ALCALDÍA MAYOR
DE BOGOTÁ D.C.
AMBIENTE
Instituto Distrital de Gestión de Riesgos y Cambio Climático

# Manual de Políticas de Seguridad de la Información

CODIGO: TICS–MA-2
Versión 2

## TABLA DE CONTENIDO

## Dependencia

Oficina TIC

## Proceso

TIC's Para la Gestión del Riesgo

## Objetivo

Definir las políticas y lineamientos para la Seguridad de la Información en el Instituto Distrital de Gestión de Riesgos y Cambio Climático – IDIGER

## Alcance

Este manual aplica a funcionarios, contratistas y demás partes interesadas, que en ejercicio de sus funciones o en el cumplimiento de sus obligaciones contractuales, según el caso, tengan acceso a los activos de información de la entidad.

22/07/2019

## 1. Introducción

De conformidad con lo establecido en el Decreto Único Reglamentario 1078 de 2015 del Sector de Tecnologías de la Información y las Comunicaciones, el Decreto 1008 de 2018 de la Política de Gobierno Digital, emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, la Ley 1581 de 2012 de Protección de Datos Personales, el Decreto Único Reglamentario 1074 de 2015, Capítulo 25, el Documento CONPES 3854 de 2016 en donde se establece la Política Nacional de Seguridad Digital, el Decreto 1499 de 2017 que reglamentó el Sistema Integrado de Planeación y Gestión y actualizó el Modelo Integrado de Planeación y Gestión – MIPG, como parte de la normatividad legal vigente y las buenas prácticas de seguridad de la información, basadas en la Norma NTC ISO/IEC 27001/2013, la adopción del Modelo de Seguridad y Privacidad de la Información y la Política de Seguridad y Privacidad de la Información del Instituto Distrital de Gestión de Riesgos y Cambio Climático –IDIGER, se elabora el Manual de Políticas de Seguridad de la Información que define las políticas y lineamientos para la seguridad de la información, manteniendo la confidencialidad, integridad, disponibilidad y privacidad de los activos de información que están bajo la gestión y custodia de la entidad.

Las políticas y lineamientos incluidos en el presente manual serán divulgados y deberán ser adoptados por los funcionarios, contratistas y demás partes interesadas que en ejercicio de sus funciones o en el cumplimiento de sus obligaciones contractuales, según el caso, tengan acceso a los activos de información de la entidad.

La Seguridad de la Información es una prioridad para IDIGER, por lo tanto, es responsabilidad de todos velar porque no se realicen actividades que vayan en contra del fundamento de cada una de estas políticas y lineamientos.

## 2. Definiciones

- **Activo de Información:** Es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección.[1]
- **Confidencialidad:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.[2]
- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.[3]
- **Fuga de Información:** Incidente de seguridad que pone información confidencial de la entidad en manos de terceros, los cuales no deberían tener acceso a la misma. Este incidente puede ser tanto interno como externo y puede ser intencional o no.
- **Información:** Conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.[4]
- **Integridad:** Consiste en asegurar o salvaguardar que el activo de información cuente con las propiedades de: exactitud, precisión, consistencia, confiabilidad y totalidad
- **Medio Extraíble:** Dispositivo que permite almacenar o transportar información como memorias USB, tarjetas de memoria, cintas magnéticas, CD, DVD, discos duros externos

## 3. Tipos de Ataques y Atacantes

- **Hoax (correos falsos).-** Es un mensaje de correo electrónico con contenido falso o engañoso. Normalmente es distribuido en cadena por sus sucesivos receptores debido a su contenido impactante, a que parece provenir de una fuente seria y fiable o porque el mismo mensaje pide ser reenviado.

[1] Tomado de la NTC-ISO-IEC 27000
[2] Ibídem
[3] Ibídem
[4] Tomado de la Ley 1712 de 2014

- **Phishing (Pesca).-** Es el acto de pescar usuarios mediante señuelos y de este modo obtener información financiera y contraseñas para intentar adquirir información confidencial de forma fraudulenta.

