PLAN DE SEGURIDAD DE LA INFORMACION

CENTRO NACIONAL DE MEMORIA HISTÓRICA

NOVIEMBRE DE 2017

	NOMBRE	CARGO	FECHA
ELABORÓ			
REVISÓ			
APROBÓ			

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La información como el activo más importante para el CNMH y debe protegerse con base en los requerimientos de seguridad de la información definidos con base en un proceso permanente de Gestión de Riesgos. Adicional a esto, el CNMH debe plantearse una seria de metas estratégicas encaminadas a aumentar los niveles de seguridad de la información, en marcados en un plan y más aún pensado en la importancia cada vez mayor que el CNMH va a adquirir dada la situación actual del país.

2. ASPECTOS GENERALES

2.1. OBJETIVO

Aumentar los niveles de seguridad de la información en el CNMH para las vigencias 2017 a 2018, con miras aumentar la seguridad, cerrando brechas, implementando controles, administrando los riegos de la información para mantenerlos en el nivel más reducido posible.

2.2. 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.

3. 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 este disponible o que sea revelada a individuos no autorizados, entidades o procesos.

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 informacion: 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 así 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

4. METODOLOGÍA

La metodología propuesta para la creación del Plan de seguridad de la información, es en 3 etapas:

- Conocer la entidad.
- Diagnóstico inicial.
- Generación del plan.

4.1. 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.

4.2. 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 Min TIC. Este instrumento no solo evalúa los requerimientos solicitados Min TIC y los de la norma ISO 27001: 2013. Adicionalmente mide evalúa ciberseguridad y el ciclo PHVA. Por lo tanto, esta herramienta es la adecuada esta tarea.

4.3. GENERACION DEL PLAN

Con base en la información recopilada se genera el plan de seguridad.

5. ANALISIS PARA DEL DESARROLLO DEL PLAN

La época del año (finales de septiembre de 2017) donde se contrató el servicio para gestionar el SGSI del CNMH y los altos niveles de ocupación de los líderes de proceso y personas claves dentro del CNMH, no ha permitido realizar las entrevistas requeridas, por esta razón se trabaja con lo recopilado

por una consultoría realizada en el 2014 por la empresa Globaltek Security, que generó una serie de documentos para el SGSI y lo descubierto por el profesional que ejecuta el contrato de prestación de servicios N°569 de 2017.

5.1. RIESGOS

Con base en lo recopilado, se observa el siguiente panorama de riesgos a fecha del 2015:

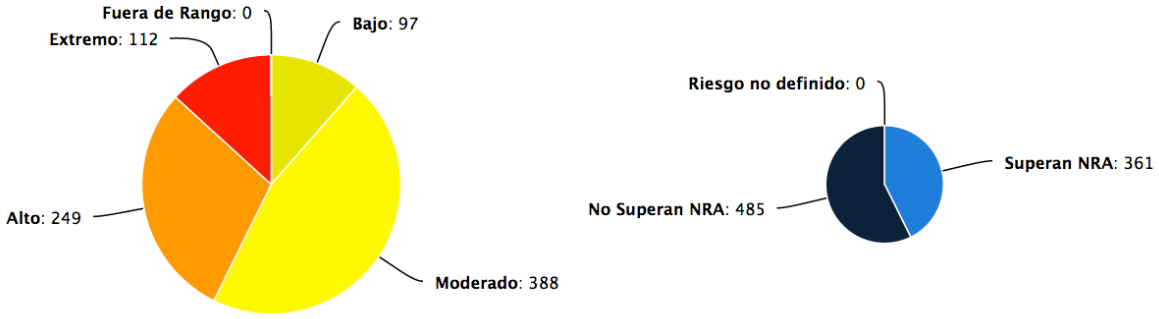

Figura 1 Riesgos 2015

5.2. AMENAZAS ASOCIADAS

La consultoría identificó las siguientes amenazas asociadas a los riesgos:

- **Divulgación no autorizada de información:** Existen datos clasificados en los niveles más altos de confidencialidad, que se encuentran en computadores personales donde no se cuenta con mecanismos de trazabilidad, ni controles criptográficos; adicionalmente en el CNMH existe una buena parte de los computadores que son propiedad de los Contratistas y para estos no existe formalmente controles para la instalación de software. Lo expuesto más la carencia en la cultura de seguridad hacen que el único control existente como es la autenticación por usuario y contraseña sea insuficiente.
- **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 la falta de validación en el 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:** No hay una conciencia clara 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.
    - Los visitantes pueden moverse dentro del edificio sin ningún tipo de acompañamiento
    - No existe un mecanismo de validación por parte de los Funcionarios para los visitantes o personas de las que no se tenga certeza sobre su razón en permanecer dentro de las oficinas
    - **Interrupción de servicio:** No se cuenta con un Sistema de Gestión de Continuidad, ni tampoco se ha llevado a cabo el Análisis de Impacto de Negocio (BIA) que permita determinar los requerimientos específicos de continuidad de la Entidad. En lo que respecta a Tecnología de Información y Comunicación, debido a la ausencia de esquemas de monitoreo, no es posible reaccionar oportunamente ante amenazas que puedan afectar la continuidad del servicio en el CNMH.

5.3. VULNERABILIDADES

La consultoría identificó las siguientes 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 responsabilizado a los funcionarios en cuanto al uso del sistema antimalware.
    - No hay una cultura frente al uso de un protector de pantalla.
    - No se evidencia una política de escritorio despejado.
    - No existe un procedimiento que responsabilice a los Funcionarios en el proceso de validación de personas ajenas a la Entidad que se encuentren dentro del edificio.
- **Gestión de vulnerabilidades:** No se cuenta con un mecanismo, tecnología o procedimiento formal para la detección proactiva de vulnerabilidades, esta situación fue evidenciada con los resultados de las pruebas de vulnerabilidad y ethical hacking ejecutadas como parte de la Consultoría.
- **Gestión de incidentes de seguridad de la información:** Actualmente el CNMH cuenta con un servicio de mesa de ayuda ejecutado por una empresa externa y apoyado con el Software HEAT (Fabricante Front Range) pero no se cuenta con procedimientos formales para la identificación, valoración y tratamiento para los incidentes de seguridad de la información.
- **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.
    - Soporte para los incidentes de la aplicación, cuales son los canales de atención ante la ocurrencia de fallas, imprevistos, accesos no autorizados y todo lo que conlleve a

violación de las Políticas de Seguridad de la Información de CNMH con el uso de dicha aplicación.

- Evaluación de la funcionalidad de la herramienta verificando que está totalmente justificada por uno o más procesos definidos formalmente dentro de CNMH.
- Implementación de la Política de Control de acceso, especificando los roles autorizados y los privilegios de acceso.
- Gestión de monitoreo, especificar e implementar que datos se requieren registrar para identificar violaciones a las Políticas de Seguridad de CNMH y la correspondiente Gestión de Incidentes.

- **Controles Criptográficos:** No se han definido formalmente los algoritmos y el software correspondiente para la protección de la integridad y confidencialidad de los datos.
- **Control de acceso físico:** El control biométrico únicamente cubre una de los dos accesos para la sede principal, dejando el acceso alterno (de conexión directa al segundo piso) sin un registro automático. Se evidenció que el control de salida lo efectúa cualquier funcionario sin que medie una previa validación.

5.4. PLANES DE TRATAMIENTO

La consultoría presento los siguientes tratamientos a los riesgos:

- El primer paso para que sea la piedra angular del Plan de Tratamiento de Riesgos y como tal del SGSI es la formalización a través del acto administrativo, con el cual se van a soportar todas las labores recomendadas y se evidenciará el compromiso de la Dirección General.

