MANUAL OPERATIVO
POLITICAS DE SEGURIDAD DE LA INFORMACION

Control de Versiones

Versión	Fecha	Descripción Modificación	Folios
5	**2021-11-12**	**Es incluido un apartado de copia de seguridad para equipos de usuario final, y se ajusta el apartado Uso de los dispositivos de almacenamiento extraíbles.**	40
4	2021-04-29	Actualización del tiempo de vigencia de las contraseñas. Fue incluida una cita al Manual de Desarrollo Seguro de Software (MG-TI-19). Fue actualizado el número de la resolución de Roles y Responsabilidades frente al SGSI (5044 de 2019 por 761 de 2021) en 2 citas.	37
3	2020/09/17	Retiro de las políticas de operación de TI. Actualización del marco Normativo. Inclusión de las políticas de seguridad referente a: Registros y eventos, dispositivos que no son propiedad de la entidad, gestión de accesos a usuarios, transferencia de información en medio físico y derechos de propiedad intelectual. Se modificaron todos los numerales del documento.	37
2	15/102019	Ajuste de las políticas en redacción y alcance basados en las recomendaciones de la preauditoria de certificación del SGSI.	36
1	-	Versión inicial	19

El documento original ha sido aprobado mediante el SID (Sistema Información Documentada del IDU). La autenticidad puede ser verificada a través del código

Participaron en la elaboración[1]	Carlos Fernando Campos Sosa, OAP / Hector Andres Mafla Trujillo, STRT /
Validado por	Sandra Milena Del Pilar Rueda Ochoa, OAP Validado el 2021-10-26
Revisado por	Julio Cesar Pinto Villamizar, STRT Revisado el 2021-10-26 Mercy Yasmin Parra Rodriguez, DTAF Revisado el 2021-10-28
Aprobado por	Rosita Esther Barrios Figueroa, SGGC Aprobado el 2021-11-12

CONTENIDO

CONTENIDO

INTRODUCCIÓN

El Instituto de Desarrollo Urbano – IDU, reconoce la importancia de identificar y proteger sus activos de información, para evitar la destrucción, divulgación, modificación y utilización no autorizadas de la información que se gestiona en la Entidad. Además, está comprometido con la implementación, mantenimiento y mejora continua del Subsistema de Gestión de Seguridad de la Información (SGSI).

Considerando lo anterior el IDU, determina la necesidad de implementar políticas que permitan proteger la confidencialidad, integridad y disponibilidad de la información y sus activos relacionados, para lo cual se establece el presente manual de políticas de seguridad de la información, las cuales son de obligatorio cumplimiento por todos los servidores públicos, (en todos los niveles jerárquicos, desde los directivos hasta los asistenciales), contratistas de prestación de servicios, contratistas de outsourcing, proveedores en general, visitantes y terceros que tengan acceso a la información institucional.

1 OBJETIVO

Establecer políticas que definan la seguridad de la información en el IDU, las cuales contribuyen mediante su implementación y cumplimiento a preservar la confidencialidad, integridad y disponibilidad de la información.

2 ALCANCE

Las políticas de seguridad de la información descritas en el presente manual, serán aplicadas a todos los procesos de la Entidad, deben ser conocidas y acatadas por todos servidores públicos (en todos los niveles jerárquicos, desde los directivos hasta los asistenciales), contratistas de prestación de servicios, contratistas de outsourcing, proveedores en general, visitantes y terceros que tengan acceso a la información institucional.

3 MARCO NORMATIVO

- Ley 23 de 1982. Ley sobre derechos de autor
- Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 1273 de 05 de enero 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.
- Ley 1450 de 2011. Por la cual se expide el Plan Nacional de Desarrollo, 2010-2014
- Ley Estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014. Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.
- Directiva Presidencial 03 de 2021. Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
- Resolución 2710 DE 2017, Por la cual se establecen lineamientos para la adopción del protocolo IPv6.
- Resolución 001519 de 2020 de MINTIC. Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos
- Resolución 00500 de 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
- Resolución 1126 DE 2021 de MINTIC. Por la cual se modifica la Resolución 2710 de 2017.
- Resolución Distrital 305 de 2008, Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, caridad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre
- Resolución 004 de 2017, Por la cual se modifica la Resolución 305 de 2008 de la CDS.

- Documento CONPES 3701 de 2011 - Lineamientos de Políticas sobre ciberseguridad y ciberdefensa.
- Documento CONPES 3854 de 2016 - Política Nacional de Seguridad Digital.
- Documento CONPES 3975 de 2019 - Política Nacional para la Transformación Digital e Inteligencia Artificial
- Documento CONPES 3995 de 2020 - Política Nacional De Confianza y Seguridad Digital
- NTC/ISO 27001:2013. Sistemas de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

Nota Las normas de aplicación general y documentos internos (circulares, resoluciones, memorandos) que son parte de este documento, están relacionadas en el normograma del proceso Tecnologías de Información y comunicación publicado en el mapa de procesos.

4 TÉRMINOS Y DEFINICIONES

Los términos y definiciones aplicables al procedimiento pueden ser consultados en el micro sitio DICCIONARIO DE TÉRMINOS IDU (https://www.idu.gov.co/page/transparencia/informacion-de-interes/glosario).

- Dark Web
- Deep Web
- Malware

5 POLITICA OPERACIONAL

El presente Manual de Políticas de Seguridad de la Información se debe revisar y de ser necesario actualizar mínimo una vez al año o cuando sea requerido, para asegurar que las políticas son claras y aplicables.

6 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El IDU cuenta con una política general para el sistema integrado de gestión. Es por ello que los subsistemas de gestión poseen una directriz, que hace las veces de Política, la cual fue adoptada mediante Resolución interna número 1123 de 2021.

6.1 DIRECTRIZ

El Instituto de Desarrollo Urbano se compromete a generar las condiciones de seguridad necesarias en términos de confidencialidad, integridad y disponibilidad adecuadas a la información institucional, en todos sus medios de conservación y divulgación, con los recursos asignados para administrar de forma efectiva los riesgos asociados a sus activos de información, aumentar la credibilidad y confianza de las partes interesadas, implementar estrategias para el mejoramiento continuo y cumplir con la normatividad vigente.

6.2 RESPONSABILIDADES DE LA GENTE IDU CON EL SGSI

Todos servidores públicos (en todos los niveles jerárquicos, desde los directivos hasta los asistenciales), contratistas de prestación de servicios, contratistas de outsourcing, proveedores en general, visitantes y terceros que tengan acceso a la información institucional, deben cumplir con las políticas descritas en el presente manual, es decir, son de obligatorio cumplimiento y deben

acatar los lineamientos dados en la Resolución interna número 761 de 2021, en la cual se definen los roles y responsabilidades frente al subsistema.

6.3 POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

El IDU define las siguientes políticas de seguridad de la información, que involucran actividades de operación, gestión y administración de la seguridad:

6.3.1 POLÍTICA PARA DISPOSITIVOS MÓVILES[1]

Esta política establece lineamientos para el uso y manejo de dispositivos móviles (teléfonos inteligentes y tabletas), y aplica tanto para los dispositivos suministrados por el IDU, como para los dispositivos personales en los que se consulte o almacene información de la Entidad:

Para el caso de los dispositivos asignados por la Entidad, se seguirá el procedimiento *PR-RF-103 ADMINISTRACIÓN DE INVENTARIO DE BIENES MUEBLES* vigente.

Una vez recibido el dispositivo móvil por parte del funcionario, este deberá ser configurado de acuerdo a los lineamientos fijados por la STRT.

En aras de prevenir los riesgos asociados a los dispositivos móviles que el Instituto ha identificado y valorado, se deberá evitar en la medida de lo posible el almacenamiento de información identificada como pública clasificada o pública reservada, de acuerdo con lo establecido en el instructivo *IN-TI-13 - IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN Y USO DEL MÓDULO DE APOYO A LA GESTIÓN DE ACTIVOS DE INFORMACIÓN*. Si es estrictamente necesario guardar este tipo de información en estos dispositivos, esta se deberá proteger con los mecanismos indicados por la Subdirección Técnica de Recursos Tecnológicos- STRT, en este documento.

Se debe configurar un método para el bloqueo de la pantalla en el dispositivo móvil, para controlar el acceso de personas no autorizadas.

No se deben instalar aplicaciones de origen desconocido, o cuyo dato "*ofrecido por*"[2] no corresponda a una empresa conocida, ya que podrían contener virus y/o malware para robar la información.

Si desea conectarse a la red inalámbrica (WIFI) debe:
1. Utilizar la red de directivos IDU, si usted es jefe de alguna dependencia.
2. Utilizar la red de funcionarios IDU, si usted es servidor público o contratista de prestación de servicios.
3. Utilizar la red de Visitantes - IDU para cualquier otro caso.

Para los directivos, servidores públicos y contratistas deben registrar su identidad (usuario) y contraseña de red (son los mismos con los que inicia sesión en su computador), para el caso de la red de invitados se debe seguir el protocolo de conexión definido en su momento.

[1] ISO 27001:2013, Tabla A.1 Objetivos de control y controles- control 6.2.1 Política para dispositivos móviles
[2] Se puede verificar ingresando a Google Play Store, ubicando la aplicación y en más información

Generalmente los dispositivos móviles basados en sistema Android cuentan con la aplicación Google Play Protect (se puede verificar ingresando a “Google Play Store”, “mis apps y juegos”), la cual ayuda a validar que las aplicaciones que se instalan en el dispositivo son seguras; por lo cual se debe verificar que las aplicaciones en el dispositivo asignado o de uso personal son de confianza. Se sugiere que esta verificación se realice al menos una vez cada 3 meses.

En caso de hallar algún malware y/o virus en los dispositivos asignados por el instituto debe reportarlo a través de la *mesa de servicios*[3]. Para los usuarios que utilizan sus propios dispositivos y que hallaron algún malware o virus en él, deberán garantizar la eliminación de la amenaza, o la eliminación de la cuenta de correo e información institucional contenida en el dispositivo.

En caso de pérdida del dispositivo móvil, debe buscar inmediatamente la forma de ingresar a su correo electrónico y dirigirse a la opción cuenta de Google, encontrar tu móvil[4] para realizar el borrado del contenido del dispositivo, cerrar la sesión y bloquear el teléfono. Si el dispositivo es de propiedad del IDU, debe además reportar la situación a la Subdirección Técnica de Recursos Físicos.

Si almacena información del IDU en el dispositivo móvil, se recomienda realizar copia de seguridad de los documentos en algún medio de confianza, al menos cada 30 días.

El patrón, PIN o contraseña se deben cambiar cada 90 días.

El número mínimo de cambios para reutilizar la contraseña, es cinco (5)

Bloqueo automático del dispositivo tras 1 minuto de inactividad

La cuenta corporativa será eliminada del dispositivo, si este no ha sido sincronizado durante 90 días continuos.

Se habilitará la verificación automática de aplicaciones; esto evita que los usuarios instalen aplicaciones en el dispositivo móvil que llevan un software dañino.

El usuario podrá configurar el modo “perfil de trabajo”, para separar el acceso a las cuentas personales e institucionales. Esto será opcional para el usuario.

Adicional, tenga en cuenta estas recomendaciones:

- Evite sostener conversaciones confidenciales en sitios públicos.
- Nunca dicte contraseñas o instrucciones a través del teléfono móvil.
- No pierda de vista su dispositivo móvil.
- No preste el dispositivo móvil a personas desconocidas.
- No use el dispositivo móvil en la calle o en sitios públicos.