- **Spoofing (suplantación de identidad).-** Es una técnica que consiste en hacer creer al receptor de un mensaje de correo electrónico, que quien remite el mensaje es alguien de confianza. El verdadero emisor queda suplantado por una dirección real, que ofrece garantías al receptor, que abrirá ingenuamente el mensaje sin conocer los verdaderos motivos (ocultos).

- **Spammers.-** Correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido; habitualmente de tipo publicitario, enviados en grandes cantidades que perjudican de alguna o varias maneras al receptor.

- **Spamblock.** Texto que se inserta en una dirección de correo electrónico ocultando la verdadera dirección, cuyo objetivo es burlar a los spammers. Por ejemplo, si mi dirección de correo es grupo@compañiaf.com.co, mediante esta técnica se puede transformar en grupo@rcompañiaf.com.co.

- **Crimeware.-** Es un software diseñado específicamente para cometer delitos financieros en entornos en línea, técnicas mediante la ingeniería social u otras técnicas genéricas de fraude en línea. El objetivo es robar identidades en línea para acceder a los datos financieros de un usuario, con el fin de obtener los fondos de dichas cuentas, o de completar transacciones no autorizadas por su propietario legítimo, que enriquecerán al ladrón que controla el crimeware.

- **Malware (Software malicioso).-** Es un tipo de software que tiene como objetivo infiltrarse o dañar un Pc sin el consentimiento de su dueño.

- **Virus.-** Es un software que se copia por sí mismo, infecta un Pc, se propaga dentro de todo los archivos, luego se copia de Pc a Pc; estos virus se adhieren en archivos específicos (de arranque, script, macros o ejecutables); el fin de este software es alterar o corromper el funcionamiento normal de un Pc.

- **Spyware.-** Es un software cuyo objetivo es mandar información a un tercero de toda las páginas visitadas; el fin es espiar y recabar información de las páginas a las cuales fueron visitadas (incluyen claves de cuenta, correos, etc.) para luego en lo posterior, enviar o saturar de publicidades. La recolección de esta información es mediante un canal falso, produciendo un consumo de ancho de banda de internet y a su vez poniendo lento el computador.

- **Gusano.-** Es un software cuyo único cometido radica en pasar de Pc en Pc a través de redes informáticas en forma automática sin la intervención de ningún

usuario; estos normalmente buscan traspasar los agujeros de seguridad para infectar toda la red a su alcance.

- **Adware.-** Se trata de un software que permite publicidad no deseada vía Internet y que generalmente se instala sin nuestro consentimiento.
- **Scareware (Software de miedo).-** Es un software que engaña a un usuario para descargar un programa haciendo creer que está infectado de virus; es un método de estafa para hacer comprar un software utilizando prácticas comerciales poco éticas.
- **Caballo de Troya.-** Es un software inocente que contiene códigos escondidos que permiten la modificación no autorizada y la explotación o destrucción de la información. Los troyanos se distribuyen por Internet, juegos, protectores de pantalla y crack de programas.
- **Botnet.-** Son redes de computadoras infectadas, también llamadas "zombies", que pueden ser controladas a la vez por un individuo y realizan distintos ataques (envío masivo de spam o para lanzar ataques DDos). El fin de este ataque puede ser de extorsión, impedir su correcto funcionamiento, etc.
- **Rogue software.-** Software que hace creer al usuario que la computadora está infectada por algún tipo de virus u otro tipo de software malicioso; esto induce al usuario a pagar por un software inútil o a instalar un software malicioso que supuestamente elimina las infecciones, pero el usuario no necesita ese software puesto que no está infectado.
- **Hijacking.-** Es una técnica ilegal que tiene por objetivo el adueñarse o robar (TCP/IP, página web, dominio, navegadores, módems, temas de foros, sesiones de terminal, servicios etc.) mediante una conexión de red.
- **Carding.-** Uso ilegítimo de las tarjetas de crédito ajenas, generar números de tarjetas de crédito y cualquier otra actividad ilegal relacionada con las mismas.
- **Trashing.-** Se trata de buscar en la basura (física o informática) información que pueda ser útil para realizar fraudes, copias, suplantaciones, etc.
- **Graffiti.** Modificación que un hacker hace de la página web de un servidor para evidenciar la falta de protección de un sistema.
- **Defacement.-** Hace referencia a la deformación o cambio de manera intencionada a una página web, ya sea por venganza, diversión o burla; esto se debe a algún error de programación de la página por algún bug en el propio servidor o por una mala administración de este.

