INCI
Trabajamos por una forma diferente de ver el mundo

RESOLUCIÓN No. 20161010000683

16-03-2016

Por la cual se actualiza la política de seguridad de la información y el uso adecuado de las tecnologías de la información y las comunicaciones en el Instituto Nacional para Ciegos – INCI, con el propósito de orientar su adecuada utilización para el desarrollo de las funciones

EL DIRECTOR GENERAL DEL INSTITUTO NACIONAL PARA CIEGOS –INCI

En ejercicio de sus facultades legales y en especial las que le confiere el Decreto 1006 de 2004, Ley 527 de 1999 y el Decreto 1151 de 2008, y

CONSIDERANDO:

Que para el Instituto Nacional para Ciegos – INCI es de vital importancia el adecuado y seguro manejo de la información para garantizar un óptimo y oportuno servicio a los usuarios de la plataforma informática de la Entidad;

Que al interior de la Entidad es necesario adoptar políticas, directrices, mejores prácticas y lineamientos con el fin de garantizar la eficiencia en la utilización de los recursos informáticos; la confiabilidad, consistencia, integridad y oportunidad de la información y la efectividad de los controles en los sistemas de información;

Que el Decreto 2573 de 2014 del 12 de diciembre, establece los lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones;

Que la Ley 527 de 1999 define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales;

Que el uso de estos medios electrónicos se ha incrementado en los últimos años con diferentes aplicativos como son el Correo Electrónico, la Web, la Intranet Empresarial, los aplicativos de desarrollo y diseño, que toda institución debe convertir en herramientas de carácter estratégico como garantía de soporte y seguridad a la gestión institucional;

Que en las Leyes 23 de 1982 y 44 de 1993; y las Directivas Presidenciales 01 de 1999 y 02 de 2002, se señalan de manera expresa el respeto que entidades, organismos y servidores públicos deben observar en materia de protección a los derechos de autor y derechos conexos, particularmente con el uso y adquisición de programas de computador;

Que con la Ley 1273 de 2009 por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "De la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones;

Que la Ley 734 de 2002, artículo 34, numerales 21 y 22, señala el deber de los funcionarios públicos de vigilar y salvaguardar los bienes que le han sido encomendados y cuidar que sean utilizados debida y racionalmente, de conformidad con los fines a que han sido destinados y responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización;

Que es indispensable y necesario reglamentar para los usuarios de la institución, la utilización correcta de estos activos de información para proteger, asegurar, controlar y administrar la información con garantías de integridad, confidencialidad y disponibilidad, de conformidad con lo establecido en las normas de Control Interno, Ley 87 de 1993 Reglamentada por el Decreto Nacional 1826 de 1994 y de Archivo Ley 594 de 2000 Reglamentada parcialmente por el Decreto Nacional 4124 de 2004;

Que la entidad se dirige hacia Implementación del "***Sello de excelencia de gobierno en línea"***, de conformidad con el artículo 13 del decreto 2573 de 2014, y el aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización;

INCI
Trabajamos por una forma diferente de ver el mundo

RESOLUCIÓN No. 20161010000683

16-03-2016

Que en consideración a lo anterior, es obligatorio reglamentar la Política de seguridad y privacidad de la información y el uso de las herramientas de Software y Hardware en el Instituto Nacional para Ciegos- INCI.

Que por lo anterior expuesto,

R E S U E L V E:

TITULO I. GENERALIDADES

ARTÍCULO 1.- ACTUALIZACIÓN DE LA POLÍTICA: Actualizar la política de seguridad y privacidad de la información y el uso adecuado de las tecnologías de la información y las comunicaciones en el Instituto Nacional para Ciegos – INCI, la cual se regirá por las disposiciones, contenidas en la presente Resolución.

ARTÍCULO 2.- PRINCIPIOS DE LA POLITICA: Son principios de la presente política los siguientes:

1. **Principio de Transparencia:** la actividad administrativa es del dominio público, por consiguiente, toda persona puede conocer las actuaciones de la administración, salvo reserva legal, por lo tanto, la política de seguridad y privacidad de la información es información Pública de conformidad con el literal b) del artículo 6 de la ley 1712 de 2014.
2. **Principio de Precaución**: Todo servidor público o contratista del INCI, tiene el deber del cuidado de la información que maneja pues cualquier dato o información que genere, procese, transfiera, o modifique en el ejercicio de sus funciones es de carácter público y pertenece al INCI.
3. **Principio de Planeación**: La política de seguridad y privacidad de la información debe entenderse como de vital importancia para el adecuado y seguro manejo de la información y como parte integral de la gestión, por lo tanto, hace parte del ciclo PHVA (planear-hacer-verificar y actuar) de la gestión.
4. **Principio de Economía:** La política de seguridad y privacidad de la información debe buscar la optimización económica de los recursos, para lo cual debe fundarse en procesos y tecnologías eficientes que garanticen la calidad y el cumplimiento de las políticas y obtener los beneficios de la economía de escala.
5. **Principio de la prevención:** La identificación, el análisis y la valoración de riesgos debe ser una herramienta permanente en la gestión de las TIC del INCI para formular el PETIC y sus acciones correspondientes, buscando priorizar las acciones en función de la disponibilidad de recursos.

ARTÍCULO 3.- DEFINICIÓN DE POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN: La Política de seguridad y privacidad de la información es el conjunto de directrices, lineamientos, reglas y mejores prácticas que regulan la protección de la información contra la pérdida de confidencialidad, integridad o disponibilidad, tanto de forma accidental como intencionada. La seguridad de la información aplica las técnicas fundamentales para preservar los activos de información y también la protección del acceso a todos los recursos de la plataforma informática.

ARTÍCULO 4.- DEFINICIÓN DEL SISTEMA INFORMÁTICO DEL INCI: Entiéndase como sistema informático del INCI, al conjunto de elementos conformado por los planes, procesos, procedimientos, políticas, la plataforma de tecnologías de la información y las comunicaciones (hardware y software), servicios, sistemas de información, información, datos, usuarios y beneficiarios de la información.

ARTÍCULO 5.- SUJETOS DE LAS POLÍTICA: Se definen como sujetos de la política de seguridad y privacidad de la información, en el Instituto Nacional para Ciegos – INCI los siguientes:

1. Servidores Públicos del INCI.
2. Contratistas del INCI.
3. Servidores Públicos de Órganos de Control y/o Entidades Gubernamentales que en cumplimiento de su función hagan uso de los activos de información del INCI, o la plataforma tecnológica del INCI, en cumplimiento del principio de coordinación de que trata el artículo sexto de la ley 489 de 1998 a las cuales aplica la presente Política.
4. Invitados y demás visitantes que utilicen los activos de información de la entidad, o algún activo de información de la entidad o alguno de los elementos de la plataforma Informática en desarrollo de los proyectos del INCI, tales como actividades de capacitación, formación o asistencia técnica.

ARTICULO 6.- INCLUSION EN OBLIGACIONES DE CONTRATISTAS: Para todos los contratos de prestación de servicios y/o cualquier contrato que pueda afectar la infraestructura tecnológica tales como obras de mantenimiento, adecuación de espacios físicos, entre otros, la oficina asesora jurídica incluirá dentro de la minuta del contrato en las obligaciones para el contratista la obligación perentoria de cumplir con la presente Política de seguridad y privacidad de la información y la prevención de riesgos frente a la plataforma informática.

TITULO II. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CAPÍTULO PRIMERO

DEBERES Y PROHIBICIONES DE LOS SERVIDORES PÚBLICOS DEL INCI FRENTE A LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ARTÍCULO 7.- DEBERES DE LOS SERVIDORES PÚBLICOS DEL INCI: Los siguientes son los deberes que en materia de seguridad informática y privacidad de la información deben cumplir todos los servidores públicos:

1. Mantener la confidencialidad y privacidad de Información pública clasificada, información pública reservada y proteger dicha información para evitar su divulgación no autorizada.
2. Mantener la custodia de Información pública, Información pública clasificada, información pública reservada a su cargo.
3. Publicar en el portal Web del INCI la información pública a su cargo, de conformidad con el ordenamiento jurídico y la reglamentación interna y los procedimientos establecidos.
4. Proteger la Información Pública que administre, custodie o genere.
5. Realizar los procedimientos de protección de la información establecidos en el INCI.
6. Seguir las reglas de seguridad cuando utilice aplicativos institucionales tales como:
   a. No permitir que terceros visualicen su nombre de usuario y claves de acceso en las aplicaciones a las cuales tiene acceso.
   b. Cerrar las aplicaciones cuando se retire del escritorio.
   c. No compartir las claves de acceso a las aplicaciones.
   d. No compartir las claves de Administración de las aplicaciones y/o bases de datos.
   e. No permitir acceso a los equipos de escritorio a personal no autorizado.
7. Realizar los backup de la información que estén a su cargo de conformidad con los procedimientos del sistema integrado de gestión (SIG).
8. Ubicar todo archivo de trabajo en las carpetas definidas en los escritorios de los computadores entregados para su trabajo definido como "Información Institucional".
9. Informar inmediatamente a la Oficina Asesora de Planeación, todo indicio de ataque interno o externo que pueda llegar a dañar la información del INCI.

10. Hacer entrega oportuna de la información pública a su cargo en las siguientes situaciones administrativas siguiendo los procedimientos establecidos en el Sistema Integrado de Gestión (SIG):
    a. Por retiro definitivo de la institución.
    b. Por traslado interno.
    c. Por vacaciones.
    d. Por licencias o comisiones mayores a 30 días.
11. Custodiar el punto de red asignado de posibles conexiones no autorizadas de dispositivos que representen amenazas, tales como: computadores ajenos a la entidad o cualquier otro dispositivo con conexión a Ethernet.
12. Cambiar las claves de acceso a los distintos aplicativos a los que tiene acceso mínimo cada 3 meses.
13. Asegurarse que los correos electrónicos institucionales estén provistos de la firma establecida de conformidad con los criterios fijados en esta resolución.

ARTÍCULO 8.- PROHIBICIONES DE LOS SERVIDORES PÚBLICOS DEL INCI: Los siguientes son las prohibiciones que en materia de seguridad informática y privacidad de la información deben cumplir todos los servidores públicos:

1. Revelar, divulgar, exhibir, mostrar, comunicar, utilizar y/o emplear Información pública clasificada, Información pública reservada con cualquier persona natural o jurídica, en su favor o en el de terceros.
2. Utilizar la Información Confidencial en detrimento de la Entidad o para fines diferentes a los establecidos en la presente política.
3. Dañar o destruir, la información pública que este a su cargo en cualquier calidad y medio.
4. Adquirir bienes o servicios de TIC´s violando la restricción de que está función solo la puede realizar la oficina asesora de planeación.
5. Entregar licencias y su documentación a servidores públicos distintos a los designados por la oficina asesora de planeación.
6. Utilizar las licencias del software instalado en sus computadores para hacer instalaciones en equipos personales o ajenos a la institución.
7. Utilizar el software instalado en sus computadores para uso personal o ajeno a la institución.
8. Instalar software en los equipos bajo su responsabilidad.
9. Permitir que se instale software no autorizado en los equipos bajo su responsabilidad.
10. Modificar las configuraciones del software instalado en los equipos bajo su responsabilidad.
11. Desinstalar el Software de los equipos bajo su responsabilidad.
12. Instalar Software en los equipos bajo su responsabilidad.
13. Actualizar el software instalado en los equipos bajo su responsabilidad.
14. Utilizar las claves de acceso de otro servidor público para acceder al software del INCI.
15. Infectar los equipos de cómputo bajo su cargo con virus por el uso de dispositivos externos.
16. Usar dispositivos de memoria externos sin vacunarlos con el antivirus institucional.
17. Descargar software malicioso de internet.
18. Activar las actualizaciones, complementos, plugins, etc, para que se ejecuten de forma automática.
19. Descargar, instalar y/o ejecutar programas o herramientas que:
    a. Predigan las contraseñas, rastreen vulnerabilidades en los sistemas de cómputo y monitoreen la actividad de los sistemas informáticos de equipos de cómputo locales o remotos.
    b. Tengan un carácter de juegos, pornografía, descarga de música, videos o similares que promuevan el ocio o faciliten el ingreso de agentes externos como hackers, virus, etc.
14. Retardar de manera intencional la entrega de la información cuyo deber debe cumplir en las situaciones administrativas tales como: retiro definitivo, traslado, vacaciones, licencias, comisiones, o retiros por periodos superiores a 30 días.
15. Permitir que personas ajenas a la entidad conecten computadores o dispositivos a los puntos de red que le hayan sido asignados para su uso.
16. Conectar dispositivos tales como: tablets, celulares, computadores portátiles, etc, a la red WIFI en los canales distintos a los asignados para visitantes.
17. Retirar o modificar la firma del correo electrónico.

ARTÍCULO 9.- DEBERES DE LA SECRETARIA GENERAL: Los siguientes son los deberes de la secretaria general frente a la Política de seguridad y privacidad de la información:

1. Notificar dentro de los dos (2) días hábiles siguientes al nombramiento de cualquier funcionario que deba ser incluido en el servicio de correo electrónico y nombrar las aplicaciones a las cuales tendrá acceso.
2. Notificar a la oficina asesora de planeación con mínimo dos (2) días hábiles antes del retiro definitivo o temporal de cualquier funcionario en las siguientes situaciones.
    a. Por retiro definitivo
    b. Por traslado interno.
    c. Por vacaciones.
    d. Por licencias o comisiones mayores a 30 días.
3. Iniciar las acciones disciplinarias pertinentes cuando se incumpla el presente reglamento sobre la política de seguridad y privacidad de la información, de conformidad con la ley 734 de 2002.

ARTÍCULO 10.- DEBERES DE LA OFICINA JURIDICA: Los siguientes son los deberes de la oficina asesora jurídica frente a la Política de seguridad y privacidad de la información:

1. Incluir en todos los contratos de prestación de servicios de apoyo a la gestión la obligación de cumplir con la Política de seguridad y privacidad de la información del INCI.
2. Informar a la oficina asesora de planeación en la etapa de revisión de estudios previos para prestación de servicios de apoyo a la gestión cuando se incluya en las obligaciones del contratante lo siguiente:
    a. Que el gestor de la necesidad pretenda otorgar cuenta de correo electrónico.
    b. Que el gestor de la necesidad pretenda asignar computador en virtud de la seguridad y privacidad de la información pública que este contratista manejará.
3. No aprobar estudios previos para contratos de prestación de servicios que incluyan el numeral 2 sin el concepto previo escrito de disponibilidad por la parte de la oficina asesora de planeación.
4. Informar a la oficina de planeación que información digital tiene carácter de reservada o clasificada.

ARTÍCULO 11.- DEBERES DE LA OFICINA ASESORA DE PLANEACIÓN: Los siguientes son los deberes de la oficina asesora de planeación frente a la Política de seguridad y privacidad de la información:

1. Suspender inmediatamente los accesos y permisos a las aplicaciones cuando haya sido notificado por la secretaría general del retiro temporal o definitivo de un funcionario del INCI.
2. Crear en un plazo no mayor a dos (2) días hábiles después de posesionado un nuevo funcionario la cuenta de correo electrónico y el acceso a las aplicaciones que le hayan sido notificadas por el jefe de la dependencia o el secretario general.
3. Modificar en un plazo no mayor a dos (2) días hábiles después de notificada una situación administrativa de traslado, la cuenta de correo electrónico y el acceso a las aplicaciones que le hayan sido notificadas por el jefe de la dependencia o el secretario general.
4. Emitir concepto técnico a las solicitudes hechas por la oficina jurídica en la etapa de revisión de estudios previos para prestación de servicios de apoyo a la gestión sobre los siguientes asuntos:
    a. Evaluar si la pretensión de otorgar la cuenta de correo electrónico cumple con los requisitos establecidos en la presente Política de seguridad y privacidad de la información para contratistas.
    b. Evaluar si la pretensión de otorgar equipo de cómputo cumple con los requisitos establecidos en la presente Política de seguridad y privacidad de la información para contratistas.
    c. Si existe o no disponibilidad de cuenta de correo.
    d. Si existe o no disponibilidad de equipo de cómputo.
5. Suscribir acuerdos de confidencialidad para el intercambio de datos con otras entidades del estado.
6. Configurar las cuentas de correo electrónico institucional con la firma establecida en las condiciones fijadas en la presente resolución.