[3] Es un conjunto de recursos tecnológicos y humanos, para prestar servicios con la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral, junto con la atención de requerimientos relacionados a las TIC

[4] Servicio de GOOGLE para dispositivos Android perdidos, mayor información en: https://support.google.com/accounts/answer/6160491

- No use conexiones inalámbricas de establecimientos públicos o de acceso libre (por ejemplo, Wifi Gratis).

El uso de dispositivos de Internet Móvil, tales como módems de banda ancha o teléfonos celulares, queda absolutamente prohibido en computadores que pertenezcan al Instituto, para realizar conexión a Internet de forma directa, salvo autorización expresa de la Subdirección Técnica de Recursos Tecnológicos.

6.3.2 POLÍTICA PARA TELETRABAJO O TRABAJO REMOTO[5]

Esta política aplica para las conexiones que se realizan a los servicios tecnológicos privados del IDU, desde una red pública como internet. Es decir, aplica para los servidores públicos que realizan teletrabajo, teletrabajo extraordinario o trabajo remoto, para los contratistas de prestación de servicios que hacen trabajo en casa y terceros que acceden a los servicios de TI de forma remota. En ella se establecen lineamientos para proteger la información a la que se tiene acceso desde un lugar diferente a las instalaciones del IDU.

La conexión remota constituye un elemento técnico dentro de la modalidad de trabajo fuera de oficina, razón por la cual todos los servidores públicos y/o contratistas de prestación de servicios que han sido autorizados a realizar sus actividades bajo esta modalidad deben entender que la conexión remota es parte de los servicios del Instituto y por tanto pueden ser controlados, restringidos y monitoreados tal como si estuviesen en cualquiera de las sedes físicas de la entidad.

La modalidad de Teletrabajo para los servidores públicos se detalla en la guía *GU-TH-01 - Libro Blanco de Teletrabajo IDU*, del proceso de Gestión de Talento Humano.

Todas las conexiones remotas que se hagan para acceder a la red institucional, a través de un canal público, como la red internet, deben usar la conexión segura (VPN) que provee el instituto, cumpliendo los lineamientos del procedimiento *PR-TI-10 - CREACIÓN CONEXIÓN SEGURA VPN* y entregando el formato *FO-TI-22 - SOLICITUD ACCESO REMOTO A TRAVÉS DE VPN* debidamente diligenciado y firmado por el jefe inmediato del solicitante, en la ventanilla de la STRT.

Para configurar la VPN y conectarse a la red corporativa, debe hacerse desde los equipos de cómputo personal o institucional. En ningún caso está permitido utilizar computadores de establecimientos de internet u otros computadores de uso público que no sean seguros.

Los usuarios de conexión remota del IDU son responsables de la seguridad física del sitio de trabajo y deben resguardar su computador o dispositivo desde el cual se establece la conexión.

Los usuarios de conexión remota, no deben desatender su sesión de trabajo, ni utilizar conexiones inseguras (por ejemplo, conexiones Wifi gratuitas[6] , acceder a conexiones y/o redes públicas).

La STRT debe mantener un registro de los accesos que se han realizado a través de la VPN para efectos de trazabilidad y posterior revisión en caso de ser requerido.

---

[5] ISO 27001:2013, Tabla A.1 Objetivos de control y controles- control 6.2.2 Política para teletrabajo

[6] De acuerdo con lo indicado en la Política de dispositivos móviles

Se prohíbe el ingreso a través de cualquiera de las aplicaciones de libre distribución (TeamViewer, Weezo, AMMYY, RealVNC, LogMeIn, entre otros) para acceso remoto desde y hacia cualquiera de los equipos y sedes del Instituto que no se hayan autorizado de manera explícita por la Subdirección Técnica de Recursos Tecnológicos.

Son complemento de estas políticas, Lineamientos Operacionales para Conexión Segura Desde Casa (DU-TI-11).

6.3.3 POLÍTICA DE SEGURIDAD PARA DISPOSITIVOS QUE NO SON PROPIEDAD DE LA ENTIDAD (Trae tu propio dispositivo)

Esta política aplica para equipos de cómputo de escritorio, equipos portátiles, tabletas, teléfonos celulares, discos duros y otros equipos tecnológicos que permitan el procesamiento y almacenamiento de información y que sean propiedad de los servidores públicos, contratistas de prestación de servicios o terceros que tengan acceso a la información institucional.

Por definición el Instituto no recomienda esta práctica, pero si un servidor público o contratista de prestación de servicios es autorizado, deberá cumplir con las siguientes políticas:

Su uso debe ser autorizado por el jefe del área donde se utilizará el equipo.

Una vez autorizado su uso, se debe solicitar formalmente la conexión a la red local, cableada o inalámbrica, usando los formatos dispuestos para tal fin, como los formatos *FO-TI-07 SOLICITUD ACCESO RED IDU WIRELESS* y *FO-PE-20 COMPROMISO DE INTEGRIDAD, TRANSPARENCIA Y CONFIDENCIALIDAD*, cuando apliquen.

Para el caso de la emergencia sanitaria decretada por el Gobierno Nacional, se entiende que el uso de los dispositivos personales fue autorizado tácitamente.

Las licencias de software tanto de sistemas operativos como de programas específicos que estén instalados en el dispositivo, son del propietario del equipo y por tanto éste será responsable por su conformidad legal en lo que a este tema se refiere y exonera de toda multa o daño legal al Instituto, por cualquier irregularidad relacionada con la propiedad intelectual.

No se instalará software licenciado por el Instituto en el equipo.

La información producida en el dispositivo del usuario, como parte de la relación contractual o laboral es institucional, por lo tanto, al finalizar dicha relación, esta debe ser entregada al Instituto. Ver numeral 6.3.23 Política de cumplimiento de derechos de propiedad intelectual.

La información institucional producto del trabajo debe ser respaldada así:

- Las personas que tengan acceso vía VPN en las carpetas compartidas del área.
- Quienes no tengan acceso vía VPN en carpetas compartidas en DRIVE. El jefe del área debe garantizar que él tiene acceso a dicha carpeta compartida.

La frecuencia de generación de copias de seguridad de la información ubicada de los dispositivos que no son propiedad de la entidad dependerá de la dinámica de cada proceso y cada persona. Por lo anterior, se sugiere generar al menos una copia de seguridad al mes.

Las tareas de mantenimiento físico y/o lógico sobre el dispositivo, estarán a cargo del propietario del mismo, así como los costos derivados de ellas.

Toda la responsabilidad por la seguridad física del dispositivo estará a cargo del propietario del mismo y en ningún caso el Instituto se hará solidario por daños o pérdidas de dicho dispositivo.
El Instituto podrá exigir la instalación de aplicaciones que gestionen las políticas definidas, con el objetivo de proteger la información de la entidad. El usuario que desee trabajar con su propio dispositivo deberá aceptar esta política.

Si el dispositivo va a estar conectado a la red LAN de la Entidad, deberán aceptarse estos lineamientos:

- Mientras el dispositivo se pueda conectar a los servicios de red del Instituto, se aplicarán todas las directivas de grupo, medidas de revisión, control y seguridad vigentes para el Instituto.

- Al terminar la relación contractual o laboral, el equipo deberá ser sometido a un proceso de desvinculación de los servicios institucionales, así como el retiro de permisos, privilegios y configuraciones realizadas sobre dicho dispositivo.
- El propietario del equipo acepta las directivas de seguridad del sistema operativo, tales como permisos de acceso a directorios, privilegios del usuario, fondo de escritorio, protector de pantalla, tiempo de bloqueo de sesión y privilegios de la cuenta de usuario en la red de datos institucional.

Se deben tener en cuenta los numerales 6.3.1 Política para dispositivos móviles, 6.3.2 Política para teletrabajo o trabajo remoto, 6.3.9 Política de transferencia de información y 6.3.13 Uso aceptable de los activos.

6.3.4 POLÍTICA DE CONTROL DE ACCESO A LOS SERVICIOS TECNOLÓGICOS

Esta política establece los lineamientos mínimos de seguridad para la autenticación de los usuarios en los servicios de TI dispuestos por el Instituto, para mitigar el riesgo de suplantación de identidad, aumentar la certeza de identificación del usuario y reducir el fraude.

Con base en los anterior, se definen las siguientes políticas:

Se deben usar los mecanismos de autenticación apropiados para acceder a sistemas o aplicaciones críticas (Ej.: corporativas o incluidas en el BIA), tales como: doble factor de autenticación, custodia dual o superior, autenticación unificada basada en un repositorio central o Acceso a través de una herramienta PAM que monitoree las actividades de los usuarios.

El sistema base que presta el servicio debe solicitar a cualquier actor (usuario o sistema) que intenta autenticarse, como mínimo un nombre de usuario y una contraseña. No usar solo identificadores como documento, correo, userID, APIkey o ClientID.

El sistema debe garantizar que quien realiza las acciones de registro, autenticación y restablecimiento de contraseña es un humano (usando CAPTCHA o retrasos incrementales).

Los sistemas que tengan SSO (Single Sign On, por sus siglas en inglés) deben permitir que el usuario pueda visualizar una lista de las sesiones abiertas y poder cerrarlas.

Los sistemas que tengan SSO deben permitir que el usuario pueda cerrar todas las sesiones activas en todas las aplicaciones ante un cambio de contraseña.

Se deben usar al menos dos (2) mecanismos de autenticación para acceder remotamente a los servicios y plataformas en la nube. Ej.: Usuario, Contraseña y OTP (One Time Password).

De otra parte, el IDU basa los niveles de acceso en dos principios que rigen la política de control de acceso:

a) lo que necesita conocer: solamente se concede acceso a la información que la persona necesita para la realización de sus tareas.

b) lo que necesita usar: solamente se le concede acceso a los sistemas y servicios tecnológicos que la persona necesita para la realización de sus tareas.

En ese sentido, se definen las siguientes políticas:

Para el caso de requerirse acceso mediante conexión remota, debe cumplir con el numeral 6.3.2 Política para teletrabajo o trabajo remoto.

Se debe restringir el acceso al código fuente de los sistemas de información solo para el personal autorizado de la STRT.

Teniendo en cuenta que el Instituto es el propietario de la red de datos corporativa, es potestad de Él, realizar actividades de cifrado, revisión y monitoreo de uso de los servicios prestados a través de la mencionada red.

No intente ingresar a páginas de internet sospechosas o restringidas, así mismo, evite abrir mensajes de correo con enlaces o archivos adjuntos que provengan de fuentes desconocidas, pueden contener programas de “secuestro de datos - ransomware” o ser phishing, entre otros.

Queda prohibido que los servidores públicos o contratistas de prestación de servicios accedan a otras redes privadas sin la autorización de la Subdirección Técnica de Recursos Tecnológicos.

La Subdirección Técnica de Recursos Tecnológicos, a través del grupo infraestructura, podrá realizar seguimientos para determinar el cumplimiento de los lineamientos expuestos en esta política, mediante las herramientas con las que cuenta.

6.3.5 POLÍTICA DE GESTIÓN DE ACCESO DE USUARIOS

6.3.5.1 Registro, suministro y cancelación del acceso de los usuarios

La creación del usuario y cuenta de correo electrónico, así como la respectiva administración de permisos de acceso y/o revocación de los mismos, debe realizarse de acuerdo a lo estipulado en el Procedimiento *PR-TI-02 - GESTIONAR USUARIOS TECNOLÓGICOS*.

6.3.5.2 Gestión de derechos de acceso privilegiado

Los usuarios con derechos de acceso privilegiado, son aquellos que pueden realizar actividades de administración de algún servicio, sistema de información o módulo de los recursos suministrados por la Subdirección Técnica de Recursos Tecnológicos.