- **Phreaking.-** Son individuos que orientan sus estudios u ocio hacia el aprendizaje y comprensión del funcionamiento de teléfonos de diversa índole, tecnologías de telecomunicaciones, funcionamiento de compañías telefónicas y sistemas que componen una red telefónica, electrónica aplicada a sistemas telefónicos.

- **Cracker.-** Son individuos que se dedican a desproteger programas, como evitar tener que pagar las licencias de los mismos, comprar una copia y usarla en 20 puestos simultáneamente.

- **Hacker.-** Persona que es capaz de eludir los sistemas de seguridad de un computador para acceder a la información que contiene ya sea con fines maléficos o benéficos.

- **Hacktivista.-** Persona especialista que se moviliza con conocimientos informáticos contra la mundialización, las multinacionales y en defensa de los internautas.

- **Ankle-Biter (packet-monkeys, script kiddies o crashers)** Son personas que indagan por la red ya sea por diversión o pasatiempo para realizar ataques sólo para divertirse, sin importar quién los recibe.

- **Rootkit** es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers que consiguen acceder ilícitamente a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos.

## 4. Política General 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.

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración del Instituto Distrital de Gestión de Riesgos y Cambio Climático – IDIGER con respecto a fortalecer los niveles de seguridad de la información y la protección de los activos de información que soportan los procesos de la entidad y apoyan la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI alineado con el Sistema de Gestión de Seguridad de la Información - SGSI, mediante la generación y publicación de políticas, procedimientos, guías e instructivos, al igual, que la asignación de responsabilidades para la gestión de la

seguridad de la información y generar una cultura en seguridad y privacidad al interior de la entidad.[5]

## 5. Organización de la Seguridad de la Información

### 5.1 Organización Interna

El IDIGER debe definir una estructura organizacional con las funciones y responsabilidades para la ejecución de las actividades de operación, gestión y administración de la seguridad de la información, alineado al Modelo de Seguridad y Privacidad de la Información - MSPI y la Norma NTC ISO/IEC 27001:2013

La Oficina TIC debe identificar las autoridades a contactar para reportar de manera oportuna un incidente de seguridad de la información que lo amerite. Así mismo, debe mantener contactos apropiados con grupos de interés especial relacionados con la seguridad de la información que aporten a la identificación de riesgos.

#### 5.1.1 Roles y Responsabilidades

Todos los funcionarios, contratistas y demás partes interesadas del IDIGER son responsables de la seguridad de la información; adicionalmente, se establecen los siguientes roles y responsabilidades[6]

| Rol | Responsable | Responsabilidades |
|---|---|---|
| Comité Institucional de Gestión y Desempeño | Líderes de Proceso | Conforme a lo establecido en MIPG tiene la responsabilidad de impulsar la implementación del Modelo de Seguridad y Privacidad de la Información alineado al Sistema de Gestión de Seguridad de la Información - SGSI en el IDIGER, además de realizar el seguimiento y /o verificación de la implementación del mismo. |
| Oficina TIC | Director TI | Será el responsable del funcionamiento del Modelo de Seguridad y Privacidad de la Información - MSPI alineado con el Sistema de Gestión de Seguridad de la Información – SGSI. |

[5] Documento de Política de Seguridad y Privacidad de la Información
[6] Ibídem

| Rol | Responsable | Responsabilidades |
|---|---|---|
| Oficial de Seguridad | Gestor de la Oficina TIC | Tendrá la responsabilidad de coordinar la implementación y cumplimiento del Modelo de Seguridad y Privacidad de la Información – MSPI alineado con el Sistema de Gestión de Seguridad de la Información - SGSI |
| Propietario | Director, Subdirector o Jefe de Oficina | Serán los responsables de la gestión apropiada del activo de información, como clasificar y definir la criticidad del mismo. |
| Custodio | Funcionario o contratista de una oficina o subdirección específica | Serán los responsables de administrar y hacer efectivos los controles y clasificaciones definidos por el propietario. |
| Usuario | Funcionario, contratistas y/o terceros autorizados para utilizar la información en el ejercicio de sus funciones o en el cumplimiento de sus obligaciones contractuales o vigencia del respectivo contrato | Serán los responsables del buen uso de los activos de información durante el cumplimiento de sus labores o compromisos, según de quien se trate. |