- A partir de la formalización del SGSI, los funcionarios y proveedores del CNMH deben firmar los acuerdos y formatos correspondientes que corroboren que entienden y aceptan las nuevas responsabilidades que le son asignadas y que su incumplimiento puede llevar a un Proceso disciplinario o de tipo legal.

- El Plan de Tratamiento propuesto en Global Suite se soporta en las Políticas y Procedimientos que componen el SGSI y que fueron entregados como parte de los resultados de la Consultoría.

- Se deben priorizar las labores de sensibilización y entrenamiento de los Funcionarios 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 debe asumir que a partir de la implementación del SGSI se establece 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.

- Es importante considerar que en la medida que se permita que los Funcionarios hagan uso del soporte técnico dispuesto por la Entidad, por carencias en su Cultura de Seguridad o conocimientos técnicos mínimos, esto seguirá generando vulnerabilidades que expondrán la seguridad de la información.

- Se debe replantear la relación con todos los proveedores para que se cumpla con la Política de Seguridad de la Información establecida.

- 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.

- Considerando el arduo trabajo que representa la implementación del SGSI, se debe trabajar priorizando los esfuerzos con base en la calificación de los riesgos, es decir empezando por los catalogados como Nivel Extremo.

5.5. REVISION DE AUDITORIAS

Se revisa la auditorias realizada en el 20014 y se observan los siguientes hallazgos:

- Si bien se ha identificado un conjunto de indicadores para el SGSI, estos nos han sido aprobados y, por tanto, no se han comenzado a tomar valores.
- Se debe finalizar la aprobación de la documentación del SGSI.
- Se deben analizar los resultados de las acciones de concienciación en seguridad de la información.
- Se debe delimitar de manera concisa las responsabilidades relativas a la seguridad de la información, pues no existe oficial de seguridad.
- Algunos usuarios tienen deshabilitada la directiva de caducidad de las contraseñas del directorio activo.

- Se debe revisar la política de contraseña actual en el directorio activo.
- No se ha llevado a cabo la remediación de las vulnerabilidades encontradas en la infraestructura por parte del proveedor custodio de la infraestructura.
- No se han llevado a cabo las mejoras propuestas en la arquitectura de seguridad tecnológica.
- Los planes de acción propuestos para la mitigación de del riesgo residual deberían ser aprobados de manera formal por el dueño del riesgo / proceso.
- Planificar las sesiones de capacitación necesarias para el personal en la herramienta de gestión usada para el SGSI.
- Se debe planificar una de las fechas de las revisiones cuyo alcance sea la totalidad del SGSI para la certificación del sistema.
- Se debe incluir en el “manual de seguridad” la política de contraseñas que está definida en el directorio activo.
- Se debe definir una periodicidad de (por ejemplo, mensual) para la revisión de los indicadores que orece la consola de antivirus, el firewall y el almacenamiento de red entre otros.
- Se debe hacer una nueva revisión interna de tipo formal independiente de los consultores que ayudaron en el SGSI.
- Leyendo la arquitectura de los controles tecnológicos propuestos y si el dueño del riesgo los aprueba basados en el NRA la organización debería presupuestarse para el 2015 una inversión para la compra de controles.
  Leyendo el plan de tratamiento de riesgos se debe internamente iniciar la creación de registros o formatos que en detalle cumplan con las mejores propuestas, estas acciones y actitudes no se pueden comprar, requieren de un cambio cultural y de actitud que cuesta tiempo del recurso humano y solo se puede medir con las métricas ya diseñadas del SGSI.

5.5.1.1. DIAGNOSTICO DEL CNMH (GAP)

Se evaluó el cumplimiento de los documentos y registros exigidos por la norma ISO 27001:2013 a través del Instrumento de evaluación MSPI. según el requerimiento de Min TIC. La madurez esperada es del 100%:

Figura 2 Madurez de los controles del SGSI

Como se puede apreciar en la gráfica, la seguridad en la gestión de los recursos humanos presenta un alto nivel de madurez (que puede mejorar aún más), los demás dominios de la norma necesitan atención urgente y en el de gestión de incidentes.