ARTÍCULO 12.- DEBERES DE LOS SUPERVISORES DE CONTRATOS: Los siguientes son los deberes de los supervisores de contrato frente a la Política de seguridad y privacidad de la información:

1. Hacer cumplir la Política de seguridad y privacidad de la información del INCI de conformidad con las obligaciones contractuales por parte de los contratistas.
2. Evaluar los riesgos de daño a la plataforma informática cuando en las actividades que realice el contratista en cumplimiento de su objeto contractual se vea afectada.
3. Coordinar con la oficina asesora de planeación las actividades que deba realizar el contratista en cumplimiento del objeto contractual y que afecten de alguna manera la plataforma informática para prevenir riesgos.
4. Informar a la oficina asesora de planeación con mínimo dos (2) días hábiles de anticipación el retiro de cuentas de correo, hardware o software en las siguientes situaciones contractuales:
    a. Terminación del contrato.
    b. Suspensión del contrato.
    c. Terminación anticipada del contrato por alguna causal estipulada en la ley.
    d. Por sanción o declaración de incumplimiento del contrato.
    e. Por cualquier otra situación de conformidad con la ley.

ARTÍCULO 13.- DEBERES DE LOS JEFES DE LAS DEPENDENCIAS: Los siguientes son los deberes de los jefes de las dependencias como responsables de la implementación del control interno de conformidad con la ley 87 de 1993 respecto de la Política de seguridad y privacidad de la información:

1. Hacer cumplir la Política de seguridad y privacidad de la información por parte de los funcionarios a su cargo.
2. Incluir en todos los estudios previos de los procesos precontractuales que realice en su dependencia y de conformidad con el objeto contractual el cumplimiento de la Política de seguridad y privacidad de la información y el debido cuidado, precaución y prevención en la realización de las actividades de objeto contractual que constituyan riesgo para la plataforma.
3. Solicitar a la Jefatura de la oficina asesora de planeación en la etapa de elaboración de estudios previos para prestación de servicios de apoyo a la gestión la disponibilidad de los siguientes recursos para determinar si se deben incluir o no en las obligaciones del contratante:
    a. Que el potencial contratista necesita cuenta de correo electrónico dentro los límites establecidos en la presente política.
    b. Que el potencial contratista requerirá un computador en virtud de la seguridad y privacidad de la información pública que este manejará.
4. Solicitar a que servidores públicos o contratistas se les debe asignar correo electrónico institucional.

CAPITULO SEGUNDO

MEDIDAS DE PROTECCIÓN CONTRA EL RIESGO DE ATAQUES TECNOLÓGICOS INTERNOS Y EXTERNOS A LA INFORMACIÓN Y A LA PROTECCIÓN DE DATOS DEL INCI

ARTÍCULO 14.- DEFINICIONES: Las siguientes definiciones serán tenidas en cuenta para el siguiente capítulo:

- **Access Point:** Es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica
- **Actualización automática:** Modificaciones que se programan sobre el sistema operativo o el software instalado en el equipo de forma automática.
- **Antivirus:** Programa que busca la detección y eliminación de archivos ejecutables o documentos que fuesen potencialmente peligrosos para el sistema operativo.
- **Clave(Password):** Es el proceso mediante el cual se controla el acceso individual a un sistema informático mediante la identificación del usuario utilizando credenciales provistas por un administrador.

- **Cookies:** Es una pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del usuario.
- **Ethernet:** Es un estándar que define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI
- **Ficha backup de la aplicación:** Es un formato dentro del procedimiento de backups para cada aplicación residente en los servidores del INCI en los cuales se especifica: nombre de la aplicación, periodicidad de copia de la base de datos, periodicidad de copia de la máquina virtual, lugar de alojamiento y responsable.
- **Firewall:** Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.
- **Hacker:** Persona con grandes conocimientos de informática que se dedica a acceder ilegalmente a sistemas informáticos ajenos y a manipularlos.
- **Internet:** Es la unión de todas las redes y computadoras distribuidas por todo el mundo que utilizan protocolos TCP/IP y que son compatibles entre sí.
- **Login:** Es el proceso mediante el cual se controla el acceso individual a un sistema informático mediante la identificación del usuario utilizando credenciales provistas por el usuario administrador.
- **Mensaje de datos:** La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax
- **Plugin:** Es aquella aplicación que, en un programa informático, añade una funcionalidad adicional o una nueva característica o complemento al software.
- **Procedimiento de backups:** Conjunto de pasos y tareas que deben realizar los responsables para realizar copias de seguridad de los datos o aplicaciones de conformidad con el sistema integrado de gestión.
- **Red LAN:** Son las siglas de Local Área Network, Red de área local. Una LAN es una red que conecta los ordenadores en un área relativamente pequeña.
- **Riesgo tecnológico:** son riesgos asociados a la actividad humana. Se trata de los riesgos percibidos como fenómenos controlables por el hombre o que son fruto de su actividad
- **Software:** es un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora
- **Usuario(User):** Es un conjunto de permisos y de recursos (o dispositivos) a los cuales se tiene acceso. Es decir, un usuario puede ser tanto una persona como una máquina, un programa.
- **WIFI:** es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica.

ARTÍCULO 15.- CONFORMACIÓN DE LA PLATAFORMA TECNOLOGICA INFORMATICA QUE SOPORTA EL MANEJO DE LA INFORMACION EN MEDIOS DIGITALES: Para efectos de la presente política, la plataforma tecnológica informática del INCI está compuesta por los siguientes componentes y elementos:

Componente de comunicaciones: Este componente se encarga de comunicar todos los dispositivos que general adquieren o envían datos, los elementos que conforman este componente son los siguientes:

- **Red LAN:** esta red está compuesta por puntos de datos a los cuales se conectan los dispositivos, cableado estructurado, switch de comunicaciones que distribuyen las comunicaciones y el servidor que administra las comunicaciones, y telefonía IP.
- **Red WIFI:** Esta red está compuesta por Access point que son los encargados de recibir y transmitir los datos por ondas de radio, cableado estructurado que comunica los Access point con los switch de distribución, y el servidor que administra las comunicaciones.

Componente de almacenamiento de información digital: este componente se encarga de almacenar los datos que se generan o se adquieren, los elementos que conforman este componente son los siguientes:

Sistema de Almacenamiento por red (SAN): este elemento se encarga de hacer almacenamientos masivos por procesos de backup de los datos del INCI.

- **Discos duros de los PC y portátiles:** estos elementos se encargan de almacenar la información generada por cada máquina y su respectivo usuario.
- **Discos duros de los servidores:** estos elementos se encargan de almacenar información generada por las aplicaciones y sus configuraciones.
- **Almacenamiento en nube pública:** este elemento se encarga de almacenar la información relacionada con aplicación web y biblioteca virtual.
- **Almacenamiento en servidor de correos:** este elemento se encarga de almacenar la información correspondiente a los correos institucionales, esto es todo lo correspondiente al dominio @inci.gov.co.
- **Almacenamiento en Servidor de streaming:** en este elemento se almacena toda la información referente a la producción de contenido audio que produce la emisora INCIRADIO.
- **Almacenamiento en dispositivos externos tales como USB, discos externos:** este elemento almacena información que es susceptible de manipulación del usuario y sólo este actor es responsable de su buen uso.
- **Componente de procesamiento de datos:** este componente se encarga de procesar los datos para generar información inteligible, para soportar los procesos de la entidad, los elementos que conforman este componente son los siguientes:
- **Servidores:** estos elementos se encargan de accesar, procesar y administrar la información de las bases de datos, así como administrar y controlar el tráfico de datos entre los diferentes dispositivos de la red interna y externa.
- **Computadores de escritorio y portátiles:** equipos informáticos proporcionados a todos los funcionarios para su uso, su manipulación está bajo la responsabilidad de cada funcionario.
- **Componente de administración:** este componente se encarga de administrar los demás componentes, los elementos que conforman este componente son los siguientes:
- **Administrador funcional:** Persona encargada de administrar algún sistema de información o software, desde lo funcional (funcionamiento del sistema para usuario final), sin incluir administración de servidores u otros, que son responsabilidad del administrador técnico
- **Administrador Técnico:** Persona encargada de administrar algún sistema de información o software, desde lo técnico, incluida la administración de servidores u otros.
- **Software de administración:** Programas que permiten realizar configuraciones o parametrizaciones a las aplicaciones que tenga el INCI, bajo los lineamientos de la política de seguridad y privacidad de la información.
- **Componente red de corriente eléctrica regulada:** Este componte se encarga de suministrar la corriente eléctrica a todos los dispositivos de la plataforma tecnológica y comprende desde la acometida de suministro hasta los tomacorrientes de alimentación para dispositivos, en este se distinguen los siguientes elementos:
    - **Acometida de suministro externa:** Este elemento incluye los cables de suministro, los ductos el medidor y el tablero de distribución principal y los dispositivos de protección de sobre carga.
    - **Acometida de suministro interna:** Este elemento incluye los cables de distribución desde la cometida de suministro hasta los nodos de distribución en los distintos pisos donde se ubican la UPS.
    - **Dispositivos de regulación, estabilización y protección:** Son los elementos encargados de controlar los picos de voltaje que ingresan por la red de suministro, manteniendo una tensión de salida estable y en caso de sobrecarga disparar los dispositivos de protección tales como los interruptores termomagneticos dentro de estos se encuentran los tableros de distribución, las UPS, las unidades reguladoras o estabilizadores.
    - **Red de distribución:** comprende los elementos que permiten la distribución de la corriente regulada a los equipos de la plataforma informática, incluye canaletas, cableado, tomacorrientes.
- **Componente dispositivo de salida y entrada en red:** Este componente se integra por los siguientes elementos:
    - **Impresoras de red:** La impresora de red es un objeto auxiliar, que está conectado a una unidad central de procesamiento de una computadora, por medio de un cable, lo que le permite a cualquier usuario de la red imprimir documentos.
    - **Escáner de red:** Es un periférico que se utiliza para convertir, mediante el uso de la luz, imágenes impresas o documentos a formato digital.

- **Cámara IP:** Una cámara IP es una cámara que emite las imágenes directamente a la red (intranet o internet) sin necesidad de un ordenador.
- **Lectores Biométricos:** Es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos de un individuo para verificar su identidad.

ARTÍCULO 16.- MEDIDAS PARA LA PROTECCION DE ATAQUES TECNOLOGICOS EXTERNOS: Para la protección de los datos que están soportados en la plataforma informática del INCI se implementan las siguientes medidas:

1. Implementación y mantenimiento de Seguridad perimetral para evitar ataques externos.
2. Implementación y mantenimiento de la seguridad interna de la red LAN y WIFI para evitar ataques internos.
3. Implementación y mantenimiento de las copias de seguridad.
4. Implementar un programa de inducción y reinducción sobre riesgos informáticos por ataques externos a todos los funcionarios del INCI que incluya las buenas prácticas así como las recomendaciones sobre malas prácticas.

ARTÍCULO 17.- IMPLEMENTACIÓN Y MANTENIMIENTO DE SEGURIDAD PERIMETRAL PARA ATAQUES EXTERNOS: La implementación y mantenimiento de la seguridad perimetral para ataques externos es responsabilidad de la oficina asesora de planeación, para esto se realizarán las siguientes actividades:

1. Implementación y mantenimiento de muros de protección (Firewall) para retener y filtrar amenazas externas realizadas por hackers o personas mal intencionadas indeseables, con el propósito de destruir datos, propagar virus, sustraer datos, dañar o destruir aplicaciones o componentes de software. Estas paredes de fuego deben proteger tanto la red LAN como la red WIFI.
2. Implementación y mantenimiento de antivirus informático para proteger la red LAN, la red WIFI y los computadores y dispositivos de procesamiento.
3. Parametrización en servidor de correo para prevenir correo spam o malicioso.

ARTÍCULO 18.- IMPLEMENTACIÓN Y MANTENIMIENTO DE SEGURIDAD INTERNA DE LA RED LAN Y WIFI PARA ATAQUES INTERNOS: La implementación de la seguridad de la red interna de la red LAN y WIFI está a cargo de la oficina Asesora de Planeación, pero la aplicación de las políticas de seguridad de datos será de obligatorio cumplimiento para todos los servidores públicos y demás actores a los que le aplica lo Política de seguridad y privacidad de la información, para este propósito se desarrollarán las siguientes actividades:

1. **Implementación y mantenimiento del Directorio Activo:** Es una herramienta para la administración de los permisos y restricciones que se le asignan a cada usuario y cada máquina que hace parte de la plataforma informática del INCI, para garantizar el buen uso de la información y los elementos de la plataforma y optimizar el tráfico de datos por los diferentes canales.
2. **Implementación y mantenimiento de antivirus informático:** es un software para proteger la red LAN, la red WIFI y los computadores y dispositivos de procesamiento de los ataques internos provocados por el uso de dispositivos tales como USB, CD, DVD, discos duros externos, entre otros, o conexiones ilegales por la red LAN, o la red WIFI.
3. **Mantener deshabilitado los puntos de red:** los puntos de red que no estén asignados a servidores públicos.
4. **Implementación de perfilamiento de firewall (muros de protección):** es una herramienta para protección de ataques internos provocado por funcionarios o contratistas que hacen uso de la navegación hacia la internet a sitios con contenido malicioso.

ARTÍCULO 19.- IMPLEMENTACIÓN Y MANTENIMIENTO DE LAS COPIAS DE SEGURIDAD DIGITAL A DIGITAL: La implementación de las copias de seguridad de digital a digital se realizará de conformidad con las siguientes categorías:

1. **Bases de datos de aplicaciones residentes en los servidores del INCI:** estas se realizarán por parte de la oficina asesora de Planeación de conformidad con el procedimiento de backups y la ficha backup de la aplicación.
2. **Servidores virtualizados:** Esta se realizará por parte de la oficina asesora de Planeación con sus aplicaciones.

3. **Portal web:** Lo realizará la oficina asesora de planeación, de conformidad con los procedimientos de backup y la ficha de backup de la aplicación, exceptuando las publicaciones realizadas por la asesora de comunicaciones cuyo backup será responsabilidad de la asesora de comunicaciones en su computador.
4. **Correo electrónico:** Las copias de seguridad de los correos electrónicos se realizarán de conformidad con las siguientes reglas:
    a. **Cuentas de correo electrónico institucional nivel uno:** La copia de seguridad de estos correos lo realizará la oficina de planeación, de conformidad con el procedimiento de backup y ficha backup de aplicaciones.
    b. **Cuentas de correo institucional nivel dos:** La copia de seguridad de estos correos lo realizará la oficina de planeación de conformidad con el procedimiento de backup y ficha backup de aplicaciones.
    c. **Cuentas de correo institucional nivel tres:** La copia de seguridad de estos correos lo realizará el coordinador, responsable del procedimiento o proyecto especial de conformidad con el procedimiento de backup y ficha backup de aplicaciones.
    d. **Cuentas de correo institucional nivel cuatro:** La copia de seguridad de estos correos será responsabilidad del servidor público o contratista de conformidad con el procedimiento de backup y ficha backup de aplicaciones.
    e. **Copia de seguridad para operadores judiciales o disciplinarios:** la oficina de planeación realizará una copia de seguridad de todos los correos electrónicos en un periodo de tiempo razonable únicamente con el propósito de atender requerimientos de los operadores judiciales o disciplinarios, esta copia en ningún momento sustituye las copias de seguridad que es responsabilidad de los actores de conformidad con los literales anteriores.
5. **Información de los computadores de escritorio y portátiles:** Todos los archivos de trabajo que genere un servidor público o contratista que tenga asignado un computador tiene la obligación de guardarlos dentro de la única carpeta denominada "Información Institucional" ubicada en el escritorio de cada computador, las copias de seguridad de estos computadores es responsabilidad de cada servidor público o contratista las cuales deberán realizarlos de conformidad con el procedimiento de backup y la ficha de backup de la aplicación, y su disposición final se hará de la siguiente manera:
    a. **Disposición final de la copia de seguridad:** cada jefe de dependencia designará a cada servidor público un custodio de la copia de seguridad que será otro servidor público, el cual alojará en su equipo la copia de seguridad del funcionario que le fue asignado.
    b. De manera recíproca el servidor público o contratista custodio guardará su información en el equipo de la contraparte.
6. **Copias especiales:** La oficina de planeación se reserva la facultad de hacer las copias de la información pública almacenada en cualquier equipo por instrucciones de la dirección cuando las necesidades así lo requieran.

