INTRODUCCIÓN

El presente documento se define la Política de Seguridad de la Red del ICANH y sus componentes, con el fin de proteger la información contra amenazas para asegurar la continuidad de las actividades del Instituto y reducir los impactos que se puedan causar por la materialización de un evento dañino.

POLÍTICA

Para el cumplimiento de las funciones del Instituto Colombiano de Antropología e Historia, dentro de su proceso de gestión de soporte tecnológico, se definieron orientaciones generales para la seguridad en el manejo de la red de sistemas y de la información de institucional de diferente índole. En este sentido las decisiones en materia de software y hardware utilizaran soluciones originales que garanticen un correcto uso de la red y sus aplicaciones y que conduzcan al mejor desarrollo de las capacidades de las personas al servicio de la Entidad. El uso y manejo de la red y sus componentes, al igual que las soluciones implementadas se enmarcan en las recomendaciones dadas por los fabricantes de las mismas. La seguridad en la administración de la red y en el manejo de la información, es una prioridad institucional, por tal motivo la red será manejada o administrada por personal idóneo y cumpliendo las funciones establecidas en el manual de la Entidad. Se diseñaran e implementaran los diferentes dispositivos de firewall en software y hardware para la protección de la red, bases de datos e información. Los usuarios y grupos de interés que utilicen los servicios de la red institucional deberán cumplir con los protocolos y lineamientos de seguridad definidos. Igualmente el cumplimiento de las disposiciones en materia de derechos de autor define las decisiones en cuanto al uso de las soluciones y servicios tecnológicos de la Institución.

Se generarán los mecanismos de protección, mantenimiento, modernización y adquisición tanto de la Red del ICANH como de equipos de cómputo adoptando los criterios para proteger la integridad técnica de la institución, reduciendo los daños que pueda causar un evento nocivo. Los funcionarios y contratistas del Instituto son responsables de la información que manejan y deberán seguir las directrices orientadoras para protegerla y evitar pérdidas, accesos no autorizados y utilización indebida de la misma.

El área de Sistemas define, implementa, controla y mantiene las políticas, normas, estándares, procedimientos, funciones y responsabilidades necesarias para preservar y proteger la confidencialidad, disponibilidad e integridad de la información del Instituto donde ésta resida (aplicaciones, bases de datos, sistemas operativos, redes, back Ups y medios). De igual forma desarrolla las acciones de seguridad que permite controlar el entorno lógico y físico de la información teniendo en cuenta los criterios de confidencialidad, integridad, auditabilidad, disponibilidad, autenticidad y no repudiación de la información. Desarrolla métodos y técnicas para monitorear efectivamente los sistemas de seguridad de la información y reportar periódicamente su efectividad a la Alta Dirección.

La presente política es aplicable a todos los empleados y contratistas del Instituto. Los empleados con funciones y responsabilidades para con el software y hardware institucional deben seguir los lineamientos para proteger este activo y la información.

1. SEGURIDAD LÓGICA

Se cuenta con un conjunto de controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de dar buen uso de los mismos y mantener los niveles de seguridad, los cuales se administran directamente por la persona responsable del área de sistemas y tiene las siguientes competencias:

1.1 Crear Grupos de Usuarios (Unidades Organizaciones OU Microsoft) y Políticas de Grupo
1.2 Crear Grupos de Distribución de Correo
1.3 Establecer las Políticas de Acceso, con las siguientes características:

- Cuentas de red: Primera letra del Nombre y Apellido completo
- Lineamientos para la construcción de Contraseñas de seguridad: Mínimo ocho (8) caracteres, debe contener letras (mayúsculas y minúsculas), números y caracteres especiales como $ % @*.
- Tamaño de los buzones de correo restringido
- Tamaño máximo de archivos adjuntos en correo restringido

1.4 Restringir Permisos de acceso por usuario/carpeta/equipo:

- Restringir el acceso (de personas del instituto y de las que no lo son) a los programas y archivos
- Asegurar que los usuarios puedan trabajar, pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).
- Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.

1.5 Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se hace enviado y que no le llegue a otro.

1.6 Establecer la obligatoriedad en la actualización de las contraseñas de acceso a la red cada 45 días.

1.7 Monitorear la red.

1.8 Utilizar tecnologías repelentes o protectoras: cortafuegos (firewall) y sistemas de detección de intrusos

1.9 Utilizar un solución integral de protección contra virus para la red del ICANH que incluya como mínimo: antivirus para PC´s y servidores, solución antispam y antispyware, protección contra correo indeseado y una consola de actualización y distribución automática que mantenga todos los PC´s y servidores protegidos

1.10 Restringir tipos de archivos que se puedan considerar peligrosos en el correo:

- De acuerdo con recomendaciones de seguridad dadas por Softsecurity Ltda, representante de McAfee y proveedor del ICANH, está bloqueada la entrada a la red (por medio de correo electrónico), de cierto tipo de archivos que pueden ser peligrosos para la seguridad de la misma.