A continuación, se presenta la tabla de madurez con la que se realizó la evaluación:

Tabla de Escala de Valoración de Controles ISO 27001:2013 ANEXO A		
Descripción	**Calificación**	**Criterio**
No Aplica	N/A	No aplica.
Inexistente	0	Total, falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Tabla 1 - Modelo de madurez ISO 27002

6. PROPUESTA DE PLAN DE SEGURIDAD DE LA INFORMACION

6.1. VIGENCIA 2017

Con base en los argumentos ya expuestos la propuesta para lo que resta del 2017 es la publicación y divulgación de la política de seguridad de la información y como parte de esta divulgación presentar a los líderes de los procesos y la alta gerencia que en la vigencia 2018 se van a realizar tareas en conjunto con ellos como lo son el levantamiento de activos, análisis de riesgos, planes de tratamiento, presentación y aprobación de diversas políticas y procedimientos asociados al SGSI que son de su alcance.

6.2. VIGENCIA 2018

En esta vigencia se deben concentrar esfuerzos en fortalecer el SGSI, para ello se deben realizar las siguientes tareas puntuales:

- Divulgación del SGSI.
- Capacitación a los usuarios respecto a seguridad e la información.
- Realizar la primera auditoria interna.
- Ajustes y aprobación de la documentación obligatoria del SGSI.
- Generación de la documentación solicitada por Min TIC en el MSPI.
- Cerrar las brechas halladas al diligenciar el “Instrumento de evaluación MSPI”.
- Realizar levantamiento de activos.
- Realizar análisis de riesgos.
- Generar planes de tratamiento.
- Revisar, reforzar e implementar los controles que surgen de los planes de tratamiento.
- Comenzar a realizar tareas de supervisión para formar a los usuarios para que cumplan las políticas de seguridad de la información.
- Implementar y documentar controles de seguridad enfocados en cumplir la normatividad que aplica el CNMH.
- Generar e implementar un procedimiento actualizado de atención de incidentes de seguridad de la información.
- Generar aprobación por parte de la alta gerencia de la documentación asociada al SGSI.
- Apoyar en le implementación de buenas prácticas de seguridad de la información en la infraestructura tecnológica.

Basándose en el trabajo de la empresa Globaltek en el 2014-2015, se deben utilizar los elementos ya trabajados por la consultoría prestada por esta empresa, sin embargo, se debe realizar un re análisis / reproceso en muchos de los elementos trabajados por ellos y principalmente corregir el inconveniente que dejaron el cual consiste en dejar el SGSI "amarrado" a una herramienta tecnológica llamada Globalsuite, dicha herramienta ya no se posee licencia y no se puede acceder a la misma.

Presentar a los líderes de los procesos y la alta gerencia que en la vigencia 2018 se van a realizar tareas en conjunto con ellos como lo son el levantamiento de activos, análisis de riesgos, planes de tratamiento.

7. REQUISITOS

- Aprobación de la política de seguridad de la información en el CNMH.
- Reiteración del compromiso con el SGSI y el MSPI por parte de la alta gerencia.
- Disponibilidad de tiempo suficiente pro parte de los líderes del proceso y personas claves dentro de los procesos en el momento de ser requeridos.
- Asignación de por lo menos una persona para trabajar el SGSI.
- La persona asignada para trabajar el SGSI deberá tener la suficiente "potestad" de convocar a líderes de proceso y convocar reuniones, así como poder interactuar con todos los procesos del CNMH.

CONTROL DE CAMBIOS			
ACTIVIDADES QUE SUFRIERON CAMBIOS	**CAMBIOS EFECTUADOS**	**FECHA DE CAMBIO**	**VERSIÓN**
No Aplica	Creación del Documento	25/11/2017	001
