POLITICA DE SEGURIDAD DEL SGSI EN EL ICANH

La política de seguridad de la información, representa la posición del Instituto Colombiano de Antropologia e Historia (ICANH) con respecto a la protección de los activos de información (los funcionarios, la información, los procesos, las tecnologías de información incluido el hardware y el software) y respecto a la implementación del Sistema de Gestión de Seguridad de la Información y al apoyo, generación y publicación de sus políticas, procedimientos e instructivos.

El Instituto Colombiano de Antropologia e Historia (ICANH) para el cumplimiento de su misión, visión, objetivo estratégico y apegado a sus valores corporativos establece la función de seguridad de la información en la entidad, con el objetivo de:

- Minimizar los riesgos en las funciones más importantes de la entidad
- Cumplir con los principios de la seguridad de la información
- Cumplir con los principios de la función administrativa
- Mantener la confianza de los funcionarios, contratistas y usuarios del Instituto
- Apoyar la innovación tecnológica
- Implementar el sistema de gestión de seguridad de la información SGSIen el ICANH
- Proteger los activos tecnológicos del instituto
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información
- Fortalecer la cultura de seguridad de la información en funcionarios, contratistas, practicantes y usuarios del ICANH
- Garantizar la continuidad de operación del Instituto, frente a incidentes de seguridad

Alcance/Aplicabilidad

Esta política aplica a toda la entidad, sus funcionarios, contratistas, practicantes, proveedores del ICANH y a la ciudadanía en general

Nivel de Cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad, se espera que se adhieran en un 100% de la política.

Políticas de seguridad generales que soportan el SGSI del ICANH:

1. El ICANH deberá implementar, operar, y mejorar de forma continua un sistema de gestión de seguridad de la información SGSI, soportado en lineamientos claros, alineados a las necesidades del instituto, a los procesos de la entidad(SIGAP) y a los requerimientos regulatorios de ley.
2. El ICANH protegerá la información generada, procesada o resguardada por los procesos del Instituto, su infraestructura tecnológica, y activos, de los riesgos que se generanal autorizar accesos a terceros o como resultado de un servicio interno de *outsourcing* (los contratos deben contener cláusulas de confidencialidad).
3. El ICANH deberá definir y mantener actualizada la clasificación y confidencialidad de su información, a fin de establecer las políticas de acceso correspondientes.
4. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, contratistas y usuarios en general del ICANH.
5. El ICANH protegerá la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar los impactos financieros, operativos o legales, debido a un uso incorrecto de dicha información. Para ello es fundamental la aplicación de controles en cada proceso, de acuerdo con la clasificación de la información, de su propiedad o en custodia.
6. El ICANH protegerá su información de amenazas de fuga o pérdida de información originadas por parte funcionarios y contratistas.
7. El ICANH protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos, implementando medidas de seguridad física y lógicas.
8. El ICANH controlará la operación de sus procesos, garantizando la seguridad de los recursos tecnológicos y la red de datos.
9. El ICANH deberá tomar las medidas necesarias para garantizar la seguridad de la información cuyo manejo sea en la nube.
10. El ICANH implementará control de acceso de los usuarios, a la información, sistemas y recursos de red.
11. El ICANH garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información y deberá asegurar la implementación de protecciones a aplicativos Web y portal Web institucional.
12. El ICANH garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información, para una mejora efectiva de su modelo de seguridad.
13. El ICANH garantizará la disponibilidad de sus procesos y la continuidad de su operación, basado en el impacto que pueden generar los incidentes de seguridad.
14. El ICANH deberá mantener vigentes los contratos de mantenimiento preventivos y correctivos de equipos de tecnología que sean requeridos, para un adecuado funcionamiento de su infraestructura tecnológica.
15. El ICANH deberá asegurar que se hagan estudios periódicos de seguridad, mediante análisis de vulnerabilidades que permitan establecer acciones de mejora a la infraestructura tecnológica y a la seguridad de la información.

16. El ICANH adoptará las recomendaciones (buenas prácticas y estándares de la industria) de los fabricantes de tecnología, en materia de seguridad y manejo de los elementos tecnológicos que proveen.
17. El ICANH adoptará la configuración, habilitación y revisión periódica de registros históricos, que permitan la detección de intentos de accesos no autorizados y la revisión de transacciones electrónicas, como evidencia para auditorías.
18. El ICANH deberá tener una política de actualización tecnológica permanente, lo cual incide directamente en la utilización de recursos tecnológicos actualizados, más seguros y acordes a los continuos cambios tecnológicos.
19. El ICANH tendrá en cuenta que toda transmisión electrónica de datos deberá cumplir con lo establecido en el marco de interoperabilidad de Gobierno en Línea.
20. El ICANH deberá implementar medidas de seguridad y dar un manejo responsable a los datos personales de los usuarios de los servicios que presta el Instituto.
21. El ICANH garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas para la seguridad de la información.