Los privilegios diferenciados de estas cuentas de usuario, se otorgarán bajo una solicitud explícita del jefe Inmediato del usuario. En estos casos, el superior inmediato deberá supervisar el correcto uso de dichos privilegios.

También se consideran usuarios privilegiados o cuentas privilegiadas, a todas las cuentas con permisos para cambiar la configuración actual de un equipo de cómputo, de un sistema de información o de un elemento activo de red.

Como regla general, se debe tener el menor número posible de usuarios privilegiados en los diferentes sistemas de información y equipos del Instituto.

Cada cuenta de usuario privilegiado, deberá tener un único responsable de uso y se asociarán sus permisos exclusivamente al rol de las funciones que deben ser realizadas por dicho usuario.

Las contraseñas de las cuentas de administración asociadas con estas credenciales privilegiadas, deben cumplir con la Guía para el manejo de credenciales TIC en contingencia (GU-TI-02), con el propósito de facilitar el acceso a dichas cuentas en caso de materialización de algún evento catastrófico o ausencia no programada del titular de dicha cuenta.

Los usuarios privilegiados o cuentas privilegiadas, podrán ser monitoreados periódicamente y se podrán revisar los registros de auditoría dejados por los diferentes sistemas, sin necesidad de pedir una autorización específica del jefe inmediato o de algún ente de control.

A los usuarios privilegiados o cuentas privilegiadas se les prohíbe de manera explícita, modificar o borrar algún dato o el registro completo de auditoría del recurso tecnológico sobre el cual tiene privilegios.

En razón a los privilegios otorgados, se deberán usar contraseñas fuertes, las cuales deberán cambiar periódicamente, cumpliendo al menos con lo dispuesto en el apartado 6.3.5.3 Gestión de información de autenticación secreta de usuarios.

Se debe verificar que los servicios requeridos por las aplicaciones no dependan de la cuenta con privilegios de administrador de dominio. Las aplicaciones que requieran este tipo de cuentas, serán

monitoreadas periódicamente y se podrán revisar los registros de auditoría dejados por dichos servicios.

La cuenta de usuario usada para la configuración de equipos de cómputo por parte de la mesa de servicios de TIC, tiene privilegios de administrador, pero su uso es compartido entre los técnicos de soporte, razón por la cual se exige a este grupo, confidencialidad y responsabilidad al hacer uso de la misma y en todo caso, soportar sus acciones con la documentación de los casos en donde se haga explícita la necesidad de su uso.

El uso inapropiado de los privilegios de administración a través de uno de los usuarios con derecho de acceso privilegiado, será considerado un incidente grave de seguridad de la información, que puede llevar a la apertura de investigación por parte de las autoridades competentes.

6.3.5.3 Gestión de información de autenticación secreta de usuarios

Las contraseñas son el complemento de identificación de un usuario ante un sistema informático, es decir que la combinación de la cuenta de usuario (login) y la contraseña (password) son la llave de autenticidad en la identificación de dicho usuario. La contraseña DEBE ser totalmente privada, es personal e intransferible.

La aceptación de credenciales de acceso por parte de los usuarios es el equivalente a una declaración de aceptación de la obligación de mantener la confidencialidad respecto a la información secreta de autenticación, es decir que quien las recibe acepta explícitamente los derechos, deberes y responsabilidades derivadas del uso de dichas credenciales de acceso a los recursos tecnológicos del Instituto, que se encuentran en la resolución 761 de 2021 Roles y Responsabilidades ante el SGSI.

En virtud de lo expuesto anteriormente, el Instituto reconoce la importancia del componente secreto de autenticación conformado por las claves de acceso o contraseñas y por tanto adopta los siguientes parámetros de control y estructura para las contraseñas y la periodicidad de cambio de las mismas, para que formen parte de la cultura institucional de los elementos de identificación de los usuarios.

En términos generales y a partir de la fecha de publicación de este documento, las condiciones que rigen las contraseñas en el Instituto de Desarrollo Urbano son:

- **Longitud de las contraseñas:** Se establece que las contraseñas deben tener una longitud mínima de doce (12) caracteres alfanuméricos.
- **Tiempo de Expiración de la contraseña:** "La idea histórica es que [los cambios regulares de contraseña] aumentan la seguridad, aunque la ganancia implícita nunca se ha cuantificado".[7]

  Los estudios han demostrado que requerir cambios frecuentes de contraseña es contraproducente para una buena seguridad de la misma ya que debido a la gran cantidad de registros que un usuario debe recordar, estos elegirán contraseñas más débiles o predecibles, las reutilizarán o usarán almacenamiento inseguro si se ven obligados a cambiarlas con regularidad.

[7] Facultad de Ciencias de la Computación de la Universidad de Carlton, Ottawa.

Muchos sistemas obligan a los usuarios a cambiar su contraseña a intervalos regulares, generalmente cada 30, 60 o 90 días. Esto impone cargas al usuario y genera costos adicionales asociados con la recuperación de cuentas.

Forzar la caducidad de la contraseña no tiene ningún beneficio real porque:
- Es probable que el usuario elija nuevas contraseñas que sean sólo variaciones menores de las antiguas.
- Restablecer la contraseña no brinda información sobre si se ha producido un compromiso
- Un atacante con acceso a la cuenta probablemente también recibirá la solicitud para restablecer la contraseña
- Si la contraseña se compromete a través de un almacenamiento inseguro, el atacante podrá encontrar la nueva en el mismo lugar

Dado lo anterior, el Instituto Nacional de Estándares y Tecnología de Estados Unidos – NIST, en su publicación especial 800-63B Lineamientos sobre Identidad Digital (Digital Identity Guidelines), en la Sección 5.1.1.2 recomienda acerca de las contraseñas:
"Los verificadores NO DEBEN requerir que las contraseñas se cambien arbitrariamente (por ejemplo, periódicamente). Sin embargo, los verificadores DEBEN forzar un cambio si hay evidencia de compromiso de la contraseña misma." [8]

Por lo anterior, todas las contraseñas deben ser cambiadas por lo menos una vez cada cuatro meses, razón por la cual se formaliza como tiempo máximo de validez de una contraseña 120 días calendario.

- **Número de intentos fallidos permitidos:** Este es el parámetro que controla la cantidad de veces que un usuario puede intentar ingresar al sistema sin ser bloqueado. El número máximo de intentos fallidos para ingresar a las aplicaciones es tres (3) intentos.

- **Memoria de reutilización de las contraseñas:** Este parámetro define cuantas veces debe ser cambiada una contraseña para poder volver a utilizarla. El número mínimo de cambios para reutilizar la contraseña, es cinco (5).

- **Tiempo de Inactividad (no uso de los recursos):** Se determina como tiempo de inactividad, la cantidad de días transcurridos entre la última vez que se produjo una autenticación de la cuenta de usuario y la fecha actual. Si se supera este valor, se considera que la cuenta de usuario está inactiva y se procede a bloquearla. Este valor está configurado en 30 días calendario.

- **Tiempo de desconexión de sesión:** Este es el parámetro de tiempo definido para que una sesión de trabajo sea desconectada de forma automática por no registrar ninguna actividad en las aplicaciones. Este parámetro dependerá del ambiente de trabajo, el perfil del usuario y el nivel de importancia de la información administrada en la plataforma correspondiente.

  El tiempo de desconexión se aplica a todas las estaciones de trabajo, a los equipos servidores, a los equipos activos de red y a los dispositivos de seguridad.

[8] https://pages.nist.gov/800-63-3/sp800-63b.html#sec5

Para los equipos de usuario final que hacen parte del dominio de red, el tiempo de desconexión está asociados al bloqueo de pantalla que está configurado para activarse a los tres (3) minutos de inactividad y se protege a través de la contraseña que se debe ingresar para poder reanudar la sesión.

Los usuarios no deben revelar la contraseña a ninguna persona, incluyendo, más no limitándose a servidores públicos o contratistas de prestación de servicios de la Subdirección Técnica de Recursos Tecnológicos.

Ningún usuario deberá acceder a los servicios de tecnología prestados por la Entidad, utilizando una cuenta de usuario y contraseña asignada a otro funcionario.

No se deben incluir contraseñas en ningún sistema de registro automatizado, por ejemplo, registro de usuario y contraseña en una macro o en una función de herramientas de ofimática.

No se deben guardar las contraseñas en los navegadores.

Se prohíbe la inclusión de nombre de usuario y contraseña de autenticación por parte del personal de la Subdirección Técnica de Recursos Tecnológicos en los guiones (scripts) de trabajo o en el código fuente de las soluciones desarrolladas, a fin de evitar la "autoconexión" de usuarios no autorizados al usar estas credenciales "quemadas" en el código.

Se exceptúan del cumplimiento de esta política, los sistemas de información legados que poseen módulo de autenticación de usuarios propio, de los cuales no se disponga código fuente, o no tengan forma de personalizar estas políticas.

6.3.5.4 Revisión de los derechos de acceso de usuarios

Cada jefe de dependencia es responsable de asignar, revisar y actualizar mínimo trimestralmente y en los periodos de contratación masiva, los permisos y restricciones de acceso a los distintos servicios tecnológicos, pues él es quien conoce la labor de su equipo de trabajo y las herramientas que requiere para hacerlo.

Se deben revisar los accesos y privilegios a:

- La red institucional,
- Las carpetas compartidas,
- Los servicios en la nube, como el correo electrónico, y
- Los sistemas de información;

Todo lo anterior de acuerdo a lo descrito en el instructivo *IN-TI-16 - REVISIÓN DERECHOS ACCESO RECURSOS TI* del proceso de Gestión de Tecnologías de la Información y Comunicación.

6.3.5.5 Retiro o ajuste de los derechos de acceso

6.3.5.5.1 Ajuste de los derechos de acceso

Se deben retirar todos los derechos de acceso a los servicios de TIC, cuando un usuario cambia el rol que viene desempeñando, bien sea por cambio dentro del área o porque pasa a otra área o por cambio de tipo de vinculación, y volverse a asignar, de acuerdo con el nuevo rol, cargo o tipo de vinculación que vaya a desempeñar, considerándose esto como un ajuste a los derechos actuales.

6.3.5.5.2 Retiro temporal de los derechos de acceso a los servicios de TI

Se debe suspender temporalmente el acceso a los servicios de TIC cuando un servidor público está disfrutando de sus vacaciones, de licencias remuneradas o no remuneradas, o en caso de sanción disciplinaria.

Se debe suspender temporalmente el acceso a los servicios de TIC cuando un contratista de prestación de servicios pide la suspensión de su contrato.

6.3.5.5.3 Retiro definitivo de los derechos de acceso a los servicios de TI.

Se les debe suspender el acceso a los servicios de TI a los servidores públicos o contratistas de prestación de servicios cuando pierden su vinculación con la entidad.

Los jefes inmediatos o supervisores de contrato deberán tomar las medidas correspondientes para que estas personas finalicen sus pendientes dentro del tiempo de vinculación con la Entidad.

Por ningún motivo, salvo casos de fuerza mayor debidamente justificados, se deben habilitar los servicios de TI a personas que no cuenten con vinculación con la Entidad.

6.3.6 POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

Esta política aplica para los activos de información que se identifican como públicos clasificados o públicos reservados[9] según los criterios de seguridad de la información y brinda lineamientos que permitan proteger a los activos, fortaleciendo la confidencialidad, disponibilidad e integridad.

La información institucional a la que aplica esta política no necesitará cifrarse mientras se mantenga en su medio de conservación original.

