MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

TC-MN-02

Tecnologías de la Información y las Comunicaciones

12/07/2023

Versión 3

ALCALDÍA MAYOR DE BOGOTÁ D.C.

INSTITUTO DISTRITAL DE GESTIÓN DE RIESGOS Y CAMBIO CLIMÁTICO

BOGOTÁ

Control de Cambios		
Versión	**Fecha**	**Descripción de la Modificación**
1	02/05/2017	Versión inicial del documento.
2	10/07/2019	Inclusión de nuevas políticas, actualización y restructuración del contenido del Manual de Seguridad de la Información conforme a los lineamientos del Modelo de Seguridad y Privacidad de la Información y la norma NTC ISO 27001/2013. Se realiza inclusión de codificación al documento.
3	12/07/2023	Actualización de las políticas complementarias de Gestión de Seguridad de la Información y reestructuración del contenido. Actualización de la plantilla.

Elaboró	Revisó	Aprobó
Francisco Andrés Daza Cardona Contratista	Claudia Marcela Ladino Herrera Jefe Oficina Tecnologías de la Información y las Comunicaciones	Claudia Marcela Ladino Herrera Jefe Oficina Tecnologías de la Información y las Comunicaciones Nelson Jairo Rincón Martínez Jefe Oficina Asesora de Planeación

Tabla de contenido

1. Introducción

La alta dirección adquiere el compromiso de implementar, mantener y mejorar el Sistema de Gestión Sistema de Gestión de Seguridad y Privacidad de la información – SGSI alineado a Modelo de Seguridad y Privacidad de la información – MSPI del MinTIC, se definen en el presente manual los lineamientos y políticas complementarias de seguridad de la información para el Instituto Distrital de Gestión de Riesgos y Cambio climático – IDIGER, y está dirigida a los funcionarios, colaboradores, proveedores de servicios y bienes de la entidad.

Las políticas complementarias de seguridad y privacidad de la información que a continuación se definen, están acorde con las mejores prácticas definidas en ISO 27001:2013, por tanto, cada colaborador, servidor público, contratista, proveedor o tercera parte interesada tomará las medidas aplicables para garantizar su cumplimiento.

2. Objetivo

Definir los lineamientos y política de Seguridad y Privacidad de la información del Instituto Distrital de Gestión de Riesgos y Cambio climático - IDIGER, que permita preservar la integridad, confidencialidad, disponibilidad y privacidad de la información alineado al Modelo de Seguridad y Privacidad de la información - MSPI y la Norma NTC-ISO-IEC 27001:2013.

3. Alcance

Las políticas definidas en el presente manual aplican a todos los procesos del Instituto Distrital de Gestión de Riesgos y Cambio climático – IDIGER, así como a los funcionarios, colaboradores y demás partes interesadas, que accedan a los activos de información y servicios de la entidad con el fin de garantizar la salvaguarda, confidencialidad, integridad, disponibilidad de la información.

4. Responsables

Los funcionarios, colaboradores y demás partes interesadas son responsables de comprender y cumplir las políticas complementarias de seguridad de la información, así como, gestionar y mitigar los riesgos que se puedan presentar para proteger los activos de información del Instituto Distrital de Gestión de Riesgos y Cambio climático – IDIGER contra ataques, robo, intrusiones, accesos no autorizados y fuga de información, que afecten a la imagen, los intereses y el buen nombre de la entidad.

5. Definiciones

- **Activos de Información:** Los activos de información son datos o información propietaria en medios electrónicos, impreso o entre otros medios, considerados sensitivos o críticos para los objetivos del proceso.
- **Almacenamiento:** Se refiere a la forma en la que se almacena el activo, como en medios magnéticos, salas, cajas, PC's, Servidores, CD's, DVD's, USBs, Cintas magnéticas, etc.
- **Aranda:** Herramienta para la gestión de los casos atendidos por la mesa de ayuda.
- **Cifrado:** Se estipula si es necesario cifrar o no la información digital y las características técnicas mínimas que deben tenerse en cuenta.
- **Clasificación de la Información:** es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulado por la entidad. Tiene como objetivo asegurar que la información tenga el nivel de protección adecuado. La información debe clasificarse en términos de sensibilidad e importancia para la entidad.
- **Confidencialidad**: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **CPD:** Sigla de Centro de Procesamiento de Datos
- **Custodio**: persona delegada de ejercer el cuidado o vigilancia sobre un activo que le ha sido encargado.
- **Destrucción:** Se refiere a la dinámica para la destrucción de la información que maneja el activo en el momento en el que este finaliza su ciclo de vida:
  - Incineración: destrucción de información exponiéndola a altas temperaturas para quemarla.
  - Borrado Seguro: aplica solo para medio magnéticos, es un borrado a bajo nivel.
  - Trituración: esto aplica más que todo a la destrucción de papel por medio de máquinas trituradoras.
- **Disponibilidad**: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Etiquetado**: Colocar una etiqueta o rótulo para identificar un elemento.
- **Evento de Seguridad de la Información:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