# 6. Gestión de Activos de Información

## 6.1 Política de Gestión de Activos de Información

Identificar todos los activos asociados con la información y las instalaciones de procesamiento de información con los que cuenta la entidad, con el fin de clasificarlos y protegerlos de una forma adecuada de acuerdo a su importancia y establecer los criterios y lineamientos para el tratamiento de los mismos.

## 6.2 Responsabilidad sobre los Activos de Información

- 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 a 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 los mismos, con el fin de determinar los controles para disminuir el impacto que pueda producirse.

- Todos los funcionarios y contratistas serán responsables de proteger la información a la cual accedan o procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
- Cada usuario es responsable de dar uso adecuado y en ningún momento el activo de información puede ser usado para realizar prácticas ilícitas o malintencionadas que atenten contra terceros o afecten a la entidad.
- Los funcionarios y contratistas 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 de la subdirección u oficina a la que pertenece o a quién 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.
- Se debe revisar, actualizar y consolidar el inventario de activos de información mínimo con una periodicidad anual o cada vez que sea requerido.
- El área de inventario gestión documental o quién que haga sus funciones es el responsable del inventario de los activos de información física y digital
- La Oficina TIC es el responsable del inventario de los activos de información de software, hardware y servicios.
- La actualización y consolidación del inventario de activos de información debe ser publicado en el sitio web http://www.idiger.gov.co/

## 6.3 Lineamientos para Uso Adecuado de Software

Los funcionarios y contratistas no deben:

- Copiar software licenciado de la entidad para utilizar en sus computadores personales o en cualquier dispositivo diferente a los autorizados por IDIGER.
- Introducir programas maliciosos en las redes o en los servidores (ejemplo: virus informáticos, gusanos, troyanos, spyware, adware, puertas traseras, spam, phishing, pharming, ataques DDOS, keyloggers o cualquier otro tipo de malware).
- Instalar software no autorizado por IDIGER, en cualquier equipo de cómputo o servidor de la entidad, sin autorización del jefe de la oficina TIC o el coordinador del área de Infraestructura TIC.

## 6.4 Lineamientos para el Uso de Equipos de Cómputo

- Los usuarios[7] no deben realizar ninguna alteración física de los componentes de los equipos de cómputo.

[7] Funcionarios y contratistas que utilizan los recursos informáticos para el cumplimiento de sus funciones o de sus obligaciones contractuales, según el caso

- Los usuarios no deben realizar cambios en la configuración de los equipos, como conexiones de red, usuarios locales de la máquina y fondo de pantalla.
- Los equipos portátiles siempre deben ser transportados como equipaje de mano, evitando golpes, exponerlo a líquidos, y prevenir la pérdida y/o hurto de los mismos
- Los equipos deben tener credenciales de administrador (local o dominio) para evitar instalaciones no autorizadas.
- Los equipos portátiles que se usan por fuera de la entidad, sólo 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 no pueden ser expuestos para que sean utilizados por terceros, a fin de evitar fuga de información.
- El usuario debe realizar back-up 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 disco duro del equipo debe estar cifrado
- Los usuarios no deben mantener almacenados en los discos duros de los equipos de cómputo o discos virtuales de red, archivos de vídeo, 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 TIC procederá a su eliminación.
- En caso de pérdida o robo de un equipo de cómputo del IDIGER, el usuario responsable debe instaurar la denuncia correspondiente ante la autoridad competente, e informar al Almacén de acuerdo al procedimiento establecido en el proceso de Gestión Administrativa.
- Los equipos de cómputo deben contar con actualización constante del antivirus para evitar contagio y propagación de virus o software malicioso en la red de datos del IDIGER.

