este ambiente de pruebas para verificar su consistencia.
- En caso de encontrarse anomalías al realizar el reporte del Incidente aplicando el procedimiento de Gestión de incidentes. "GTC-PR-004 V2 Gestión de Soporte a Usua e Incid TIC".
- Si las pruebas son existosas debe guardarse el registro para corroborar el buen estado de la copia de Respaldo.

7.14. Política para la Transferencia de Información

La transferencia de Información debe realizarse protegiendo la confidencialidad e integridad de los datos con los mecanismos que se encuentren establecidos en el SGSI de acuerdo con la clasificación del activo de información involucrado.

Formas de Transferencia Aceptadas

Para el Centro Nacional de Memoria Histórica - CNMH las formas de Transferencia de datos son los siguientes:

- Correo electrónico
- Protocolo de Transferencia de archivos "SIP-PT-001 Protocolo de intercambio seguro de información".

Aunque la copia de archivos a través de medios removibles es una forma de Transferencia de información, ésta se aborda en el "SIP-PT-001 Protocolo de intercambio seguro de información".

Clasificación

Considerando que siempre el objeto de una Transferencia de datos es un activo de información, este debió haber cumplido previamente un proceso de clasificación aplicando el "Documento General - Metodología Clasificación de activos SGSI".

Protección de la Confidencialidad y la Integridad

Previo a la transferencia de la información se debe aplicar la protección de la confidencialidad y la integridad de los datos, aplicando el "SIP-PT-001 Protocolo de intercambio seguro de información".

Es importante señalar que si se hace uso de un protocolo de transmisión que soporte los algoritmos criptográficos establecidos por el CNMH para protección de la confidencialidad y la integridad, esto complementará el uso del Protocolo señalado.

Protección de la Disponibilidad

Se debe validar que el medio de comunicación ofrecido para la Transferencia de la Información cumple con el nivel de disponibilidad adecuado (entre el 99,5% y el 99.9%)

Este aspecto debe ser registrados formalmente en cada uno de los enlaces requeridos para transferencia de información .

Registro de la Transferencia de datos

Las transferencias de información realizadas en el CNMH deben ser registradas en los servidores correspondientes almacenando los siguientes datos referentes al evento:

- Fecha
- Hora
- Dirección IP origen
- Dirección IP Destino
- Usuario que envía
- Usuario que recibe
- Transmisión exitosa / fallida
- Tamaño de los datos transmitidos
- Protocolo utilizado
- Algoritmo de cifrado o firmado

Manejo de excepciones

Debe ser provista la información correspondiente a la ocurrencia de anomalías en el proceso de transferencia de datos. A continuación, se citan los casos sin limitarse a estos:

- Congestión de la Red
- Indisponibilidad del destino
- Paquetes malformados
- Bloqueo por comportamiento anómalo
- Bloqueo por firma de ataque
- Bloqueo por dirección IP origen
- Bloqueo por dirección IP destino

7.15. Política de uso de correo electrónico

El CNMH define las pautas generales para asegurar una adecuada protección de la información del CNMH, en el uso del servicio de correo electrónico por parte de los usuarios autorizados.

- La cuenta de correo electrónico es personal e intransferible, no existe justificación para que una cuenta de correo sea usada por otra persona ya que esto se cataloga como una suplantación, ningún funcionario del CNMH está autorizado para utilizar una cuenta diferente a la asignada.
- La cuenta de correo asignado es para uso exclusivo de temas laborales concernientes al CNMH y el desempeño de las funciones correspondientes a cada cargo.
- Los buzones de correo asignados a los servidores públicos, contratistas o terceros que pertenecen al CNMH, por lo tanto, su contenido también es propiedad de la Entidad.