Para el cifrado de archivos institucionales se podrán utilizar los siguientes algoritmos[10]:

- SHA1[11]
- SHA256

[9] Instructivo IN-TI-13 Identificación De Activos De Información Y Uso Del Módulo De Apoyo A La Gestión De Activos De Información, numeral 7.3.1.5.3.1 CRITERIOS DE SEGURIDAD DE LA INFORMACIÓN pág.: 17 Disponible en: http://intranet/manualProcesos/Gestion_TIC/04_Instructivos_Guias_Cartillas/INTI13_USO_DEL_MODULO_DE_APOYO_A_LA_GESTION_DE_ACTIVOS_DE_INFORMACION_V_2.0.pdf

[10] Un algoritmo de cifrado utiliza una función matemática para “ocultar” el contenido real del archivo original, para lo cual utiliza una clave también ingresada por el usuario. Para que el archivo cifrado se pueda volver a leer, debe pasar por un proceso de descifrado, el cual utiliza la clave que se empleó para cifrarlo.

[11] Secure Hash Algorithm, Algoritmo de Hash Seguro.

Cuando se requiera transportar información pública clasificada o pública reservada fuera de las instalaciones de la Entidad, en medios removibles de almacenamiento, tales como discos duros o memorias, entre otros, el medio o la información deberán estar cifrados.

Serán responsables de cifrar sus archivos, las áreas que manejen información pública clasificada o pública reservada, según la clasificación dada en la identificación de activos de información.

Las llaves de cifrado deberán ser protegidas, para lo cual deberán ser entregadas al jefe de la Dependencia en un sobre cerrado, para prevenir pérdidas u olvidos y atender posibles solicitudes de tipo legal. Copia de estas llaves deberá ser entregada en sobre cerrado al Subdirector Técnico de Recursos Tecnológicos, para que sea custodiada en la cajilla de seguridad asignada a esta dependencia.

En caso de evidenciar o sospechar que una llave de cifrado ha sido interceptada o divulgada a usuarios no autorizados, proceda inmediatamente a cambiarla en todos los archivos que se hayan protegido a través de la misma.

Para aplicar cifrado a la información institucional que cumpla con las características mencionadas, consulte el instructivo IN-TI-19 – CIFRADO DE INFORMACIÓN CONFIDENCIAL.

6.3.7 POLÍTICA DE GESTIÓN DE LLAVES

Tomando como base lo dispuesto por la Ley 527 de 1999 en donde se consagró el equivalente electrónico de la firma, se debe recordar que la firma electrónica corresponde a un acuerdo de voluntades entre dos partes, mediante el cual se estipulan las condiciones legales y técnicas a las cuales se ajustarán las partes para realizar comunicaciones, efectuar transacciones, crear documentos electrónicos o cualquier otra actividad mediante el uso del intercambio electrónico de datos.
Por tanto, la política de uso de las firmas electrónicas incluye:
Todo documento firmado mediante el uso de estos mecanismos tendrá validez y efectos jurídicos.

El servidor público del Instituto a quien se le haya asignado una firma electrónica o un mecanismo de autenticación digital será el responsable directo por el uso adecuado de dicho elemento.

Debe evitar dejar desprotegidos o fuera del alcance visual estos elementos.

El portador o titular de la firma electrónica o mecanismo de autenticación sabe que éste es único, personal e intransferible, y que al igual que las credenciales de acceso, lo vinculan directamente con los registros que se asocien a dichas firmas.

Esta política aplica para transacciones que realiza el IDU a través de sistemas de información, en las cuales se debe transmitir información pública clasificada o pública reservada; por lo cual deberá ser protegida mediante cifrado a través de la firma electrónica o certificados de función pública adquiridos con una entidad certificadora (tercero de confianza).

Se le entregará un token (físico) o certificado de firma electrónica (virtual) por solicitud expresa a cada ordenador del gasto con su respectivo certificado de función pública, para que, en su calidad de servidor público, realice los trámites relacionados con las funciones propias de su cargo en el IDU (emisión de mensaje digital o documento electrónico) y de esta manera garantizar la autenticidad, integridad y no repudio.

La divulgación, extravío o sospecha de interceptación de la clave privada asignada a la firma electrónica, debe ser reportada urgentemente por el servidor público responsable a través de la mesa de servicios a la STRT, a la Oficina de Control Disciplinario (OCD), a la Dirección Técnica Administrativa y Financiera (DTAF) y a la entidad certificadora de la firma para que se tomen las medidas de seguridad correspondientes.

La STRT es la responsable de la administración de los certificados de función pública adquiridos por el IDU que no han sido asignados.

Es responsabilidad de cada usuario del token (certificado de función pública), estar atento a su vencimiento y a la realización de las diligencias a que haya lugar para su renovación.

Para la expedición de un token o certificado de firma digital, el interesado deberá elevar la solicitud respectiva a la STRT a través de Aranda, incluyendo la documentación requerida para el trámite.

Los certificados de firma electrónica (virtual), podrán estar almacenados en los servidores de la Entidad, siempre y cuando se cumplan las condiciones mínimas de seguridad recomendadas por el proveedor. En caso de que los certificados estén almacenados en la infraestructura del proveedor, se deberán cumplir las políticas indicadas en el numeral 6.3.9 Políticas de Transferencia de Información.

El olvido de la clave privada asignada al certificado de firma electrónica, implica perder dicho certificado, toda vez que es la única forma de generar la firma.

Para la entrega de las claves privadas de uso de los certificados deberá realizarse a través correo electrónico seguro.

En caso de que un servidor público usuario de un certificado de firma electrónica se retire de la Entidad, se deberán tener en cuenta las siguientes condiciones:

- Si el certificado aún está vigente y puede ser reasignado, se debe gestionar su suspensión ante el proveedor.
- Si está vigente, pero no se puede reasignar, este deberá ser revocado y la STRT debe asegurar su destrucción, tanto si es físico, como si es virtual.
- En caso de que el certificado ya no esté vigente, no será necesario adelantar ninguna gestión.

En caso de contar con certificados de firma electrónica físicos (token) y uno de ellos se pierda, este deberá ser revocado, tan pronto sea reportada la situación

Todo certificado de firma electrónica que aún tenga vigencia, que no pueda ser reutilizado, deberá ser destruido.

Los contratos de adquisición de certificados de firma digital deben incluir obligaciones relacionadas con la responsabilidad civil, la confiabilidad de los servicios y los tiempos de respuesta para la prestación de los servicios.

6.3.8 POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA

Esta política aplica para todos los funcionarios del IDU, sus puestos de trabajo y equipos de cómputo en pro de mantener un puesto de trabajo limpio y datos de procesamiento de información no expuestos, para reducir los riesgos de acceso no autorizado, pérdida y daño de la información durante y después de la jornada laboral.

Se entiende por escritorio, el puesto de trabajo de cada servidor público o contratista de prestación de servicios e incluye la mesa principal donde se ubica el computador, la sobremesa de la cajonera y los elementos que delimitan estos espacios.

La STRT debe implementar controles orientados a restringir algunas funcionalidades de copiado y ubicación de archivos en los equipos asignados a los servidores públicos y/o contratistas de prestación de servicios, los cuales no deben ser modificados sin la debida autorización de la STRT.

Se debe configurar en todos los equipos de escritorio el bloqueo de sesión, el cual debe activarse automáticamente después de tres (3) minutos de inactividad y será necesario para reactivar la sesión, escribir la contraseña del usuario.

Siempre que un usuario se ausente de su computador de trabajo, debe realizar el bloqueo de la sesión para evitar riesgos de acceso no autorizado a la información o sistemas de información de la Entidad.

No se deben escribir las contraseñas en las notas rápidas del escritorio, mantenerlas a la vista de las demás personas, ni escribirlas en documentos físicos.

Sobre la mesa de trabajo solamente deben estar los documentos con los cuales está trabajando.

Cuando deba atender visitas en su puesto de trabajo, cierre o guarde los documentos con los que está trabajando.

Procure no tener en el puesto de trabajo fotografías personales o portarretratos digitales con imágenes que puedan suministrar información sobre sus hábitos, costumbres o núcleo familiar.

Evite tener cajas de documentos que no esté usando para su actual labor. Estas cajas deberían ser custodiadas por el archivo central (proceso de Gestión Documental) y solamente se deben tener en los puestos de trabajo, cuando sea estrictamente necesario.

No deje notas de tareas confidenciales en curso o actividades críticas pendientes sobre el escritorio o escritas en los tableros de la dependencia.

Absténgase de tener plantas de gran tamaño y/o que requieran de constante hidratación, en el puesto de trabajo.

Cuando se envíe a impresión información sensible, debe retirarse inmediatamente de la impresora, para lo cual se implementó la funcionalidad de impresión por PIN, de tal manera que solo quien envía la impresión pueda, con su número PIN, generar la impresión y retirarla de inmediato.

Al finalizar la jornada de trabajo cada servidor público y/o contratista de prestación de servicios debe guardar en un lugar seguro bajo llave, los documentos y medios que contengan información pública clasificada o pública reservada.

Además, cumplir con los lineamientos descritos en la política de escritorio limpio y pantalla limpia, estipulados en el documento *DU-TI-06 - POLÍTICAS OPERACIONALES DE TIC*.

6.3.9 POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN

Esta política busca mantener la seguridad de los datos y aplica para toda la información que se transfiera e intercambie a través de los diferentes canales de comunicación de la Entidad, entre la Entidad y sus grupos de interés internos o externos.

En cumplimiento del artículo 15 de la Constitución Política de Colombia, “La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley”.

Con base en lo anterior, se brindan los siguientes lineamientos:

6.3.9.1 Transferencia de Información por Medios Electrónicos

Si se debe transferir información PÚBLICA CLASIFICADA o PÚBLICA RESERVADA, esta debe ser cifrada antes de ser transferida (Ver Instructivo IN-TI-19 APLICACIÓN DE CIFRADO), tanto si se utiliza el correo electrónico, como si se emplean otros servicios para enviar o recibir archivos.

Nunca publicar en redes sociales información PÚBLICA CLASIFICADA o PÚBLICA RESERVADA.

No se debe enviar información etiquetada como PÚBLICA CLASIFICADA o PÚBLICA RESERVADA a grupos de mensajería instantánea

No se deberá enviar información institucional, ni siquiera la etiquetada como PÚBLICA, a través de correos electrónicos personales, toda vez que para ello se ha dispuesto de un servicio de correo corporativo.

De requerir el envío de información a través de correo electrónico y este deba ir firmado electrónicamente, la Subdirección Técnica de Recursos Tecnológicos deberá realizar las configuraciones correspondientes, tanto en el cliente como en los servidores.

Para reducir la transferencia innecesaria de información pública clasificada o pública reservada, se deberán incluir en el plan de comunicaciones, actividades referentes a este tema, de forma tal que los usuarios estén sensibilizados al respecto.

Para evitar la divulgación de información pública clasificada o pública reservada, evite reenviar mensajes de correo electrónico de forma automática, es decir, sin verificar todo el contenido, incluyendo los mensajes anteriores que puedan venir encadenados. Tampoco utilice la opción "responder a todos" si no es estrictamente necesario.

Para todo nuevo servicio de TI, que implique al menos la posibilidad de transferir información o realizar comunicaciones electrónicas, se deberán considerar todas las implicaciones legales y los controles a que haya lugar.

Si la información que se desea transferir está en medio digital (lógico) y se ha etiquetado como pública clasificada o pública reservada, los medios que contienen la información se deben proteger contra acceso no autorizado, uso indebido o daño físico durante el transporte (ver 6.3.6 Política de Controles Criptográficos).