## 6.5 Clasificación de Información

Se debe asegurar que la información reciba un nivel apropiado de protección, de acuerdo con la importancia para la entidad, se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

## 6.6 Medios de Almacenamiento

El IDIGER evitará que la información que se encuentre en los medios de almacenamiento dispuestos para tal fin, quede expuesta y pueda llegar a terceros no autorizados, al igual que se modifique, elimine o destruya sin autorización.

### 6.6.1 Medios de Almacenamiento Extraíbles

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 un incidente seguridad.
Los equipos de cómputo 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, contratista o tercero autorizado que utilice medios de almacenamiento extraíbles con información del IDIGER, será responsable del buen uso, divulgación y distribución de la misma.
- En caso de pérdida de un medio de almacenamiento extraíble debe informarse a la Oficina TIC, informando la criticidad de la información
- 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.

### 6.6.2 Borrado Seguro de Información en Dispositivos de Almacenamiento

Se aplicará un método de borrado seguro de información o formateo de bajo nivel, cuando los dispositivos de almacenamiento se vayan a dar de baja de inventarios, reciclar y/o donar, adicionalmente, los dispositivos en los que en algún momento se almacenó información sensible y/o confidencial con el fin de evitar que la información quede expuesta y pueda llegar a terceros no autorizados. Por lo tanto, se debe documentar mediante un informe donde se indique cómo, dónde, cuándo y por qué se realizó el borrado seguro en estos dispositivos para llevar la trazabilidad del ciclo de vida de la información desde el punto de vista de la seguridad de la información.
Para los equipos de cómputo que hayan sido rentados o cualquier otro tipo de contratación externa que almacene información confidencial de la entidad, se debe incluir una cláusula contractual en donde se indique que una vez liquidado el contrato, se deberá certificar que la información almacenada queda destruida de manera segura e irreversible.

## 7. Control de Acceso

### 7.1 Acceso al Centro de Procesamiento de Datos (CPD)/Data Center Principal y al Rack de Comunicaciones

- El CPD principal deberá permanecer cerrado y su ingreso o salida deberá ser a través de un sistema de autenticación biométrica (huella dactilar) y/o con tarjeta de proximidad.
- El acceso físico al CPD y a los rack de comunicaciones debe contar con la aprobación del jefe de la oficina TIC 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, debe 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, visto bueno de la persona que autoriza el ingreso, fecha y hora de salida y las tareas realizadas, como medida de control y seguimiento a las actividades realizadas en esta área.
- No está permitido fumar e introducir alimentos o bebidas en el centro de procesamiento de datos
- Las luces deben permanecer apagadas mientras no se encuentre personal dentro del centro de datos.

### 7.2 Política de 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 el principio del menor privilegio necesario para que funcionarios, contratistas y demás partes interesadas del IDIGER, puedan desempeñar las funciones o cumplir sus obligaciones contractuales, según sea el caso.

### 7.3 Política de 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 área de infraestructura de la Oficina TIC y solo tendrán acceso usuarios autorizados, los cuales deben cumplir los lineamientos establecidos para el uso apropiado del servicio de VPN.

### 7.3.1 Lineamientos para el Servicio de VPN

#### 7.3.1.1 Solicitud de Acceso al Servicio de VPN

El servicio de VPN debe ser solicitado por el jefe inmediato o el supervisor del contrato y tramitado por ARANDA, donde se incluya el nombre completo del usuario que va a utilizar el servicio, área de trabajo, correo institucional del usuario, una breve descripción de las necesidades del acceso remoto, y la fecha límite que debe estar activo el servicio (para contratistas no debe superar el tiempo de la prestación de servicios.

#### 7.3.1.2 Condiciones de Uso del Servicio de VPN

- Se asignará el servicio de VPN dependiendo de la disponibilidad de licencias
- Sólo usuarios previamente autorizados podrán utilizar el servicio de VPN, los cuales serán los responsables del correcto uso del acceso remoto.
- El IDIGER sólo proveerá la habilitación del servicio de VPN y el usuario correrá con los gastos adicionales que se genere para hacer uso de éste servicio, como por ejemplo la contratación de un servicio de internet.
- 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 un usuario y una 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 usuario deberá autenticarse nuevamente para acceder al servicio de VPN.
- En caso que el usuario detecte que una persona no autorizada haya utilizado sus datos 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 del proveedor del usuario, por virus o mala configuración del computador o dispositivo con el que accede.
- Los usuarios que no cumplan la política de acceso remoto (VPN) y los lineamientos para el servicio de VPN, se les bloqueará inmediatamente el acceso a este servicio.