- Extensiones recomendadas para bloquear en el GroupSHield - McaFee recomienda agregar las siguientes extensiones dentro de su configuración GroupShield si esta seleccionada como “tipos de archivos”:

001	Bo?	Dot	Js?	Ole	Shs	Wpd
002	Cdr	Drv	Mb?	Ov?	Smm	Xml
386	Chm	Exe	Md?	Pif	Sys	Xsl
adt	Cla	Gms	Mpp	Pot	Tar	Xtp
app	Cmd	Gz?	Mpt	Pps	Tdo	Mp?
arc	Com	Hlp	Msg	Qlb	Vbs	
asp	Csc	Ice	Mso	Qpw	Vs?	
bat	Dev	Im?	Obd	Reg	Vxd	
Bin	Dl?	ini	Obt	scr	Wbk	
			ocx		Wiz	

1.11 Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad.

1.12 Restringir la instalación de software no licenciado en PC´s.

1.13 Mantener al máximo el número de recursos de red sólo en modo lectura.

1.14 Restringir el acceso vía VPN.

1.15 Controlar y monitorizar el acceso a Internet.

1.16 Mantener vigentes contratos de soporte tecnológico especializado, en caso de fallas de hardware o problemas de software en servidores.

1.17 Mantener disponible la información sobre las personas a contactar en caso de detectar una posible intrusión en la seguridad de la red o falla en su infraestructura.

1.18 Mantener el sitio seguro para correo remoto.

1.19 Elaborar procedimientos para el área de sistemas.

1.20 Generar back ups según lo especificado en el procedimiento “Generación de Copias de Seguridad de Datos” (Pr-PGST-SIS-1) y en el procedimiento “Generación de Copias de Seguridad de Configuración de Servidores” (Pr-PGST-SIS-2).

1.21 Administrar la custodia externa e interna de los back ups (Una copia de los back ups en disco externo, es llevada fuera de la entidad semanalmente por la persona responsable de sistemas custodia externa y una copia en disco y cintas se mantiene en la caja fuerte de Tesorería del Instituto custodia interna).

1.22 Mantener condiciones de seguridad adecuadas para el uso de los sistemas de información institucional ICANH que incluyan como mínimo:

- Asignación de usuarios y contraseñas, a nivel administrador y a nivel de usuario no administrador
- Asignación de permisos a nivel de red.
- Solo los usuarios autorizados ingresarán datos a las bases de datos de los aplicativos del ICANH.
- Cada usuario será responsable de los datos ingresados.
- Se deben crear ambientes de prueba que permitan la verificación de la funcionalidad de nuevas versiones liberadas de aplicativos y solo una vez certificadas se instalan en ambiente de producción

2. SEGURIDAD FISICA

Para el uso de los activos informáticos, compromete a los usuarios en el cumplimiento de las normas y estándares establecidos para la seguridad informática y el buen uso de los mismos. Para ello se establecen las siguientes decisiones:

a. Seguridad física del Centro de Cómputo:

El centro de cómputo está bajo la responsabilidad exclusiva del área de sistemas de la Entidad.

Para ello se toman las siguientes previsiones:

1. Restringir el acceso al centro de cómputo, de personas ajenas al área de sistemas.
2. Mantener los servidores en condiciones ambientales adecuadas. (aíre acondicionado)
3. Instalar cámaras de vigilancia y detector de humo.
4. Instalar redes de corriente regulada para los servidores y PC´s, apoyada por UPS´s.
5. Programar Ups´s para cada uno de los servidores.
6. Realizar mantenimiento preventivo y correctivo a todos los equipos de cómputo y otros equipos como UPS´s, aire acondicionado, etc.

Condiciones requeridas para el normal funcionamiento del centro de cómputo del ICANH

Condiciones ambientales:

- Mantener el centro de cómputo en condiciones ambientales de temperatura adecuadas que prevengan daños en los equipos servidores y UPS´s que allí están ubicados.
- El centro de cómputo debe contar con un equipo de aire acondicionado tipo Minisplit de 18000 BTU como mínimo.
- El equipo de aire acondicionado debe funcionar 7días x 24 horas, a 18 grados centígrados de temperatura como máximo.
- El extractor de aire del centro de cómputo debe estar funcionando permanentemente.
- El ventilador del rack de servidores debe permanecer encendido 7 días x 24 horas.
- El área debe mantenerse limpia.
- El aire acondicionado del centro de cómputo debe recibir mantenimiento preventivo y correctivo adecuado, que asegure su óptimo funcionamiento (mantenimiento preventivo mensual).

- Las luces del centro de cómputo deben permanecer apagadas mientras no haya personal en dicha área.

