POLITICA DE SEGURIDAD DE LA INFORMACIÓN

NOMBRE	CARGO	FECHA
Néstor Julio Corredor	Profesional Especializado	11/2017
Néstor Julio Corredor	Profesional Especializado	11/2017
Cesar Augusto Rincón Vicentes	Director Administrativo y Financiero (e)	30/11/2017

POLITICA DE SEGURIDAD DE LA INFORMACIÓN

La información como el activo más importante y activo fundamental para prestar sus servicios y cumplir su misión y visión para el Centro Nacional de Memoria Histórica (CNMH) debe protegerse con base en los requerimientos de seguridad de la información definidos en un proceso permanente de Gestión de Riesgos. Esta protección se logra con la implementación de un Sistema de Gestión de Seguridad de la Información que establece el ciclo de Planear, Hacer, Verificar y Actuar para los controles que le den el tratamiento a los riesgos para mantener la confidencialidad, integridad y disponibilidad de los datos manejados por CNMH.

La Política del Sistema de Gestión de Seguridad de la Información de CNMH establece unas directrices ciertas, por lo cual el CNMH:

R E S U E L V E:

ARTÍCULO PRIMERO. ASPECTOS GENERALES. Establecer y desarrollar la Política de Gestión de Seguridad de la Información para el Centro Nacional de Memoria Histórica a través de la implementación procedimientos y controles que mitiguen los riesgos identificados sobre los activos de información y el tratamiento de los posibles riesgos relacionados con ataques a la seguridad de la información y posibles pérdidas o fuga de datos que puedan afectar la gestión institucional; garantizando de esta forma el cumplimiento de la misión, visión y objetivos institucionales, así como la alineación con la planificación estratégica del Centro Nacional de Memoria Histórica.

ARTÍCULO SEGUNDO. OBJETIVO. Considerando la misión del Centro de Memoria Histórica en su contribución a la reparación integral, el esclarecimiento histórico, las garantías de no repetición y la construcción de paz sostenible a través de la recopilación, análisis, tratamiento, almacenamiento y difusión de información producto de hechos clasificados para dicha misión, decide implementar la política de Seguridad de la Información con el objetivo de preservar la confidencialidad, integridad y disponibilidad de esta información para apoyar el cumplimiento de lo estipulado en la Constitución Política de Colombia y el Marco Legal y Regulatorio.

ARTÍCULO TERCERO. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO. El Centro Nacional de Memoria Histórica se compromete a implementar los controles identificados en el Plan de Tratamiento de Riesgos de Seguridad de la Información, los cuales estarán sujetos al seguimiento, monitoreo, control y actualización mediante la aplicación de herramientas y procedimientos establecidos, incluyendo acciones para evitar, reducir, compartir o transferir, o asumir el riesgo; con la participación de los servidores públicos y contratistas de la Entidad y dando respuesta a los lineamientos estratégicos y los requisitos legales.

ARTÍCULO CUARTO. ALCANCE. La política de seguridad de la Información establece la guía de acción para que todos los servidores públicos y contratistas del Centro Nacional de Memoria Histórica, coordinen y administren los eventos que puedan impedir el logro de las metas a través del tratamiento y manejo de los riesgos de seguridad de la información con base en su valoración y que permitan tomar decisiones adecuadas para evitar, reducir, compartir o transferir, o asumir el riesgo. La administración de los riesgos se hará para todos los procesos del Centro Nacional de Memoria Histórica (estratégicos, misionales, apoyo o de evaluación).

ARTÍCULO QUINTO. RESPONSABLES. Existirá un Comité de seguridad de la información, que será el responsable del mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información de CNMH. Dicho comité estará conformado por la alta gerencia o su representante, los líderes de procesos y el oficial de seguridad de la información.

La implementación de la política de Seguridad de la Información debe ser coordinada por el representante de la alta dirección del CNMH y su equipo directivo. Igualmente contar con el apoyo del oficial de seguridad de la Información, Comité Institucional de Desarrollo Administrativo del Centro Nacional de Memoria Histórica y el apoyo del equipo operativo del Sistema Integrado de Gestión del Centro Nacional de Memoria Histórica, acorde con la legislación vigente aplicable y la normatividad interna; también debe ser conocida y apropiada por todos los servidores públicos y contratistas que sean responsables y/o participen en el desarrollo de los diferentes planes, programas, proyectos, procesos o actividades en el CNMH. Los líderes de proceso deben dar a conocer a su equipo de trabajo los lineamientos determinados en la presente política.