#### 7.3.1.3 Recomendaciones para el Uso del Servicio de VPN

- El computador o dispositivo con el que va a iniciar la conexión debe tener instalado un firewall o cortafuegos, antivirus actualizado, aplicaciones y sistema operativo actualizado, además debe estar configurada la activación automática del protector de pantalla con la contraseña de entrada, para que en caso de dejar abierta la sesión de manera involuntaria se pueda evitar el acceso al equipo por personal no autorizado.
- No usar el servicio de VPN en caso de que el computador o dispositivo con el que va a iniciar la conexión se encuentre infectado por virus o cualquier amenaza informática.
- El servicio de VPN no debe utilizarse desde computadores públicos y redes no confiables como cafés internet o redes inalámbricas públicas.
- En caso de pérdida o robo del equipo con el que accede al servicio de VPN, debe informar lo más pronto posible a la Oficina TIC para bloquear la cuenta de acceso asignada.
- Cerrar sesión y desconectarse del servicio de VPN una vez finalizadas las labores realizadas en la conexión remota.
- En caso de presentar algún inconveniente con el uso del servicio de VPN, debe reportarlo al área de infraestructura de la Oficina TIC.

#### 7.3.1.4 Suspensión o Eliminación del Acceso al Servicio de VPN

- El jefe o supervisor de contrato mediante un ARANDA debe solicitar la suspensión o eliminación del servicio de VPN con la respectiva justificación.
- El usuario que no utilice el servicio de VPN durante un periodo de tiempo de 2 meses consecutivos, se le suspenderá el acceso y la Oficina TIC notificará dicha suspensión mediante correo electrónico al usuario y al jefe o supervisor de contrato. En caso de no tener alguna comunicación de activación del acceso durante el mes siguiente a la notificación se eliminarán los datos de acceso al servicio de VPN.
- En caso de eliminarse los datos de acceso al servicio de VPN por inactividad o solicitud expresa y el usuario requiere nuevamente el servicio de VPN, se debe realizar nuevamente la solicitud.
  Si el usuario se desvincula de la entidad, se eliminarán los datos de acceso al servicio de VPN.

## 7.4 Equipos

### 7.4.1 Ubicación y Protección de los Equipos

- Los funcionarios, contratistas y demás partes interesadas no deben mover o reubicar los equipos de cómputo del IDIGER, al igual que instalar o desinstalar dispositivos sin la autorización del área de Infraestructura Tecnológica de la Oficina TIC
- Se debe atender las recomendaciones del fabricante del equipo, referente a la protección física y ambiental del mismo, p.ej. contra la exposición de campos electromagnéticos muy fuertes.
- Se debe realizar periódicamente pruebas de operación de las UPS, previamente programadas y en un horario que no afecte la disponibilidad de los recursos de información del IDIGER. Estas pruebas deben ser documentadas como medida de control y seguimiento.
- Para los equipos portátiles, si la conexión a internet se realiza desde otro lugar que no sea la red inalámbrica o alámbrica de la entidad, se debe realizar la conexión a través de un protocolo seguro (red inalámbrica con seguro WPA, WPA2, etc.).
- Se debe realizar mantenimiento trimestral y/o semestral a las plantas eléctricas instaladas en IDIGER. Esta actividad se debe programar de manera coordinada entre la Oficina TIC y Subdirección Corporativa. Al final de cada mantenimiento la empresa contratada para tal efecto, debe entregar un informe de la labor realizada.

### 7.4.2 Política de Escritorio y Pantalla Limpia de Información

Esta política busca prevenir el acceso no autorizado, pérdida y/o daño 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 contratistas.[8]

## 8. Seguridad de las Operaciones

### 8.1 Ambiente de Producción, Desarrollo y Pruebas.

- El IDIGER debe contar con los tres ambientes diferenciados claramente en cuanto a servidores de aplicaciones y BD.
- Se debe proteger cada uno de los computadores, dispositivos de red y de comunicaciones que se consideren críticos por intervenir directamente en el

[8] Documento Política de Escritorio y Pantalla Limpia de Información

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.