- **Hash:** Son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos).
- **IDIGER:** Sigla para referirse al Instituto Distrital de Gestión de Riesgo y Cambio Climático.
- **Incidente de seguridad:** Suceso imprevisto que tiene la probabilidad de comprometer las operaciones del negocio o amenazar la seguridad de la información de los activos críticos que almacenen, procesen y/o gestionen información.
- **Integridad**: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Inventario de activos de información:** Listado de recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.)
- **Medio Removible:** Los dispositivos de almacenamiento removibles son dispositivos de almacenamiento independientes del computador y que pueden ser transportados libremente. Los dispositivos móviles más comunes son: Memorias USB, discos duros extraíbles, DVD y CD.
- **MIPG :** Sigla de Modelo Integrado de Planeación y Gestión
- **MSPI:** Sigla de Modelo de Seguridad y Privacidad de la Información, el cual forma parte de la estrategia del proyecto de Gobierno Digital – MinTIC.
- **Parte interesada:** Persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad.
- **Política General de seguridad de la información:** Establece a alto nivel los objetivos y metas relacionados con la seguridad de la información.
- **Programas Utilitarios**: Los utilitarios o utilidades, son programas diseñados para realizar una función determinada, por ejemplo, un editor, un depurador de código o un programa para recuperar datos perdidos o borrados accidentalmente en el disco duro
- **Propietario**: Es el cargo responsable de definir el nivel de clasificación de la información, dar las directrices de uso del activo, autorizar privilegios y definir el ciclo de vida de este.
- **Seguridad de la Información:** Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.

- **Teletrabajo:** Es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo[1].
- **Teletrabajador:** es la persona que utiliza las tecnologías de la información y comunicación como medio o fin para realizar su actividad laboral fuera del local del empleador, en el marco de un contrato de trabajo o de una relación laboral dependiente, en la cual le sean garantizados todos sus derechos laborales.
- **VPN**: Sigla del inglés Virtual Private Network, es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet.
- **Vulnerabilidad**: Posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

6. Política de Seguridad y Privacidad de la Información

El Instituto Distrital de Gestión de Riesgos y Cambio climático - IDIGER, comprendiendo la importancia de la protección de la información como principal activo, se ha comprometido con la implementación, mantenimiento y mejora continua del Modelo de Seguridad y Privacidad de la información - MSPI alineado con el Sistema de Gestión de Seguridad de la información - SGSI, aplicando la administración y gestión de riesgos para prevenir o minimizar el impacto generado sobre los activos de información, así como fortalecer las capacidades de su personal en temas relacionados con la prevención e identificación de riesgos de seguridad y privacidad de la información y sus respectivos contramedidas de mitigación.

6.1 Roles de seguridad de la información

La Oficina de Tecnologías de la Información y las Comunicaciones, será la responsable del funcionamiento del MSPI alineado con el SGSI. A continuación, se encuentran los roles que intervienen en la gestión de las políticas de seguridad de la información:

- Comité institucional de gestión y desempeño conforme a lo establecido en MIPG, tiene la responsabilidad de impulsar la implementación del MSPI alineado con el SGSI en el IDIGER, además de realizar el seguimiento y /o verificación de la implementación de este.

1 Ley 1221 de 2008

- El Líder de la Oficina Tecnologías de la Información y las Comunicaciones, tendrá la responsabilidad de liderar la implementación y cumplimiento de las políticas definidas en el marco de la implementación del MSPI alineado con el SGSI.
- Oficial de Seguridad, será el responsable de coordinar la implementación y cumplimiento del MSPI alineado con el SGSI.
- El propietario de los Activos de información será el funcionario o colaborador que tiene la responsabilidad de la gestión apropiada del activo, así como de clasificar y definir la criticidad de este.
- El Custodio de los Activos de información, será el funcionario o colaborador responsable de administrar y hacer efectivos los controles y clasificaciones definidos por el propietario, alineado al cumplimiento de las políticas de seguridad de la información.
- Los funcionarios y colaboradores de la información, es el funcionario, colaborador y/o tercero autorizado para utilizar la información en el ejercicio de sus funciones o en el cumplimiento de sus obligaciones contractuales o vigencia del respectivo contrato y es el responsable del buen uso de los activos de información durante el cumplimiento de sus labores o compromisos y el cumplimiento de las políticas de seguridad de la información definidas en la entidad.

7. Políticas Complementarias de Seguridad de la Información

Las políticas enunciadas a continuación se encuentran enmarcadas dentro del alcance definido en el numeral 3. Alcance, y se rigen bajo las normas y regulaciones del actual del gobierno de Colombia. Cualquier excepción a las políticas complementarias de seguridad y privacidad de la información debe seguir lo descrito en el numeral 9. Excepciones a las Políticas Complementarias de Seguridad de la Información.

7.1 Teletrabajo, trabajo en casa y acceso remoto

La información generada, procesada o almacenada por los funcionarios o colaboradores que desempeñen sus funciones y obligaciones mediante la modalidad de Teletrabajo, trabajo en casa y acceso remoto deberá ser protegida para salvaguardar la confidencialidad y privacidad de esta. Todos los equipos de cómputo que sean usados en la modalidad de teletrabajo deben cumplir con los estándares de instalación y adecuación de seguridad de la información. Para ello se deberá tener en cuenta:

- Los funcionarios y colaboradores deberán contar con los permisos y aprobaciones de acceso pertinentes, y se debe llevar un control de los que trabajan bajo estas modalidades.
- Realizar el seguimiento a las conexiones remotas con el fin de identificar comportamientos sospechosos.
- Informar a los funcionarios y colaboradores sobre como mitigar los riesgos asociados a la seguridad de la información.
- Proporcionar una conexión segura a través de una VPN para acceder remotamente a los servicios que le permitan desarrollar las actividades asignadas.
- Denegar el acceso remoto al área de operaciones financieras y otras estaciones o sistemas que por su criticidad deban tener acceso presencial exclusivamente.