ARTÍCULO 20.- IMPLEMENTACIÓN Y MANTENIMIENTO DE LAS COPIAS DE SEGURIDAD FISICA A DIGITAL: La implementación de las copias de seguridad de físico a digital se realizará de conformidad con las siguientes reglas:

1. Será responsabilidad de la secretaria general dentro del marco del programa de gestión documental, definido en la ley 1712 de 2014 establecer y priorizar los documentos físicos que deberán ser llevados a soporte digital del 31 de diciembre de 2015 hacia atrás.
2. La secretaria general será la responsable de implementar y mantener en el sub-programa de reprografía del programa de gestión documental para garantizar la seguridad de los documentos de origen físico del 31 de diciembre de 2015 hacia atrás.
3. Será obligación de la secretaria del área de talento humano llevar a soporte digital todo documento que ingrese a partir del 1 de enero de 2016 a las historias laborales.
4. Será obligación de la secretaria de la oficina jurídica llevar a soporte digital todo documento que ingrese a partir del 1 de enero de 2016 de los expedientes contractuales y de defensa judicial.
5. Será responsabilidad de todas las secretarias de las distintas dependencias llevar a soporte digital los documentos que hagan parte de los expedientes que se constituyan en el sistema de información ORFEO,

exceptuando la sub dirección técnica que será responsabilidad de cada profesional dependiendo lo s expedientes definidos por los coordinadores de grupo y la subdirectora.

6. Será responsabilidad del(la) servidor(a) publico(a) encargado de la radicación de documentos que lleguen a la entidad, llevar a soporte digital en el sistema de información ORFEO.

CAPÍTULO TERCERO

PROTECCIÓN CONTRA RIESGOS DE ATAQUES O AMENAZAS FÍSICAS A LA INFORMACIÓN Y A LA PROTECCIÓN DE DATOS DEL INCI

ARTÍCULO 21.- DEFINICIONES: Las siguientes definiciones serán tenidas en cuenta para el siguiente capítulo:

- **Ataque biológico:** Es aquel acto mediante el cual se ven infectados los equipos y la información por un virus, bacterias u hongos a los medios de soporte ocasionando la alteración total de documentos, programas e información, o comprometer su integridad.
- **Ataque por orden público:** Atentado o acto vandálico ocasionado a las instalaciones donde se pueden ver afectados los equipos de la plataforma informática y la información.
- **Control biométrico:** Control de acceso de los funcionarios de una empresa por un sistema que detecta la huella o en casos donde no es una huella legible se controla mediante clave.
- **Desastres naturales:** Hace referencia a grandes pérdidas materiales y/o de vidas humanas, ocasionadas por eventos o fenómenos naturales como los terremotos, inundaciones, entre otros, comprometiendo el buen funcionamiento de los procesos de la entidad.
- **DVR:** Un grabador de vídeo digital es un dispositivo interactivo de grabación de televisión y video en formato digital.
- **Molinete:** Control de acceso de los funcionarios de una empresa por un sistema que detecta la huella o mediante clave.
- **Reproducción indebida:** Es el acto mediante el cual se comparte o se sustrae información de propiedad del INCI.
- **Riesgo físico:** Hace referencia a daños ocasionados a una máquina en específico y pueden darse por mala manipulación del equipo o factores externos que no llegan a ser desastres naturales tales como:
  - Descarga eléctrica.
  - Humedad.
  - Deterioro de las instalaciones.
  - Entre otros.
- **Robo de documentos o información:** Es el acto mediante el cual es tomada la información o los documentos de la entidad sin autorización.

ARTÍCULO 22.- MEDIDAS DE PROTECCIÓN CONTRA AMENAZAS FISICAS A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN: Como medidas de protección contra amenazas físicas a la seguridad y privacidad de la información se tomarán las siguientes:

1. Implementación y mantenimiento del control de acceso de servidores públicos y contratistas a los edificios del INCI.
2. Implementación y mantenimiento del control de acceso de usuarios y particulares a los edificios del INCI.
3. Implementación y mantenimiento de un sub-programa de control de plagas y roedores para los sitios de almacenamiento de los documentos físicos que contienen información pública, dentro del programa de gestión documental.
4. Implementación y mantenimiento de un sub-programa de prevención contra amenazas por fenómenos tales como: humedades, inundaciones, incendios, para los sitios de almacenamiento de los documentos físicos que contienen información pública, dentro del programa de gestión documental.

ARTÍCULO 23.- CONTROL DE ACCESO DE PERSONAS A LA INSTITUCIÓN: para proteger la seguridad y privacidad de la información por personas ajenas a la institución se controlará el ingreso a los edificios del INCI teniendo en cuenta las siguientes disposiciones:

1. Se implementará y mantendrá un control biométrico de acceso a los servidores públicos, contratistas y visitantes.
2. Se implementará un molinete al ingreso de la entidad para control físico del acceso de servidores públicos, contratistas y visitantes.
3. Cada jefe de dependencia definirá las áreas en las cuales se encuentran almacenados los documentos físicos o digitales que deban tener acceso restringido a servidores públicos o contratistas no autorizados.
4. La secretaria general mediante circular informará las áreas de los edificios del INCI en las cuales se implementará el acceso restringido e indicará que funcionarios tienen autorización.
5. Implementación de un sistema de monitoreo por cámaras.
6. Los contratistas del servicio de vigilancia de los edificios del INCI, tienen las siguientes obligaciones:
    a. Revisar todo vehículo que ingrese y salga de la entidad.
    b. Queda expresamente prohibido permitir el parqueo en las instalaciones internas del INCI de vehículos y motos de contratistas que vengan a desarrollar alguna actividad de mantenimiento o suministro sin previa autorización del director.
    c. En los casos del literal anterior a los contratistas que sean autorizados por el director solo lo podrán hacer por el tiempo necesario para el descargue de materiales o bienes, o la recolección de escombros, residuos o material de reciclaje. En cuyo caso el secretario general asignara una persona que vigile el cargue o descargue de estos elementos.
    d. Para los casos del literal b la secretaria general debe llevar un registro indicando nombre del contratista, fecha y hora de la autorización tiempo límite de duración, objeto del cargue o descargue placa del vehículo y funcionario asignado para la vigilancia.
7. El contratista encargado de la vigilancia tiene la obligación de revisar y registrar en la bitácora los equipos electrónicos de los servidores públicos y contratistas que ingresen y salgan de la entidad y no sean de propiedad del INCI.
8. Los servidores públicos y/o contratistas no podrán sacar de la entidad ningún dispositivo electrónico o equipo de cómputo de propiedad del INCI, sin antes presentar al contratista encargado de la vigilancia la orden de salida expedida por el jefe de la dependencia.
9. En el evento en que un equipo o dispositivo electrónico deba ser retirado por garantía o mantenimiento este debe ser notificado por el supervisor del contrato y registrado por el contratista encargado de la vigilancia.

ARTÍCULO 24.- CONTROL DE ACCESO A LOS USUARIOS PARTICULARES EN LOS EDIFICIOS DEL INCI: Para proteger la seguridad y privacidad de la información por amenazas de personas ajenas a la institución se controlará el ingreso a los edificios del INCI teniendo en cuenta las siguientes disposiciones:

1. Se implementará y mantendrá un control biométrico de acceso a los usuarios particulares el cual les generará un sticker de identificación de visitante dentro de las instalaciones del INCI el cual debe ser portado por el visitante en lugar visible.
2. Se implementará un molinete al ingreso de la entidad para control físico del acceso.
3. El servidor público que atienda la recepción deberá notificar al servidor público del INCI al cual requiere el particular para confirmar su autorización para el ingreso.
4. El servidor público que atienda la recepción solo autorizará el ingreso de particulares en los siguientes casos:
    a. Por autorización de un jefe de dependencia
    b. Por autorización de un coordinador, pero solo a las áreas destinadas para su atención de conformidad con los lineamientos dados por la secretaria general.
    c. Por autorización del supervisor de un contrato y solo a las áreas objeto de desarrollo del contrato.
    d. Por los asesores de la dirección dentro de las áreas destinadas para su atención de conformidad con los lineamientos dados por la secretaria general.
5. Implementación de un sistema de monitoreo por cámaras.
6. Los contratistas del servicio de vigilancia de los edificios del INCI, tienen las siguientes obligaciones:

a. Revisar todo vehículo que ingrese y salga de la entidad.
b. Queda expresamente prohibido permitir el parqueo en las instalaciones internas del INCI de vehículos particulares no autorizados por el director general.

7. El contratista encargado de la vigilancia tiene la obligación de revisar y registrar en la bitácora los equipos electrónicos de los usuarios particulares que ingresen y salgan de la entidad y no sean de propiedad del INCI.
8. Los servidores públicos y/o contratistas no podrán sacar de la entidad ningún dispositivo electrónico o equipo de cómputo de propiedad del INCI, sin antes presentar al contratista encargado de la vigilancia la orden de salida expedida por el jefe de la dependencia.
9. En el evento en que un equipo o dispositivo electrónico deba ser retirado por garantía o mantenimiento este debe ser notificado por el supervisor del contrato y registrado por el contratista encargado de la vigilancia.

ARTÍCULO 25.- CONTROL DE PLAGAS Y ROEDORES EN LAS INSTALACIONES DEL INCI: La secretaria general del INCI, deberá programar y promover jornadas de fumigación para el control de plagas y roedores dentro de las instalaciones del INCI, en especial las áreas que donde se almacenan documentos susceptibles, para garantizar la seguridad y el buen estado de los documentos o en zonas donde se extiendan redes cableadas para datos o corriente eléctrica.

ARTÍCULO 26.- SUB-PROGRAMA DE PREVENCIÓN CONTRA AMENAZAS DE FENÓMENOS TALES COMO: HUMEDAD, INUNDACIONES, INCENDIOS: La secretaria general del INCI deberá implementar un sistema de alarmas y sensores que permitan detectar los diferentes fenómenos y generar una alarma que permita un control oportuno ante algún riesgo que comprometa la seguridad de los documentos físicos que contienen información pública, dentro del programa de gestión documental.

ARTÍCULO 27.- INSTALACIÓN O DESINSTALACIÓN DE SOFTWARE: La única dependencia autorizada para instalar o desinstalar software de los equipos de escritorio, portátiles o móviles del INCI, son los servidores públicos de la oficina asesora de planeación asignados para esta función, autorizados por el jefe de la oficina asesora de planeación, por lo tanto queda expresamente prohibido a los servidores públicos o contratistas ajenos a la oficina de planeación del INCI, instalar o desinstalar cualquier tipo de software, so pena de las acciones disciplinarias, fiscales y penales a que haya lugar.

CAPITULO CUARTO

MEDIDAS DE PROTECCIÓN CONTRA EL RIESGO DE ATAQUES INTERNOS A LA INFORMACIÓN Y A LA PROTECCIÓN DE DATOS DEL INCI.

ARTÍCULO 28.- PROPIEDAD DE LA INFORMACIÓN EN MEDIOS ELECTRÓNICOS: Todos aquellos archivos electrónicos de información que se encuentren almacenados en cualquiera de los medios electrónicos como equipos de cómputo, discos duros externos o cualquier otro medio físico o Electrónico del INCI son información Pública del INCI, por esta razón ningún funcionario está autorizado a darle un manejo inapropiado, uso no autorizado o fraudulento (sustracción, venta, deterioro, donación, perdida o alteración) que afecte de alguna manera la integridad institucional y la continuidad de los servicios.

ARTÍCULO 29.- CLAVES DE ACCESO A EQUIPOS DE ESCRITORIO Y PORTÁTILES: Las contraseñas de los equipos de escritorio, se asignarán por primera vez por el administrador que disponga la Oficina Asesora de Planeación, esta clave debe ser cambiada en el primer ingreso y cada tres meses y será compuesta por mínimo ocho caracteres, con la combinación de números, letras, mayúsculas y minúsculas, de acuerdo a los lineamientos de seguridad parametrizadas en el servidor de dominio.

ARTÍCULO 30.- PROTECCIÓN CONTRA RIESGOS DE ATAQUES TECNOLÓGICOS A LA INFORMACIÓN Y A LA PROTECCIÓN DE DATOS DEL INCI: En este ítem se definen los mecanismos de seguridad y protección implementados para asegurar la privacidad de la información pública del INCI.

ARTÍCULO 31.- USO OBLIGATORIO DEL SOFTWARE ANTIVIRUS: Todos los servidores públicos y contratistas del INCI, tienen la obligación de vacunar con el antivirus institucional todos los dispositivos externos que conecten a los equipos de cómputo del INCI, la propagación de los virus a los computadores por estos dispositivos y sus efectos en la red será responsabilidad del servidor público encargado del equipo de cómputo, que permitió el uso sin las debidas precauciones.

ARTÍCULO 32.- ACTUALIZACIONES DEL SISTEMA OPERATIVO: La oficina asesora de planeación realizará actualizaciones automáticas de los parches de seguridad para los sistemas operativos instalados en los equipos de cómputo del INCI.

CAPITULO QUINTO

MEDIDAS DE PROTECCIÓN CONTRA EL RIESGO ELÉCTRICO AL HARDWARE, SOFTWARE Y DATOS DEL INCI.

ARTÍCULO 33.- DEFINICIONES: Definiciones para facilitar la comprensión técnica relacionada con el presente capítulo

- **Corriente Alterna:** Corriente eléctrica variable en la que las cargas eléctricas cambian el sentido del movimiento de manera periódica.
- **Corriente Eléctrica:** La corriente eléctrica es la tasa de flujo de carga que pasa por un determinado punto de un circuito eléctrico, medido en Culombios/segundo, denominado Amperio.
- **Estabilizador de Corriente:** Es un aparato que asegura que la cantidad de amperios que recibe un equipo sea constante.
- **Estabilizador de Tensión:** Es un aparato que recibe en la entrada una tensión que puede variar entre un valor mínimo y un valor máximo (denominado rango de tensión de entrada), dando a la salida una tensión estabilizada que puede tener un valor dentro de un rango de la tensión de salida (denominado precisión de la tensión de salida, o error de la misma, valuado en un porcentaje).
- **Frecuencia Eléctrica:** Constituye un fenómeno físico que se repite cíclicamente un número determinado de veces durante un segundo de tiempo y puede abarcar desde uno hasta millones de ciclos por segundo o hertz (Hz).
- **Interruptor Termo magnético:** Elemento de maniobra y protección cuya capacidad de ruptura a la tensión de servicio deberá ser igual o mayor a la corriente de cortocircuito en el punto de su utilización.
- **Pico de Voltaje:** Es el incremento en el potencial eléctrico, más allá del nivel para el que un aparato está diseñado.
- **Potencia Eléctrica Reactiva:** La potencia reactiva es la consumen los motores, transformadores y todos los dispositivos o aparatos eléctricos que poseen algún tipo de bobina o enrollado para crear un campo electromagnético.
- **Potencia Eléctrica:** Es la relación de paso de energía de un flujo por unidad de tiempo; es decir, la cantidad de energía entregada o absorbida por un elemento en un tiempo determinado.
- **Suministro supletorio de energía:** Es el suministro de energía eléctrica que se realiza mediante las baterías y un conversor CC a CA a los equipos de la plataforma informática cuando se presenta un corte del suministro de energía eléctrica externa por un tiempo limitado para poder hacer las operaciones de protección o salvado de datos.
- **Tensión eléctrica:** Es una magnitud física que cuantifica la diferencia de potencial eléctrico entre dos puntos.
- **Unidad de Potencia de Suministro UPS:** Es un dispositivo que, gracias a sus baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado y durante un apagón eléctrico a todos los dispositivos que tenga conectados.