## 9. Seguridad de las Comunicaciones

### 9.1 Política de Uso de Correo Electrónico

- 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.
- Queda terminantemente prohibido a los usuarios el envío de mensajes masivos a través de correo electrónico; este tipo de mensajes sólo puede ser enviado por usuarios debidamente autorizados, como lo son: El Director general, subdirectores y/o jefes de oficina o quien sea autorizado por el Director General.
- Es responsabilidad del Usuario 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 del usuario 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 TIC en caso de comprometer en alguna medida, la seguridad de la información de la entidad.
- Es responsabilidad del usuario evitar que su cuenta de correo electrónico sea utilizada por terceros.
- Es responsabilidad del usuario 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 usuarios 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.
- Es responsabilidad de los usuarios eliminar periódicamente de sus dispositivos de almacenamiento los mensajes que ya no necesiten. Con esto se reducen los riesgos de que otros usuarios puedan acceder a esa información; y además, se libera espacio en disco.
- La cuenta de correo electrónico institucional asignada a cada usuario, sólo podrá ser utilizada para el desempeño de las funciones o el cumplimiento de las obligaciones contractuales

## 9.2 Política de Seguridad Aplicable a Logs

- Es responsabilidad de la Oficina TIC asegurar que se generen logs para toda la plataforma tecnológica, especialmente para los equipos y aplicaciones calificados como críticos, dichos logs deben ser custodiados en forma segura para evitar su modificación.
- Es responsabilidad de la Oficina TIC que los logs generados sean monitoreados regularmente para detección temprana de posibles fallas en los equipos y aplicaciones o vulnerabilidades de seguridad.

## 10. Cumplimiento

### 10.1 Cumplimiento de los Requisitos Legales y Contractuales

El IDIGER velará por la identificación, documentación y cumplimiento de la legislación aplicable y requisitos contractuales concernientes a la seguridad de la información

### 10.1.1 Derechos de Propiedad Intelectual (DPI)

La Oficina TIC propenderá porque el software instalado en los equipos de cómputo del IDIGER, esté debidamente licenciado, cumpliendo con los derechos de autor o que el mismo sea de libre distribución y uso.

## 11. Revisión

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, contratistas y demás partes interesadas, utilizando los medios que se considere pertinentes para garantizar su divulgación.

## 12. Control de Cambios

| Versión | Fecha | Descripción de la Modificación | Aprobado por |
|---|---|---|---|
| 1.0 | 02/05/2017 | Creación Manual de Seguridad de la Información | Dirección General |
| 2.0 | 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 | David Giovanni Flórez Reyes - Jefe Oficina TIC |
| | | | |

## 13. Aprobación.

| Elaborado por | Validado por | Aprobado por |
|---|---|---|
| **JULIE MARITZA CARRILLO CÁRDENAS**<br>PROFESIONAL OFICINA TECNOLOGÍAS DE INFORMACIÓN Y LAS COMUNICACIONES | **ANA MILENA ALVAREZ**<br>OFICINA ASESORA DE PLANEACIÓN<br><br>**KAREN ROSSANA CERVANTES SCOTT**<br>PROFESIONAL ESPECIALIZADO GRADO 23 OFICINA TECNOLOGÍAS DE INFORMACIÓN Y LAS COMUNICACIONES<br><br>**JUAN CAMILO JIMÉNEZ ESCOBAR**<br>PROFESIONAL OFICINA TECNOLOGÍAS DE INFORMACIÓN Y LAS COMUNICACIONES | **DAVID GIOVANNI FLOREZ REYES**<br>JEFE DE OFICINA TECNOLOGÍAS DE INFORMACIÓN Y LAS COMUNICACIONES<br><br>**JORGE ANDRES CASTRO RIVERA**<br>JEFE OFICINA ASESORA DE PLANEACIÓN |

**Nota**: Para una mayor información referente a este documento comunicarse con la dependencia responsable.