Para realizar transferencia de información PÚBLICA CLASIFICADA o PÚBLICA RESERVADA se deberán suscribir acuerdos de confidencialidad, a través de contratos interadministrativos u otros que establezcan el buen uso y manejo de la información, y que reflejen las obligaciones particulares de la contraparte para su protección. Tramitar estos acuerdos será responsabilidad del área propietaria de la información.

Cuando sea pertinente, se deberán acordar y especificar el uso de controles adicionales necesarios para el intercambio de información, a través de medios digitales o físicos entre la entidad externa y el Instituto, o viceversa. Para ello se definirán acuerdos, en los cuales se hará mención específica de los responsables de ambas partes para desarrollar los protocolos particulares de intercambio de datos o información definidos.

Para los terceros a quienes que se les suministre información PÚBLICA CLASIFICADA o PÚBLICA RESERVADA en el ejercicio de sus obligaciones contractuales, deben firmar el *FO-PE-20 COMPROMISO DE INTEGRIDAD TRANSPARENCIA Y CONFIDENCIALIDAD*. Para los terceros a quienes se les brinde información PÚBLICA CLASIFICADA o PÚBLICA RESERVADA y no tengan una vinculación con el Instituto, deberán firmar el formato *FO-TI-04 - ACUERDO DE CONFIDENCIALIDAD CON TERCEROS*.

6.3.9.2 Transferencia de Información por Medios Físicos

Se deben tener en cuenta los lineamientos sobre retención y disposición de correspondencia y documentación de la Entidad, dados en el *MG-DO-01 MANUAL DE GESTION DOCUMENTAL*, en concordancia con las Tablas de Retención Documental de la Entidad.

El proceso Gestión Documental tiene a cargo el servicio oficial de mensajería de la entidad, por lo tanto, es quien dicta los lineamientos para su utilización.

La información que es enviada y recibida en correspondencia, mediante préstamo o transferencia documental a través del proceso Gestión Documental debe ser registrada adecuadamente, para facilitar un seguimiento detallado del despacho, entrega y recibo de la misma.

Se deben proteger los medios en los que se encuentra la información a ser transferida, de acuerdo a sus características, para evitar cualquier daño físico que pudiera presentarse durante el tránsito, por ejemplo, contra cualquier factor ambiental que pueda afectar la integridad de la información, tal como exposición al calor, humedad, lluvia o campos electromagnéticos.

Se deben proteger los medios en los que se encuentra la información a ser transferida para evitar la sustracción o robo. Los medios de protección deberán estar acordes con el nivel de criticidad de la información transportada. Será responsabilidad del área propietaria de la información, determinar el control respectivo.

La información que se transfiera a la bodega de custodia de documentos, deberá ser embalada utilizando para su protección precintos de seguridad.

En caso de pérdida, hurto o daño de información en tránsito, la empresa responsable de la mensajería y o almacenamiento de archivos deberá informar al IDU por medio de oficio, adjuntando el denuncio correspondiente. Será responsabilidad de la Entidad generar nuevamente los documentos y los soportes correspondientes para volver a hacer el envío de los documentos y/o la reconstrucción de los mismos.

6.3.10 POLÍTICA PARA LOS SISTEMAS DE INFORMACIÓN

Esta política aplica durante la adquisición, desarrollo y mantenimiento de aplicaciones de software y permite brindar seguridad a todos los componentes que se van generando durante el ciclo de vida de desarrollo y hacen parte integral de los sistemas de información.

Los requerimientos de aplicaciones nuevas o que se consideren relevantes por parte del líder de los grupos funcionales de administración o desarrollo de software de la STRT, deberán ser validados desde el aspecto de seguridad, por el Oficial de Seguridad de la Información.

Todos los desarrollos de software, se deben regir por los principios de construcción de aplicaciones seguras adoptadas por el Instituto en el procedimiento “Desarrollo de Soluciones" (PR-TI-04) y por el Manual de Desarrollo Seguro de Software MG-TI-19, que contiene las políticas de seguridad para el desarrollo de este tipo de herramientas.

Con el fin de brindar confidencialidad, integridad y disponibilidad a través de las soluciones de software, se realizarán los procedimientos de pruebas descritos en el instructivo *IN-TI-10 - REALIZACIÓN DE PRUEBAS A LOS DESARROLLOS DE SOFTWARE*.

Se prohíbe el intento de acceso y/o uso total o parcial de código fuente de las aplicaciones desarrolladas internamente y/o adquiridas por el Instituto.

Dentro de la fase inicial de establecimiento de requerimientos para el desarrollo, actualización y mantenimiento de sistemas de información, se deben identificar los relacionados con seguridad, por ejemplo: autenticación a través de Directorio Activo, módulos de administración propios del sistema e, identificación de riesgos.

De lo anterior, todos los sistemas de información que vayan a ser desarrollados internamente o que sean adquiridos en el mercado, posterior a la publicación de este Manual, deberán contar con un módulo de autenticación a través del Directorio Activo.

Cuando el desarrollo del software se encuentra en la fase de análisis y diseño, deben establecerse requisitos de acceso a los diferentes componentes y administración del sistema, tales como pistas de auditoría, gestión de sesiones, datos históricos, manejo apropiado de errores. En conclusión, para desarrollar software en el IDU se deben aplicar buenas prácticas de seguridad en el ciclo de vida del software.

Cuando el sistema de información es adquirido, además de las pruebas funcionales, se deben realizar pruebas de seguridad para evitar la exposición de la información institucional.

Si por mandato externo a la Subdirección Técnica de Recursos Tecnológicos se va a implementar un software o un sistema de información, este deberá contar con certificación o informe de realización de las pruebas de seguridad.

Antes de recibir un software contratado, se deben solicitar las evidencias adecuadas de que se realizaron las pruebas suficientes para proteger contra contenido malicioso intencional, no intencional y vulnerabilidades conocidas.

Los sistemas de información que requieran instalarse (o instalar un módulo o agente) en los equipos de usuario final, deberán contar con una guía para configuración de seguridad.

Se deberán realizar al menos una vez al año, ejercicios de análisis del código fuente, para identificar errores, optimizar la aplicación, mejorar la calidad del código y de la arquitectura, determinar la existencia de códigos no utilizados y/o exposiciones potenciales de código, para de esta manera aumentar la eficiencia del sistema en desarrollo.

Siempre que sea posible técnicamente, se deben incluir múltiples factores de autenticación para los procesos sensibles de los sistemas de información, lo cual permitirá reforzar la seguridad del sistema.

Se debe configurar la comunicación segura entre cliente y servidor de manera que esta se cifre, sobre todo cuando se trata de envíos de formularios, por ejemplo, para autenticarse en aplicaciones web.

En el IDU no se desarrollarán servicios de tipo pasarela de pagos. En caso de necesitar de este servicio, deberá ser contratado entre las ofertas existentes en el mercado.
Se deberán tomar las medidas necesarias para evitar la pérdida o duplicación de información de una transacción.

Se debe llevar un control de las versiones del software, así como mantenerlo actualizado desde que se libera una nueva versión.

Se deben realizar pruebas de seguridad en las aplicaciones, teniendo en cuenta las recomendaciones del proyecto abierto de seguridad de aplicaciones web - **OWASP** (acrónimo de

Open Web Application Security Project). A la fecha se recomienda atender las siguientes recomendaciones para evitar que las aplicaciones tengan vulnerabilidades de tipo Cross-Site Scripting (XSS):

- No permitir la ejecución de código al cual se le modifiquen los parámetros de entrada.
- No permitir que sea posible añadir código.
- No permitir que la aplicación responda a los parámetros modificados en el navegador del cliente.

Se deben incluir tokens dinámicos en los frameworks de desarrollo para la protección de los formularios de aplicaciones web, esto evitará vulnerabilidades de tipo Cross Site Request/Reference Forgery (CSRF).

Se deben ocultar los errores provocados por consultas en bases de datos (BBDD), parametrizar las consultas, filtrar y comprobar el valor de las entradas.

Se deben restringir al máximo los permisos del usuario con el que la aplicación se conecta a la base de datos, con esto se evitará la presencia de vulnerabilidades de tipo SQL INJECTION.

Por lo menos dos veces al año, se deben realizar ejercicios de escaneo de vulnerabilidades para identificar brechas en las aplicaciones, que puedan dar pie a explotaciones futuras, fugas de información, denegación de servicios entre otros incidentes de seguridad.

Identificar y proteger los datos de carácter público clasificado y público reservado[12] que serán tratados en la aplicación, aplicarle controles criptográficos, enmascaramiento u otras medidas de seguridad para garantizar el cumplimiento legal y evitar posibles fugas de información.

Todas las aplicaciones que manejen datos personales, deben realizar la solicitud explicita de autorización de tratamiento de los datos. Además, resguardar dicha autorización en la base de datos para futuros requerimientos legales.

Se recomienda involucrar en la toma de decisiones de desarrollo de software al personal de seguridad de la información, de arquitectura, de infraestructura y los demás que se consideren necesarios para generar sinergia entre los diferentes equipos, lo que permitirá el despliegue de aplicaciones robustas, seguras y rentables.

Todos los contratos suscritos para el desarrollo de soluciones de software, deben incluir acuerdos de confidencialidad, tanto de la empresa como de las personas que participen en el proyecto. Además de incluirse en el contrato las cláusulas específicas de confidencialidad, se debe usar el formato *FO-PE-20 COMPROMISO DE INTEGRIDAD TRANSPARENCIA Y CONFIDENCIALIDAD.*

NO se deberían usar datos reales para hacer pruebas. Si se requieren utilizar, estos deberán ser permutados o, de ser posible, ofuscados. Solo se podrán usar en su estado natural, en ambientes de soporte para poder reproducir el error que se presente, siempre y cuando se tenga autorización

[12] Instructivo Identificación de activos de información y uso del módulo de apoyo a la gestión de activos de información (IN-TI-13) Tabla 4. Clasificación frente a confidencialidad Disponible en: http://intranet/manualprocesos/gestion_tic/04_instructivos_guias_cartillas/inti13_uso_del_modulo_de_apoyo_a_la_gestion_de_activos_de_informacion_v_2.0.pdf

expresa del propietario del sistema de información (ver circular 27 de 2020 o la que la reemplace). Esta autorización se debe expedir cada vez que se requiera tomar datos de producción para un ambiente de pruebas. Si esta información se debe retirar de la entidad, el medio externo debe estar cifrado, ver 6.3.6 Política de Controles Criptográficos.

Se deben dejar registros de auditoría cada vez que se copien datos de producción hacia un ambiente de pruebas.

Se prohíbe a todos los usuarios la realización de acciones que pretendan revelar el código fuente de las soluciones de software desarrolladas o adquiridas por el Instituto.

Se prohíbe de manera expresa, la ejecución de conjuntos de comandos o despliegue de aplicaciones que extraigan la estructura y/o listados de objetos y/o del catálogo de componentes de los manejadores de bases de datos de los diferentes ambientes de trabajo (producción, pruebas o desarrollo).

De igual forma se prohíbe de manera expresa, el intento de extracción sin autorización del código fuente de las aplicaciones de software (adquiridas, o desarrolladas), de módulos parciales o de la totalidad de los elementos que conforman los sistemas de información del Instituto. Hace parte de este código fuente la documentación técnica relacionada, los resultados de las pruebas y las actas de aceptación de los productos o servicios pasados al ambiente de producción.