ARTÍCULO 34.- COMPOSICION DE LA RED ELECTRICA DEL INCI: la red eléctrica del INCI está compuesta por la red eléctrica no regulada y la red eléctrica regulada.

ARTÍCULO 35.- RED ELECTRICA NO REGULADA: Es la red eléctrica que transporta el fluido eléctrico desde la acometida del comercializador de energía hasta las diferentes áreas de los edificios del INCI.

ARTÍCULO 36.- RED ELECTRICA REGULADA: Es la red eléctrica que transporta el fluido eléctrico desde la acometida del comercializador de energía hasta los diferentes dispositivos de la plataforma tecnológica del INCI pasando por un sistema de regulación y suministro supletorio de energía.

ARTÍCULO 37.- DISEÑO DE LA RED ELECTRICA NO REGULADA: El diseño de la red eléctrica no regulada corresponde a los diseños eléctricos al momento de la construcción de los edificios, su modificación, actualización o mejoramiento le corresponden a la secretaria general de conformidad con las normas que regulan la materia.

ARTÍCULO 38.- DISEÑO DE LA RED ELECTRICA REGULADA: El diseño de la red eléctrica regulada, su implementación y actualización o mejoramiento le corresponden a la oficina asesora de planeación de conformidad con las normas que regulan la materia.

ARTÍCULO 39.- DISPOSICION DEL MANTENIMIETO DE LA RED ELECTRICA NO REGULADA: El mantenimiento de la red eléctrica no regulada corresponde a la secretaria general para lo cual deberá:

1. Realizar un diagnóstico del estado de la red eléctrica no regulada
2. Identificar los riesgos que puedan afectar la seguridad de los funcionarios, así como la seguridad de los equipos conectados a esta red.
3. Formular un plan de acción para tomar medidas preventivas y correctivas recomendadas en el diagnóstico para prevenir los riesgos o corregir los hallazgos.
4. Gestionar los recursos necesarios para financiar el mantenimiento, actualización o mejoramiento de la red eléctrica no regulada.
5. Gestionar los contratos necesarios para realizar las acciones preventivas y correctivas.
6. Supervisar la ejecución y los contratos que desarrollan las acciones preventivas y correctivas.
7. En los procesos de intervención de la red eléctrica no regulada no deben tocar los elementos o dispositivos de la red eléctrica regulada; cuando por alguna circunstancia se requiera deberá coordinarse con la oficina asesora de planeación.
8. Deberá consolidar y custodiar la documentación de la red no regulada tales como manuales, planos eléctricos, guías técnicas, manual de especificaciones, informes diagnósticos, etc. y deberá conformarse una tabla de retención documental con sus respectivas series documentales para este propósito.

ARTÍCULO 40.- DISPOSICIÓN DE MANTENIMIETO SOBRE RED ELECTRICA REGULADA: El mantenimiento de la red eléctrica no regulada corresponde a la oficina asesora de planeación para lo cual deberá:

1. Realizar un diagnóstico del estado de la red eléctrica no regulada
2. Identificar los riesgos que puedan afectar la seguridad de los funcionarios, así como la seguridad de los equipos conectados a esta red.
3. Formular un plan de acción para tomar medidas preventivas y correctivas recomendadas en el diagnóstico para prevenir los riesgos o corregir los hallazgos.
4. Gestionar los recursos necesarios para financiar el mantenimiento, actualización o mejoramiento de la red eléctrica no regulada.
5. Gestionar los contratos necesarios para realizar las acciones preventivas y correctivas.
6. Supervisar la ejecución y los contratos que desarrollan las acciones preventivas y correctivas.
7. En los procesos de intervención de la red eléctrica regulada no deben tocar los elementos o dispositivos de la red eléctrica no regulada; cuando por alguna circunstancia se requiera deberá coordinarse con la secretaria general.
8. Deberá consolidar y custodiar la documentación de la red regulada tales como manuales, planos eléctricos, guías técnicas, manual de especificaciones, informes de diagnóstico, etc. y deberá conformarse una tabla de retención documental con sus respectivas series documentales para este propósito.

INCI
Trabajamos por una forma diferente de ver el mundo

RESOLUCIÓN No. 20161010000683

16-03-2016

TITULO III. DISPOSICIONES SOBRE SOFTWARE UTILIZADO POR EL INCI.

CAPITULO PRIMERO

DISPOSICIONES SOBRE ADQUISICIÓN O DESARROLLO DE SOFTWARE

ARTÍCULO 41.- DEFINICIONES: Definiciones para facilitar la comprensión técnica relacionada con el presente título:

- **Activo de Información:** Son todos aquellos datos e información que estén en cualquier medio físico o electrónico o en forma de documento de conformidad con el ordenamiento legal y que representan para el INCI, la posibilidad de Generar Valor o Destruir valor en caso de su perdida.
- **Comité técnico:** Es un conjunto de personas conformado por los directivos del INCI que aprueban o no las decisiones que incidan en la actual política de seguridad informática y privacidad de la información.
- **Estructura de datos**: Una estructura de datos es una forma de organizar un conjunto de datos elementales con el objetivo de facilitar su manipulación.
- **Información:** Es el conjunto de datos que genera conocimiento y por lo tanto es un activo, que como otros activos importantes tiene valor y requiere en consecuencia una protección adecuada. La información puede estar registrada en papel, medios electrónicos o cualquier otro documento de conformidad con el ordenamiento jurídico colombiano.
- **Métodos:** Es una subrutina que consiste generalmente de una serie de sentencias para llevar a cabo una acción, un juego de parámetros de entrada que regularán dicha acción o, posiblemente, un valor de salida (o valor de retorno) de algún tipo.
- **Modelo Entidad Relación:** Es una herramienta para el modelado de datos que permite representar las entidades relevantes de un sistema de información, así como sus interrelaciones y propiedades.
- **Objetos:** Un objeto es una unidad dentro de un programa de computadora que consta de un estado y de un comportamiento, que a su vez constan respectivamente de datos almacenados y de tareas realizables durante el tiempo de ejecución.
- **Propiedades:** es un mecanismo que permite acceder fácilmente a los datos a la vez que proporciona la seguridad y la flexibilidad de los métodos.
- **Software:** La Real Academia Española, define el software como un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora.

ARTÍCULO 42.- RESPONSABILIDAD DE LA ADQUISICIÓN DE SOFTWARE: De conformidad con el Decreto 1006 de 2004, la única Dependencia autorizada para adquirir o desarrollar a cualquier título, software y servicios de conectividad para la plataforma de tecnologías de la información y las comunicaciones del INCI, es la Oficina Asesora de Planeación.

PARÁGRAFO 1: Se exceptúan de esta restricción el hardware y software embebidos en las máquinas que se adquieran para la imprenta por parte de la subdirección técnica.

ARTÍCULO 43.- TIPOS DE ADQUISICIÓN DE SOFTWARE: Para efectos del presente capitulo se entiende por adquisición de software la facultad de uso sobre un software dentro del marco de los derechos de autor para el desarrollo de sus operaciones, estas adquisiciones pueden darse en las siguientes situaciones:

1. **Por desarrollo propio:** Se entiende por desarrollo propio el que es desarrollado por los ingenieros que hacen parte de la planta del INCI.
2. **Por desarrollo contratado**: Se entiende por desarrollo contratado los desarrollos de software que se realizan mediante contratación de un tercero y este desarrolla para el INCI.
3. **Por donación de una persona natural o jurídica:** Se entiende por donación la adquisición que hace de un software el INCI, por convenio o acuerdo con una persona jurídica o natural que traslada los derechos de uso al INCI sin pagar los derechos patrimoniales, pero manteniendo los derechos morales.

4. **Por intercambio interinstitucional:** Es el software que se adquiere producto de un convenio interinstitucional con otra entidad del Estado en desarrollo de algún programa o proyecto, en la cual se transfieren totalmente los derechos de uso.
5. **Por uso de software libre:** Este tipo de adquisición se regula por las normas y costumbres del autor del desarrollo y sus condiciones de uso.

ARTÍCULO 44.- ADQUISICIÓN DE SOFTWARE COMERCIAL: Es el software adquirido para uso de la entidad, cuyo código fuente y derechos patrimoniales y morales corresponden a la entidad dueña de la marca, para adquirir software comercial se deben seguir las siguientes reglas:

1. Que la licencia de uso sea perpetua y en consecuencia no genere gastos recurrentes de pagos anuales de licencia.
2. Que la adquisición no genere dependencia para el mantenimiento y soporte, que amarre a contratos que generen gastos recurrentes.
3. Que junto con la licencia se entregue documentación técnica necesaria para que los ingenieros de la entidad puedan realizar el soporte y mantenimiento.
4. Que cumpla con los estándares de accesibilidad para personas con discapacidad visual, en la medida de las posibilidades.

PARÁGRAFO 2: Se exceptúan de estos criterios el software que va ligado a servicios que se contratan por un periodo específico de tiempo, como el caso del streaming o servicio de correo o alojamiento hosting.

ARTICULO 45.- DESARROLLO DE SOFTWARE: Para todos los desarrollos de software, el INCI deberá contar con la propiedad o derecho de modificación del código fuente certificada, poseer el código fuente, el modelo entidad relación (estructura de la base de datos), casos de uso, diccionario de datos, instaladores, manual técnico y de administración, manual de usuario, módulo de administración, ficha técnica que describa como mínimo la versión del software, motor de base de datos, lenguaje de programación y desarrollador.

PARÁGRAFO 3: Queda prohibido contratar desarrollos de software que no incluyan la propiedad y en consecuencia la entrega de código fuente para el INCI.

ARTÍCULO 46.- PROCEDIMIENTOS PARA EL DESARROLLO DE SOFTWARE: los desarrollos de software que el INCI contrate o realice directamente con los funcionarios, deberán cumplir con los principios y requisitos relacionados en el numeral siete de la norma técnica de calidad NTC-GP1000.

ARTÍCULO 47.- REGISTROS Y DOCPUMENTOS PARA EL DESARROLLO DE SOFTWARE: Los ingenieros de la oficina asesora de planeación responsables del desarrollo de software o la supervisión de contratistas que desarrollen software para el INCI deberán:

1. Documentar el proceso de diseño y desarrollo incluyendo todas las validaciones con usuarios.
2. Documentar el manual técnico de desarrollo que permita en futuras ocasiones hacer modificaciones o mejoras al código fuente, este manual debe incluir entre otros: fichas técnicas de objetos, métodos, propiedades de los objetos; funciones, sub-procedimientos, detalles de variables públicas, privadas y librerías.
3. Documentar los manuales para los métodos y procedimientos de compilación.
4. Documentar las estructuras de datos, la descripción del modelo entidad relación y la descripción de cada uno de las tablas y sus respectivos campos indicando los detalles de cada campo.
5. Documentar los diferentes casos de uso relacionados con el software desarrollado.
6. Documentar la metodología de software utilizada durante la etapa de análisis y desarrollo del software.
7. Diligenciar las fichas técnicas del software que hacen parte de la plataforma de desarrollo y establecer los requerimientos para la compilación como para la operación, así como el sistema operativo requerido.
8. Documentar la ficha técnica de requerimientos mínimos de hardware para el buen desempeño del software.
9. Documentar los resultados de las pruebas de funcionalidad realizadas con el usuario final con respecto al software desarrollado.

10. Documentar el registro de las versiones desarrolladas desde su versión inicial incluyendo todas las versiones de mejora, en la cual se documenten los cambios o mejoras respecto a la versión anterior.
11. Documentar el manual de instalación por cada versión desarrollada.
12. Documentar en medio físico y digital el código fuente debidamente comentado.
13. La oficina de planeación creara las tablas de retención documental necesarias para guardar toda la documentación anteriormente descrita.
14. Generar un backup de respaldo de todos los archivos digitales del software, incluyendo código fuente y demás, antes de realizar cualquier cambio, documentando en la copia de respaldo la versión.

CAPITULO SEGUNDO

DISPOSICIONES SOBRE INSTALACIÓN DE SOFTWARE

ARTÍCULO 48.- INSTALACIÓN O DESINSTALACIÓN DE SOFTWARE: La única dependencia autorizada para instalar o desinstalar software de los equipos de escritorio, portátiles o móviles de INCI, son los servidores públicos de la oficina asesora de planeación asignados para esta función, autorizados por el jefe de la oficina, por lo tanto queda expresamente prohibido a los servidores públicos o contratistas del INCI, instalar o desinstalar cualquier tipo de software, so pena de las acciones disciplinarias, fiscales y penales a que haya lugar. De conformidad con el artículo 48 numeral 43 de la ley 734 de 2002.

ARTICULO 49.- DOCUMENTACIÓN DE DAÑOS AL SOFTWARE INSTALADO: Cuando los ingenieros de la oficina asesora de planeación tengan que re-instalar un software en los equipos de escritorio, portátiles o los servidores deberán registrar en un acta las causas por las cuales se generó el daño o la desinstalación del software, y deberán reportar por escrito a la secretaría general cuando existan evidencias o indicios que la desinstalación fue producto de una intervención no autorizada.

CAPITULO TERCERO

DISPOSICIONES SOBRE MANTENIMIENTO Y SOPORTE DE SOFTWARE Y APLICACIONES

ARTÍCULO 50.- ADMINISTRADOR FUNCIONAL DE LOS SISTEMAS DE INFORMACIÓN DEL INCI: Todo sistema de información o aplicación, contará con un administrador, quien será designado por el líder del proceso, de conformidad con el sistema integrado de gestión (SIG), el cual tendrá las siguientes responsabilidades:

1. Configurar las tablas del sistema de información.
2. Parametrizar las variables que requiere el sistema de información para su desempeño, tales como: fechas, numeradores, consecutivos, tasas, etc.
3. Administrar los usuarios del sistema, otorgándoles los permisos de consulta, acceso, o cualquier otra transacción que se autorice.
4. Brindar el soporte a nivel funcional a los usuarios finales del sistema de información, y en caso que el soporte funcional transcienda al soporte técnico, el administrador funcional deberá escalar el requerimiento a través del procedimiento definido para ello por la oficina asesora de planeación.
5. Apoyar los procesos de inducción o reinducción de usuarios.
6. Identificar oportunidades de mejora del sistema de información y trasladarlas al comité técnico.
7. Notificar al comité técnico las necesidades de soporte o actualizaciones que se requieran del sistema de información.
8. Notificar al administrador técnico por escrito, las fallas técnicas que presente el sistema de información.
9. Llevar un registro de los cambios a las configuraciones y parámetros del sistema de información, de conformidad con el procedimiento establecido para ello.
10. Llevar un registro de las novedades de usuarios del sistema.
11. Crear, eliminar o inactivar usuarios dentro del sistema de información, de conformidad con las notificaciones de novedades de personal que realice la secretaría general.

12. Formular las políticas de uso del sistema de información y presentarlas al comité técnico para su aprobación.

ARTÍCULO 51.- ADMINISTRADOR TÉCNICO DEL SISTEMA DE INFORMACIÓN: Todo sistema de información o aplicación, contará con un administrador técnico, quien será designado por el jefe de la oficina asesora de planeación, el cual tendrá las siguientes responsabilidades:

1. Brindar el soporte técnico, ante incidentes que el administrador funcional reporte por escrito.
2. Administrar los servidores que soportan el sistema de información.
3. Realizar los backups de las bases de datos y aplicaciones del sistema de información de conformidad con los procedimientos establecidos para ello en el sistema integrado de gestión (SIG).
4. Realizar copia de los backups al dispositivo de almacenamiento por red (SAN) adquirido por el INCI para salvaguardar la información que corresponda y esté dispuesta en caso de contingencia.
5. Vigilar las pólizas de calidad de los contratos de desarrollo o adquisición del sistema de información a cargo, y realizar los trámites para hacerlas efectivas cuando se presenten fallas de calidad del sistema, dentro del periodo de la vigencia.
6. Notificar por escrito al jefe de la oficina asesora de planeación de las necesidades de realización o contratación de soporte técnico para corregir errores o fallas del sistema de información o de la plataforma tecnológica.
7. Formular los planes de contingencia para el sistema de información, en conjunto con el administrador funcional y presentarlo a consideración del comité técnico.
8. Realizar simulaciones del plan de contingencias del sistema de información, en conjunto con el administrador funcional y remitir el informe técnico al comité técnico.
9. Realizar las actividades del plan de contingencias del sistema de información, que le correspondan en caso de una situación de crisis.
10. Documentar de conformidad con el procedimiento, cada incidente que se presente con los sistemas de información o la plataforma tecnológica.
11. Registrar cada soporte técnico que realice al sistema de información o a la plataforma tecnológica, de conformidad con el procedimiento establecido para ello.
12. Realizar seguimiento a los incidentes o fallas presentadas en el sistema de información y/o la plataforma tecnológica, para determinar si se corrigió de forma eficaz.