ANEXO
PROCEDIMIENTOS DE SEGURIDAD ICANH

1) **Implementar manejo adecuado y seguro de contraseñas**:
   - A cada usuario de la red ICANH se le asignará un nombre de usuario y un *password* (la solicitud deberá hacerla mediante correo electrónico al área de sistemas, el jefe de área o supervisor del contrato). A partir de la asignación, el usuario se compromete en el cumplimiento de las normas y estándares establecidos para el buen uso de todos los recursos tecnológicos del ICANH:
   - El *password* es personal e intransferible. 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 la misma.Todo lo realizado con el usuario (cuenta de red y correo) y el *password*, es responsabilidad de la persona a quien se le asignó la cuenta
   - El *password* debe memorizarse y no escribirse, por tanto debe ser fácil de recordar. 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 *password* 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.
   - 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.
   - El cambio automático de contraseñas es cada noventa (90) días.
   - Los nombres de las cuentas de red se construirán con la primera letra del Nombre y luego el Apellido completo del usuario. Si se da el caso de nombres repetidos se colocará la primera letra del segundo nombre o el segundo apellido.
   - Los lineamientos para la construcción de Contraseñas de seguridad son: mínimo ocho (8) caracteres, debe contener letras (mayúsculas y minúsculas), números y caracteres especiales como $ % @*. No deben ser palabras comunes.
   - La asignación de contraseñas se realiza de forma individual, por lo que el uso de *passwords* compartidos está prohibido.
   - 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 cinco (5) el número de intentos consecutivos e infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda bloqueada.
   - 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.
   - Se debe proteger la cuenta de administrador:

a) Para el trabajo cotidiano, no se debe usar la cuenta de administrador, de manera que se minimice el impacto por errores accidentales
b) No se debe navegar en Internet con la cuenta de administrador
c) Los usuarios con derecho de administrador deben tener una cuenta normal y otra de administrador
d) Siempre que el sistema lo permita, la cuenta de administrador debe ser renombrada

2) **Administrar privilegios de usuarios**:

- Establecer permisos de acceso a nivel de usuario (privilegios y restricciones)
- Para acceso a la información y aplicativos de la red ICANH:
    - Asignar permisos para acceso a programas y archivos
    - Mantener al máximo el número de recursos de red sólo en modo lectura
    - Asignar permisos para acceso a aplicativos Web internos y externos

b. Establecer permisos de acceso a los usuarios administradores y editores del portal Web ICANH
c. Establecer permisos de acceso a la Intranet del instituto
d. Establecer restricciones para el acceso a servidores (únicamente usuarios administradores)
e. Crear Grupos de Usuarios (Unidades Organizaciones) y Políticas de Grupo

3) Implementar medidas de seguridad a nivel de red, servidores y PC del instituto

A nivel de red:

- Utilizar herramientas de monitoreo que permitan verificar los servicios de la red.
- Utilizar tecnologías repelentes o protectoras (seguridad perimetral)
- Utilizar una solución integral de protección contra virus para la red del ICANH que incluya como mínimo: antivirus para PC y servidores y una consola de actualización y distribución automática que mantenga todos los PC y servidores protegidos
- Restringir el acceso a internet:
    - El acceso a Internet deberá hacerse únicamente mediante dos formas: canal dedicado de la entidad
    - El canal dedicado de la entidad, debe estar protegido con reglas de seguridad específicasde seguridad perimetral
    - Se debe restringir el acceso a sitios no seguros y según recomendación técnica de los especialistas de seguridad
    - Cada jefe de área o supervisor de contrato debe justificar la necesidad del servicio (canal dedicado)para un nuevo usuario de la red ICANH
- Restringir el acceso a redes sociales, de acuerdo con las funciones de los usuarios
- Restringir el acceso vía VPN.