7.2 Uso de dispositivos móviles, medios extraíbles y equipos personales

El uso de medios de almacenamiento extraíble como memorias USB, tarjetas de memoria, CD, DVD, discos duros externos, entre otros, son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada, lo cual puede producir una incidente seguridad.

Para los equipos de cómputo que tienen habilitados los puertos USB y las unidades reproductoras de CD/DVD, por lo tanto, se deben seguir las siguientes directrices:

- El escaneo automático de virus debe estar habilitado.
- En el software de antivirus debe configurarse el bloqueo de la reproducción automática de archivos ejecutables.
- Los medios extraíbles que contengan información pública reservada, información pública clasificada y/o datos sensibles debe etiquetarse como tal y deben estar almacenados dentro de entornos seguros, al igual que deben inventariarse por lo menos una vez al año o cada vez que se requiera.
- El funcionario, colaborador o tercero autorizado que utilice medios de almacenamiento extraíbles con información del IDIGER, será responsable del buen uso, divulgación y distribución de esta.
- En caso de pérdida de un medio de almacenamiento extraíble debe informarse a través de la mesa de servicios, precisando la criticidad de la información. En caso de ser crítica se debe realizar el denuncio ante autoridad policial.
- En caso de ser transportados los medios de almacenamiento extraíble deben protegerse del acceso no autorizado o uso indebido, además de enviarse o entregarse por medio de un mensajero confiable u otro método de entrega que pueda rastrearse de modo preciso.

7.3 Seguridad de los recursos humanos

El IDIGER se cuenta con procedimientos establecidos para la vinculación de personal atendiendo los lineamientos de la legislación vigente, realizando la verificación y cumplimiento de los requisitos de los cargos, ***TH-PD-31 Procedimiento de vinculación***.

Así mismo, se cuenta con el procedimiento ***TH-PD-37 Procedimiento contratación de prestación de servicios banco de hojas de vida***, cuyo objetivo es "*Promover y establecer las actividades para la vinculación de personal conforme las necesidades identificadas por el IDIGER en el plan anual de adquisiciones, a fin de realizar la vinculación mediante la modalidad de contrato de prestación de servicios profesionales y de apoyo a la gestión*[2]".

7.4 Gestión de los activos de información

Es preciso realizar la identificación de todos los activos asociados con la información y las instalaciones de procesamiento de información con los que cuenta el IDIGER, con el fin de clasificarlos y protegerlos de una forma adecuada de acuerdo con su importancia y establecer los criterios y lineamientos para el tratamiento de estos. Así mismo, definir controles para salvaguardar la información creada, procesada, transmitida y/o almacenada en los procesos de la entidad, con el fin de minimizar impactos financieros, operativos y/o legales debido al uso incorrecto de la información. Para ello se deberá tener en cuenta:

- Todos los activos de información deben tener un propietario, el cual tiene la responsabilidad de la gestión apropiada del activo, además de clasificarlos y protegerlos apropiadamente de acuerdo con los criterios establecidos por la entidad.
- Se debe establecer la criticidad de los activos de información frente al impacto que pueda generar la pérdida, daño o mal funcionamiento de estos, con el fin de determinar los controles para disminuir el impacto que pueda producir.
- Todos los funcionarios y colaboradores serán responsables de proteger la información a la cual accedan o procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
- Los funcionarios y colaboradores son responsables de dar uso adecuado a los activos de información y en ningún momento puede ser usado para

[2] Objetivo: (idiger.gov.co)

realizar prácticas ilícitas o malintencionadas que atenten contra terceros o afecten a la entidad.

- Los funcionarios y colaboradores deben devolver todos los activos de información que se encuentran a su cargo al finalizar su empleo o contrato. Estos deberán ser entregados al jefe inmediato u oficina a la que pertenece o a quien se delegue, según sea el caso.
- Se debe promover el buen uso de los activos de Información, conservando el derecho a la intimidad, la privacidad, el habeas data, y la protección de los datos de sus propietarios o custodios. Así mismo, sensibilizar a los funcionarios y colaboradores respecto de las ciber amenazas como: Spear phishing, Spoofing, Watering hole, Ransomware y suplantación de identidad.

- Los líderes de proceso o quien haga sus veces son responsables del inventario de los activos de información física y digital.
- Se debe revisar, actualizar y consolidar el inventario de activos de información mínimo con una periodicidad anual o cada vez que sea requerido.
- La Oficina TICS es la responsable de realizar el inventario de los activos de información como, software, hardware y servicios de TI adquiridos por IDIGER.