Los funcionarios públicos y contratistas del CNMH participarán en la implementación de la política de Gestión de Seguridad de la Información definida por el CNMH y por lo tanto deben conocer y apropiar dicha política.

ARTÍCULO SEXTO. DIRECTRICES. La Política del Sistema de Gestión de Seguridad de la Información del CNMH establece las siguientes directrices:

- Es prioridad para la Entidad la protección de la Confidencialidad de los datos personales de los ciudadanos que participen en los procesos de Construcción de la Memoria Histórica.
- Es de gran criticidad para CNMH la protección de la integridad de los datos relacionados directamente con la construcción de la memoria histórica.
- Los funcionarios y contratistas CNMH deben garantizar su permanente actualización, entrenamiento y sensibilización sobre las políticas y procedimientos del Sistema de Gestión de Seguridad de la Información.
- Los funcionarios y contratistas del CNMH son responsables de identificar y reportar posibles incidentes de seguridad de la información.
- Todas las operaciones que se lleven a cabo sobre la información de CNMH debe tener una previa validación para aplicar los controles requeridos frente a la confidencialidad, integridad y disponibilidad.
- Es mandatorio para Funcionarios y contratistas el uso de las tecnologías de seguridad de la información como son sistemas antimalware, software para controles criptográficos y en general los exigidos dentro el Sistema de Gestión de Seguridad de la Información que posea el CNMH.
- El soporte del área de sistemas para labores de seguridad de la información debe limitarse a lo que realmente se justifique y no podrá desgastarse en Funcionarios que desconozcan las políticas o carezcan del entrenamiento citado en el punto anterior.
- Es mandatorio el cumplimiento de las Políticas y Procedimientos del SGSI en la medida que aplique, para todos los funcionarios, contratistas y proveedores del CNMH.
- El compromiso del cumplimiento de los objetivos del SGSI está en cabeza del Director General de CNMH, los líderes de los procesos, apoyados por el oficial de seguridad.

ARTÍCULO SÉPTIMO. OBJETIVOS:

Los objetivos aceptados por la Dirección General para el Sistema de gestión de seguridad de la información en el CNMH son los que se listan a continuación:

- Cumplir con el marco legal y regulatorio del CNMH para los aspectos de seguridad de la Información, especialmente orientada al cumplimiento de la estrategia de Gobierno en Línea.
- Mantener el nivel de riesgo para la Seguridad de la Información en los niveles bajo y moderado.
- Los riesgos identificados en los niveles extremo o alto deben ser tratados inmediatamente con el fin de mitigar afectaciones negativas en la operación y buen nombre de la entidad.
- Registrar y tomar acciones correctivas y/o preventivas sobre todos los incumplimientos a las Políticas de Seguridad de la Información.
- Mantener el nivel de las vulnerabilidades técnicas asociadas a los riesgos en los niveles medio y bajo, aquellas asociadas a los riesgos altos y extremos deben ser corregidas inmediatamente.
- Realizar al menos una auditoría externa de seguridad de la información al año, como principal entrada para la mejora continua del SGSI.
- Establecer una estrategia de sensibilización y capacitación a los funcionarios del CNMH para minimizar los riesgos inherentes a las personas (Ingeniería Social).

ARTÍCULO OCTAVO: CUMPLIMIENTO:

Todos los funcionarios, contratistas y proveedores de Centro de Memoria Histórica deben cumplir en la medida que corresponda con las Políticas y Procedimientos específicos de seguridad de la información que hacen parte del SGSI y que se listan a continuación:

- Política de control de acceso a la información
- Política de Gestión de Cambios
- Política de transferencia de información
- Política de desarrollo seguro de software
- Política de generación y restauración de copias respaldo
- Política de llaves criptográficas
- Política de uso de Dispositivos móviles
- Política de teletrabajo
- Política de escritorio limpio y pantalla limpia
- Política de seguridad de la información para relaciones con proveedores
- Política de protección de datos personales
- Proceso disciplinario
- Procedimiento de clasificación de Información
- Procedimiento de etiquetado de información
- Procedimiento de gestión de incidentes de seguridad
- Procedimiento de registro y cancelación de cuentas de usuario
- Procedimiento de gestión de roles y privilegios
- Procedimiento de verificación para el cumplimiento legislativo y regulatorio en cuanto a derechos de Autor
- Procedimiento de la continuidad de la Seguridad en caso de contingencia
- Procedimiento de control de cambios
- Procedimiento para autorización de instalación de Software
- Procedimiento de transferencia de información
- Procedimiento para trabajo en áreas seguras
- Procedimiento de gestión de medios removibles

POLÍTICA DE USO ACEPTABLE DE LOS RECURSOS INFORMÁTICOS

A continuación, se presentan las normas que definen el uso de los recursos informáticos que deben ser acogidas por los funcionarios del CNMH para cumplir con las políticas de seguridad de la información.

Requerimientos para el uso de servicios informáticos

- 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 por parte de la dirección Administrativa y Financiera.

- El uso de la cuenta asignada por parte de la dirección Administrativa y Financiera para cada acceder los servicios tecnológicos que se prestan, tienen como mecanismo de acceso el Factor de Usuario y contraseña, que son de total responsabilidad del funcionario o contratista correspondiente.

- El máximo periodo de vigencia de una contraseña es de 1 mes, plazo en el cual el usuario debe proceder con su cambio, evitando repetir valores usados en los 10 últimos periodos.

- La contraseña debe tener una longitud entre 10 y 14 caracteres, conteniendo al menos una letra minúscula, una letra mayúscula, un digito y un carácter especial.

- La responsabilidad del uso de la cuenta asignada al funcionario 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 la mesa de ayuda usos no autorizados detectados con la cuenta asignada en cualquiera de los servicios informáticos proporcionados por la Entidad.

Acceso a Internet

- 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 reportar a la mesa de ayuda registrando fecha, hora y acción ejecutada.

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

- 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 provisto 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.

- 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; esto deben ser reportado inmediatamente a la mesa de ayuda.

- 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.

Correo Electrónico

- 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.

- La cuenta de correo de una persona desvinculada 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 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

- No utilizar el correo asignado por el CNMH para propósitos diferentes al laboral

- La información clasificada como confidencial solo puede ser enviada en forma cifrada

- Los correos cuyo destino es toda la Entidad, lo pueden hacer los jefes de área.

- Información por fuera de lo 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 al Departamento de Sistemas.

- Si por error es ejecutado un archivo recibido de un correo no validado debe reportarse la situación inmediatamente a la mesa de ayuda y en lo posible aislar el equipo.

- Cuando la cuenta de correo sea bloqueada o se olvide la contraseña, el funcionario debe enviar un correo desde su cuenta personal registrada en Talento Humano solicitando el desbloqueo.

Uso del Computador Personal

- No es aceptado el uso de un computador que no sea el que fue asignado por el CNMH. No se permite el uso de computadores o equipos con licenciamiento no Profesional (Home User)

- El acceso al computador personal es exclusivo del funcionario al que fue asignado. La excepción a esta regla es para los casos de soporte por parte de los funcionarios del departamento de sistemas.

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

- El software instalado en el computador debe estar explícitamente autorizado por el jefe del área correspondiente y el departamento de sistemas.

- 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 departamento de sistemas, previa solicitud formalizada.

- El uso del computador personal únicamente se puede realizar cuando el Antimalware este activado y su fecha de actualización no difiera en más de un día con respecto a la fecha actual.

- Los documentos personales deben ser almacenados en la carpeta con el nombre “NombreUsuario-Personal” ubicada dentro de la carpeta Mis Documentos. Toda la información por fuera de esta carpeta no será tratada como personal del usuario.

- Cualquier novedad, anomalía, comportamiento diferente, cambio o situación que no pueda ser justificada por la operación normal en el computador personal, debe ser reportada inmediatamente por el usuario siguiendo el procedimiento de Gestión de Incidentes.

- No se deben almacenar en el computador archivos o información que presente violación a los derechos de autor.