Condiciones de seguridad eléctrica:

- En el centro de cómputo del ICANH, las tomas de corriente regulada son de color naranja y las tomas beige son de corriente directa.
- Se debe contar con dos UPS's generales: una UPS de 8 KVA ubicada en el centro de cómputo y UPS de 10 KVA ubicada en el centro de cableado de la sede de calle 12 2 - 41 Bogotá.
- Cada servidor debe contar con una UPS programable de 1.5 KVA, con apagado automático.
- Las UPS´s programables de los servidores, deben estar conectadas a la UPS principal del Centro de Computo de manera que exista doble protección..
- Las UPS´s programables deben estar configuradas en cada servidor, de manera que ante una falla de energía prolongada, éstas apaguen los servidores de manera adecuada y los enciendan cuando la falla de energía sea superada.
- Las UPS´s del ICANH (UPS de 8 KVA ubicada en el centro de cómputo y UPS de 10 KVA ubicada en el centro de cableado de la sede de investigadores del ICANH) deben recibir mantenimiento preventivo y correctivo adecuado, que asegure su óptimo funcionamiento. (por lo menos tres servicios de mantenimiento preventivo al año).
- Las baterías de las UPS´s deben cambiarse, de acuerdo con la garantía de las mismas y su uso (cada tres años como máximo).

Condiciones de acceso restringido:

- El centro de Cómputo y Centro de Cableado deberá estar asegurado con llave en la puerta de acceso principal 7 días x 24 horas.
- La limpieza de las áreas deben estar supervisadas por algún funcionario del área de sistemas.

b. Condiciones requeridas para el normal funcionamiento de los computadores PCs del ICANH

- Los computadores del ICANH deben estar conectados a la corriente regulada, así:

  - En los puestos de trabajo con tomas color beige y tomas color blanco en la canaleta: los computadores deben estar conectados a las tomas color beige (corriente regulada) y cualquier otro tipo de aparato electrónico (impresoras láser, calentadores, radios, etc) deben estar conectados a las tomas de color blanco (corriente directa).

  - En los puestos de trabajo con tomas color naranja y tomas color beige en la canaleta: los computadores deben estar conectados a las tomas color naranja (corriente regulada) y cualquier otro tipo de aparato electrónico (impresoras láser, calentadores, radios, etc) deben estar conectados a las tomas de color beige (corriente directa).

- Los computadores se deben apagar en la forma debida (incluido el monitor), para evitar deterioro del sistema operativo.

- Cuando se presenten fallas de energía, las UPS´s entran a funcionar por unos minutos, por lo que es aconsejable grabar la información que se esté trabajando en el momento y apagar normalmente el computador.
- Se debe evitar mover cables, conexiones y PC's, sin la supervisión de algún funcionario del área de sistemas del ICANH.
- Se prohíbe fumar y consumir alimentos o bebidas frente a los computadores.
- El ICANH utiliza software licenciado por tanto no está permitido instalar software no licenciado.

c. Seguridad contraseñas y equipos

- La asignación de contraseñas se realiza de forma individual, por lo que el uso de passwords compartidos está prohibido.
- Las contraseñas no deben estar en forma legible en cualquier medio digital y/o impreso, y no deben ser dejadas en lugares donde personas no autorizadas puedan descubrirlos. Los usuarios no deben almacenar los passwords en ningún programa o sistema que proporcione esta facilidad. No se deben usar contraseñas que hayan sido idénticas o substancialmente similares a contraseñas previamente empleadas.
- Sin importar las circunstancias, las contraseñas nunca se deben compartir o revelar. Hacer esto responsabiliza al usuario que prestó su contraseña de todas las acciones que se realicen con el mismo.
- La contraseña inicial emitida a un nuevo usuario sólo es válida para la primera sesión. El usuario deberá cambiar la contraseña.
- Para prevenir ataques está limitado a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida.
- La contraseña debe ser difícil de adivinar, esto implica que no deben relacionarse con el trabajo o la vida personal del usuario, y no deben contener caracteres que expresen listas secuenciales.
- Si no hay ninguna actividad en un PC durante cierto periodo de tiempo, el sistema suspende la sesión. El re-establecimiento de la sesión requiere que el usuario proporcione nuevamente su contraseña.
- Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá informar al área de sistemas para que se le proporcione un nuevo password y una vez que lo reciba deberá cambiarlo en el momento en que acceda nuevamente a la infraestructura tecnológica.

3. RECUPERACIÓN ANTE DESASTRES

El plan de recuperación ante desastres, se basa en back ups en custodia tanto interna como externa, de configuración de servidores y back ups de datos generados diaria, semanal y mensualmente.

Ante estos eventos el ICANH cuenta con el soporte técnico especializado 7 x 24, para la plataforma de servidores y para lo que corresponde a seguridad.