7.4.1 Control de acceso a centros de procesamiento de datos y centros de cableado

Se deben implementar controles de acceso a los activos de información, con el fin de otorgar acceso solo a personas autorizados, determinando mecanismos de protección y administración de los accesos tanto electrónicos como físicos. Así como, para el acceso al Centro de Procesamiento de Datos (CPD) principal o alterno y centros de cableado :

- Los CPD principal o alterno deberán permanecer cerrados y su ingreso o salida deberá ser a través de un sistema de autenticación biométrica (huella dactilar o lector de Iris ocular) y/o con tarjeta de proximidad.
- El acceso físico al CPD principal o alterno, así como a los centros de cableado debe contar con la aprobación del jefe de la Oficina TICS o el líder de Infraestructura.
- El acceso para visitantes y proveedores es restringido, por lo tanto, todo ingreso y salida de personas al CPD principal o alterno y centros de cableado, debe contar la debida autorización y ser registrada en una bitácora o planilla que identifique la fecha y hora de ingreso, nombre completo de la persona que visita el CPD principal, motivo de la visita, nombre de la persona que autoriza el ingreso, fecha y hora de salida y las

tareas realizadas. Lo anterior, como medida de control, trazabilidad y seguimiento a las actividades realizadas en estas áreas.

- No está permitido fumar e introducir alimentos o bebidas al CDP principal o alterno y centros de cableado.
- Las luces deben permanecer apagadas mientras no se encuentre personal dentro del centro de datos.

7.4.2 Control de Acceso a los Sistemas de información

Se restringirá el acceso a la información y a los sistemas de información, definiendo perfiles de acceso que apliquen al principio del menor privilegio necesario para que funcionarios, colaboradores y demás partes interesadas del IDIGER, puedan desempeñar las funciones o cumplir sus obligaciones contractuales, según sea el

caso, así como, poder individualizar los registros de acceso y la respectiva trazabilidad.

7.5 Acceso Remoto -VPN

La conexión remota a la red interna de IDIGER debe realizarse por medio de una conexión de VPN segura que será suministrada por el grupo de infraestructura de la Oficina TICS y solo tendrá acceso funcionarios y colaboradores autorizados, los cuales deben cumplir los lineamientos establecidos para el uso apropiado del servicio de VPN, teniendo en cuenta los siguientes lineamientos:

- Se asignará el servicio de VPN dependiendo de la disponibilidad de licencias.
- Solo funcionarios y colaboradores previamente autorizados podrán utilizar el servicio de VPN, los cuales serán los responsables del correcto uso del acceso remoto.
- El servicio de VPN solo debe utilizarse exclusivamente para labores relacionadas con las funciones o el cumplimiento de las obligaciones contractuales y se debe mantener la confidencialidad e integridad de la información a la cual se tiene acceso mediante la conexión remota.
- Para acceso al servicio del VPN se proporcionará a un funcionario o colaborador un usuario y contraseña, los cuales son de uso personal y no deben compartirse ni dejarlos a la vista de terceras personas.
- Transcurridos 10 minutos de inactividad, la sesión será desconectada automáticamente y el funcionario o colaborador deberá autenticarse nuevamente para acceder al servicio de VPN.

- En caso de que el funcionario o contratista detecte que una persona no autorizada haya utilizado sus credenciales de acceso o se presente algún problema de seguridad debe informar inmediatamente a la Oficina TIC.
- El IDIGER no se hace responsable por la pérdida de información, resultante de interrupciones en el servicio de internet contratado por el funcionario o colaborador, así como, por virus o mala configuración del computador o dispositivo que el colaborador acceda.
- Los funcionarios y colaboradores que no cumplan la política de acceso remoto (VPN) y los lineamientos para el servicio de VPN, se le bloqueará inmediatamente el acceso a este servicio.

7.6 Criptografía

Teniendo en cuenta el valor y criticidad de los activos de información, es preciso establecer controles que protejan la información respaldada y transmitida haciendo uso de la criptografía, a fin de proteger la confidencialidad de la información, teniendo en cuenta los siguientes lineamientos:

- Utilizar cifrado para proteger la información crítica ya sea en su medio de transmisión, procesamiento y almacenamiento.
- Hacer uso tokens, certificados SSL y firmas digitales para cifrar y/o proteger contra modificaciones no autorizadas de la información. Así mismo, estos medios de cifrado deben contar con la posibilidad de ser restaurados en caso de pérdida o hurto.
- Contar con cifrado mediante certificados SSL en lo referente sitios web de la Entidad.
- Contar con instructivos de recuperación de la información cifrada en caso de pérdida o destrucción de las claves.
- Los administradores de infraestructura y de sistemas de información deben usar una herramienta para la gestión de las contraseñas, así como, entregar en sobre sellado la clave maestra al jefe o supervisor, para que la custodie en lugar seguro dentro de la Entidad o un servicio de custodia de información externo a la Entidad, de tal forma que en un caso fortuito, con la supervisión de la Oficina de Control Interno, una tercera parte autorizada pueda tener acceso para poder descifrar los datos.
- Hacer uso de certificados SSL para los aplicativos que se encuentran expuestos a internet, así como para servicios internos que por su criticidad lo requieran.

7.7 Seguridad física y del entorno

Los visitantes deben acceder a las instalaciones del IDIGER mediante la aplicación del procedimiento de identificación en la recepción y deben ser recibidos por un funcionario o contratista para el acompañamiento obligatorio dentro de las instalaciones, atendiendo los lineamientos emitidos el área Administrativa.