- La cuenta de correo de un usuario desvinculado de la Entidad podrá ser consultada por un funcionario formalmente autorizado por el líder del proceso, pero no podrá enviar correos desde la misma.
- Solo pueden ser descargados archivos verificados por el sistema Antimalware provisto por el CNMH.
- Se deben borrar sin abrir los correos de los cuales no se tenga certeza del origen y propósito.
- Se deben clasificar como spam las cuentas de correo que lo ameriten.
- La información clasificada como confidencial solo puede ser enviada en forma cifrada.
- Los correos cuyo destino es toda la Entidad, los pueden remitir únicamente la Dirección Administrativa y Financiera, los profesionales autorizados de Comunicaciones y el Administrador de las cuentas de correo electrónico.
- Información por fuera del ámbito laboral que pueda ser catalogada de interés y que se considere deba ser compartida a todos los empleados debe ser enviada a Talento Humano donde se decidirá si debe ser replicada. Para los aspectos técnicos el correo debe ser enviado a la Dirección Administrativa y Financiera – Gestión de TIC.
- Si por error es ejecutado un archivo recibido de un correo no validado debe reportarse la situación inmediatamente a Soporte TIC y en lo posible aislar el equipo de cómputo.
- Cuando la cuenta de correo sea bloqueada o se olvide la contraseña, el funcionario o contratista debe recurrir al aplicativo de Soporte TIC solicitando la respectiva solución.
- La Dirección Administrativa y Financiera – Gestión de TIC podrá verificar el contenido de los buzones de los correos electrónicos en los casos que se requiera acudir a información para continuar con la prestación del servicio o para investigaciones específicas.

7.16. Política de Revisiones de Seguridad de la Información.

Garantizar el funcionamiento del sistema de gestión de seguridad de la información de acuerdo con las políticas y procedimientos implementados en el CNMH.

El CNMH realiza auditorías con personal interno y/o externo a la Entidad, al sistema de gestión de seguridad de la información, para la verificación y cumplimiento de objetivos, controles, políticas y procedimientos de seguridad de la Información.

Los directivos, jefes de dependencia y Asesores, deben verificar y supervisar el cumplimiento de las políticas de seguridad de la información en la dependencia a su cargo.

7.17. Política de adquisición, desarrollo y mantenimiento de sistemas de información.

El CNMH No realiza desarrollos internos de software, sin embargo, en caso de llegar a darse, se plantean las siguientes condiciones.

- El desarrollo por realizar para el uso del CNMH (sea contratado a un tercero o realizado internamente) debe acoger como principio, que la seguridad es parte integral de los sistemas de información y por tanto debe cumplir integralmente las políticas de seguridad y privacidad de la información formuladas en este documento.

La Dirección Administrativa y Financiera – Gestión de TIC, velará por que los sistemas de información que sean implementados en la Entidad cumplan con los requerimientos de seguridad y buenas prácticas.

Todos los dependencias de la Entidad deberán informar a la Dirección Administrativa y Financiera – Gestión de TIC sobre sus proyectos de adquisición de sistemas de información, con el fin de brindar las observaciones correspondientes y revisar los aspectos técnicos necesario para su desarrollo e implementación.

CONFIDENCIALIDAD

Considerando la clasificación para los activos de información del SGSI de cada aplicación debe proveer los mecanismos para proteger la confidencialidad con base en el nivel al que pertenezca el activo que se va a proteger. Los mecanismos que las aplicaciones desarrolladas para el CNMH deben proveer son:

- **Cifrado de datos sensibles:** Opción de cifrar los datos en tránsito y almacenamiento con un algoritmo criptográfico fuerte, como lo son a la fecha del desarrollo de este documento, AES y 3DES.
- **Control de acceso:** Mecanismos de autenticación por usuario y contraseña siguiendo la Política de control de acceso a la información del CNMH. Este control de acceso debe establecerse para cada activo de información con base en la matriz de acceso definida por cada Área responsable de los datos.

INTEGRIDAD

Para proteger la integridad de la información las aplicaciones deben desarrollar las siguientes utilidades, que serán aplicadas con base en la clasificación del activo de información a proteger:

- **Control de acceso:** Equivale a la funcionalidad descrita para la protección de la Confidencialidad
- **Verificación por hashing:** Opción que permita validar la integridad de los datos almacenados y/o transmitidos utilizando un campo de hashing que se genere con el algoritmo SHA que será calculado en la capa de acceso a datos con el uso de una librería validada. Este valor será almacenado hasta el momento en que se requiera la validación de integridad, momento en que se volverá a calcular el hashing y se realizará la comparación con el valor almacenado anteriormente.