CAPITULO CUARTO

DISPOSICIONES SOBRE ACTUALIZACIÓN DE SOFTWARE

ARTÍCULO 52.- ACTUALIZACION DE SOFTWARE DESARROLLADO: Todo software adquirido o desarrollado por el INCI que requiera actualización será aprobada en primera instancia por la oficina asesora de planeación y deberá ser documentado para llevar registro de las mejoras realizadas teniendo en cuenta los siguientes lineamientos:

1. Se debe especificar la versión a la cual se va a actualizar.
2. Se debe solicitar documentación de las mejoras al software.
3. Debe estar probada en las versiones del sistema operativo que disponga el INCI para el correcto funcionamiento del software.
4. Debe contar con los estándares de accesibilidad para personas con discapacidad visual, según corresponda.

ARTÍCULO 53.- ACTUALIZACION DE SOFTWARE COMERCIAL: para la actualización de todo software comercial adquirido por el INCI deberán tenerse en cuenta los siguientes lineamientos:

1. Que la versión de la licencia que se tiene es obsoleta en cuanto a usos y funcionalidades frente a los sistemas operativos, el intercambio de datos.
2. Que la versión de la licencia es obsoleta genera conflicto con los sistemas operativos o incompatibilidad con los sistemas de intercambio.

3. Que la versión a la cual se pretende actualizar genera beneficios para la entidad expresados en:
   a. Mejoramiento del rendimiento en procesamiento.
   b. Mejoramiento en el control de operaciones.
   c. Mejoramiento en la capacidad de procesamiento.
   d. Mejoramiento en la disponibilidad de nuevas herramientas.
   e. Mejoramiento de la funcionalidad que permite la mejora en la administración y el uso por parte del usuario final.
   f. Que no genere cambios bruscos en la cultura informática de la entidad.
   g. Que la nueva versión cumpla con estándares de accesibilidad, para personas con discapacidad visual.
4. Que el soporte que el fabricante otorga de manera gratuita después de un periodo de tiempo mayor a cinco años expira dificultando el mantenimiento.

CAPITULO QUINTO

DISPOSICIONES SOBRE CORREO ELECTRÓNICO INSTITUCIONAL

ARTÍCULO 54.- DEFINICIONES PARA EL PRESENTE CAPÍTULO: para el presente capitulo se tendrán en cuenta las siguientes definiciones:

1. **Cliente de correo electrónico:** es un programa de ordenador usado para leer y enviar mensajes de correo electrónico tales como: Outlook, webmail, etc.
2. **Correo electrónico certificado:** es un tipo especial de servicio de reparto de correspondencia proporcionado por las agencias postales y se caracteriza por que el correo queda registrado desde el momento de ser depositado en el sistema postal hasta su recepción por parte del destinatario.
3. **Correo electrónico:** Es un servicio que permite el intercambio de mensajes a través de sistemas de comunicación electrónicos.
4. **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.
5. **Información:** Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.
6. **Listas de distribución:** Es la agrupación de más de dos correos electrónicos que permiten el envío de información de manera grupal facilitando las comunicaciones.
7. **Mensaje de datos:** Es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, digitales, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), redes sociales, Internet, el correo electrónico, SMS, y cualquier medio electrónico.

ARTICULO 55.- CARÁCTER JURIDICO DE CORREO ELECTRONICO: De conformidad con los artículos dos y cinco de la ley 527 de 1999, el correo electrónico es el medio por el cual se transmiten y reciben mensajes de datos, en consecuencia todos los mensajes de datos enviados y recibidos por las cuentas de correo institucional del INCI tienen reconocimiento jurídico, son información pública y se constituyen en un documento público digital de conformidad con los artículos dos y dieciocho del decreto 2609 de 2012.

PARÁGRAFO 4: la información pública contenida en las cuentas del correo con extensión @inci.gov.co es propiedad del INCI y no de los funcionarios.

ARTÍCULO 56.- CLASES DE CUENTAS DE CORREO ELECTRONICO INSTITUCIONAL: Las cuentas de correo electrónico institucional tendrán la siguiente clasificación:

1. **Correo electrónico institucional Nivel uno:** Son aquellas cuentas de correo electrónico institucional que tienen las siguientes características:

a. Los mensajes de datos enviados o recibidos por estos correos tienen carácter oficial y generan efectos jurídicos para la institución.
b. Son establecidos por una norma jurídica.
c. Estos correos deben estar permanentemente monitoreados.
d. Estos correos deben ser certificados en la medida de las posibilidades presupuestales.
e. La información histórica de este correo se hereda con el cambio del servidor público responsable de la cuenta, y hace parte del acta de entrega.

2. **Correo electrónico institucional Nivel dos:** Son aquellas cuentas de correo electrónico institucional que tienen las siguientes características:
   a. El nombre del correo electrónico institucional debe obedecer a un nombre de una dependencia.
   b. Los mensajes de datos enviados y recibidos comprometen la posición oficial del INCI en los asuntos que se manejen en dicha dependencia.
   c. Este correo puede ser consultado por más de un servidor público, previa configuración y autorización.
   d. Este correo puede enviar mensajes de datos a la lista de distribución "Incilista".
   e. La información histórica de este correo se hereda con el cambio del servidor público responsable de la cuenta, y hace parte del acta de entrega.
3. **Correo electrónico institucional Nivel tres:** Son aquellas cuentas de correo electrónico institucional que tienen las siguientes características:
   a. Este correo está dirigido a grupos de trabajo, proyectos o procedimientos especiales.
   b. La información histórica de este correo se hereda con el cambio del servidor público responsable de la cuenta, y hace parte del acta de entrega.
   c. Los mensajes de datos enviados y recibidos no comprometen la posición oficial del INCI en los asuntos que se manejen en dicha dependencia.
   d. Su propósito específico es la coordinación de operaciones o gestión de servicios.
   e. Este correo puede enviar mensajes de datos solo en temas específicos autorizados por el jefe de la dependencia a la lista de distribución "Incilista".
4. **Correo electrónico institucional Nivel Cuatro:** Son aquellas cuentas de correo electrónico institucional que tienen las siguientes características:
   a. Estas cuentas tienen una asignación individual.
   b. Son de uso exclusivo para coordinación de operaciones dentro de la dependencia o la entidad o con servidores públicos de otras entidades del estado en las cuales no se compromete ninguna posición oficial del INCI.
   c. No tiene permisos para enviar mensajes de datos a la lista de distribución "incilista".

ARTÍCULO 57.- FIRMAS DE CORREO ELECTRÓNICO INSTITUCIONAL: Como parte de la imagen corporativa todos los correos electrónicos institucionales del INCI deben llevar la firma estandarizada por la oficina asesora de planeación la cual debe tener los siguientes datos mínimos:

1. Logo del INCI el cual debe ser el diseñado o actualizado por el proceso de comunicaciones.
2. Logo del Ministerio de Educación remitido oficialmente por este.
3. Logos y eslogan de Presidencia de la República remitidos oficialmente.
4. Restricciones y exclusiones sobre el contenido del correo que deben ser tenidos en cuenta en cumplimiento del marco legal que los regula.
5. Redes sociales del INCI.
6. Nombre del servidor público o contratista responsable.
7. Cargo o rol del servidor público o contratista responsable.
8. Dependencia o proyecto del servidor público o contratista responsable.
9. Teléfonos de contacto del servidor público o contratista responsable.
10. Dirección del INCI.
11. Dirección de correo electrónico institucional para respuestas.

PARÁGRAFO 5: Queda prohibido a todo servidor público o contratista retirar o modificar la firma del correo electrónico.

ARTÍCULO 58.- PROCEDIMIENTO PARA ASIGNACIÓN DE CORREO ELECTRÓNICO INSTITUCIONAL: El procedimiento que se deberá seguir para la asignación de un correo electrónico institucional para un funcionario público o contratista será el siguiente:

1. El jefe de la dependencia evaluará la necesidad de un correo electrónico institucional para los servidores públicos a su cargo o los contratistas de apoyo a la gestión supervisados por su dependencia.
2. Realizar la solicitud formal por correo electrónico al jefe de la oficina asesora de planeación adjuntando la justificación, de conformidad con las directrices de la presente resolución.
3. El jefe de la oficina asesora de planeación evaluará la solicitud teniendo en cuenta los siguientes criterios:
    a. Que exista disponibilidad de cuentas de correo electrónico institucional.
    b. Que si no existe disponibilidad de correo electrónico institucional existan los recursos económicos para ampliar la cobertura de cuentas.
    c. Que la sustentación presentada por el jefe de la dependencia corresponda a las políticas fijada por la dirección general para esta materia, o se deriven por compromisos de convenios interadministrativos.
4. El jefe de la oficina asesora de planeación aprobará o rechazara la solicitud indicando por escrito las razones, e informando al jefe de la dependencia que realizó la solicitud.
5. En el caso de que la solicitud sea aprobada se informará a los ingenieros de la oficina para que creen la cuenta de correo correspondiente.

ARTÍCULO 59.- NOMENCLATURA DE CORREOS ELECTRONICOS INSTITUCIONALES: La nomenclatura que tendrán los correos electrónicos institucionales será la siguiente:

1. Para las cuentas de nivel uno y nivel dos se seguirán las siguientes reglas:
    a. Se escribirá el nombre de la dependencia o de la oficina.
    b. Para el caso de atención al ciudadano será aciudadano@inci.gov.co.
2. Para las cuentas de nivel tres se seguirán la siguiente regla:
    a. Se escribirá el nombre del grupo o proyecto especial.
3. Para las cuentas de nivel cuatro se seguirán las siguientes reglas:
    a. Se escribe con la primera letra del primer nombre seguida del primer apellido.
    b. Si existe un homónimo se escribe la primera letra del segundo nombre seguida del primer apellido.
    c. Si aun así persiste el homónimo, se escribe la primera letra del segundo apellido seguida del primer apellido.
    d. En caso de que persista el homónimo, se escribirá la primera letra del primer apellido, seguida del segundo apellido

ARTÍCULO 60.- ALMACENAMIENTO DE LAS CUENTAS DE CORREOS: Por seguridad de los correos y la información contenida, se almacenará un repositorio local de los correos en cada computador, que será responsabilidad de cada funcionario, de igual forma se realizará una copia de seguridad periódica con fines disciplinarios y operadores judiciales.

ARTÍCULO 61.- TAMAÑO DE LOS ARCHIVOS ADJUNTOS: El tamaño máximo para envíos de archivos adjuntos es de 2 MB, para un tamaño superior debe usarse un link por la herramienta de alojamiento en la nube.

ARTÍCULO 62.- CRITERIOS PARA ASIGNACIÓN DE CUENTAS DE CORREO ELECTRONICO: La oficina asesora de planeación para asignar cuentas de correo electrónico institucional tendrá en cuenta los siguientes criterios:

1. **Para servidores públicos del INCI:** Para asignar una cuenta de correo electrónico a un servidor público del INCI, se deben tener en cuenta los siguientes criterios:
    a. Que deba mantener comunicación escrita permanente con su superior jerárquico y que existan intercambios de documentos digitales.

b. Que tenga supervisiones contractuales a su cargo.
c. Que requiera tener comunicación con servidores públicos de otras agencias del Estado para coordinar operaciones.
d. Que requiera de comunicación escrita para coordinar operaciones con otros servidores públicos del INCI y que exista intercambio de documentos digitales.

2. **Para contratistas de prestación de servicios de apoyo a la gestión del INCI:** Para asignar cuenta de correo electrónico a un contratista de prestación de servicios de apoyo a la gestión del INCI, deberá tener en cuenta los siguientes criterios:
   a. Que deba mantener comunicación escrita permanente con el jefe de la dependencia a la cual presta sus servicios y que existan intercambios de documentos digitales para el cumplimiento de sus obligaciones, y estos a su vez se constituyen en parte de los activos de información del INCI que deben tener un control por parte de la entidad en cumplimiento de normas jurídicas.
   b. Que deba mantener comunicación escrita permanente con otros servidores públicos de la entidad en la cual existen intercambios de documentos digitales para el cumplimiento de sus obligaciones, y estos a su vez se constituyen en parte de los activos de información del INCI que deben tener un control por parte de la entidad en cumplimiento de normas jurídicas.
   c. Que los mensajes de datos entre el potencial contratista y las partes internas del INCI configuran el manejo de información privilegiada que pueda poner en riesgo los procesos de la entidad.

3. **Para procedimientos o proyectos especiales del INCI:** Para asignar cuenta de correo electrónico a un procedimiento o proyecto especial, se deberá tener en cuenta los siguientes criterios:
   a. Que haga parte de las obligaciones del INCI en cumplimiento de un convenio interadministrativo en el cual se desarrollan proyectos o programas coordinados con otra entidad, estos correos electrónicos tienen las siguientes características:
      i. La vigencia del correo electrónico solo será por el tiempo que dure el desarrollo del proyecto o convenio.
      ii. Se debe dejar backup específico de este correo electrónico y hará parte integral del expediente contractual de convenio.
      iii. El nombre del correo electrónico debe corresponder a las acciones que ejecuta.
      iv. En caso de cambio de la persona responsable se debe cambiar su configuración y acceso para garantizar la continuidad y la integridad de la información.
      v. Estos correos deben llevar obligatoriamente firma oficial del INCI y del proyecto.
   b. Que de conformidad con los procedimientos del sistema integrado de calidad se requiera para prestar un adecuado servicio a la comunidad.
      i. La vigencia del correo electrónico solo será permanente mientras exista el procedimiento que lo respalde.
      ii. Se debe dejar backup específico de este correo electrónico y hará parte integral de las tablas de retención documental del proceso al cual pertenece.
      iii. El nombre del correo electrónico debe corresponder al nombre del procedimiento.
      iv. En caso de cambio de la persona responsable se debe cambiar su configuración y acceso para garantizar la continuidad y la integridad de la información.
      v. Estos correos deben llevar obligatoriamente firma oficial del INCI.

ARTÍCULO 63.- DEBERES PARA LOS SUJETOS DE LA POLÍTICA RESPECTO AL CORREO ELECTRÓNICO INSTITUCIONAL: Son deberes de los sujetos de la política respecto del correo electrónico institucional, las siguientes:

1. Todos los servidores públicos y contratistas del INCI, están obligados a usar la herramienta de correo Outlook, o el que disponga la oficina asesora de planeación en la política de manejo de correos en la nube.
2. Mantener, eliminar y depurar por lo menos una vez al mes, la información contenida en éste.
3. Verificar que todos los correos enviados se encuentren con la firma institucional suministrada por la Oficina Asesora de Planeación.

4. Realizar Backup del correo que le ha sido asignado en cumplimiento de sus funciones.
5. Cuando se reciba un mensaje de datos que sea del resorte de otra dependencia o funcionario dentro de la dependencia deberá re-enviarlo de manera inmediata al jefe de la dependencia.