- Malware, ataques informáticos o afectación a la red de datos de la Entidad originada en el computador del usuario será su responsabilidad si se identifica el incumplimiento de alguna de estas normas.

Uso de la Red de Datos

- La instalación, configuración, cambio en cualquiera de los equipos de la red como son: switches, enrutadores, puntos de acceso inalámbricos etc. son tarea exclusiva de los funcionarios del departamento de sistemas que usan como base la Norma de Seguridad en la red. Es importante considerar que esta restricción aplica para los teléfonos inteligentes (Smart Phones) que pueden ser usados como Módems.

- La transferencia de archivos a través de la red, sea con destino interno o externo debe contar con mecanismos de cifrado para los archivos que sean catalogados como Confidenciales.

- El uso de repositorios o sitios de almacenamiento externos como Google Drive, Dropbox, Taringa y Mega, entre otros deben estar previamente autorizados por el departamento de sistemas.

- La instalación de equipos en la red como servidores, computadores personales, routers, puntos de accesos inalámbricos, switches y equipos de seguridad es de responsabilidad exclusiva del departamento de sistemas y su ejecución se debe orientar por la Norma de Seguridad de la red.

- Cualquier equipo que se conecte a la red del CNMH, debe contar con la autorización previa del departamento de sistemas.

- El usuario debe reportar anomalías en la red, aplicando el procedimiento de Gestión de Incidentes.

Servidores y Servicios

- La instalación, desinstalación, configuración o cambio en cualquiera de los servidores o servicios que se presten en la red del CNMH, es responsabilidad exclusiva del Departamento de sistemas; esto incluye a los servidores o servicios de pruebas.

- Los servidores o servicios solamente deben ser implementados sobre equipos con sistemas operativos tipo servidor.

- Es aceptado el uso de servicios o servidores por fuera de la red del CNMH, siempre y cuando estos sean soportados por un Contrato formal aprobado por la Dirección General del CNMH. No es aceptado el uso de servicios gratuitos como por ejemplo los Repositorios para el manejo de archivos clasificados como confidenciales o con nivel alto de criticidad para Integridad.

- Los servidores o servicios habilitados en la Red del CNMH deben cumplir con los requerimientos para el uso de servicios informáticos descritos en el punto 1 de esta política.

- Los servidores o servicios deben poder contar con la opción de configuración de perfiles que permitan aplicar el principio de asignación de mínimo privilegio posible y la segregación de funciones.

ARTÍCULO NOVENO. DIVULGACIÓN. La política de Gestión de Seguridad de la Información, se divulgarán al interior del Centro Nacional de Memoria Histórica a través de los medios de comunicación, charlas informativas, así como la socialización al interior de cada uno de los procesos a los servidores públicos y contratistas de la entidad por parte de los líderes de proceso y la participación del equipo de trabajo en el monitoreo y revisión de los riesgos del proceso.

ARTÍCULO DÉCIMO. TÉRMINOS Y DEFINICIONES: Se relaciona los términos relevantes en la Política de Gestión de Seguridad de la Información en el Centro Nacional de Memoria Histórica. Tomando como base la norma ISO 27000 e ISO 31000.

Activo: cualquier elemento que tiene valor para la organización y que para Gestión de riesgos de seguridad de la información se consideran los siguientes información, software, físicos, servicios, personas e intangibles.
Amenaza: causa potencial de un incidente no deseado, el cual puede resultar en daño al sistema o a la Organización.
[Fuente: ISO 27000]
Confidencialidad: propiedad de la información que hace que no esté disponible o que sea revelada a individuos no autorizados, entidades o procesos.
Disponibilidad: propiedad de ser accesible y utilizable ante 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 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]
Vulnerabilidad: debilidad identificada sobre un activo y que puede ser aprovechado por una amenaza para causar una afectación sobre la confidencialidad, integridad y/o disponibilidad de la información.

Proyectó: Área de Tecnología – Dirección Administrativa y Financiera – CNMH

CONTROL DE CAMBIOS			
ACTIVIDADES QUE SUFRIERON CAMBIOS	CAMBIOS EFECTUADOS	FECHA DE CAMBIO	VERSIÓN
No Aplica	Elaboración de Documento	30-11-2017	001