El cumplimiento del procedimiento de control de acceso físico es responsabilidad de todos los funcionarios y colaboradores, asegurar el acompañamiento de sus visitantes en las instalaciones de la entidad.

- Las áreas donde se ejecutan procesos relacionados con información confidencial o restringida deben contar con controles de acceso que sólo permitan el ingreso a los funcionarios y/o colaboradores autorizados, así como dejar el respectivo registro del ingreso y salida.
- Los funcionarios y colaboradores que tienen acceso a las áreas restringidas son responsables de proteger las credenciales de acceso que se les ha conferido en custodia, así mismo, responder por los actos indebidos en los que se evidencie negligencia o descuido de sus credenciales de acceso.

7.7.1 Uso y ubicación de equipos de cómputo personales

- Los funcionarios, colaboradores y terceros que por sus labores requieren tener acceso a los recursos de información del IDIGER a través de sus computadores personales, deben aceptar las políticas y controles que se establezcan con el fin de proteger los activos de información a los cuales acceden.
- A los equipos de cómputo se les debe realizar mantenimientos periódicos gestionados por la Oficina de Tecnologías de la Información y las Comunicaciones.
- Los funcionarios y colaboradores que tengan a su cargo equipos de cómputo asignados por IDIGER, deben protegerlos contra la intemperie (humedad, altas temperaturas, polvo o excesiva polución) en especial aquellos que deban tener movilidad por motivos de sus funciones.
- Dentro de las instalaciones de IDIGER, los funcionarios y colaboradores con equipos de cómputo a su cargo, son responsables de la adecuada conexión a las tomas eléctricas reguladas, las cuales son diferenciadas por su color naranja.
- Los funcionarios y colaboradores no deben realizar ninguna alteración física de los componentes de los equipos de cómputo asignados a su cargo por

El IDIGER. Lo anterior, es solo permitido por el personal autorizado de la Oficina TIC.

- Los funcionarios y colaboradores no deben realizar cambios en la configuración de los equipos, como conexiones de red, funcionarios y colaboradores locales de la máquina y fondo de pantalla.
- Los equipos de cómputo de IDIGER deben tener credenciales de administrador (local o dominio) gestionada por la Oficina de TIC.
- Los equipos portátiles que se usan por fuera del IDIGER, solo deben utilizarse para el cumplimiento de las funciones o de las obligaciones contractuales y no pueden ser utilizados en actividades distintas a las antes mencionadas. Adicionalmente está prohibido la manipulación por terceros o personal no autorizado, a fin de alteración, pérdida o fuga de información.
- El funcionario y colaborador debe realizar copia permanente de toda la información, para que, en caso de pérdida o robo del equipo portátil, esta pueda ser de restaurada de manera más ágil. En caso de que se maneje información confidencial o sensible, el medio de almacenamiento debe estar cifrado.
- Los funcionarios y colaboradores no deben mantener almacenados en los discos duros de los equipos de cómputo o discos virtuales de red, archivos de video, música, fotos y cualquier tipo de archivo que no sean de carácter institucional. En caso de encontrarse estos tipos de archivos no institucionales en los discos virtuales de red, la Oficina TICS procederá a su eliminación.

- En caso de pérdida o robo de un equipo de cómputo del IDIGER, el funcionario o colaborador es responsable de instaurar la denuncia correspondiente ante la autoridad competente, e informar al almacén de acuerdo con el procedimiento establecido en el proceso de Gestión Administrativa.
- Los equipos de cómputo que se encuentren fuera de la red de datos de IDIGER deben contar con actualización constante del antivirus para evitar contagio y propagación de virus o software malicioso en la red de datos del IDIGER.
- No podrán conectarse a las tomas eléctricas reguladas (tomas color naranja) los equipos eléctricos o electrónicos como impresoras, fotocopiadoras, celulares y sus respectivos cargadores, aspiradoras, brilladoras, entre otros, diferentes a los equipos de cómputo o dispositivos de informática como equipos de red comunicaciones (Switches, access points, firewalls, balanceadores, entre otros), sensores electrónicos, equipos electrónicos de control de acceso. Lo anterior, con el propósito de evitar sobre cargas en el fluido eléctrico regulado que genere daños en los equipos de cómputo.

7.7.2 Protección física de los equipos servidores de cómputo, equipos de comunicaciones y sensores relacionados

Los equipos servidores de cómputo, equipos de comunicaciones y sensores relacionados deberán estar protegidos en un área adecuada para su correcto funcionamiento que como mínimo cuente con los siguientes controles:

- Se debe contar con un sistema de protección automático contra incendios.
- Es imprescindible contar con sistema de refrigeración que garantice las condiciones técnicas de funcionamiento emitidas por los fabricantes de los equipos servidores de cómputo, equipos de comunicaciones y sensores relacionados.
- Suministro de energía eléctrica regulada, así como con suministro temporal de energía eléctrica en caso de interrupción temporal del fluido eléctrico comercial.
- Aislamiento de humedad o impermeabilización techos y paredes expuestos a la humedad del medio ambiente respecto de las áreas físicas que alojan estos equipos.
- Control de humedad ambiental al interior áreas físicas que alojan estos equipos en cumplimiento de los requisitos de funcionamiento expedidos por los fabricantes.
- Contar con planes de mantenimientos periódicos de acuerdo con las recomendaciones de los fabricantes.