ARTÍCULO 64.- PROHIBICIONES PARA LOS SUJETOS DE LA POLÍTICA RESPECTO AL CORREO ELECTRÓNICO INSTITUCIONAL: Son Prohibiciones de los sujetos de la política respecto del correo electrónico institucional, las siguientes:

1. Enviar mensajes con contenido de acoso en marco de la Ley, obscenos, amenazadores, maltrato (moral, ético, profesional) o de cualquier otro contenido inadecuado o inapropiado, a otro usuario.
2. Distribuir, acceder o guardar material ofensivo, abusivo, obsceno, racista, ilegal o no laboral, utilizando los medios electrónicos de la institución.
3. Enviar, reenviar o responder correos electrónicos basura (SPAM), mensajes con ánimo de lucro o mensajes en cadena cualquiera sea su contenido en especial si hace referencia a falsos virus, el cual debe tomarse como no deseado.
4. Abrir mensajes de correo electrónico o con archivos adjuntos que considere de remitente sospechoso o desconocido, de dudosa procedencia, e inclusive de remitentes conocidos pero cuyo asunto pueda levantar sospecha (mensajes SPAM).
5. Instalar clientes de correos diferentes al establecido para el uso institucional (Outlook).
6. Utilizar la cuenta de correo institucional para fines personales o ajenos al cumplimiento de la misión del INCI.
7. Sincronizar la cuenta de correo institucional con otros proveedores de servicio de correo tales como Gmail, Hotmail, Yahoo, entre otros.
8. Retirar la firma establecida por la oficina de planeación.
9. Para los correos electrónicos de los niveles tres y cuatro, responder correos en donde se comprometa la posición oficial.
10. Para los correos electrónicos de nivel dos, responder correos en donde se comprometa la posición oficial en asuntos distintos a los autorizados.

ARTÍCULO 65.- DISPOSICIONES SOBRE BACKUP AL CORREO ELECTRÓNICO INSTITUCIONAL: Para efectos de realizar las copias de seguridad de los correos electrónicos, se tendrán en cuenta los siguientes lineamientos:

1. Para garantizar la confiabilidad de las copias de los correos electrónicos el responsable de generar el backup de la información contenida en el correo será de cada servidor público o supervisor de contratista.
2. Queda prohibido usar clientes de correo residentes diferentes al del proveedor oficial de correos del INCI, en los computadores de escritorio o portátiles.
3. La oficina asesora de planeación generará periódicamente las copias alternas de seguridad del correo electrónico, a las cuentas institucionales de nivel uno, dos y tres, las cuales serán realizadas manualmente por el administrador de correo desde el servidor dispuesto para tal fin y serán alojadas en el dispositivo de almacenamiento por red (SAN), según los lineamientos descritos en el procedimiento de backup, sin exonerar de la responsabilidad que tiene cada funcionario de realizar su propio backup, estas copias solo tienen como propósito apoyar a los operadores judiciales o disciplinarios.
4. Las copias de los correos electrónicos que están bajo custodia de la oficina asesora de planeación llevarán una bitácora y se conservarán como mínimo un año, para atender consultas de cualquier operador disciplinario o judicial.

CAPITULO SEXTO

DISPOSICIONES SOBRE CUSTODIA Y ADMINISTRACIÓN DE LICENCIAS

ARTÍCULO 66.- DEBERES PARA CONSERVACIÓN Y CUSTODIA DE LICENCIAS DE SOFTWARE: Todas las licencias adquiridas a cualquier título para el INCI, así como sus claves de instalación e instaladores, deberán ser conservadas y custodiadas por los servidores públicos de la oficina asesora de planeación asignados para esta

función, quienes llevarán un inventario y registro, por lo tanto, queda prohibida la entrega de las licencias, claves, instaladores y su documentación a servidores públicos distintos.

PARÁGRAFO 6: Para el registro de las licencias instaladas se deberá llevar una base de datos en donde se registren los softwares que están instalados en cada uno de los equipos de escritorio, equipos portátiles y equipos móviles.

PARÁGRAFO 7: Para el registro o activación de las licencias en los portales web de los proveedores sólo lo podrá hacer el servidor público autorizado por la oficina de planeación y nunca podrá registrar nombres de servidores públicos sino el nombre de la institución.

ARTÍCULO 67.- USO DE SOFTWARE LIBRE: Teniendo en cuenta la directiva presidencial sobre austeridad del gasto, la oficina de planeación procurará como primera opción para resolver necesidades de software para los distintos procesos, el uso de software libre.

ARTÍCULO 68.- PROHIBICIONES PARA USO DE LICENCIAS DE SOFTWARE: los lineamientos descritos a continuación limitan el uso de las licencias adquiridas por el INCI para el correcto funcionamiento de los sistemas de información en la plataforma tecnológica:

1. El funcionario designado por la oficina de planeación para tener custodia de las licencias no podrá compartir ni disponer bajo ninguna circunstancia con personas ajenas a la dependencia las llaves del producto ni ningún otro tipo de información que sea de uso exclusivo del INCI.
2. El funcionario que tenga en custodia las licencias de software de propiedad del INCI, no podrá hacer uso de ellas para fines personales, ni en equipos distintos a los de la entidad.

TITULO IV. DISPOSICIONES SOBRE HARDWARE UTILIZADO POR EL INCI

CAPITULO PRIMERO

DISPOSICIONES SOBRE ADQUISICIÓN DE HARDWARE

ARTÍCULO 69.- DEFINICIONES: Para el presente capítulo se seguirán las siguientes definiciones:

- **Actualización de hardware:** Cambio de piezas físicas a cualquier dispositivo de la plataforma tecnológica para mejorar las condiciones de operación de un equipo.
- **CPU:** Es el hardware dentro de una computadora u otros dispositivos programables, que interpreta las instrucciones de un programa informático mediante la realización de las operaciones básicas aritméticas, lógicas y de entrada/salida del sistema.
- **Embebido:** Un sistema embebido o empotrado es un sistema de computación diseñado para realizar una o algunas pocas funciones dedicadas frecuentemente en un sistema de computación en tiempo real.
- **Hardware:** Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.
- **Mantenimiento de Hardware:** Consiste en la reparación o cambio de componentes o piezas que afectan su normal operación.
- **Periféricos:** Se consideran periféricos a las unidades o dispositivos de hardware a través de los cuales la computadora se comunica con el exterior, y también a los sistemas que almacenan o archivan la información, sirviendo de memoria auxiliar de la memoria principal.
- **Repotenciación:** acción de mejorar las capacidades o prestaciones de un equipo a través del cambio o mejora de alguna de sus partes.
- **Soporte técnico:** Es un rango de servicios que proporcionan asistencia con el hardware o software de una computadora, o algún otro dispositivo tecnológico.

ARTÍCULO 70.- ADQUISICIÓN DEL HARDWARE: Corresponde únicamente a la Oficina Asesora de Planeación la adquisición de hardware para la institución conforme al plan de adquisiciones y proyecciones en actualización de la plataforma tecnológica.

PARÁGRAFO 8: Se exceptúan de esta restricción el hardware y software embebidos en las máquinas que se adquieran para la imprenta por parte de la subdirección técnica.

ARTÍCULO 71.- CRITERIOS PARA LA ADQUISICION DE HARDWARE: La oficina de planeación en los procesos de adquisición de hardware deberá tener en cuenta los siguientes criterios:

1. No adquirir hardware que genere gastos recurrentes por licencias de uso.
2. Para la adquisición de hardware que requiere de insumos se deberá evaluar previamente lo siguiente:
   a. Que el costo de los insumos sea razonable a las limitaciones presupuestales de INCI y que no agregue costo a las operaciones del INCI y que sus costos no sean onerosos.
   b. Que exista suficiente disponibilidad de proveedores en el mercado.
   c. Que exista suficiente disponibilidad de insumos en el mercado.
   d. Que exista suficiente disponibilidad de proveedores en el mercado para el mantenimiento.
   e. Que los costos de los repuestos de cambio regular sean de precios razonables en el mercado
   f. Que el hardware que se adquiera en lo posible sea con especificaciones de trabajo pesado.
   g. Que en la adquisición del hardware se incluyan los dispositivos de regulación, estabilización y protección de corriente necesarios.
   h. Que tanto la tecnología como los insumos requeridos sean amigables con el ambiente.
3. Verificar si el hardware a adquirir requiere conexión a la red de datos LAN o Wi_Fi. Para lo cual deberá tener en cuenta los siguientes lineamientos:
   a. Si requiere conexión, verificar el lugar de operación y establecer si hay punto de red disponible.
   b. En caso de no haber, deberá notificar al ingeniero responsable de las redes para que amplié el punto.
4. Verificar si requiere interconectarse con otro hardware en tal caso se deberá verificar la compatibilidad con este.

PARÁGRAFO 9: La oficina de Planeación deberá establecer una ficha que incluya una lista de chequeo con los requisitos aquí fijados, y hará parte de los estudios previos para la adquisición de hardware.

ARTÍCULO 72.- SOPORTE TÉCNICO, ADMINISTRACIÓN Y CONTROL DEL HARDWARE: La prestación del soporte técnico requerido, la administración y control sobre el uso que se hace del hardware y que hace parte de la plataforma informática corresponde a la Oficina Asesora de Planeación.

PARÁGRAFO 10: Se exceptúan de esta restricción el hardware y software embebidos en las máquinas que se adquieran para la imprenta por parte de la subdirección técnica.

CAPITULO SEGUNDO

DISPOSICIONES SOBRE INSTALACIÓN DE HARDWARE

ARTÍCULO 73.- INSTALACION DEL HARDWARE: Corresponde únicamente a los servidores públicos de la oficina de planeación realizar cualquier tipo de instalación de hardware que haga parte de la plataforma tecnológica del INCI.

PARÁGRAFO 11: Se exceptúan de esta restricción el hardware y software embebidos en las máquinas que se adquieran para la imprenta por parte de la subdirección técnica.

ARTÍCULO 74.- REQUISITOS PREVIOS PARA LA INSTALACIÓN DE HARDWARE: La oficina asesora de planeación al momento de instalar un hardware tendrá en cuenta los siguientes requisitos previos:

1. Establecer si el hardware requiere conexión a la red de datos (LAN o WIFI).

2. En caso de requerir red deberá verificar si existe punto de red disponible para su conexión.
3. Verificar, si en la etapa de compra se notificó la ampliación del punto de red, y si se realizó la ampliación respectiva; Si aún no está disponible el punto de red, se debe suspender la instalación hasta tanto no se gestione la ampliación de dicho punto.
4. Cuando se requiere interconectarse con otro hardware se deberá seguir las instrucciones del fabricante para configurar dicha conexión.
5. En caso de instalación por mantenimiento y si se trata de un dispositivo de almacenamiento, deberá realizarse previamente una copia de seguridad de la información que está contenida en él, para este caso no se puede continuar con la instalación hasta tanto el usuario no certifique por escrito su conformidad con la copia de seguridad.
6. Para instalaciones de hardware en computadores de escritorio que demoren más de un día, la oficina de planeación podrá dar de manera transitoria un equipo comodín al usuario mientras se hacen los ajustes de la máquina.

CAPITULO TERCERO

DISPOSICIONES SOBRE ACTUALIZACIÓN O RENOVACIÓN DE HARDWARE

ARTÍCULO 75.- ACTUALIZACION DEL HARDWARE: Corresponde a la Oficina de Planeación realizar las labores correspondientes a la adquisición y reemplazo de las partes que correspondan a hardware por daño parcial o pérdida total de algún dispositivo de los equipos de escritorio o servidores en caso de ser requerido, para esto se seguirán las siguientes reglas:

1. Para computadores de escritorio o portátiles:
   a. Renovación de memoria RAM: para los computadores de escritorio del INCI, se actualizará la capacidad de memoria RAM de tal manera que permita sacar el mejor provecho del procesador durante su vida útil, también cuando se instale un software que exija mayor requerimiento de memoria RAM.
   b. Renovación de Disco Duro: este solamente se cambiará o actualizará cuando presente fallas físicas el disco duro y el computador este en el marco de tiempo de la vida útil tolerable.
   c. Renovación total: Los computadores deben renovarse cuando cumplan un ciclo de vida mayor a cuatro años siempre y cuando las posibilidades presupuestales lo permitan esto con el propósito de disminuir el número de mantenimientos y sus costos asociados que hace onerosa la operación.
   d. Al momento de renovar un hardware total o parcial, la oficina de planeación debe evaluar entre el costo de reposición frente al costo de mantenimiento y se inclinara por la opción que genere mayor conveniencia para la entidad.
2. Para servidores:
   a. La oficina de planeación deberá evaluar la posibilidad de repotenciación del servidor analizando su costo, la mejora del rendimiento y las restricciones por compatibilidad y tomará la decisión más conveniente para la entidad.
   b. Por obsolescencia sistémica entendida esta como la obsolescencia que le genera el servidor a toda la plataforma informática a pesar que existan otros equipos de tecnología de punta como parte de la misma.
   c. Por daño total.
3. Para impresoras:
   a. Las impresoras de la plataforma tecnológica del INCI, deberán renovarse cuando presente dificultades para conseguir los insumos o los repuestos.
   b. Las impresoras de la plataforma tecnológica del INCI, deberán renovarse cuando se evalué que los costos en mantenimiento son muy altos y se aproximen al valor de un equipo nuevo.
   c. Las impresoras de la plataforma tecnológica del INCI, deberán renovarse por obsolescencia e incompatibilidad con la plataforma informática.
   d. Las impresoras de la plataforma tecnológica del INCI, deberán renovarse por daño total.

e. Las impresoras de la plataforma tecnológica del INCI, deberán repotenciarse cuando exista la posibilidad de mejorar las prestaciones a un costo razonable.
f. Las impresoras de la plataforma tecnológica del INCI, deberán renovarse cuando su operación dependa de licencias periódicas que generen costos recurrentes.

4. Otros dispositivos de hardware:
   a. Cuando el dispositivo presente obsolescencia tecnológica.
   b. Cuando el dispositivo presente algún daño irremediable.
   c. Cuando el dispositivo presente algún daño y se evalúe que el costo de mantenimiento es más elevado que el reemplazo total.
   d. Cuando el dispositivo genere incompatibilidad tecnológica con los demás elementos que hacen parte del sistema.
   e. Cuando se requiera especificaciones superiores a las que se tengan.

CAPITULO CUARTO

DISPOSICIONES SOBRE ASIGNACIÓN DE HARDWARE A SERVIDORES PÚBLICOS DEL INCI

ARTÍCULO 76.- AUDITORÍA DEL HARDWARE: Corresponde a la Oficina Asesora de Planeación realizar las auditorias periódicas a los responsables de los equipos de cómputo, para actualizar las hojas de vida de los mismos, según lo establecido en el Procedimiento Administración de la Plataforma Tecnológica Institucional.

ARTÍCULO 77.- DEBERES PARA LOS SUJETOS DE LA POLÍTICA RESPECTO AL HARDWARE: Son deberes de los sujetos de la política respecto al hardware, las siguientes:

1. Guardar la información institucional en una única carpeta llamada "Información institucional", creada por la oficina de planeación en el disco duro del computador.
2. Cuidar y hacer buen uso de los recursos tecnológicos entregados y asignados para realizar sus actividades, los cuales serán para uso exclusivo institucional y no personal.
3. El fondo de escritorio será controlado desde el servidor de Directorio Activo y no podrá ser modificado por el funcionario, sólo se subirá al servidor el que haya sido entregado por la Oficina Asesora de Comunicaciones.
4. Escanear con el antivirus institucional instalado en los equipos de cómputo, los dispositivos USB, para examinar y eliminar virus, malware, Troyanos, Gusanos, entre otros, que pongan en riesgo la seguridad de la información y de los recursos informáticos.
5. Revisar la guía de errores frecuentes que se encuentra en la carpeta del SIG en el proceso de informática y tecnología al presentarse un problema con el hardware, y tratar de dar solución al problema ocurrido con el hardware con las instrucciones contenidas allí en cada caso, y en caso de lograrse resolver la situación de esta manera.
6. Informar a la Oficina Asesora de Planeación, oportunamente y a través de los canales dispuestos para ello, la ocurrencia de novedades por problemas de tipo técnico, eléctrico, electrónico y en general tecnológico, en el uso del hardware, que altere, impida o modifique su funcionalidad.
7. Evitar la exposición de los equipos de cómputo a factores externos que comprometan su integridad (sol, humedad, agua, imanes, humo, polución, polvo, electricidad estática, entre otros).
8. Apagar correctamente los equipos de cómputo (reguladores, estabilizadores y multi-tomas que lo acompañan) en ausencias prolongadas (mayor a 2 horas) y al final de la jornada laboral. En ausencias no prolongadas (inferior a 2 horas) se debe bloquear el equipo o cerrar sesión y apagar el monitor.
9. Registrar en la minuta de la empresa de vigilancia y seguridad, la salida o entrada, de equipos de cómputo y/o periféricos no institucionales.