DISPONIBILIDAD

Para cumplir con los requerimientos de Disponibilidad, las aplicaciones desarrolladas para el CNMH deben mitigar el riesgo de interrupciones con la aplicación de mejores prácticas relacionadas con manejo de excepciones.

REQUERIMIENTOS GENERALES

- **Eventos a ser registrados**
  Las aplicaciones para el CNMH deben contar con la opción de registrar las siguientes acciones:

  - Creación, modificación y/o eliminación de usuarios
  - Creación, modificación y/o eliminación de perfiles de usuario
  - Cambios en la configuración de la aplicación

- **Datos a registrar**

Se requiere que las aplicaciones cuenten con la opción de registrar los siguientes datos:

- **Fecha y Hora:** Señalando el año, mes, día, hora y segundos de la recepción del requerimiento
- **Usuario:** Identificación de la cuenta responsable de la acción
- **Tipo de Requerimiento:** Señalar cual fue la acción solicitada por el usuario
- **Id:** Identificador de la transacción. Para dar un ejemplo en Java, se tomará del campo Sesion-id que establece un número único por sesión

y que se complementará con un contador que identificaría cada transacción en particular.

- **Alerta:** Registrar si durante la ejecución de la transacción se presentó alguna situación Anormal. Es necesario implementar una función de manejo de excepción en las capas de presentación, lógica de misional y acceso a datos para lograr capturar el código de error, en el caso de presentarse, se tomaría del componente web y/o de los mensajes manejados que pueden ser http por ejemplo.
- **Exitosa Técnicamente:** Saber si la transacción cumplió con el proceso y se dió una respuesta al usuario dentro del período de tiempo definido, esto se logrará registrar verificando si hay algún código de error como se explicó en el punto anterior.
- **Problema Identificado:** Si la transacción no fue exitosa, especificar la causa correspondiente como problemas en la conexión, no hay respuesta de la Base de Datos, problemas en el enlace; se utilizará el mismo mecanismo descrito en el campo de Alerta.
- **Registro afectado:** ID del registro objetivo de la acción del usuario
- **Base de Datos:** ID de la Base de Datos afectada por la acción del usuario
- **Tabla:** ID de la tabla afectada por la acción del usuario
- **Dirección IP:** Desde donde se realizó el requerimiento. Esto depende de las limitantes que se puedan tener Java con el manejo del protocolo http y lo que el browser envíe – las limitantes serían inherentes a la tecnología.
- **Tamaño de la trama:** Registrar el tamaño del mensaje enviado para la solicitud.
- **Tamaño de la trama de respuesta:** Registrar el tamaño del mensaje que la aplicación respondió.

- **Validación de Datos de Entrada**

Si hay carencias en esta funcionalidad se presentarán vulnerabilidades de inyección o buffer overflow, que pueden causar ataques de negación de servicio que afecten la disponibilidad o acceso no autorizados que afectarían la integridad y/o confidencialidad. En el desarrollo de la aplicación se tendrán las siguientes consideraciones:

- **Protección contra buffer overflow:** Aplicación de las mejores prácticas en el desarrollo para tener un estricto control en la definición del tipo de variables para que se ajusten a los requerimientos. La validación se realiza analizando el código en cada una de las sentencias de definición de variables para que se limiten a un dominio o rango requerido por la función correspondiente. Un buffer overflow se

presenta cuando se acepta como entrada grandes cantidades de caracteres que logran desbordar el segmento de datos y que adicionalmente con una longitud específica pueden llegar a un segmento privilegiado de la memoria, donde se pueden ejecutar ciertos comandos; es decir que el atacante debe encontrar esta longitud y adicionalmente definir el comando que lograría ejecutar. Considerando lo anterior cada variable definida debe tener un tipo de datos limitado, preferiblemente definido por el programador y que los mecanismos sean diseñados para que solo capturen lo estipulado por los formatos aceptados o lo estrictamente requerido, por ejemplo si se va a capturar un número celular, la variable definida debe ser un campo tipo texto de 10 caracteres y cuando se capture dicho campo se debe validar que solo se acepten valores entre 0 y 9 y que la entrada solo puede ser de 10 caracteres rechazando cadenas de texto de menor o mayor longitud; si dentro de la revisión de código se evidencia que no se implementan estas restricciones, a pesar de que funcionalmente sea aprobado se está generando una vulnerabilidad.