Los programas o herramientas de descompilación o desensamble de aplicaciones de software solamente podrán ser usados por personal autorizado por el Instituto, para efectos de atender una investigación de un incidente de seguridad y solamente con el propósito de la revisión de dicho contenido ante la sospecha de posibles segmentos maliciosos incluidos en el programa objeto de estudio.

Se considera información de acceso limitado al proceso de Gestión de Tecnologías de Información y Comunicación del instituto, todos los modelos y gráficos de los sistemas de información, incluyendo el código fuente, la topología de las redes, los diagramas de ubicación de equipos de cómputo (servidores o de usuario final).

Se deben asegurar los ambientes físicos en los que desempeñen sus labores los desarrolladores de software.

Se deberán determinar puntos de verificación de la seguridad del software que se encuentra en etapa de desarrollo, al menos en cada iteración del ciclo de desarrollo.

Se debe proteger del acceso no autorizado, al repositorio de código fuente.

Todos los cambios a los sistemas de información deben ser aprobados por la mesa de control de cambios de la STRT según lo indicado en el *PR-TI-08 GESTIÓN DE CAMBIOS*.

Los cambios realizados a los sistemas de información en producción, deben ser reflejados en la estrategia de recuperación ante desastres de tecnología – DRP, incluyendo los cambios realizados a la plataforma operacional.

Los proveedores de desarrollo de software deberán contar con una metodología que asegure que el producto realizado cumpla con características de seguridad, que sea de características similares o superiores a la del IDU.

En aquellos casos que se requiera el uso de un servicio web público, se deberán adelantar pruebas de seguridad y calidad de la información, previas al uso de dicho servicio en ambientes de producción.

6.3.11 POLÍTICA PARA LA RELACIÓN CON PROVEEDORES

Esta política busca proteger la información institucional a la cual podrán tener acceso los terceros que tengan una relación contractual con la Entidad. Esta protección debe contemplarse antes, durante y a la finalización del servicio o contrato, por lo cual se establecen los siguientes lineamientos:

El proveedor deberá definir a una persona de contacto para temas relacionados con seguridad de la información.

En caso de presentarse eventos o incidentes de seguridad con la información a la que tengan acceso los proveedores, estos deberán reportarlo de inmediato al oficial de seguridad de la información, a través del correo electrónico seguridaddigital@idu.gov.co, y de ser posible, colaborar en la resolución del incidente.

En los contratos en los que se prevea que se va a intercambiar información etiquetada como pública clasificada o pública reservada, se deberá realizar una reunión entre las partes, en la que se acuerde el protocolo de intercambio de información. En dicha reunión estará un representante del Equipo (técnico) de Seguridad de la Información y en ella el proveedor deberá definir un responsable de la custodia de dicha información. Esta reunión deberá ser una de las primeras en el marco de la ejecución del contrato. Debe hacer parte integral del contrato un documento en el que se establezcan las responsabilidades de cada parte frente a la información a la que tendrá acceso el proveedor. Si este caso se presenta, se debe hacer una identificación de los activos de información (datos e información a los que se vaya a tener acceso y hacer una identificación y valoración de riesgos aplicables a dichos activos.

Para la correcta ejecución de los contratos referidos en el párrafo anterior, las partes deben contar con las estrategias de contingencia o recuperación adecuadas, de tal forma que se cuente con la información requerida en el momento necesario. El supervisor del contrato tendrá la responsabilidad de hacer las respectivas validaciones.

Los proveedores deberán consultar el presente manual de políticas de seguridad de la información en el sitio web del IDU, (https://www.idu.gov.co/page/documentacion-contractual) para que tengan presente el cumplimiento que se debe dar a estas.

Se debe dar a los contratistas y a los proveedores de servicio, una indicación clara de los requisitos institucionales que deben cumplir, tales como los controles de acceso, lógicos y físicos.

El personal de vigilancia debe mitigar los riesgos de seguridad con referencia al acceso de los proveedores y/o contratistas a las instalaciones del IDU, y cumplir los lineamientos estipulados en el documento *MG-RF-03 - MANUAL SEGURIDAD Y VIGILANCIA*.

Los propietarios de los diferentes sistemas de información deben mitigar los riesgos de seguridad con referencia al acceso de los proveedores y/o contratistas a ellos; es decir que deben aplicar la política de control de acceso, ver 6.3.5 Política de gestión de acceso de usuarios, e indicar claramente a la STRT los roles y permisos que debe tener cada usuario en cada sistema de información.

En cada ocasión en que un proveedor requiera información del IDU para el cumplimiento del objeto contractual, el propietario de la información solicitada analizará el requerimiento y podrá aprobar o rechazar la solicitud. Ver circular 85 de 2020 (o la que la reemplace) y el inventario de activos de información, para determinar la propiedad de la información.

Se debe mantener un registro de los accesos que se han realizado a través de la VPN para efectos de trazabilidad y posterior revisión en caso de ser requerido.

Para el intercambio de información con los proveedores, se deberán tener en cuenta las políticas del numeral 6.3.9 Política de transferencia de información.

Se debe verificar que la información a la que tenga acceso un proveedor mantenga su integridad.

El IDU podrá realizar pruebas de selección al personal que disponga el proveedor, así como análisis de antecedentes, con el fin de garantizar la confidencialidad e integridad de la información. De dicho análisis se podrá aceptar o rechazar al personal que no satisfaga las necesidades institucionales.

Se deben realizar actividades de toma de conciencia a los servidores públicos y contratistas de prestación de servicios que se relacionen con el proceso institucional de Gestión Contractual, en lo referente a una segura relación con los proveedores.

En ningún caso, la información institucional podrá ser elemento de disputa en caso de presentarse conflictos entre la Entidad y el proveedor, durante la ejecución del contrato.

La información institucional a la que tiene acceso el proveedor no podrá ser utilizada en contra del Instituto en ninguna disputa jurídica (legal).

El proveedor no puede compartir información del IDU con sus proveedores sin contar con una autorización formal por parte del IDU, la cual debe estar justificada adecuadamente.

Los contratos relacionados con adquisición de servicios deben contar con acuerdos de nivel de servicio, que garanticen una disponibilidad mínima que satisfaga las necesidades del IDU.

Los proveedores deben disponer, al menos, de un plan de continuidad de negocio, para no afectar o afectar lo menos posible la disponibilidad de los servicios de TI de la Entidad.

Cuando sea necesario, se deben definir las condiciones aplicables sobre la propiedad intelectual del producto o servicio contratado. Ver 6.3.23 Política de cumplimiento de derechos de propiedad intelectual.

Los proveedores de servicios tecnológicos podrán acceder en forma remota a los activos tecnológicos a través de una Red Privada Virtual (VPN) acordada con el IDU, cuando ello fuere necesario para el cumplimiento de las obligaciones contractuales, y previa autorización del propietario de la información, quien analizará los motivos de dicho requerimiento y procederá a otorgarla o denegarla. En cualquier situación, dicho acceso será gestionado por la STRT y sólo podrá tener por finalidad dar soporte a equipos tecnológicos o sistemas de información, revisar errores de funcionamiento o prestar servicios de seguridad y/o monitoreo.

Cuando se requiera contratar servicios de manipulación, transmisión, tratamiento de activos de información, tales como servicios de hosting, infraestructura tecnológica, centros de procesamiento de datos, almacenamiento de información física o digital, entre otros, se deberán incorporar cláusulas de seguridad que permitan verificar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información, derechos de auditar los procesos involucrados en el contrato, los procedimientos aplicados frente a incidentes de seguridad, como también la extensión de dichos deberes a empresas subcontratadas por los mismos.

En los casos donde los proveedores requieran hacer instalaciones de activos de información de tipo tecnológico, tales como servidores, equipos de red, equipos de soporte o software, será requisito base implementar configuraciones que cumplan con el estándar de seguridad establecido por la STRT; para lo cual, en caso necesario, deberán considerar ajustes en el acceso a los equipos, el monitoreo de capacidad, la sincronización de hora, el registro de auditoría y los servicios de nombre de dominio (DNS). La STRT tendrá la responsabilidad de verificar y validar la configuración de los equipos instalados, así como también de reportar las debilidades y oportunidades de mejora al proveedor del servicio a través de los procedimientos internos establecidos para estos efectos.

Para los proveedores que tengan relación con almacenamiento, comunicación, infraestructura, plataforma o software que sean entregados al IDU en la modalidad de servicio, también conocidos como servicios en la nube, además de los equipos tecnológicos que sean adquiridos, se deberán comunicar entre las partes, establecer y documentar procedimientos para la gestión de incidentes de seguridad, y además la STRT, podrá solicitar informes relacionados con las mediciones de incidentes de algún período, información que deberá estar disponible durante la vigencia del contrato entre el proveedor y el IDU.

6.3.12 POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

Esta política busca prevenir el acceso físico no autorizado, el daño y la interceptación a la información, de acuerdo con las siguientes consideraciones:

Se debe contar con un área de recepción y/o vigilancia para controlar el acceso físico a las instalaciones del IDU y a las áreas seguras.

Se debe cumplir los lineamientos estipulados en el *MG-RF-03 - MANUAL DE SEGURIDAD Y VIGILANCIA* para el control de acceso físico a las diferentes sedes y áreas.

Se debe diligenciar y resguardar el contenido del formato *FO-RF-06 - PLANILLA DE CONTROL DE PERSONAS QUE INGRESAN A ÁREAS RESTRINGIDAS IDU*.

La última persona que salga de la oficina o área segura, debe ser quien vele por la seguridad física y ambiental, realizando el cierre de las ventanas y puertas del área e informar al personal de vigilancia que no queda nadie en este espacio.

El control de acceso al IDU debe realizarse de acuerdo a lo estipulado en el *MG-RF-03 - MANUAL DE SEGURIDAD Y VIGILANCIA*.

Todo el personal del IDU, tanto contratistas de prestación de servicios como personal de planta, en todos los niveles jerárquicos, desde los directivos hasta los asistenciales, deben portar el carnet institucional en un lugar visible. Si en el momento de ingresar el servidor público y/o contratista de apoyo a la gestión no cuenta con el carnet, debe realizar el registro en el sistema de control de visitantes con el personal de vigilancia en la recepción de la sede correspondiente.

Todas las personas visitantes que ingresen a las instalaciones del IDU deben ser registradas en la recepción de la respectiva sede y deben portar en un lugar visible el distintivo que los identifica como tal.

El IDU debe contar con un Circuito Cerrado de Televisión - CCTV para el monitoreo del perímetro interno y externo.
Las áreas seguras de acceso restringido[13] deben contar con cerramiento físico y control de acceso al espacio físico, que permita el ingreso solamente al personal autorizado.

ÁREAS SEGURAS RELACIONADAS CON TECNOLOGÍA.

Para la Subdirección Técnica de Recursos Tecnológicos, las siguientes áreas del Instituto son consideradas restringidas o aseguradas:

a) Centro de Cómputo,
b) Centros de cableado en cada piso y sede,
c) Zona de ubicación de los dispositivos que complementan el sistema de aire acondicionado del centro de cómputo,
d) Armarios de cableado de datos de acceso externo,
e) Armarios de energía eléctrica regulada de las sedes,
f) Zona donde se ubican las plantas de suministro de energía eléctrica y
g) Zona donde se ubican las UPS.

A estas zonas únicamente puede ingresar personal autorizado y preferiblemente en compañía de personal de la Subdirección Técnica de Recursos Tecnológicos.

[13] Las áreas seguras están definidas en el MG-RF-03 - MANUAL DE SEGURIDAD Y VIGILANCIA

El ingreso a estas áreas debe ser registrado en la bitácora de acceso que se encuentra en cada una de estas, formato *FO-RF-06 PLANILLA DE CONTROL DE PERSONAS QUE INGRESAN A ÁREAS RESTRINGIDAS IDU*.