ARTÍCULO 78.- PROHIBICIONES PARA LOS SUJETOS DE LA POLÍTICA RESPECTO AL HARDWARE: Son Prohibiciones de los sujetos de la política respecto del hardware, las siguientes:

1. Utilizar para uso personal los equipos de escritorio, portátiles o móviles.
2. Conectar a las UPS aparatos de alto consumo eléctrico tales como: reguladores, impresoras láser o de matriz de punto, cualquier tipo de electrodoméstico, y otros que desmejoren el buen funcionamiento o la vida útil de esta.
3. Ingerir alimentos o bebidas en el área de trabajo donde se encuentren los equipos.
4. Imprimir o fotocopiar documentos personales o ajenos a la labor institucional.
5. Cambiar la configuración que inicialmente realiza la oficina de planeación en los equipos de escritorio, portátiles y móviles, que son entregados a los funcionarios para el ejercicio de sus funciones.

CAPITULO QUINTO

DISPOSICIONES SOBRE EL MANTENIMIENTO DE HARDWARE

ARTÍCULO 79.- TIPOS DE MANTENIMIENTO: Asociados al hardware existen los siguientes niveles de mantenimiento para la plataforma informática actual del INCI de la cual es responsable la oficina asesora de planeación:

1. **Mantenimiento preventivo:** Es el mantenimiento destinado a la conservación de equipos o instalaciones de la plataforma informática mediante realización de revisión y reparación que garantice su buen funcionamiento.
2. **Mantenimiento correctivo:** Es el mantenimiento que se realiza cuando sucede algún evento que ocasione daño en el hardware de la plataforma informática, para este caso la oficina de planeación deberá evaluar si la corrección requiere un cambio en hardware deberá remitirse al artículo creado para tal fin.
3. **Mantenimiento de redes:** Este tipo de mantenimiento se realiza cuando se presenta daño en cualquiera de los componentes de comunicaciones de la red LAN y WIFI.

PARÁGRAFO: PARÁGRAFO: Se exceptúan de estos niveles de mantenimiento el hardware y software embebidos en las máquinas que se adquieran para la imprenta por parte de la subdirección técnica.

ARTÍCULO 80.- REGLAS PARA CONTRATOS DE MANTENIMIENTO: La oficina asesora de planeación deberá realizar los contratos de mantenimiento incluyendo una bolsa de horas y bolsa de repuestos teniendo en cuenta las siguientes consideraciones:

1. **Cuando un equipo es sometido a una carga de trabajo alta e intervienen en el cumplimiento de los procesos:** Son los equipos de la plataforma tecnológica que por su alta carga de trabajo o su importancia deben tener vigente un contrato de mantenimiento para que los servicios del INCI no se vean interrumpidos por largos periodos de tiempo.
2. **Cuando el equipo hace parte de una cadena de valor:** Independientemente de su volumen de trabajo y no existe la posibilidad de una sustitución.

ARTÍCULO 81.- PLAN DE MANTENIMIENTO DE LA PLATAFORMA INFORMATICA DEL INCI: La oficina de planeación deberá formular anualmente en el mes de diciembre de cada año el plan de mantenimiento de la plataforma informática para la vigencia siguiente, este plan debe contemplar todas las acciones necesarias para garantizar la operación de la plataforma, para lo cual deberá seguir los siguientes lineamientos:

1. Definir todas las acciones, responsables, cronograma y recursos necesarios para hacer los mantenimientos.
2. Se deben privilegiar los mantenimientos preventivos sobre los correctivos.
3. Frente a los mantenimientos correctivos deben estimarse los recursos requeridos y garantizar su disponibilidad en servicio y bolsa de repuestos.
4. Deben establecerse que acciones se realizarán mediante contratos con terceros y cuales se harán con la mano de obra de la oficina en cuyo caso debe calcularse y estimarse los insumos requeridos para los mantenimientos.
5. Los contratos de mantenimiento con terceros, o los contrataos de recursos para hacer mantenimiento deberán hacer parte del plan de adquisiciones.

6. Frente a la limitación de recursos económicos disponibles para mantenimiento debe fijarse una priorización con criterios de impacto.
7. En la ejecución del plan de adquisiciones deben priorizarse los contratos que tengan que ver con mantenimiento de la plataforma informática.
8. Se deberá llevar una hoja de vida del mantenimiento por cada equipo la cual debe servir de base para la programación anual de mantenimientos preventivos cuando los recursos lo permitan.

TITULO V. DISPOSICIONES SOBRE EL PORTAL WEB DEL INCI

CAPITULO PRIMERO

DISPOSICIONES SOBRE LA ACTUALIZACIÓN DE LOS CONTENIDOS DIGITALES

ARTÍCULO 82.- ACTUALIZACIÓN DE CONTENIDO DIGITAL DE LA PÁGINA WEB DEL INCI: Las actualizaciones de los contenidos digitales de la página del INCI serán realizadas bajo la responsabilidad del funcionario público designado por el jefe de la dependencia correspondiente, de acuerdo a las siguientes categorías:

1. **Dirección General:** Realizará las actualizaciones correspondientes a los contenidos digitales que están dispuestos en la página web en el módulo de noticias y revista.
2. **Oficina Asesora de planeación:** realizará las actualizaciones siguientes:
   a. Administrara el sistema manejador de contenidos (página Web) de acuerdo a lo dispuesto y aprobado.
   b. Contenidos que están dispuestos en la página en el módulo de transparencia y acceso a la información pública que son de su competencia.
   c. **Asesora de Control Interno:** Realizará las actualizaciones correspondientes a los contenidos que están dispuestos en la página en el módulo de transparencia y acceso a la información pública que son de su competencia.
3. **Secretaria General:** Realizará las actualizaciones correspondientes a los contenidos que están dispuestos en la página respecto al área de talento humano y al área financiera.
4. **Oficina Jurídica:** Realizará las actualizaciones correspondientes a los contenidos que están dispuestos en la página en el módulo de transparencia y acceso a la información pública que son de su competencia.
5. **Subdirección Técnica:** Será la responsable de administrar los contenidos digitales del área misional correspondientes a los TIC de servicios y las TIC de gobierno abierto que preste el INCI.

ARTÍCULO 83.- CREACION DE GRUPOS DE CONTENIDO: Cada jefe de dependencia en coordinación con el jefe de la oficina de planeación podrán crear los grupos de contenidos digitales que harán parte del portal web del INCI siguiendo los siguientes lineamientos:

1. Que el grupo esté organizado de conformidad con la caracterización de los usuarios para los distintos servicios según lineamientos de gobierno en línea.
2. El grupo de contenidos debe corresponder a un servicio específico o un requerimiento legal de publicación dentro del marco de la ley 1712 de 2014.
3. Que haya contenidos comunes entre usuarios y servicios.

PARÁGRAFO 12: la instrumentalización e implementación de los grupos corresponde a la oficina asesora de planeación.

ARTÍCULO 84.- ROLES PARA LA ADMINSITRACION DE CONTENDOS EN LOS GRUPOS DE CONTENIDOS: Para la administración de contenidos en los grupos de contenidos que se establezcan se distinguirán los siguientes roles:

1. **Administrador:** este funcionario puede crear, modificar, eliminar, contenidos respecto de: menús, botones, artículos, módulos, categorías, roles, dentro del grupo al cual se le asignó el rol. Para desempeñar este rol el funcionario debe tener formación en administración de páginas web manejador de contenidos (CMS-System Management Content).
2. **Editor de contenidos:** este funcionario puede únicamente modificar cualquier artículo.
3. **Gestor de contenidos:** este funcionario puede crear, modificar y eliminar única y exclusivamente contenidos en los artículos
4. **Super-administrador:** Es el funcionario que puede crear, modificar, eliminar, contenidos respecto de: menús, botones, artículos, módulos, categorías, roles, grupos y cualquier elemento que afecte la estructura del portal, este rol será desempeñado siempre por un ingeniero de la oficina asesora de planeación.

PARÁGRAFO 13: para efectos de comprensión del presenté título interprétese la expresión *"articulo"* como una página que hace parte del portal.

ARTÍCULO 85.- CREACIÓN DE USUARIOS Y ASIGNACIÓN DE NUEVOS ROLES PARA LA ADMINISTRACIÓN DE CONTENIDOS DE LA PÁGINA WEB DEL INCI: Para la creación de usuarios y asignación de nuevos roles se tendrán en cuenta los siguientes lineamientos:

1. La solicitud para creación de nuevos usuarios, la realizara el jefe de la dependencia por medio de correo electrónico institucional al Jefe de la Oficina De Planeación, indicando los siguientes datos:
   a. Nombres y apellidos completos del funcionario público
   b. Correo electrónico institucional
   c. Grupo de contenido
   d. Rol a desempeñar dentro del grupo
   e. Para el caso de los roles administradores anexar certificación de la formación en CMS.
2. Una vez recibida y analizada la solicitud el jefe de la oficina asesora de planeación evaluará y aprobará el requerimiento.

PARÁGRAFO 14: Se dará una capacitación en cabeza del funcionario público que designe la Oficina Asesora de Planeacion para los funcionarios públicos que realizaran la modificación de los contenidos digitales de la página web.

TITULO VI. DISPOSICIONES SOBRE LA EXTRANET

CAPÍTULO PRIMERO

DISPOSICIONES PARA EL USO DE LA EXTRANET

ARTÍCULO 86.- DEFINICIONES: Para el presente capítulo se seguirán las siguientes definiciones:

- **Extranet:** Se refiere a todas aquellas aplicaciones (software) o soluciones informáticas que pertenecen a otras Entidades y con las cuales el INCI requiere interactuar o utiliza en desarrollo de sus funciones. Por ejemplo: SIIF Nación.

ARTÍCULO 87.- EXTRANET: El INCI, en cumplimiento de su misión, interactúa con otros Sistemas de Información que hacen parte fundamental de su gestión [(Sistema Integrado de Información Financiera – SIIF NACION (Ministerio de Hacienda y Crédito Público), Sistema de Seguimiento a Proyectos – SSP (Ministerio de Educación Nacional), Sistema de Información y Gestión del Empleo Público – SIGEP (Departamento Administrativo de la Función Pública), Sistema de Seguimiento a Proyectos de Inversión – SPI (Departamento Nacional de Planeación), Sistema Único de Informe de Finanzas Públicas –SUIFP (Departamento Nacional de Planeación) , Sistema Único de Información de Trámites -SUIT, (Departamento Administrativo de la Función Pública) Red Bancaria, Sistema Electrónico para la Contratación Pública – SECOP (Colombia Compra Eficiente), entre otros]. Por lo cual, la oficina de planeación gestionará las condiciones técnicas con las que funcionará la extranet.

ARTÍCULO 88.- CONFIGURACIONES TÉCNICAS PARA EL FUNCIONAMIENTO DE APLICACIONES EXTRANET: La configuración técnica de las aplicaciones de extranet serán responsabilidad de las entidades dueñas de la aplicación, por lo tanto, los usuarios del INCI deberán gestionar ante las unidades de soporte de las respectivas entidades cualquier requerimiento por fallas o inconsistencias en el funcionamiento.

ARTÍCULO 89.- AMBIENTE PARA EJECUCIÓN DE APLICACIONES DE LA EXTRANET: Las condiciones del ambiente para la ejecución de estas aplicaciones dentro de la red del INCI, estará a cargo del funcionario que designe el jefe de la oficina asesora de planeación.

ARTÍCULO 90.- TRÁMITE DE PERMISOS PARA USUARIOS DE LA EXTRANET: la responsabilidad del trámite de los permisos para usuarios, así como los dispositivos de hardware para el acceso tales como llaves o token serán responsabilidad del jefe de la dependencia usuaria de la aplicación de extranet, según sea el caso.

CAPÍTULO SEGUNDO

DISPOSICIONES DE LOS DEBERES Y PROHIBICIONES SOBRE LA EXTRANET

ARTÍCULO 91.- DEBERES PARA LOS SUJETOS DE LA POLÍTICA REPECTO A LA EXTRANET: Son deberes de los usuarios de las aplicaciones de extranet, las siguientes:

1. Informar de incidentes presentados en las aplicaciones extranet, que impidan o pongan en riesgo su correcto funcionamiento, la integridad de los datos o la seguridad a la unidad de soporte de la entidad propietaria de la aplicación.
2. Gestionar a través de la mesa de ayuda de la unidad de soporte de la entidad propietaria de la aplicación, los tickets o incidentes técnicos que se presenten.
3. Reportar a la oficina asesora de planeación los requerimientos de acondicionamiento del ambiente de la red interna para acceder a la aplicación extranet, tales como navegadores, complementos, plugins, entre otros.

ARTÍCULO 92.- PROHIBICIONES PARA LOS SUJETOS DE LA POLÍTICA REPECTO A LA EXTRANET: Son Prohibiciones de los usuarios de la política respecto a la extranet, las siguientes:

1. Efectuar configuraciones técnicas para el funcionamiento de las aplicaciones extranet.
2. Modificar las configuraciones o condiciones técnicas en el ambiente de la red interna para acceder a las aplicaciones extranet.
3. Desinstalar software asociado a las aplicaciones de la extranet.
4. Utilizar datos de ingreso de las aplicaciones de la extranet para fines diferentes a los relacionados con los procesos de la institución.
5. Compartir las claves de ingreso de las aplicaciones a la extranet con usuarios ajenos al proceso o a la entidad.

INCI
Trabajamos por una forma diferente de ver el mundo

RESOLUCIÓN No. 20161010000683

16-03-2016

TITULO VII. DISPOSICIÓN SOBRE EL USO DE INTERNET (WIFI Y RED CABLEADA)

CAPÍTULO PRIMERO

DISPOSICIONES PARA LA RED LAN E INALÁMBRICA

ARTÍCULO 93.- DEFINICIONES: Para el presente capítulo se seguirán las siguientes definiciones:

1. **Ancho de banda:** Es la medida de datos y recursos de comunicación disponible o consumida expresados en bits.
2. **Dirección IP**: Una dirección IP es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red.
3. **IP:** Es un protocolo de comunicación de datos digitales clasificado funcionalmente en la capa de red según el modelo internacional OSI.
4. **ISP:** Proveedor de servicios de Internet.
5. **Red LAN:** Son las siglas de Local Area Network, Red de área local, Es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada
6. **Sistema Redundante:** Los sistemas redundantes, en ingeniería de computadores, son aquellos en los que se repiten aquellos datos o hardware de carácter crítico que se quiere asegurar ante los posibles fallos que puedan surgir por su uso continuado.
7. **SSID**: Es un nombre incluido en todos los dispositivos de una red inalámbrica para identificarlos como parte de esa red.
8. **WI-FI:** Según sus siglas Wireless Fidelity, es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica.

ARTÍCULO 94.- REDUNDANCIA EN LA RED DEL INCI: Con el propósito de garantizar la continuidad del servicio en la red de datos del INCI se define un nivel de redundancia de dos que está conformada por los siguientes sistemas:

1. Nivel uno: Red de datos por cable (LAN)
2. Nivel dos: Red de datos inalámbrica (WI-FI)

PARÁGRAFO 15: En condiciones normales debe estar operando la red LAN y la red WI-FI funcionará como red alterna cuando falle la red LAN.

ARTÍCULO 95.- CONEXIÓN A LA RED CABLEADA (LAN): Todos los equipos de cómputo de la entidad, deben estar conectados a la red LAN del INCI, no está permitido el uso de otros canales de conexión (cableada o wireless) a los equipos de la institución, sin la previa autorización de la Oficina Asesora de Planeación.

ARTÍCULO 96.- ACCESO A LA RED WI-FI: El servicio de conexión a la red inalámbrica (Wi-Fi) sólo será posible en las siguientes situaciones:

1. Cuando la oficina de planeación esté haciendo mantenimiento a la red LAN y se requiera deshabilitar lo servicios de esta, en estos casos se anunciará con anticipación el cambio de red.
2. En procesos de capacitación que adelante la subdirección técnica a personas con discapacidad visual o agentes educativos en las instalaciones del INCI.
3. En eventos del INCI que requieran servicios inalámbricos de red en cualquiera de los dos edificios.
4. Visitantes cumpliendo el protocolo de acceso definido para este servicio.
5. Red segura de uso exclusivo.