7.7.3 Escritorio y pantalla limpios

Esta política busca prevenir el acceso no autorizado, pérdida, daño o hurto de la información que se encuentra en los puestos de trabajo, equipos de cómputo, medios extraíbles, dispositivos de impresión y digitalización de documentos, durante y fuera del horario laboral, mediante lineamientos establecidos para que sean aplicados por los funcionarios y colaboradores.

- Conservar su escritorio físico limpio y organizado. Si en cumplimiento de sus funciones requiere manipular información física (carpetas, oficios, USB, entre otras) del IDIGER, solo podrá estar sobre el escritorio mientras se requiera y bajo la custodia y supervisión del funcionario o contratista autorizado de salvaguarda la información. Ante la ausencia del puesto de trabajo o finalización de la jornada laboral, el funcionario o colaborador deberá almacenarla en sitio seguro.
- Mantener el fondo de la pantalla libre de iconos y/o accesos directos innecesarios.

- Los equipos de cómputo, portátiles deben tener el fondo de pantalla y protector de pantalla institucional, este último se debe activar después de cinco minutos de inactividad.
- Proteger la información de uso diario, así como los elementos de procesamiento y demás fuentes de datos físicos.
- Una vez se impriman documentos, estos deben ser retirados inmediatamente de las impresoras.
- Realizar el bloqueo de pantalla en el equipo de cómputo cuando se retire de su puesto de trabajo.

7.8 Seguridad de las operaciones

Estas políticas buscan asegurar las operaciones realizadas en las instalaciones de procesamiento de información del IDIGER.

7.8.1 Lineamientos para uso adecuado de software

- No está permitido copiar software licenciado de la entidad para utilizar en sus computadores personales o en cualquier dispositivo diferente a los autorizados por IDIGER.
- No está permitido introducir programas maliciosos en las redes o en los servidores, virus informáticos, gusanos, troyanos, spyware, adware, puertas traseras, spam, phishing, pharming, ataques DDOS, keyloggers o cualquier otro tipo de malware.
- Se restringe la instalación de software en cualquier equipo o servidor de cómputo de la Entidad, sin contar con la autorización de la oficina TIC.

7.8.2 Lineamientos para puerto seguro de Red

- Todo puesto de trabajo que requiera el uso de equipos de cómputo contará con un punto de red. Sin embargo, solo se permite la conexión a la red de datos de IDIGER, a los equipos previamente validados por el área de soporte técnico de la oficina TIC.
- No se permitirá el traslado de equipos de cómputo de escritorio sin la autorización de la Oficina TIC, la cual evaluará la viabilidad del traslado y la logística para que su respectiva configuración y punto de red en la nueva ubicación.
- De identificarse la conexión de un equipo que no haya sido validado por la oficina TIC, el punto de acceso se inhabilitará por seguridad.

7.8.3 Respaldo de la Información

Es importante realizar copias de respaldo de la información y recursos críticos de acuerdo con su clasificación y garantizar las medidas de protección adecuadas, dependiendo de la criticidad de los activos de información identificados. Para ello, son importantes los siguientes lineamientos:

- Realizar copias de seguridad sobre los activos de información que se consideren necesarios de acuerdo con su criticidad.
- Asegurar mediante medios tecnológicos o manuales de verificación, que la copia pueda se restaurada de forma completa y oportuna en caso de que esta actividad sea requerida.
- Definir e implementar procedimientos y herramientas tecnológicas necesarias para el respaldo de la información.
- Dependiendo de la valoración del activo de información se recomienda cifrar la copia de seguridad con el fin de velar por el principio de confidencialidad.
- Los dispositivos usados para el respaldo de la información deben ser monitoreados para mantener el correcto funcionamiento de la plataforma.

7.8.4 Gestión de cambios de TI

La administración y gestión de cambios de TI en el IDIGER debe contar con responsables, procedimientos y controles de seguridad de la información donde se tenga en cuenta la criticidad de la información, servicios, sistemas y procesos involucrados, asegurando una gestión rápida, eficaz y ordenada de las actividades a desarrollar, atendiendo los siguientes lineamientos:

- Todo cambio que se realice en los activos de información como software, hardware y servicios de red, deberá ser gestionado por la Oficina TIC, garantizando que los cambios solicitados han sido evaluados, autorizados,

  probados, aceptados con la finalidad de evitar impactos negativos en la operación la infraestructura y/o sistemas de información.
- Todas las solicitudes de cambios deberán quedar registrados y documentados a través de la mesa de servicios de la Entidad.
- Mediante un comité de cambios multidisciplinario se realizará la evaluación de las solicitudes de cambio, el cual utilizará criterios como oportunidad, prioridad y criticidad del servicio al cual afecta.
- Los cambios programados deberán ser comunicados con la debida oportunidad a los funcionarios y colaboradores del IDIGER.

- Es preciso establecer las acciones a realizar para la gestión de cambios de TI ante la necesidad de un cambio de emergencia.
- Los cambios normales y cambios de emergencia deberán contar la debida planificación, el detalle del impacto que genera, planes de rollback y medición de inactividad.

7.8.5 Desarrollo seguro

La seguridad de la información debe ser parte integral de los Sistemas de Información y aplicaciones durante todo el ciclo de vida (diseño, desarrollo, pruebas e implementación). En el IDIGER los ambientes dispuestos son: Producción Desarrollo y Pruebas.