- **Restricción de las capturas:** Los datos que se ingresen al sistema estarán restringidos por la longitud y el tipo de datos para limitar a lo estrictamente necesarios. La validación se realiza analizando el código para cada una de las sentencias de captura de datos, verificando que se realice la "sanitización" o validación que restrinja los valores que puedan ser ingresados. Para cada uno de los campos capturados el CNMH debe definir el tipo de datos que se va a capturar el cual puede seguir el estándar aceptado o entregar la especificación correspondiente; la validación debe proceder para constatar que las capturas de datos validen que no se ingresen caracteres que puedan ser usados para una intrusión y esto es cadenas de texto que correspondan a "Comandos o instrucciones en los lenguajes o sistemas operativos involucrados", de esta forma en el Programador debe considerar los filtros más exigentes posibles de tal forma que sin limitar datos validos restrinja palabras o wildcards que puedan ser usados en comandos o instrucciones. Se debe considerar que muchas veces los atacantes cambian las codificaciones (ASCII, EBCDIC, UNICODE) para saltarse los controles. Particularmente en la Aplicación para que la labor de Programación sea más efectiva en la implementación de estos filtros es requerido el mayor nivel de especificación para los datos recibidos de los usuarios y a intercambiar con las entidades. A simple vista podría exigirse que en ninguno de los campos tenga porque aceptarse caracteres diferentes a números y letras y que los signos de puntuación solo apliquen para campos tipo Memo, validando que estos no sean consecutivos, es decir nada

justificaría que alguien ingrese algo como un punto y una coma consecutivos.

- **Librerías:** Se tendrá una validación para evitar el uso de librerías con vulnerabilidades de cualquier tipo. La validación se realiza analizando el código y evaluando que cada una de las librerías utilizadas no tengan reporte de vulnerabilidades. Se tendrá una validación en el framework de desarrollo el cual alertará sobre las librerías que se encuentren obsoletas y así evitar el uso de componentes vulnerables para la aplicación. Las vulnerabilidades son catalogadas por los boletines emitidos por los fabricantes correspondientes.

- **Parámetros pasados a través de la URL:** Restringir el tamaño y el tipo de caracteres que son pasados en los parámetros de la URL para evitar ataques de Cross Site Scripting y la exploración no autorizada de directorios del servidor donde resida la aplicación. La validación se realiza analizando el código para cada una de las sentencias de captura de datos, verificando que se realice la validación que restrinja los valores que puedan ser ingresados; aplica el mismo concepto definido en la restricción de las capturas solo que en este caso aplicaría para los parámetros pasados de una URL, en el cual los filtros van a ser orientados hacia los datos que se puedan requerir en este entorno, es decir para este caso debe aceptarse el uso de la barra inclinada o slash.

- **Manejo de excepciones**

  En el desarrollo de la Aplicación, para cada una de las funciones implementadas seran contempladas las opciones resultantes de los casos de abuso, es decir evitar que la aplicación pierda el control en el flujo posible de acciones, evitando que una excepción permita violar las políticas de seguridad definidas. Todas las funciones tendrán un manejo específico para los casos que estén por fuera de los que señalan los requerimientos funcionales. Se hará uso de defunciones como en el caso de Java try-catch que permiten establecer el control para los casos de excepción en las diferentes capas.

- **Control de Sesión**

  Se debe contar con la opción de definir un tiempo máximo de sesión. Se debe hacer uso herramientas predefinidas en los diferentes entornos, en el caso de Java con el uso de la clase httpsession y el Java Web

Framework se verificarán las opciones posibles para controlar los tiempos de sesión mínimo y máximo, como también un control de memoria aplicando un reinicio de sesión por cada nueva solicitud en el menú o interface de usuario.

7.18. Política de gestión de incidentes.

Cada vez que se detecta un evento, incidente o debilidad relacionados con seguridad de la información por parte de un servidor público, contratista o tercero, se deberá reportar a la Dirección Administrativa y Financiera – Gestión de TIC por cualquiera de los medios dispuestos para tal fin.

Será responsabilidad del Dirección Administrativa y Financiera – Gestión de TIC seguir los procedimientos establecidos para la gestión de los incidentes que puedan presentarse.