El control de acceso al centro de cómputo, estará a cargo del coordinador del grupo de infraestructura, bajo los lineamientos consignados en el documento *IN-TI-04 – ACCESO AL CENTRO DE COMPUTO Y CENTROS DE CABLEADO*.

El centro de cómputo debe estar construido con materiales que impidan el acceso físico no autorizado, la contaminación ambiental y que retengan la expansión del fuego.

Se debe procurar el menor tiempo de permanencia de visitantes en dichas áreas.

El personal no autorizado, no podrá ingresar ni mucho menos permanecer en las áreas seguras.

Los equipos de cómputo que se encuentren ubicados en las áreas seguras deberán permanecer bloqueados y fuera del alcance de personas no autorizadas.

Se prohíbe el apagado de todo dispositivo tecnológico administrado por la Subdirección Técnica de Recursos Tecnológicos ubicado en las áreas seguras relacionadas con tecnología, si no se cuenta con la autorización explícita del líder del grupo de Infraestructura o del Subdirector(a) Técnico de Recursos Tecnológicos.

En las áreas seguras relacionadas con tecnología, se prohíbe el consumo de alimentos, bebidas o que se enciendan elementos que produzcan humo o vapor como cigarrillos, tabaco, cigarrillos electrónicos o algún dispositivo similar.

No se podrán ingresar dispositivos de grabación de video o de fotografía, a menos que se cuente con autorización.

6.3.13 POLÍTICA DE USO ACEPTABLE DE LOS ACTIVOS DE INFORMACIÓN

Esta política busca implementar reglas para el uso aceptable de información y de activos asociados con información.

Se entiende por uso aceptable, la manipulación de forma correcta y adecuada de los activos de información.

Se debe recordar que los activos de información son aquellos elementos que pueden contener, procesar o proteger información relevante o de valor para la Entidad, por lo que toda la Gente IDU deberá cumplir con esta política, la cual incluye:

Registrar su inventario de activos de información particular en el Sistema de Información CHIE Módulo SGSI.

Mantener actualizado el inventario de activos de información particular.

Reportar cualquier novedad respecto a los activos de información a su cargo.

Aplicar las medidas necesarias que estén a su alcance para proteger la confidencialidad, integridad y disponibilidad de los activos de información a su cargo.

Reportar cualquier novedad que se presente con los activos de información a su cargo o que estén asignados en el proceso al cual pertenece.

Para el uso de información institucional fuera de las instalaciones del Instituto, deberá ser autorizada por el líder del proceso, quien deberá establecer los controles a fin de para garantizar la preservación física de la información, así como las condiciones de confidencialidad, integridad y disponibilidad de la misma.

Si percibe que el equipo de cómputo trabaja de manera extraña o inadecuada, reporte inmediatamente el caso a la mesa de servicios indicando la anomalía, podría ser una señal de un incidente de seguridad.

Tenga en cuenta lo descrito en el documento *DU-TI-06 - POLÍTICAS OPERACIONALES DE TIC*, en particular lo relacionado en el numeral 6.1 Uso adecuado de elementos y recursos de tecnología.

6.3.14 USO DE LOS DISPOSITIVOS DE ALMACENAMIENTO EXTRAÍBLES

Se entiende por dispositivo de almacenamiento extraíble, cualquier elemento tecnológico que permita contener información o archivos de usuario final. Bajo este nombre se puede referir a cualquiera de los siguientes elementos: Memoria Flash, Memoria USB, Disco Duro Externo, PDA, Storage Card, Tablet, Celulares (Smartphone), Cámara Fotográfica. Atendiendo las prioridades de trabajo y las necesidades manifiestas, respecto al uso de este tipo de dispositivos, a continuación, se definen algunas reglas para su uso, sin que éstas excluyan o remplacen los lineamientos consignados en el instructivo IN-TI-05 USO ADECUADO DE LOS MEDIOS REMOVIBLES DE ALMACENAMIENTO DE INFORMACIÓN.

El acceso a los puertos USB de los computadores corporativos, para leer o copiar información con memorias y discos CD o DVD, son hoy en día, la principal fuente de contagio de malware indeseado en cualquier tipo de organización. De otra parte, los medios de almacenamiento masivo se convierten en un punto crítico para la fuga de información, lo cual debe ser evitado.

Conforme a lo anterior, los puertos USB en todos los equipos de cómputo institucionales deben permanecer deshabilitados y solo se autoriza su utilización a las personas que sean definidas por su jefe directo, lo cual se considera como una excepción y en ningún caso será la regla. Para dicha autorización, tanto el servidor público o contratista PSP, como su jefe directo deberán firmar el formato de responsabilidad y consentimiento informados. Se informa que en lugar de memorias USB, se podrán utilizar carpetas compartidas en servidores institucionales o en Drive.

6.3.15 POLÍTICA DE INSTALACIÓN Y USO DE SOFTWARE

Esta política brinda lineamientos en relación al uso de software e instalación controlada de aplicaciones, ya que una instalación no controlada puede conducir a que se introduzcan vulnerabilidades y posteriormente a fuga de información, pérdida de integridad u otros incidentes

de seguridad, e inclusive a la violación de derechos de propiedad intelectual, para lo cual se deben cumplir a cabalidad los siguientes lineamientos:

Los usuarios finales no están autorizados para instalar directamente aplicaciones de software. En caso de necesitar de una aplicación en particular, su instalación deberá ser solicitada a la STRT, quien definirá los controles necesarios para ello. En todo caso, se debe aplicar el principio de menor privilegio.

La STRT debe mantener un repositorio oficial con las aplicaciones institucionales autorizadas para ser instaladas en los equipos de los usuarios.

Cada servidor público o contratista de prestación de servicios será responsable de cualquier efecto NO deseado que provoque al instalar por su cuenta, un programa NO autorizado ni licenciado.

Se deben considerar los criterios descritos en el documento *DU-TI-06 - POLÍTICAS OPERACIONALES DE TIC*, en particular los relacionados con Instalación de aplicaciones de software y Utilitarios de administración.

6.3.16 POLÍTICA DE COPIAS DE RESPALDO

Sin importar que tan avanzada y moderna sea la tecnología, siempre estará presente el riesgo de pérdida o daño de los archivos electrónicos, por esta razón la principal motivación para realizar copias de seguridad de la información (o backups, del inglés) es minimizar la posibilidad de pérdida de archivos o información digital.

Solamente se realizan copias de seguridad de manera centralizada a la información (datos de usuario y aplicaciones) que se encuentra alojada en los servidores institucionales o carpetas compartidas y que son administrados por la Subdirección Técnica de Recursos Tecnológicos.

Por lo anterior, las copias de seguridad a la información contenida en el equipo de cómputo asignado a cada servidor público o contratista de la entidad, son responsabilidad de éste. Por lo tanto, deben ser realizadas por él, o solicitar acompañamiento a la mesa de servicios para llevar a cabo esta labor. Para ello la entidad dispondrá de herramientas como *Google Drive*.

6.3.16.1 COPIAS DE RESPALDO DE INFORMACIÓN CENTRALIZADA

Las tareas de copias de respaldo deben incluir el resguardo del repositorio de código fuente.

Las copias de respaldo deben tener en cuenta los lineamientos sobre retención y disposición de correspondencia y documentación de la Entidad, dados en el *MG-DO-01 MANUAL DE GESTION DOCUMENTAL*, en concordancia con las Tablas de Retención Documental de la Entidad.

Se deben realizar copias de respaldo de los equipos activos de red o seguridad perimetral de manera periódica o cuando se aplique cualquier cambio de los parámetros.

Para los servidores de procesamiento y almacenamiento se aplicará el procedimiento *PR-TI-17 – GESTION DE SERVIDORES*, numeral 4.1.1.4 7 - Programar copia de respaldo total de servidor de aplicaciones.

Las copias de los servidores virtuales, deben cumplir los plazos de conservación y retención de información, de acuerdo con las tablas de retención documental, teniendo en cuenta que son servidores obsoletos en producción, para evitar posibles restauraciones.

Se define que la estrategia de recuperación ante desastres de tecnología será el espacio que de acuerdo con análisis de impacto al negocio (BIA) sirva para operación continua de la entidad en caso de un desastre.

Las cintas de copias de seguridad que ya estén llenas, se guardarán en la cintoteca del IDU, en donde deben permanecer por un periodo mínimo seis (6) meses.

Posterior a los seis (6) meses citados en el caso anterior y máximo en el año siguiente, las copias de seguridad se deberán conservar en una bodega externa especializada en la administración, almacenamiento y custodia de medios magnéticos, que cumpla con lo indicado en el Documento *DU-DO-06 SISTEMA INTEGRADO DE CONSERVACION.*

La periodicidad de las copias de respaldo debe ser definida por los propietarios de los sistemas de información, ver circular interna 85 del 2020.

La STRT debe realizar pruebas de restauración periódicas que validen la confianza en el medio donde está respaldada la información.

Se deben cumplir a cabalidad los lineamientos descritos en el manual *MG-TI-16 - MANUAL OPERATIVO DE BACKUPS Y RECUPERACIÓN DE LA INFORMACIÓN*.

6.3.16.2 COPIAS DE RESPALDO DE INFORMACIÓN EN EQUIPOS DE USUARIO FINAL

La frecuencia de generación de copias de seguridad de los archivos locales dependerá de la dinámica de cada proceso y cada persona. Por lo anterior, se debe generar al menos una copia de seguridad al mes, utilizando los medios definidos por la STRT, como se indica previamente en el numeral 6.3.16.

Las copias de seguridad de los archivos ubicados en los equipos de cómputo institucionales, deben incluir solamente información institucional. La información personal no se debe incluir en las copias que se entregarán a la entidad como parte del trabajo realizado.

Lleve un registro de las copias de seguridad realizadas, del contenido de las mismas y de la fecha en que se realizó cada copia.

6.3.17 POLÍTICA GESTIÓN DE SERVIDORES

La STRT deberá asegurar la correcta administración, configuración y adecuado funcionamiento de la plataforma informática.

Todas las solicitudes de aprovisionamiento deberán ser analizadas y aprobadas técnicamente por el equipo de seguridad de la información de la Subdirección Técnica de Recursos Tecnológicos con el fin de validar las condiciones de configuración del equipo, esta tarea incluye la restricción total de servicios y puertos de comunicaciones que no sean necesarios para la prestación de servicios para la cual fue aprovisionado el equipo, así como la aplicación de todas las actualizaciones del sistema operativo y de las demás aplicaciones que correrán en el servidor.

6.3.18 POLÍTICA DE REDES Y SERVICIOS DE RED

Esta política aplica para la información que es transmitida a través de la red institucional (LAN y WAN) y para los servicios de TI que operan a través de dicha red.

Uso de la red de datos

Está prohibida la conectividad de equipos institucionales a la red Internet, mediante módems inalámbricos o celulares que utilizan planes de datos.

Un usuario no podrá interceptar, intentar interceptar o acceder a información que no está destinada para él.

Está prohibido obtener o intentar obtener información a través del protocolo SNMP o cualquier otro protocolo similar, de cualquiera de los dispositivos conectados a la red corporativa (LAN y WAN), a menos que se trate de los administradores de dichos dispositivos.

La conexión remota a un equipo de cómputo en modo “silencioso”, con fines de recolección de información para atender un caso específico de investigación o recolección de evidencias, deberá estar soportada con una autorización formal de monitoreo.