A nivel de servidores:

- Establecer direcciones IP fijas para los servidores
- Establecer las políticas y condiciones necesarias para las actualizaciones de seguridad de los servidores en forma segura
- No utilizar los servidores como estaciones de trabajo

- Coordinar y vigilar la realización de actualizaciones de seguridad de los servidores

A nivel de PC:

- Establecer las políticas y condiciones necesarias para las actualizaciones de seguridad de los PC en forma segura
- Restringir la instalación de software no licenciado en PC de los usuarios de la red: el software instalado en los equipos debe contar con su respectiva licencia
- Los usuarios de PC solo podrán utilizar el software de oficina oficial acogido por la entidad
- Los usuarios de PC no deberán tener acceso al *set up* de la máquina

4) Establecer medidas de seguridad para la información institucional generada por funcionarios y contratistas

En el caso de funcionarios de planta, la oficina de talento humano debe informar oportunamente a la oficina de sistemas del ICANH sobre su retiro y no permitir dicho retiro hasta que el funcionario entregue formalmente al ICANH, la información institucional generada dentro de su de trabajo.

En el caso de los contratistas, los supervisores de contratos deben informar oportunamente a la oficina de sistemas del ICANH sobre su retiro y no permitir dicho retiro hasta que el contratista entregue formalmente al ICANH, la información institucional generada dentro del desarrollo de su contrato.

5) Administrar en forma oportuna todos los contratos de soporte técnico del área de sistemas:

- Mantener vigentes los contratos de soporte tecnológico especializado para hardware, software, equipos electrónicos como UPS, aire acondicionado, etc.
- Mantener disponible la información sobre los contratistas a contactar en caso de detectar una posible intrusión en la seguridad de la red o falla en su infraestructura.

6) Establecer procedimientos claros degeneración de copias de seguridad y restauración de la información:

- Generar *back up* según lo especificado en el procedimiento “Generación de copias de seguridad” del SIGAP
- Administrar la custodia externa de los *back up*.
- Los usuarios serán responsables de colocar información institucional sensible que deba ser protegida, en el Drive de Google Apps (en la nube) que les corresponda o en el Drive donde se les haya dado privilegios de acceso

7) 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 a las bases de datos.
- 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.

8) Establecer medidas de Seguridad física en el 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:

a. Restringir el acceso al centro de cómputo, de personas ajenas al área de sistemas.
b. Mantener los servidores en condiciones ambientales adecuadas. (aíre acondicionado).
c. Instalar cámaras de vigilancia y detector de humo.
d. Instalar redes de corriente regulada para los servidores y PC, apoyada por UPS.
e. Realizar mantenimiento preventivo y correctivo a todos los equipos de cómputo y otros equipos como UPS, aire acondicionado, etc.

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

Condiciones ambientales:

a. Mantener el centro de cómputo en condiciones ambientales de temperatura adecuadas que prevengan daños en los equipos servidores y UPS que allí están ubicados.
b. El centro de cómputo debe contar con un equipo de aire acondicionado tipo Minisplit de 18000 BTU como mínimo.
c. El equipo de aire acondicionado debe funcionar 7días x 24 horas, a 22 grados centígrados de temperatura como máximo.
d. El extractor de aire del centro de cómputo debe estar funcionando permanentemente.
e. El área debe mantenerse limpia.
f. El aire acondicionado del centro de cómputo debe recibir mantenimiento preventivo y correctivo adecuado, que asegure su óptimo funcionamiento (mantenimiento preventivo mensual).
g. Las luces del centro de cómputo deben permanecer apagadas mientras no haya personal en dicha área.

Condiciones de seguridad eléctrica:

a. En el centro de cómputo del ICANH, las tomas de corriente regulada son de color naranja y las tomas beige son de corriente directa.

b. Se debe contar con mecanismos de seguridad tales como UPS, que permitan dar cierta autonomía a equipos y servidores, cuando se produzcan fallos en el flujo de corriente eléctrica. Para el caso de los servidores se debe tener la opción de apagado automático de los mismos cuando el tiempo de corte de energía sobrepase el tiempo de autonomía de las UPS
c. Las UPS del ICANH deben recibir mantenimiento preventivo y correctivo adecuado, que asegure su óptimo funcionamiento
d. Las baterías de las UPS deben cambiarse, de acuerdo con la garantía de las mismas y su uso (cada tres años como máximo).

Condiciones de acceso restringido:

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

9) Establecer medidas de Seguridad física para los computadores (PC) del ICANH

a. Los computadores del ICANH deben estar conectados a la corriente regulada, así:
   a) <u>En los puestos de trabajo con tomas color beige y tomas color blanco en la canaleta:</u> 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).
   b) <u>En los puestos de trabajo con tomas color naranja y tomas color beige en la canaleta: l</u>os 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).
b. Los computadores se deben apagar en la forma debida (incluido el monitor), para evitar deterioro del sistema operativo.
c. Cuando se presenten fallas de energía, las UPS 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.
d. No se deben mover o cortar cables, conexiones y PC, sin la supervisión de algún funcionario del área de sistemas del ICANH.
e. Se prohíbe fumar y consumir alimentos o bebidas frente a los computadores.
f. El ICANH utiliza software licenciado por tanto no está permitido instalar software no licenciado en los equipos.
g. Los equipos de tecnología deberán ser inventariados y ante el retiro del funcionario o contratista, se deben recibir los mismos, mediante chequeo contra el inventario físico.

