PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

CENTRO NACIONAL DE MEMORIA HISTÓRICA

ABRIL DE 2023

Centro Nacional de Memoria Histórica

Contenido

1. INTRODUCCIÓN

La información que corresponde al activo más importante para el CNMH debe protegerse con base a los requerimientos de seguridad y privacidad de la información definidos dentro de un proceso permanente de Gestión de Riesgos. Adicional a esto, el CNMH debe plantearse una serie de metas estratégicas encaminadas a aumentar los niveles de seguridad de la información, enmarcados en un plan y más aún pensado en la necesidad de cumplir con las obligaciones misionales de la Entidad.

2. OBJETIVO

Mantener los niveles de seguridad y privacidad de la información en el CNMH para la vigencia 2023, identificando brechas e implementando controles para su cierre, administrando los riegos a los que se puede ver expuesta la información para enmarcarlos en el menor riesgo posible.

3. ALCANCE

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

4. DEFINICIONES

Activo: Cualquier elemento que tiene valor para la organización y que para la Gestión de riesgos de seguridad de la información se consideran los siguientes entre otros como la información, el software, los elementos físicos, los servicios, las personas e intangibles.

Amenaza: Causa potencial de un incidente no deseado, el cual puede resultar en daño al sistema o a la Organización.
[Fuente: ISO 27000]

Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento**.**

Confidencialidad: Propiedad de la información que hace que no esté disponible o que no pueda ser revelada a individuos, entidades o procesos, no autorizados.

Disponibilidad: Propiedad de ser accesible y utilizable ante la demanda de una entidad autorizada.
[Fuente: ISO 27000]

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.
[Fuente: ISO 27000]

Monitoreo: Verificación, supervisión, observación crítica o determinación continua del estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.

Parte involucrada: Persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada por una decisión o una actividad. Una persona que toma decisiones puede ser una parte involucrada.
[Fuente: ISO 31000]

Propietario del activo: Persona o cargo que administra, autoriza el uso, regula o gestiona el activo de información. El propietario del activo aprueba el nivel de protección requerido frente a confidencialidad, integridad y disponibilidad.

Riesgo: Efecto de la incertidumbre sobre los objetivos. Un efecto 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, toda la organización).
[Fuente: ISO 31000]

Teletrabajo: En Colombia, el Teletrabajo se encuentra definido en la Ley 1221 de 2008 como: "*Una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y comunicación -TIC- para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio especifico de trabajo*". (Artículo 2, Ley 1221 de 2008)

Vulnerabilidad: Debilidad identificada sobre un activo y que puede ser aprovechada por una amenaza para causar una afectación sobre la confidencialidad, integridad y/o disponibilidad de la información.

5. METODOLOGÍA

La metodología propuesta para la creación del Plan de seguridad de la información ese

define en tres etapas:

- Etapa 1: Conocer la entidad.
- Etapa 2: Diagnóstico inicial.
- Etapa 3: Generación del plan.

5.1. ETAPA 1: CONOCER LA ENTIDAD

El conocimiento de la Entidad se logra mediante las siguientes actividades:

- Entrevistas: Los líderes de los procesos y algunas personas claves dentro de le Entidad dada su experiencia y conocimiento de la organización es fundamental para poder conocer y entender la organización. De igual manera es fundamental realizar entrevistas con el personal técnico clave del CNMH.
- Identificación de los riesgos identificados y evaluados para los procesos del alcance.
- Identificación de los controles implementados para la mitigación de los riesgos proporcionados.
- Revisión de los hallazgos de seguridad de la información.

5.2. ETAPA 2: DIAGNOSTICO

Consiste en la realización del análisis de brecha (GAP), frente a la norma la ISO 27001: 2013. Para este caso, el análisis se realizará mediante el uso del "Instrumento de evaluación MSPI", de MinTIC. Este instrumento no solo evalúa los requerimientos solicitados MinTIC y los de la norma ISO 27001: 2013. Adicionalmente evalúa ciberseguridad y el ciclo PHVA.