Todos los incidentes de seguridad, usarán como base de inicio de la investigación los reportes, alarmas, alertas o notificaciones manuales o de algún sistema o dispositivo que indiquen mal uso del activo de información y/o la estación de trabajo por parte del usuario.

Uso de la Web

Se prohíbe explícitamente la acción de compartir música o videos sociales o personales a través de la red. Se entiende que, por ser una red corporativa, la única información que puede ser transmitida a través de ella, es la que corresponde a acciones laborales o se considera de índole institucional.

Está totalmente prohibido instalar y usar programas para realizar descargas de software desde Internet hacia los computadores institucionales. Asimismo, queda totalmente prohibido el uso de software para intercambio de archivos, música y otros, como Emule, Ares, Kazaa, Torrent y cualquier otro tipo de software P2P (Peer to Peer).

Está totalmente prohibido instalar y usar programas como proxy, VPN no institucionales para evitar anonimizar las comunicaciones y saltarse las restricciones de navegación hacia internet.

Queda estrictamente prohibido el intento de acceso a sitios de contenido sexual, terrorismo, fanatismo religioso, movimientos políticos, descarga de software, deportes, streaming no laborales y navegación en redes de ciberdelincuencia (Deep Web o Dark Web), entre otras.

Cada servidor público o contratista de prestación de servicios será responsable de cualquier efecto NO deseado que provoque al intentar visitar algún sitio web no permitido.

Uso del correo electrónico

En cumplimiento del artículo 15 de la Constitución Política de Colombia, “La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley”.

El contenido de los mensajes no puede ser: insultante, ofensivo, amenazante, injurioso u obsceno.

No está autorizado el envío de mensajes de orden institucional, a través de cuentas de correo electrónico personales o no institucionales.

La cuenta de correo no debe utilizarse para enviar o recibir música, programas de computador, material pornográfico, fotos, videos o cualquier otro material ajeno a los fines de la Entidad. Lo anterior, también se apoya en la política de buen uso del servicio de correo electrónico institucional aplicada por el proveedor, que tiene la potestad de realizar bloqueo de buzones de correo, cuando haya evidenciado este tipo de actividades.

Si se deben enviar archivos por correo electrónico, cuyo fin sea dejar evidencia del cumplimiento de alguna actividad o proceso, se sugiere calcular la función de resumen[14] o valor matemático del archivo (HASH) con el método SHA-256 y enviar este valor como parte del mensaje, por cada archivo adjunto.

Por ningún motivo, está permitido el envío y/o reenvío de mensajes en cadena, desde cuentas de correo electrónico institucional.

6.3.19 POLÍTICA DE CLASIFICACIÓN, ETIQUETADO Y MANEJO DE LA INFORMACIÓN

Esta política aplica para toda la información institucional, de forma que se pueda asegurar que la información recibe un nivel apropiado de protección, de acuerdo con la confidencialidad de la misma.

Los principios aplicables para la clasificación de la información están expresados en la Circular Interna 21 de 2020, o la que esté vigente sobre este tema, en la cual se definen tres (3) opciones para clasificarla de acuerdo a su confidencialidad.

Esta política se centra en la obligatoriedad que tienen los procesos de aplicar las definiciones y controles sobre la clasificación de la información que generan.

El Instituto ha definido unos lineamientos para identificación y etiquetado de la información física y digital que se deben adoptar al interior de cada proceso y de acuerdo a estos criterios se deberá almacenar, respaldar y custodiar la información.

6.3.20 POLÍTICA CONTRA CÓDIGOS MALICIOSOS

Esta política busca reducir las vulnerabilidades de las que pueda aprovecharse el software malicioso (malware) y la infección de los archivos de trabajo de la Gente IDU. Para ello, la entidad cuenta con una solución de seguridad, compuesta por un sistema de prevención y detección de intrusos, herramienta anti-spam y un sistema firewall. Además de estos, se deben aplicar los siguientes lineamientos:

[14] Una función criptográfica hash- usualmente conocida como “hash”- es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

La subdirección técnica de recursos tecnológicos será responsable de la administración de la solución de seguridad mencionada en el párrafo anterior.

El equipo de seguridad de la información deberá recibir información relacionada con nuevos códigos maliciosos de fuentes confiables.

El Antivirus corporativo debe estar operativo en todos los computadores de la Entidad en todo momento.

La Gente IDU y Terceros que hacen uso de los servicios de tecnología de la información del Instituto, son responsables de reportar cualquier alerta dado por el sistema de antivirus y la sospecha de la existencia de un software o un sitio web maliciosos ante la mesa de servicios de TI.

Los equipos de terceros que son autorizados para conectarse a la red de datos del Instituto deben tener antivirus y contar con las medidas de seguridad apropiadas ver 6.3.3 Política de seguridad para dispositivos que no son propiedad de la entidad.

Se deben hacer revisiones y análisis periódicos en búsqueda de código en las estaciones de trabajo y servidores. La actividad debe ser programada de forma automática con una periodicidad semanal.

Por lo menos dos veces al año, se deben realizar ejercicios de escaneo de vulnerabilidades para identificar brechas en los activos de información, que puedan dar pie a explotaciones futuras.

La Entidad debe contar con controles para analizar, detectar y restringir el software malicioso que provenga de descargas de sitios web de baja reputación, archivos almacenados en medios de almacenamiento removibles, contenido de correo electrónico, etc.

No descargar programas (software) o archivos de sitios desconocidos o con mala reputación, ni del correo, cuando se trata de remitentes desconocidos o el contenido es sospechoso, ver 6.3.15 Política de instalación y uso de software.

La Gente IDU y los Terceros pueden iniciar en cualquier momento un análisis bajo demanda de cualquier archivo o repositorio que consideren sospechoso de contener software malicioso. En cualquier caso, cuando sea necesario siempre podrán consultar al equipo de seguridad de la información sobre el tratamiento que debe darse en caso de sospecha de malware.

6.3.21 REGISTROS DE EVENTOS AUTOMÁTICOS DE LOS ELEMENTOS DE TIC

Los registros automáticos de eventos (logs) de los diferentes componentes de la infraestructura de TI, contienen datos relevantes acerca del funcionamiento de estos componentes. Los registros son usados para llevar a cabo análisis de comportamiento y operación.
La política aplicable a estos registros incluye:

La Subdirección Técnica de Recursos Tecnológicos debe formular y aplicar una metodología de rotación de logs, de acuerdo con la capacidad de los recursos involucrados.

Se debe proteger la plataforma contra aplicaciones de “limpieza de logs” que sean instaladas sin autorización y alteren la integridad de la información registrada automáticamente por los diferentes dispositivos, para esto se deben hacer revisiones periódicas de los equipos críticos.

Los usuarios que consultan los logs no tendrán privilegios para edición o modificación de los archivos correspondientes.

Los usuarios que tienen privilegios de administrador o super–usuario de los elementos de configuración monitoreados, solamente podrán eliminar o remover los archivos de log, una vez hayan sido respaldados.

Está totalmente prohibido borrar información total o parcial de los archivos de log sin autorización del Subdirector Técnico de Recursos Tecnológicos.

Ningún archivo de log de ninguno de los componentes, se puede borrar o mover de su origen antes de un mes.

La Subdirección Técnica de Recursos Tecnológicos debe definir el espacio máximo asignado a cada elemento de la plataforma para el almacenamiento de sus logs.

Se debe llevar a cabo una revisión periódica de los logs de toda la infraestructura, para lo cual se podrán utilizar herramientas como el SIEM.

Se debe llevar a cabo una revisión semanal de los eventos de los manejadores de bases de datos, por tipo de tecnología (Oracle, MS-SQL, PostgreSQL, MySQL), para lo cual se podrán utilizar herramientas como el SIEM.

Cada que se vayan a borrar los logs, se debe hacer una copia de seguridad de ellos.

Se deben conservar los archivos de logs respaldados de acuerdo con lo indicado en las tablas de retención documental o en su defecto, por un periodo no menor a diez (10) años, en copias externas.

6.3.22 POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

Esta política busca asegurar la privacidad y la protección de datos personales, como se exige legalmente en Colombia de acuerdo con la Ley estatutaria 1581 de 2012, para lo cual se deben cumplir a cabalidad los lineamientos descritos en el manual de *MG-TI-17 - PROTECCIÓN DE DATOS PERSONALES*.

6.3.23 POLÍTICA DE CUMPLIMIENTO DE DERECHOS DE PROPIEDAD INTELECTUAL

Esta política pretende proteger la propiedad intelectual, tanto de los productos IDU, como de los de otros autores. En este sentido, se deben cumplir los siguientes lineamientos:

Adquirir software solo a través de fuentes conocidas y confiables, para asegurar que no se violan los derechos de autor.

Realizar campañas para la toma de conciencia respecto al cumplimiento de derechos de propiedad intelectual, en las cuales se informe la intención de tomar acciones disciplinarias contra el personal que las incumpla.

La Subdirección Técnica de Recursos Tecnológicos deberá mantener prueba y evidencia de la propiedad de las licencias, discos maestros, manuales, etc.

La Subdirección Técnica de Recursos Tecnológicos deberá implementar controles para asegurar que no se exceda ningún número máximo de usuarios permitido dentro de la licencia.

Se deberán llevar a cabo revisiones periódicas para verificar que solo hay instalados software autorizados y productos con licencia.

La Subdirección Técnica de Recursos Tecnológicos será la única responsable de administrar y asignar el licenciamiento de software.

El IDU mantendrá la propiedad intelectual de cualquier producto o servicio que haya sido desarrollado en el marco de la labor de sus servidores públicos y/o contratistas de prestación de servicios.

Para ceder los derechos de uso, en cualquier caso, se deberá firmar convenio o acuerdo donde se especifique el alcance del software cedido. No será necesario realizar el registro de estos productos ante la Dirección Nacional de Derechos de Autor, toda vez que la Ley 23 de 1982 señala que el propietario de los derechos de autor sobre las obras creadas por empleados, funcionarios públicos o contratistas de prestación de servicios, en cumplimiento de las obligaciones constitucionales y legales de su cargo o en el marco del contrato de prestación de servicios, serán de propiedad de la entidad pública correspondiente o contratante[15].

La información que se produjo como parte de la relación laboral o contractual con el Instituto, es considerada como Institucional y por tanto puede ser sometida a las tareas de revisión, control y monitoreo que sean dispuestas para proteger dicha información.

No copiar total ni parcialmente libros, artículos, reportajes, diseños u otros documentos diferentes de los permitidos por la ley de derechos de autor.

Se debe recordar que los monitoreos de la red efectuados por personas no autorizadas representan una seria amenaza a la disponibilidad, integridad y confidencialidad de la información y a los recursos de cómputo. Por tal razón, la realización de este tipo de análisis sin la debida autorización por parte del Subdirector Técnico de Recursos Tecnológicos será causal de investigación y aplicación de las medidas disciplinarias estipuladas para estos casos y si se trata de personal externo (contratistas o extraños) se podrá constituir en un proceso penal a la luz de la ley 1273 de enero 5 de 2009 emitida por el Congreso de la República de Colombia, específicamente en su Artículo 269C: Interceptación de datos informáticos y extensivamente en su Artículo 269F: Violación de datos personales.

7 SALVEDADES

En caso de necesitar hacer una excepción a alguno de los controles definidos en este documento, el usuario final deberá diligenciar el formato de consentimiento informado que para el efecto publique la STRT.

[15] Artículos 20 y 91 de la Ley 23 de 1982, Modificado por el artículo. 28, Ley 1450 de 2011.