Asegurar que los eventos e incidentes de seguridad que se presenten en el CNMH con los activos de información sean comunicados y atendidos oportunamente, empleando los procedimientos definidos "GTC-PR-004 Gestión de Soporte a Usua e Incid TIC", con el fin de tomar oportunamente las acciones correctivas.

7.19. Política de seguridad del centro de datos y centros de cableado.

Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte. En las instalaciones del Centro de Datos y de los centros de cableado.

No está permitido:

- Mover, desconectar y/o conectar equipo de cómputo sin autorización.
- Modificar la configuración del equipo o intentarlo sin autorización.
- Alterar software instalado en los equipos sin autorización.
- Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas.
- Extraer información de los equipos en dispositivos externos.
- Abuso y/o mal uso de los sistemas de información.
- Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.
- Fumar.
- Introducir alimentos o bebidas

- El porte de armas de fuego, corto punzantes o similares.
- Ubicar equipos o elementos que no correspondan a este lugar.

7.20. Política de seguridad de proveedores. (los proveedores también se encuadran en la categoría de contratistas, ya que prestan un servicio o suministran un bien. Si se hace ésta distinción tendría que definirse la categoría.

El CNMH deberá mantener la seguridad de la información y los servicios de procesamiento de información, a los cuales tienen acceso terceros, entidades externas o que son procesados, comunicados o dirigidos por éstas.

El Centro Nacional de Memoria Histórica establecerá políticas y requisitos de seguridad de la información para mitigar los riesgos asociados a cada proceso de contratación.

Se deben establecer criterios de selección que contemplen la experiencia y reputación de futuros contratistas, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad.

Antes de iniciar la ejecución de contratos con terceras partes, deberán suscribirse los respectivos acuerdos de confidencialidad que incluyan las cláusulas de confidencialidad y los aspectos de seguridad de la información necesario durante y después del contrato.

Se deben establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad y privacidad de la información del CNMH, las cuales deben se divulgadas por los servidores públicos responsables de la supervisión de contratos o convenios.

En los contratos o convenios suscritos con los proveedores y/o contratistas se debe incluir una causal de terminación del contrato o convenio, por el no cumplimiento de las políticas de seguridad y privacidad de la información. Los contratistas deben aceptar y firmar el acuerdo de confidencialidad establecido por el CNMH.

La Dirección Administrativa y Financiera - Gestión TIC deberá mitigar los riesgos de seguridad de información respecto al acceso de los contratistas a los sistemas de información del CNMH.

ACUERDO DE CONFIDENCIALIDAD

Este debe ser firmado sin excepción alguna con cualquier contratista con el que se establezca cualquier tipo de intercambio de información y lo que debe señalar es que el acceso a los datos que hagan parte del servicio prestado al CNMH, solo pueden ser accedidos, leídos o conocidos por las personas y/o entidades que estén formalmente autorizadas. Este acuerdo trae consigo las penalizaciones con base en los daños potenciales, ante la violación de la confidencialidad de la información.

PROTECCIÓN DE DATOS PERSONALES

Se debe incluir dentro del Contrato suscrito una cláusula que haga referencia al cumplimiento de la Política de Protección de Datos Personales del CNMH (SIP-PC-015. Política de Tratamiento de la Información y Datos Personales), documento que debe ser entregado al contratista para su conocimiento y aplicación.

PERSONAL ENCARGADO DEL SERVICIO

Los Supervisores deben velar porque se realicen las validaciones correspondientes para que el personal de la empresa prestadora que manejan información provista por él, conozcan y cumplan con las Políticas de Seguridad y Privacidad de la Información.

REQUERIMIENTOS DE SEGURIDAD DE APLICACIONES Y/O SERVICIOS

Si el proveedor es responsable por aplicaciones o servicios informáticos, estos deben cumplir con los requerimientos de protección de la Confidencialidad, Integridad y Disponibilidad definidos por él y que debe demostrar con base en el activo que va a ser manejado, uno o más de los siguientes controles:

- **Monitoreo:** Estar en capacidad de brindar los mecanismos para detectar incidentes de seguridad de la información sobre el funcionamiento de la aplicación con el que se presta el servicio al . El nivel de detección se ajustará a los requerimientos del activo involucrado en el servicio.