10) Establecer políticas de seguridad para el uso de Google Apps

- Las cuentas de correo suministradas por el ICANH deberán ser de uso institucional.
- Se deben sincronizar las claves de los usuarios en el Directorio Activo, con las claves de los buzones de correo en Google Apps.

- Se deben usar Grupos de Distribución de Correo.
- Todas las políticas de seguridad en el correo (*antispam*, antispyware, tamaño de los buzones de correo, tamaño de adjuntos, restricción de archivos peligrosos, entre otros) será de acuerdo con las políticas de Google Apps.
- Se deben establecer permisos de acceso para cada uno de los componentes de Google Apps.
- Se deberá tener en cuenta las políticas establecidas a continuación:

A. Políticas para uso del correo Gmail ICANH:

a. Las contraseñas asignadas por el ICANH para el acceso a la red y al correo son personales e intransferibles, por tanto cada usuario es completamente responsable de todas las actividades realizadas con sus cuentas de acceso a la red y buzón de correo.
b. Las políticas de seguridad de las claves de acceso de Google Apps, serán las mismas del Directorio activo de la red ICANH.
c. Para comunicaciones institucionales, todos los funcionarios del ICANH sin excepción, deben utilizar el sistema de correo Gmail de Google Apps.
d. Para funcionarios nuevos de planta, el área de Talento Humano del ICANH debe solicitar mediante correo electrónico al área de sistemas, con al menos dos (2) días de anticipación, la creación de la cuenta de red y del buzón de correo del nuevo funcionario, indicando nombre completo, número de cédula, fecha de ingreso, área en la cual se va a desempeñar, permisos de red requeridos y permisos en el portal ICANH.
e. Cuando un funcionario de planta se vaya a retirar, el área de Talento Humano debe solicitar inactivar la cuenta y buzón de correo del funcionario en cuestión, mediante correo electrónico enviado al área de sistemas. Allí deberá informar el nombre del funcionario que se va a retirar y la fecha a partir de la cual se debe inactivar.
f. Cuando se trata de nuevos contratistas que ingresarán al ICANH, se deberá tener en cuenta lo siguiente:
    - Si el contratista va a trabajar en el ICANHun periodo de tiempo superior a cuatro (4) meses y requiere correo electrónico del ICANH, el supervisor del contrato, deberá solicitar la creación la cuenta de red y buzón de correo, mediante correo electrónico dirigido al área de sistemas, informando nombre del contratista, número de cédula, fecha de inicio y fecha de terminación del contrato, área en la cual va a desempeñar sus labores, permisos de red que requiere y permisos en el portal ICANH.
    - Las cuentas y buzones de correo de los contratistas serán inhabilitadas el día siguiente a la fecha de terminación del contrato.
    - Si el contratista va a trabajar un periodo de tiempo inferior a cuatro meses, el contratista deberá abrir un correo Gmail gratuito
g. Las cuentas de red y buzones de correo inactivos deberán ser *eliminados definitivamente* veinte (20) días después de haber sido inhabilitados, a menos que el área de Talento Humano o el supervisor de contrato, remita un correo electrónico al área de sistemas donde solicite y justifique la prórroga para la

eliminación definitiva, caso en el cual la cuenta y buzón se mantendrán por veinte (20) días calendario adicionales. La cuenta y buzón de correo volverán a inactivarse pasado el tiempo indicado y posteriormente serán borrados.

h. En cuanto a los buzones institucionales de las áreas:
   - Los responsables de los buzones institucionales de las áreas son los jefes de área.
   - Solo se crearán y manejarán los buzones institucionales que requieran las áreas, lo cual deberá ser informado al área de sistemas, mediante correo electrónico.
   - El jefe de área deberá informar por correo electrónico al área de sistemas, si el buzón será revisado por algún funcionario que haya sido delegado.
   - Cuando el funcionario responsable de revisar el buzón institucional se ausente del ICANH, deberá informarse al área de sistemas del ICANH, el nuevo responsable, para hacer los ajustes técnicos que sean necesarios.

i. Los funcionarios y contratistas del ICANH deberán dar buen uso a su buzón de correo, absteniéndose de enviar correos masivos no deseados o con información inadecuada (*se considera información inadecuada: terrorismo, programas piratas, pornografía infantil, amenazas, estafas, esquemas de enriquecimiento piramidal, virus o código malicioso).*

j. Se implementará el siguiente *disclaimertext* al final de todos los mensajes enviados desde el ICANH:

   AVISO LEGAL: Este mensaje y sus anexos, pueden contener información confidencial o legalmente protegida y no puede ser divulgada. Si por error recibe este mensaje, por favor avise inmediatamente a su remitente y destruya toda copia que tenga del mismo. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje, sin autorización del ICANH, será sancionado de acuerdo con las normas legales vigentes.