ARTÍCULO 97.- NIVELES DE ACCESO A LA RED WI-FI: El servicio de conexión a la red inalámbrica wi-fi será controlado a través de los siguientes niveles de acceso:

1. **Wireless AAA:** Este nivel de acceso a la red inalámbrica tendrá todos los privilegios de navegación exceptuando las reglas o excepciones de seguridad configuradas en el firewall por lo tanto estará asociado a la dirección general del INCI y el jefe de la oficina asesora de planeación.

2. **Wireless Alterna:** esta red es la que operará como red alterna a la red LAN y tendrá las siguientes condiciones operativas:
    a. Solo se prenderá por falla en la red LAN o mantenimiento de la red LAN y durará encendida el tiempo que dure la falla de la LAN o el tiempo estimado del mantenimiento, el resto del tiempo deberá estar apagada.
    b. Los permisos de acceso para los usuarios serán los mismos que tienen en la red LAN y la identificación del ingreso de sesión al equipo.
3. **Wireless Capacitación:** Esta red está dispuesta únicamente para el servicio de la subdirección técnica en los programas de capacitación a personas con discapacidad visual o agentes educativos y operará bajo las siguientes condiciones:
    a. Se prenderá por solicitud del funcionario responsable de la subdirección técnica designado por el (la) subdirector(a) al funcionario responsable de la oficina asesora de planeación.
    b. Los permisos de acceso serán los que solicite el funcionario de acuerdo a la capacitación que va a realizar.
    c. Solo durará prendida el tiempo que el funcionario que va a realizar la capacitación haya solicitado.
    d. La responsabilidad de los permisos de acceso durante el tiempo de la capacitación será del funcionario que imparte la capacitación.

4. **Wireless Visitantes:** Esta red se utilizará para uso de visitantes y se regirá por las siguientes reglas y condiciones operativas:
    a. Esta red se prenderá únicamente en horas hábiles.
    b. Esta solo tendrá cobertura en el segundo piso, en el tercer piso para uso exclusivo de área de informática, el auditorio y la cabina de inciradio.
    c. Para ingresar a esta red se requerirá nombre de usuario y password, el usuario será el correo del visitante y la clave que sea asignada por el funcionario responsable del área que será:
        i. Visitantes del segundo piso: Serán asignados por la secretaria de la dirección general.
        ii. Visitantes del auditorio e inciradio: Serán asignados por la profesional de Inciradio.
        iii. Visitantes del área de informática: serán asignados por el profesional designado de esta área y solo podrán conectarse los contratistas y proveedores de esta área para las configuraciones en desarrollo de sus contratos.
    d. Esta red tendrá restricciones de descarga, streaming de audio y video, redes sociales y páginas maliciosas establecidas en el firewall.
    e. El permiso de acceso sólo servirá por el tiempo que le asigne el funcionario responsable y en ningún caso podrá asignar más de tres horas.
    f. Esta red funcionará en el horario entre 8:00 am hasta las 4:00 pm.

CAPÍTULO SEGUNDO

DISPOSICIONES SOBRE EL USO DE INTERNET EN LA RED DEL INCI

ARTÍCULO 98.- USO EFICIENTE DEL CANAL DE INTERNET: Para la adquisición y uso eficiente del canal de internet se deben tener en cuenta los siguientes criterios:

1. El INCI en virtud de la limitación de recursos económicos y dados los recortes presupuestales debe adquirir un canal de internet buscando las mejores especificaciones con el recurso disponible y dando cumplimiento a la directiva presidencial de austeridad del gasto.
2. La presente política busca asegurar que el uso del canal de internet cuya capacidad es muy limitada se use estrictamente en el cumplimiento de las funciones y fines misionales y garantizar la operación de la TIC de servicios, las TIC de gobierno abierto y TIC de gestión.
3. La presente política busca corregir y controlar usos inadecuados del canal de internet que generan congestión en detrimento de usos institucionales.
4. La presente política busca proteger los activos de información digitales de ataques externos e internos ocasionados por la navegación indebida de funcionarios del INCI en páginas que generen riesgos en el marco de los lineamientos de Gobierno en Línea.
5. La presente política busca optimizar el uso del canal restringiendo la navegación por niveles de uso para garantizar mayor velocidad a las áreas de la organización que lo requieran.
6. Con el propósito de mejorar la velocidad y confiabilidad de la navegación la oficina asesora de planeación deberá segmentar el canal de internet de acuerdo a los niveles de uso, priorizando las áreas de la organización que en cumplimiento de sus funciones requieran mayores especificaciones.

ARTÍCULO 99.- NIVELES DE NAVEGACIÓN EN INTERNET: Para la navegación en internet por la red del INCI se tendrán los siguientes niveles:

1. **Nivel de uso general**: Se considera este nivel el que tiene acceso a consulta en navegadores, pero restringe descargas por streaming tanto de video como de audio, descargas de aplicaciones, descargas de actualizaciones y el paquete de páginas configuradas como maliciosas en el firewall.
2. **Nivel de uso controlado:** Se considera este nivel el que tiene acceso a consulta en navegadores, permiso para descargas por streaming tanto de video como de audio, pero solo a portales y contenidos autorizados por el jefe de la dependencia, del cual se ejercerá un seguimiento a través del firewall por parte de la oficina de planeación y un control por parte del jefe de la dependencia y el coordinador de grupo.
3. **Nivel de uso en la sala virtual:** Se considera este nivel el que tiene acceso a consulta en navegadores y el acceso a descargas de streaming tanto de video como de audio, como a otras páginas se realizará de acuerdo con la programación de uso de la sala y con la autorización del (a) subdirector (a) con por lo menos dos días de anticipación en correo electrónico dirigido a la oficina de planeación.
4. **Nivel de uso comunicaciones:** Se considera este nivel el que tiene acceso a consulta en navegadores, tiene permitido descargas por streaming tanto de video como de audio, pero restringidas las descargas de aplicaciones, descargas de actualizaciones y el paquete de páginas configuradas como maliciosas en el firewall.
5. **Nivel de uso soporte informático básico:** Se considera este nivel el que tiene acceso a consulta en navegadores, descargas de aplicaciones, actualizaciones y páginas para activación de licencias, las cuales deben ser autorizadas por el jefe de la oficina asesora de planeación y tendrá restricción en las descargas por streaming de audio y video además del paquete de páginas configuradas como maliciosas en el firewall.
6. **Nivel de uso directivo y soporte informático avanzado:** Se considera este nivel el que tiene acceso a consulta en navegadores, tiene permitido descargas por streaming tanto de video como de audio, descargas de aplicaciones, descargas de actualizaciones y restringido el paquete de páginas configuradas como maliciosas en el firewall.

PARÁGRAFO 16: La oficina de planeación generará un reporte del tráfico de navegación por internet de los usuarios de uso controlado y de comunicaciones del cual remitirá copia al jefe de la dependencia y a la asesora de control interno para que haga parte del programa anual de auditorías.

ARTÍCULO 100.- ASIGNACIÓN DE LOS NIVELES DE NAVEGACIÓN: Los niveles de navegación se asignarán siguiendo los siguientes criterios:

1. Para los funcionarios de las áreas de las dependencias de apoyo se asignará el nivel de navegación general, se exceptúan de este grupo los ingenieros y técnicos de la oficina de planeación del área de informática.
2. A los funcionarios de la subdirección técnica se les asignará el nivel de navegación general exceptuando aquellos funcionarios que por solicitud del (a) subdirector (a) técnica a la oficina de planeación se les deba asignar el nivel de uso controlado.
3. El (la) subdirector (a) técnica evaluará las necesidades de navegación de conformidad con los proyectos de inversión y los proyectos especiales para ciertos profesionales que requieran accesos particulares, para lo cual solicitará por escrito a la oficina de planeación la habilitación de estos funcionarios dentro del paquete de nivel de uso controlado indicando la justificación de esta exclusión.
4. A los técnicos e ingenieros del área de informática de la oficina asesora de planeación encargados del soporte básico de la plataforma informática se les asignará el nivel de uso de soporte informático básico.
5. A los ingenieros del área de informática de la oficina asesora de planeación encargados del desarrollo de aplicaciones, que operen como super-administradores del portal web, que tengan bajo su responsabilidad la administración del alojamiento nube pública, que realicen la administración y soporte de la plataforma virtualizada, que realicen la administración de las redes, que administran la seguridad perimetral y realizan el soporte de los servicios en la nube se les asignará el nivel de uso de soporte informático avanzado.
6. A la asesora de comunicaciones se le asignará el nivel de uso de comunicaciones.
7. A los jefes de la Oficina Asesora Jurídica, Asesora de planeación, Secretaría General, subdirección, Dirección General y al Asesor de Control Interno se le asignará el nivel de uso directivo.

ARTÍCULO 101.- DEBERES PARA LOS SUJETOS DE LA POLÍTICA RESPECTO AL INTERNET: Son deberes de los sujetos de la política respecto a Internet, las siguientes:

1. Usar el servicio de Internet únicamente para el desarrollo de actividades relacionadas con el cumplimiento de la misión institucional.
2. No se deben mantener sesiones de Internet abiertas pues, aunque no se estén utilizando, las mismas siguen consumiendo el canal de Internet, si desea recordarlos se deberán usar los marcadores del navegador.
3. Informar a la Oficina Asesora de Planeación mediante correo electrónico, el uso y conexión de equipos de cómputo no institucionales a la red cableada del INCI.
4. Informar a la oficina asesora de planeación cuando quede un punto de la red de datos libre por traslado o entrega de equipos, para que ésta disponga la desconexión del switch correspondiente para evitar conexión de intrusos.

ARTÍCULO 102.- PROHIBICIONES PARA LOS SUJETOS DE LA POLÍTICA RESPECTO AL INTERNET: Son prohibiciones de los sujetos de la política respecto al uso de Internet, las siguientes:

1. Utilizar canales de mensajería instantánea (chat no institucional), o páginas de música, videos, grupos sociales, youtube, pornografía, juegos y demás páginas de ocio con fines personales.
2. Descargar de Internet o alojar en los equipos de cómputo institucional, música, videos, películas o cualquier tipo de software o contenido malicioso.
3. Abrir mensajes, sitios web, o archivos de fuente desconocida y ante cualquier duda, eliminar el mensaje, para evitar el riesgo de contaminación de virus y otros.
4. Desconectar los equipos de WIFI (Access Point) de sus puntos de red.
5. Compartir las claves de WIFI asignadas.
6. Conectar dispositivos de comunicación personales a los puntos de red LAN asignados.
7. Conectar equipos de cómputo tales como portátiles, o equipos móviles que no son propiedad del INCI a la red LAN o WIFI del INCI.
8. Desconectar los equipos de la red LAN o WIFI sin autorización.
9. Utilizar software malintencionado para acceder a la red a través de túneles.

INCI
Trabajamos por una forma diferente de ver el mundo

RESOLUCIÓN No. 20161010000683

16-03-2016

TITULO VIII. DISPOSICIÓN SOBRE EL USO DE ENERGÍA

CAPÍTULO PRIMERO

DISPOSICIONES SOBRE EL USO DE LA ENERGÍA DENTRO DE LAS INSTALACCIONES DEL INCI

ARTÍCULO 103.- POLITICAS DE AHORRO DE ENERGÍA: Teniendo en cuenta que la operación y funcionamiento de la plataforma tecnológica e informática del INCI se soporta mediante una red eléctrica las siguientes son las disposiciones que deben seguir todos los sujetos obligados frente al ahorro de energía en cumplimiento de la directiva presidencial:

1. Obligaciones de la oficina asesora de planeación:
   a. Apagar todos los sistemas los fines de semana desde el viernes hasta el lunes o martes si es puente, o durante periodos largos como semana santa y serán encendidos antes de iniciar operaciones el día hábil siguiente, de este literal se exceptúan los siguientes subsistemas:
      i. El subsistema de almacenamiento por red SAN.
      ii. El subsistema de monitoreo, tales como: Cámaras y dispositivos de acceso.
      iii. El subsistema de Aire acondicionado que protege la SAN.
   b. Apagar los sistemas de alimentación supletoria una vez hayan sido desconectados todos los demás servicios y en lo posible desconectar la salida de la UPS a la red.
   c. Deberá formular e implementar un protocolo de apagado y encendido de los sistemas.
2. Obligaciones para los sujetos de la política:
   a. Desconectar de la red eléctrica cargadores de equipos móviles, solo se permitirá por el tiempo que dure la carga del dispositivo.
   b. Es obligatorio apagar al final de la jornada los equipos de cómputo que le han sido asignados, se exceptúan los casos que, por instrucción de la oficina de planeación para efectos de mantenimientos, soportes o backups, en cuyo caso la obligación de apagar el equipo es del funcionario de la oficina de planeación, esta instrucción debe darse por correo electrónico.
3. Obligaciones de las secretarias:
   a. Apagar y desconectar las impresoras de red a las que se les asigne el control, este debe hacerse por memorando escrito firmado por el jefe de la oficina de planeación y secretaria general.
   b. En los casos en que por necesidades del servicio un funcionario requiera imprimir después del horario laboral, deberá remitirse una solicitud a la secretaria responsable del control y la responsabilidad de apagar y desconectar recae sobre el funcionario que se le otorgó el permiso.
   c. Apagar y desconectar los escáneres que tienen asignados, igual disposición aplica al responsable del centro de reprografía y gestión documental.

TITULO IX. DISPOSICIÓN SOBRE EL PLAN DE CONTINGENCIA O CONTINUIDAD DEL NEGOCIO

CAPITULO PRIMERO

DEFINICIONES PARA EL PLAN DE CONTINGENCIA O CONTINUIDAD DEL NEGOCIO

ARTÍCULO 104.- DEFINICIONES PARA EL PRESENTE TÍTULO: Las siguientes son las definiciones para el plan de contingencia y continuidad del negocio.

1. **Administración de la continuidad del negocio**: Proceso administrativo completo que identifica impactos potenciales que puedan afectar a la organización. Provee la estructura para dar flexibilidad y respuestas efectivas para salvaguardar los intereses de la organización (BCM- Business Continued Management).
2. **Plan de contingencia o continuidad del negocio:** Conjunto de procedimientos y estrategias definidos para asegurar la reanudación oportuna y ordenada de los procesos de negocio generando un impacto mínimo ante un incidente (BCP- Business Continued Plan).

INCI
Trabajamos por una forma diferente de ver el mundo

RESOLUCIÓN No. 20161010000683

16-03-2016

3. **Plan de recuperación de desastres**: Estrategias definidas para asegurar la reanudación oportuna y ordenada de los servicios informáticos críticos en caso de contingencia (DRP- Disaster recuperation plan).

ARTÍCULO 105.- RESPONSABLES DE LA FORMULACIÓN DEL PLAN DE CONTINGENCIA O CONTINUIDAD DEL NEGOCIO: Serán responsables de la formulación del plan de contingencia o continuidad del negocio el secretario General y el jefe de la oficina asesora de planeación.

ARTÍCULO 106.- APROBACIÓN DEL PLAN CONTINGENCIA O CONTINUIDAD DEL NEGOCIO: La aprobación del plan contingencia o continuidad del negocio estará a cargo del comité de desarrollo administrativo.

ARTÍCULO 107.- IMPLEMENTACIÓN DEL PLAN CONTINGENCIA O CONTINUIDAD DEL NEGOCIO: Las acciones del plan contingencia o continuidad del negocio se ejecutarán de conformidad con los cronogramas y responsabilidades fijadas en el plan.

ARTÍCULO 108.- COMITÉ DE CRISIS: Dentro de la formulación del plan de contingencia y continuidad del negocio se deberá crear un comité de crisis que debe actuar y coordinar las operaciones del plan de contingencia y continuidad del negocio frente a la ocurrencia de un desastre.

COMUNÍQUESE Y CÚMPLASE

CARLOS PARRA DUSSAN
Director General

Proyectó: Sonia Cardozo Muñoz
Revisó: Pacífico Barrera Nuban