- **Control de acceso:** Presentar los mecanismos de control de acceso a los servicios y los datos manejados con base en la Política de Control de Acceso del CNMH.
- **Gestión de incidentes:** Contar con un esquema de identificación, reporte, escalamiento, tratamiento y documentación de los incidentes que se presenten en el funcionamiento de la aplicación o servicio prestado.
- **Soporte:** El proveedor debe contar con los expertos idóneos para atender incidentes o eventos de seguridad de la información con base en el SGSI.
- **Licenciamiento:** Todas las aplicaciones y servicios prestados por el proveedor deben contar con el licenciamiento acorde con el marco legal y regulaciones que apliquen.

REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN FRENTE A TERCEROS

El CNMH exigirá unas condiciones mínimas con respecto a la Seguridad y Privacidad de la Información para las empresas proveedoras con las que se genere intercambio de información catalogada en los niveles 4, 5 y 6 de Confidencialidad y 5 y 6 de Integridad (Ver manual de clasificación de la información "(I) Documento General - Metodología Clasificación de activos SGSI").

1. Contar con un sistema de gestión de seguridad de la información.
2. Presentar la política de seguridad de la información referente al servicio o producto que se está prestando al CNMH.
3. Presentar el soporte para el procedimiento de tratamiento de los incidentes de seguridad de la información que puedan darse en el desarrollo del servicio o el producto entregado.

REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN DE PERSONAS NATURALES COMO PROVEEDORES

Las personas naturales que actúen como proveedores del CNMH, deberán seguir las Políticas de Seguridad y Privacidad de la información definidas para los servidores públicos, teniendo como excepción lo relacionado con el proceso disciplinario. En este caso hará alusión a un Incumplimiento de Contrato.

7.21. Política de cumplimiento de requisitos legales y contractuales.

La finalidad de esta política es prevenir el incumplimiento de obligaciones legales relacionadas con seguridad de la información.

El Centro Nacional de Memoria Histórica - CNMH respeta y acata las normas legales existentes relacionadas con seguridad de la información, para lo cual revisará que todos los procesos contractuales den cumplimiento a la legislación y requisitos contractuales aplicables para la entidad, relacionada con la seguridad de la información.

El CNMH establecerá el procedimiento para la protección de derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

La Dirección Administrativa y Financiera – Gestión de TIC deberá garantizar que todo el software que ejecute los activos de información del CNMH esté protegido por derechos de autor y cuente con la debida autorización para su uso.

Los usuarios y/o servidores públicos del CNMH deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es menester recordar que es ilegal duplicar software y documentación sin la autorización del propietario bajo los principios de derechos de autor; y la reproducción no autorizada es una violación a la ley.

La Dirección Administrativa y Financiera – Gestión de TIC realizará el procedimiento de copias de respaldo (backup) de los registros alojados en los sistemas de información.

El CNMH implementará los lineamientos para asegurar la privacidad y protección de datos personales, definiendo claramente los deberes en las actividades de recolección, procesamiento y transmisión de los mismos.

7.22. Política de tratamiento de datos personales.

El Centro Nacional de Memoria Histórica cuenta con la política en la intranet "(I) SIP-PC-015. Política de Tratamiento de la Información y datos personales".

7.23. Política de seguridad física y del entorno.

El Centro Nacional de Memoria Histórica adoptará medidas para el control de acceso físico a las instalaciones y áreas seguras con el fin de mitigar los riesgos asociados a la afectación de la confidencialidad, disponibilidad e integridad de la información.

La Entidad definirá áreas seguras y los controles de acceso físico correspondientes para la protección de la información que allí se resguarda.

Todas las personas que ingresen a las instalaciones del Centro Nacional de Memoria Histórica deben cumplir con los lineamientos establecidos para el control de acceso físico sin excepción.

7.24. Política de seguridad en las operaciones.

Con el fin de asegurar las operaciones realizadas en los recursos tecnológicos que soportan la operación del negocio. El Centro Nacional de Memoria Histórica planea, gestiona, respalda y monitorea la infraestructura tecnológica siguiendo los lineamientos establecidos en los procedimientos establecidos para el SGSI.