5.3. ETAPA 3: GENERACION DEL PLAN

Con base en la información anteriormente recopilada en las fases anteriores se genera el Plan de seguridad.

6. AMENAZAS ASOCIADAS

Se identificaron las siguientes amenazas asociadas a los riesgos:

- ✓ **Divulgación no autorizada de información**: Existen datos que se encuentran en computadores personales donde no se cuenta con mecanismos de trazabilidad, ni controles criptográficos; adicionalmente en el CNMH existen algunos computadores que son propiedad de los Contratistas y para estos no existe formalmente controles

para la instalación de software. Lo expuesto más algunas falencias en la cultura de seguridad hacen que el control existente como es la autenticación por usuario y contraseña deba ser complementado.

- ✓ **Modificación no autorizada de información**: En general en el CNMH se han implementado controles cruzados y chequeos que permiten la validación de los datos que hacen parte de los procesos de la Entidad; este control más la autenticación por usuario y contraseña establecen la mitigación contra los riesgos para la Integridad de la información, pero la ausencia de controles de trazabilidad, monitoreo y sobre todo mecanismos de verificación de integridad, hacen que se den riesgos no aceptables para esta amenaza.

- ✓ **Acceso no autorizado:** La ausencia de un sistema de detección de vulnerabilidades y las debilidades en la validación del software que se instala en todos los equipos del CNMH, eleva la probabilidad de puntos débiles en los sistemas y aplicaciones que pueden ser aprovechados para lograr un acceso no autorizado. Esto se incrementa con la carencia en mecanismos de monitoreo.

- ✓ **Difusión de malware**: El sistema antimalware existente requiere mayor intervención de los usuarios, quienes deben manejar las opciones requeridas para la Gestión de incidentes, como son las de chequeo permanente y reporte de anomalías. También es necesario que se configure la opción de aprendizaje en servidores y equipos de usuario para la detección de anomalías en los patrones de comportamiento establecidos como normales.

- ✓ **Ingeniería Social**: Es necesario reforzar la conciencia sobre esta amenaza, situación que puede ser aprovechada para afectar la seguridad de la información. A continuación, se citan aspectos que evidencian dicha situación:

    - No se aplican políticas de seguridad frente a la información que puede ser divulgada telefónicamente.

    - No hay una disciplina rigurosa alrededor del uso personal e intransferible de las credenciales de acceso a los sistemas de información y aplicaciones del CNMH.

    - No existe conciencia sobre el conocimiento y habilidades mínimas que deben tener todos los funcionarios sobre aspectos de seguridad de la información.

    - Se cuenta con un Sistema de Gestión de Continuidad que cubre sólo aspectos básicos y se hace necesario llevar a cabo un Análisis de Impacto de Negocio (BIA) que permita determinar los requerimientos específicos de continuidad

de la Entidad.

- A nivel de Tecnologías de la Información y Comunicaciones se requiere implementar sistemas de monitoreo automáticos que brinden elementos para la reacción oportuna en caso de situaciones contingentes.

7. VULNERABILIDADES

- ✓ **Cultura de Seguridad de la Información**: Se evidencia una carencia generalizada por los siguientes aspectos:

  - No hay rigurosidad en el manejo personal e intransferible de las cuentas de usuario asignadas.
  - Los funcionarios no cuentan con una formación en cuanto a la identificación y reporte de incidentes de seguridad de la información.
  - No hay conocimiento suficiente sobre mejores prácticas y soluciones de seguridad de la información.
  - No se ha socializado a los funcionarios en cuanto al uso del sistema antimalware.

- ✓ **Gestión de vulnerabilidades**: No se cuenta con un mecanismo, tecnología o procedimiento formal para la detección proactiva de vulnerabilidades.