- Se debe contar con los tres ambientes diferenciados claramente en cuanto a servidores de aplicaciones y Bases de Datos.
- Se debe proteger cada uno de los computadores, dispositivos de red y de comunicaciones que se consideren críticos por intervenir directamente en el ambiente de producción, del acceso físico de personal no autorizado, para garantizar la confidencialidad, disponibilidad e integridad de la información.
- Los accesos al ambiente de producción deben ser restringidos por segregación de funciones y permisos de administrador de cada ambiente.

7.8.6 Seguridad Aplicable a Logs

Es responsabilidad de la Oficina TICS asegurar que se generen logs, especialmente para los equipos y aplicaciones calificados como críticos, dichos logs deben ser custodiados en forma segura para evitar su modificación.

7.8.7 Seguridad de las comunicaciones

Esta política busca que los funcionarios y colaboradores del IDIGER, realicen el uso adecuado de la información gestionada en los servicios contenidos en la red; el acceso a Internet responde a la utilización de una herramienta de uso estrictamente laboral. Para estos efectos, cualquier propósito ajeno a las funciones estrictamente laborales serán restringidas.

- Los privilegios de uso de Internet estarán definidos de acuerdo con la necesidad de acceso que requiera el desarrollo de la labor de los funcionarios y colaboradores del IDIGER y que se encuentren acordes con los procesos que gestionan, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información.

- Los funcionarios y colaboradores no pueden asumir en nombre del IDIGER, posiciones personales en encuestas de opinión, foros u otros accesos web similares.
- Está estrictamente prohibido el ingreso a Páginas Web con contenido que se considere inapropiado, ofensivo, ilegal o que pueda atentar contra la seguridad de la información.
- Los funcionarios y colaboradores no deben descargar ningún programa o software, sin la debida autorización de la Oficina TIC.
- Cualquier cambio o excepción deberá estar soportado y con las aprobaciones respectivas.
- Mantener habilitada en los navegadores de internet la restricción de no ejecución de scripts de forma automática.
- Los funcionarios y colaboradores antes de ingresar credenciales de acceso en un sitio web deben verificar que la "URL" o dirección web inicie con "https" o se visualice el ícono de candado.
- Los funcionarios y colaboradores no deben visitar sitios web sospechosos o los que el antivirus presente alerta de inseguridad.

7.9 Política de Uso de Correo electrónico

No está permitido el uso de correo electrónico institucional para asuntos diferentes a los relacionados con las funciones u obligaciones del área de desempeño, teniendo en cuenta los siguientes lineamientos:

- Todos los mensajes enviados por medio de correo electrónico pertenecen a IDIGER, el cual se reserva el derecho de acceder y revelar los mensajes enviados por este medio para cualquier propósito.
- Está prohibido a los funcionarios y colaboradores el envío de mensajes masivos a través de correo electrónico; este tipo de mensajes solo puede ser enviado por funcionarios y colaboradores debidamente autorizados, como el Director General, subdirectores y/o jefes de oficina o quien sean autorizados.
- Es responsabilidad del funcionarios y colaboradores enmarcar todos los mensajes que envíe a través de correo electrónico dentro de las normas mínimas de respeto y protocolo electrónico, sin incluir contenidos hostiles que molesten a los receptores del mismo, tales como comentarios sobre sexo, raza, religión o preferencias sexuales, tendencia política entre otras que generen algún tipo de discriminación; así mismo, es responsabilidad de los funcionarios y colaboradores reportar al Jefe de área la recepción de este tipo de mensajes, quien a su vez deberá reportarla al área que corresponda, con copia a la Oficina TICS, en caso de comprometer la seguridad de la información de la entidad.

- Es responsabilidad de los funcionarios y colaboradores evitar que su cuenta de correo electrónico sea utilizada por terceros.
- Es responsabilidad del funcionario y colaborador evitar que la información confidencial y/o sensible sea transmitida por medio de su cuenta de correo electrónico, salvo autorización previa y escrita del dueño de la información, un subdirector o un jefe de oficina, en cuyo caso los archivos deben viajar en forma Segura (encriptados).
- Es responsabilidad de los funcionarios y colaboradores de correo electrónico mantener o archivar los mensajes enviados y/o recibidos para efectos de soportar ante terceros (internos o externos) la ejecución de operaciones o acciones.
- La cuenta de correo electrónico institucional asignada a funcionarios y colaboradores, solo podrá ser utilizada para el desempeño de las funciones o el cumplimiento de las obligaciones contractuales.
- Las cuentas personales de correo electrónico en plataformas gratuitas (Yahoo, Hotmail, Outlook etc.), deben estar bloqueadas en los equipos de la Entidad. Las excepciones para hacer uso de correo personal deben ser documentadas y justificadas.
- Las funcionarios y colaboradores no deberán abrir links que se incluyan en correos electrónicos que generen sospecha de la autenticidad de su remitente.
- Las funcionarios y colaboradores no deberán descargar adjuntos de correos que generen sospecha de la autenticidad de remitente.
- Los administradores deben hacer uso de un estándar para la creación de los nombres de correo electrónico haciendo uso de la primera letra del primer nombre seguido del primer apellido. En el caso que se encuentre repetido se debe hacer uso de las dos primeras letras del primer nombre seguido del primer apellido. Ejemplo Si la persona se llama Juan García el correo sería jgarcia@idiger.gov.co, en el caso que ya exista el usuario sería jugarcia@idiger.gov.co.