7.25. Política de seguridad de las comunicaciones.

La Dirección Administrativa y Financiera – Gestión de TIC establecerá los controles para acceso lógico y protección de las redes del El Centro Nacional de Memoria Histórica, con el fin de asegurar y cumplir con los acuerdos de niveles de servicios que sean establecidos para los servicios de red y que deberán ser acordados con la Alta Dirección.

El Centro Nacional de Memoria Histórica definirá procedimientos y lineamientos para la transferencia segura de información interna o externa, de tal forma que se garantice la integridad y confidencialidad de la información.

8. CONTROLES

Las Políticas de Seguridad y Privacidad de la Información del Centro Nacional de Memoria Histórica - CNMH dan origen a una serie de controles que el CNMH se compromete a desarrollar y que están registrados en el documento "Documento General - Declaración de aplicabilidad SGSI", que hace parte del Sistema Integrado de Gestión.

9. SENSIBILIZACIÓN Y COMUNICACIÓN

El Centro Nacional de Memoria Histórica definirá un "Plan de Comunicación en Seguridad de la Información" a través de la Estrategia de Comunicaciones y la Dirección Administrativa y Financiera – Gestión de TIC, donde se planificará ANUALMENTE la manera en que se comunicarán recomendaciones de seguridad de la información por diferentes medios a todos sus servidores públicos y contratistas, con el fin de socializar las políticas institucionales en seguridad de la información o las buenas prácticas en seguridad para aumentar las capacidades de todas las áreas y procesos de la Entidad. La creación de los contenidos se hará con apoyo de la Dirección Administrativa y Financiera – Gestión de TIC.

El Centro Nacional de Memoria Histórica dentro de sus sensibilizaciones definirá las temáticas de seguridad de la información, con el objetivo de que los servidores públicos que se vinculen a la Entidad tengan pleno conocimiento de las políticas de seguridad de seguridad de la información. Dicha actividad será apoyada por la Dirección Administrativa y Financiera – Gestión de TIC.

10. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

Las políticas aquí definidas se harán efectivas a partir de su aprobación por parte del Comité Institucional de Gestión y Desempeño, quien revisará por lo menos anualmente, cuando existan incidentes de seguridad de la información o cuando se produzcan cambios estructurales considerables, esto con el fin de asegurar su vigencia y aplicabilidad dentro del Centro Nacional de Memoria Histórica.

11. SANCIONES

La falta de conocimiento de los presentes lineamientos no libera a los servidores públicos del Centro Nacional de Memoria Histórica de las responsabilidades

establecidas en ellos por el mal uso que hagan de los recursos de TIC o por el incumplimiento de los lineamientos aquí descritos, por lo tanto:

- Se aplicarán sanciones de acuerdo con el Código General Disciplinario.
- .
- La Dirección Administrativa y Financiera – Gestión de TIC será la dependencia encargada de recopilar y entregar al proceso de Control disciplinario de la Dirección Administrativa y Financiera las evidencias de incumplimiento de los lineamientos, informes de impactos y consecuencias y cualquier otro insumo requerido para formalmente manejar la investigación inicialmente a nivel interno, así mismo, la Dirección Administrativa y Financiera – Gestión de TIC será la encargada de registrar y gestionar el incidente de seguridad derivado con el incumplimiento de las políticas.

12. 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 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. Artículo 3: De la contratación pública electrónica".
- Ley 1341 de 2009. "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la

Información y las Comunicaciones ?TIC?, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones".

- Decreto 1074 de 2015 "por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo".
- Decreto 1078 de 2015 Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"
-
- Decreto 1083 de 2015. "**por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.**".
- CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016 Política Nacional de Seguridad digital.

13. 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

14. 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	30/11/2017	001
Se realizó la actualización del documento de Política de Seguridad y Privacidad de la Información	Se actualizó el documento en cuanto a su estructura y contenido	25/09/2019	002
Se realizó la actualización del documento de Política de Seguridad y Privacidad de la Información	Se actualizó el documento en cuanto a su estructura y contenido, eliminando las acciones que no se ejecutan.	09/09/2021	003
Se realizó la actualización del documento de Política de Seguridad y Privacidad de la Información	Se actualizó el documento en cuanto al orden de numerales eliminando redundancias	27/11/2024	004