   De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad.

   Las opiniones contenidas en este mensaje electrónico, no relacionadas con la actividad del ICANH, no necesariamente representan la opinión del Instituto Colombiano de Antropología e Historia (ICANH).

k. Los mensajes de correo enviados, deberán incorporar las firmas automáticas, de acuerdo con el formato aprobado por el área de Comunicaciones del ICANH

B. Políticas para uso de Google Talk:

Los funcionarios y contratistas del ICANH que se les asigne una cuenta de correo Gmail de Google Apps, deberán dar buen uso a la aplicación de mensajería instantánea (llamadas de voz, video y texto), utilizándolo para fines institucionales.

C. Políticas para uso del Google Calendar

Los funcionarios y contratistas del ICANH deberán compartir su calendario, de forma adecuada con el fin facilitar la programación de reuniones

Los funcionarios y contratistas del ICANH, que se les asigne una cuenta de correo Gmail de Google Apps, deberán hacer uso del calendario, para la reservación de recursos requeridos para las reuniones planificadas.

D. Políticas para uso de Google Drive:

Todos los funcionarios y contratistas del ICANH que cuenten con una cuenta de correo de Google Apps, dispondrán de 30 GB para almacenar documentos en la nube.

Las áreas interesadas también pueden solicitar almacenamiento de información en el Drive del administrador de Google, el cual tiene más espacio disponible. Esta información podrá ser compartida, mediante permisos de acceso.

La información almacenada en la nube, deberá ser de carácter institucional.

Con el fin de contribuir al logro de las metas de cero papel del ICANH (requerimiento de Gobierno en línea) todos los funcionarios y contratistas deberán compartir los documentos que así lo requieran, de manera que se pueda hacer modificación conjunta de los mismos (colaboración de documentos).

E. Políticas para uso de Google Sites:

Para la publicación de información en la Intranet y sitios Web externos, se deberá tener en cuenta lo siguiente:

- Cualquier requerimiento relacionado con Google Sites deberá ser solicitado mediante correo electrónico a la Oficina de Planeación del ICANH.
- El área de sistemas del ICANH deberá definir la factibilidad técnica de la solicitud realizada y definirá los permisos requeridos.
- La publicación de información en la Intranet y sitios Web externos deberá ser aprobada por el área de Comunicaciones del ICANH.
- Las publicaciones realizadas deberán tener un diseño acorde al portal ICANH y a lo estipulado por el área de Comunicaciones del Instituto.
- La información publicada a través de la Intranet y sitios Web externos será responsabilidad de cada área del Instituto, con la supervisión del área de Comunicaciones del ICANH.
- Los funcionarios y contratistas del ICANH deberán solicitar soporte técnico en temas de Google Apps a los funcionarios del área de sistemas del Instituto o hacer uso de los tutorial que para tal efecto serán socializados en la Intranet institucional.

11) Establecer un plan de contingencia para la recuperación de desastres, que tenga en cuenta las siguientes actividades:

- Restaurar información de las copias de seguridad de la información institucional de Directorio activo, datos en servidores compartidos y los que los usuarios coloquen allíy reglas de seguridad de seguridad perimetral.
- Restaurar información de las copias de seguridad colocadas por los usuarios en el Drive de Google Apps.
- Mantener actualizados y vigentes los contratos de soporte técnico especializado 7 x 24, para la plataforma de servidores, para las soluciones de seguridad (antivirus y seguridad perimetral), para la plataforma de Google Apps y para el portal ICANH.

- Mantener el licenciamiento de *backupfly* para cuentas institucionales sensibles y el respaldo de Google para las demás.
- Mantener vigente la garantía de los servidores de la red.
- Mantener vigentes los contratos de mantenimiento preventivo y correctivo para: 1) Las UPS; 2) El equipo de aire acondicionado del centro de cómputo y 3) Los demás equipos de cómputo, incluida bolsa de repuestos.
- Mantener vigentes los contratos de soporte técnico para los aplicativos en uso.