- ✓ **Software**: Las aplicaciones son puestas en funcionamiento sin una política que exija formalmente requerimientos de seguridad de la información como son:

  - Identificación y soporte para las vulnerabilidades de la aplicación, estableciendo como el fabricante reporta las vulnerabilidades identificadas, como se implementa la protección contra ataques de día cero y la definición de los procedimientos de remediación.

- ✓ **Controles Criptográficos**: Se requieren revisar y actualizar los mecanismos y el software que se usan en el CNMH para la protección de integridad y confidencialidad de la información.

- ✓ **Control de acceso físico**: El acceso físico siempre representa vulnerabilidades razón por la cual debe considerarse en estos análisis.

8. PLAN DE TRATAMIENTO

- ✓ Si bien el SGSI se encuentra formalizado a través del Comité Institucional de Gestión

y Desempeño, el plan de tratamiento de riesgos debe ser socializado ante el mismo comité con el fin de someterlos a su revisión, modificación y aprobación.

- ✓ Tanto Funcionarios como Contratistas deben firmar un acuerdo de confidencialidad con el CNMH y es necesario recalcar la responsabilidad que esto implica.

- ✓ El Plan de Tratamiento propuesto debe estar soportado en las Políticas y Procedimientos que componen el SGSI formulado para el CNMH.

- ✓ Se deben priorizar las labores de sensibilización y entrenamiento de los Funcionarios y Contratistas, considerando las vulnerabilidades evidenciadas por la carencia de una Cultura de seguridad de la información y que con la implementación del SGSI cada funcionario adquiere nuevas responsabilidades para las cuales debe adquirir nuevos conocimientos y habilidades.

- ✓ El CNMH El CNMH debe asumir que a partir de la implementación del SGSI se debe establecer un perfil mínimo que todos los Funcionarios y Proveedores de la Entidad, deben cumplir para poder alinearse con las exigencias para la protección de la confidencialidad, integridad y disponibilidad de la información con base en la clasificación establecida.

- ✓ Se debe reforzar la relación con todos los proveedores de la Entidad con el fin de que conozcan y cumplan las políticas de seguridad y privacidad de la información del CNMH.

- ✓ Cuando se evidencie que no es posible cumplir con un control definido por el SGSI por razones de presupuesto o asignación de recursos, se debe escalar dicha situación hasta el nivel de autoridad suficiente para que se asuman los riesgos que esto conlleve.

9. ACTIVIDADES PLANTEADAS

A continuación se relacionan las actividades para reforzar la seguridad y privacidad de la información en la Entidad:

- Realizar el diagnóstico mediante la herramienta de evaluación del MSPI
- Identificación de las brechas identificadas mediante la herramienta de evaluación del MSPI.
- Análisis y planteamiento del cierre de brechas identificadas.
- Actualizar el Inventario de Activos de Información
- Realizar el análisis de riesgo de sobre los activos con el objetivo de identificar los riesgos asociados.

- Realizar el planteamiento de las acciones a llevar a cabo con el objetivo de dar tratamiento a los riesgos identificados.

✓ Realizar jornadas de socialización del SGSI con el siguiente alcance:
- Responsabilidad de cada usuario frente a la seguridad y privacidad de la información.
- Riesgos y vulnerabilidades (ingeniería social, circulación de malware en el correo electrónico, redes sociales).
- Responsabilidad de cada usuario con referencia a sus credenciales y contraseñas.
- Herramientas de seguridad disponibles en el CNMH.

✓ Gestionar la ejecución de un proceso de ethical hacking.
✓ Revisión y actualización de políticas de seguridad y privacidad de la información.
✓ Revisión y actualización de procedimientos de seguridad y privacidad de la información.
✓ Revisión y actualización de la Declaración de Aplicabilidad del CNMH.
✓ Implementar la clasificación de casos en la Herramienta de Soporte TIC, que permita mejorar la identificación de los incidentes de seguridad.
✓ Generar e implementar un procedimiento actualizado de atención de incidentes de seguridad de la información.