7.10 Relación con los proveedores

Asegurar la protección de los activos del IDIGER también involucra la relación con los proveedores, por ello es importante que éstos identifiquen y conozcan los requisitos y riesgos de seguridad de la información asociados a su interacción en la entidad de acuerdo con los siguientes lineamientos:

- Durante la Etapa Precontractual, específicamente en la construcción de los estudios previos el director/jefe/coordinador/líder de la dependencia

interesada en la contratación deberá identificar los riesgos de seguridad de la información los cuales serán parte de la estimación y cobertura de los riesgos del proceso de contratación.

- El análisis de riesgos de seguridad de la información debe incluir la identificación de estos en la respectiva contratación, su clasificación, probabilidad de ocurrencia estimada, su impacto, la determinación de la parte que debe asumirlos, el tratamiento que se les debe dar para eliminarlos o mitigarlos y las características del monitoreo más adecuado para administrarlos.
- Durante la estructuración de estudios previos se debe identificar sí el objeto de la propuesta u oferta evaluada, requiere del acceso de los proveedores a la información, sistemas de información y/o áreas seguras de la entidad.
- Durante la estructuración de estudios previos se debe realizar la inclusión de una cláusula de confidencialidad, protección de datos, derechos de propiedad intelectual y derechos de autor.
- Determinar los requisitos mínimos de seguridad y los controles necesarios por parte de los proveedores para ejecutar el contrato.
- Dar a conocer a los proveedores interesados, las políticas de seguridad de la información.
- Durante la Etapa Post Contractual, será obligación del supervisor y/o interventoría asignada, hacer seguimiento a los controles establecidos durante la etapa precontractual y contractual para asegurar la confidencialidad, integridad y disponibilidad de la información, frente a los riesgos previamente identificados.
- Para los servicios de tecnología y de comunicaciones tercerizados, se debe exigir a los proveedores que divulguen sus requisitos y prácticas de seguridad, a lo largo de la cadena de suministro.
- Para la contratación de servicios o componentes de la infraestructura de TI y/o áreas seguras, se debe exigir a los proveedores la presentación de los planes de continuidad de negocio que aseguren la disponibilidad de la información, suministrada y procesada entre las partes.

7.11 Gestión de incidentes de seguridad

El IDIGER atiende la gestión de incidentes de seguridad de la información, reportados a través de la mesa de servicio. Una vez es escalado a la oficina TIC, procederá a la identificación, detección y análisis de causas para proceder a su inmediato tratamiento y aplicación de contramedidas, hasta que sea neutralizada la amenaza.

8. Excepciones a las Políticas Complementarias de Seguridad de la Información

Cualquier excepción requerida por los funcionarios y colaboradores de la entidad a la presente política, deberá estar justificada, documentada y autorizada por los jefes o supervisores. Estas excepciones deben ser revisadas periódicamente para garantizar su adecuado uso y serán monitoreadas por la Oficina TICS a través de los encargados de seguridad de la Información.

9. Cumplimiento de requisitos legales y Propiedad Intelectual

- El IDIGER velará por la identificación, documentación y cumplimiento de la legislación aplicable y requisitos contractuales concernientes a la seguridad de la información.
- Los funcionarios y colaboradores deben mantener estricta reserva y confidencialidad sobre la información que conozca por causa o con ocasión del cumplimiento de sus obligaciones o funciones, así como, respetar la titularidad de los derechos de autor, en relación con los documentos, obras, creaciones que se desarrollen en su labor y que son propiedad exclusiva de IDIGER.
- Los funcionarios y colaboradores son responsables de hacer entrega de los equipos de cómputo y demás activos relacionados que le fueron entregados en el estado en que los recibió, salvo el deterioro normal, o daños ocasionados por caso fortuito o fuerza mayor generados en cumplimiento de las funciones que le fueron asignadas. La Oficina TICS propenderá porque el software instalado en los equipos de cómputo del IDIGER, este debidamente licenciado, cumpliendo con los derechos de autor o que el mismo sea de libre distribución y uso.

9.1 Tratamiento de datos personales

El IDIGER cuenta con la Política de Tratamiento de Datos Personales cuyo objetivo es "*Establecer una política con los criterios para la recolección, almacenamiento, uso, circulación y supresión de los datos personales tratados por Instituto Distrital De Gestión de Riesgos y Cambio Climático – IDIGER, garantizando la privacidad y seguridad de los mismos, dando cumplimiento a Ley 1581 de 2012 y sus decretos reglamentarios*"[3]

[3] https://www.idiger.gov.co/politica-de-privacidad-y-condiciones-de-uso

10. Revisión de Seguridad de la Información

El Manual de políticas de Seguridad de la información será revisado una vez al año, o en caso de que se requiera, debido a nuevas disposiciones legales que apliquen o con el fin de asegurar su eficiencia y efectividad, por lo tanto, cualquier modificación será informada a los funcionarios, colaboradores y demás partes interesadas, utilizando los medios que se considere pertinentes para garantizar su divulgación.