MANUAL OPERATIVO POLITICAS DE SEGURIDAD DE LA INFORMACION

Control de Versiones

Versión	Fecha	Descripción Modificación	Folios
6	**2024-11-06**	**Ajuste y creación de nuevos capítulos en consonancia con la nueva versión de la norma IEC-ISO 27001**	3939
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.	37
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 pre auditoria 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	**Liliana Pulido Villamil, OAP Validado el 2024-10-31**
Revisado por	**Maryid Betty Castaneda Romero, DTAF Revisado el 2024-10-31 Jose Alfredo Ruiz Peralta, STRT Revisado el 2024-10-31**
Aprobado por	**Gisele Manrique Vaca, SGGC Aprobado el 2024-11-06**

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 o utilización no autorizadas de la información que se gestiona en la Entidad. Además, está comprometido con la implementación, mantenimiento e igualmente la mejora continua del Subsistema de Gestión de Seguridad de la Información (SGSI).

Considerando lo anterior, el IDU determina la necesidad de implementar políticas, proporcionando la protección, confidencialidad, integridad, 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, e incluso 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. deberán 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, por tanto, 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, uso de los mensajes de datos, del comercio electrónico, las firmas digitales, 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-, preservando integralmente los sistemas utilizados en 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, como también el derecho de acceso a la información pública nacional, dictándose 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, definiéndose los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, así mismo los datos abiertos.
- Resolución 00500 de 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital, adoptando el modelo de seguridad, además el de 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, comunicaciones respecto a la planeación, seguridad, democratización, caridad, racionalización del gasto, conectividad, infraestructura de Datos Especiales e incluso 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 POLÍTICAS OPERACIONALES

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

5.2 El equipo de seguridad de la información de la Entidad realizará campañas de fortalecimiento de la cultura de la seguridad de la información, para dar a conocer las políticas aquí descritas.

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 por lo que los subsistemas de gestión poseen una directriz, haciendo las veces de Política, la cual ha sido adoptada mediante la Resolución 744 de 2024.

6.1 DIRECTRIZ

El Instituto de Desarrollo Urbano - IDU, se compromete a generar las condiciones de seguridad necesarias en términos de confidencialidad, integridad, como también de 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; aumentando la credibilidad, confianza de las partes interesadas, e implementando estrategias para el mejoramiento continuo, con el fin de cumplir con la normatividad vigente.

6.2 RESPONSABILIDADES DE LA GENTE IDU CON EL SGSI

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 o terceros que tengan acceso a la información institucional, deberán cumplir con las políticas descritas en el presente manual, es decir, son de obligatorio cumplimiento y deberán acatar los lineamientos dados en la Resolución interna número 6135 de 2023, 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, además del manejo de dispositivos móviles (teléfonos inteligentes y tabletas), aplicado 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 con estas políticas de seguridad.

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

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

Si desea conectarse a la red inalámbrica (WIFI) deberá:

[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

1. Utilizar la red “Directivos IDU”, si usted es jefe de alguna dependencia.
2. Utilizar la red de “Funcionarios IDU”, si usted es colaborador.
3. Utilizar la red “Visitantes IDU” para cualquier otro caso.

Para los directivos, servidores públicos, como también contratistas, deberán utilizar sus credenciales de acceso a la red (son los mismos con los que inicia sesión en su computador), para el caso de la red de invitados, se deberán seguir las instrucciones en el navegador.

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 las aplicaciones que se instalan en el dispositivo sean seguras; por lo cual se deberá verificar que las aplicaciones en el dispositivo de uso personal, sean de confianza. Esta verificación se deberá realizar cada 3 meses por parte de su propietario.

En caso de hallar algún malware en los dispositivos asignados por el instituto, deberá reportarlo a través de la *mesa de servicios*[3]. Para los colaboradores que utilizan sus propios dispositivos y hallaron algún malware en él, deberán garantizar la eliminación de la amenaza e informar del suceso al equipo de seguridad de la información.

En caso de pérdida del dispositivo móvil, deberá buscar inmediatamente la forma de ingresar a su correo electrónico y dirigirse a la opción cuenta de Google, encontrar tu móvil,[4] con el fin de realizar el borrado del contenido del dispositivo, cerrar la sesión, como también bloquear el teléfono. Si el dispositivo es de propiedad del IDU, deberá 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 una carpeta de Google Drive institucional, al menos cada 30 días.

El patrón, PIN o contraseña de desbloqueo, se deberán cambiar cada 90 días.

El dispositivo se deberá bloquear automáticamente, tras 1 minuto de inactividad.

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

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

[3] Es un conjunto de recursos tecnológicos y humanos, para prestar servicios con la posibilidad de gestionar, solucionando 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

El uso de dispositivos de internet móvil, tales como módems de banda ancha o teléfonos celulares con funcionalidad de módem, queda absolutamente prohibido en computadores que pertenezcan al Instituto.

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, se asigna a los servidores públicos, permitiéndoles realizar el teletrabajo, teletrabajo extraordinario o trabajo remoto, para los contratistas de prestación de servicios, cuyo trabajo es realizado en casa, e igualmente los terceros 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 la oficina, razón por la cual, todos los servidores públicos o contratistas de prestación de servicios, que han sido autorizados a realizar sus actividades bajo esta modalidad, deberán entender la conexión remota como parte de los servicios del Instituto, 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 los servicios de tecnología, a través de un canal público como la red internet, deberán usar una conexión segura como lo es una VPN o una conexión web segura como SSL.

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

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

La STRT deberá mantener un registro de los accesos que se han realizado de forma remota, para efectos de trazabilidad y posterior revisión en caso de ser requerido.

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

Características de la conexión a Internet:

Evalúe los servicios adicionales que se consumirá a través del canal de banda ancha, como son los servicios de televisión por streaming (Netflix, Disney+, MAX, entre otros.), videos, música, juegos en línea, videoconferencias, educación virtual y más. Identifique la cantidad de dispositivos conectados a la red wifi (Teléfonos, tablet, consolas de juegos, asistentes de voz, dispositivos inteligentes entre

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

otros), por lo anterior, deberá considerar un ancho de banda mínimo de 100 Mbps para evitar congestión.

Optimice el uso del Internet, dado que por un mismo canal se van a establecer todas las conexiones, priorice las actividades laborales en los horarios establecidos.

Los sistemas operativos para realizar las conexiones con la entidad, son Windows 10 o superior, macOS 10.X o superior y Linux con kernel versión 5.10 o superior.

El licenciamiento del equipo utilizado en teletrabajo, si no es entregado por el IDU, deberá estar a cargo del teletrabajador.

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, otros equipos tecnológicos permitiendo el procesamiento y almacenamiento de información, los cuales 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 colaborador es autorizado, deberá cumplir con las siguientes políticas:

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

Una vez autorizado su uso, se deberá 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.

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

Solamente se instalará software licenciado por el IDU en los equipos que sean de propiedad del instituto.

La información producida en el dispositivo del usuario, como parte de la relación contractual o laboral es propiedad de la Entidad, por lo tanto, al finalizar dicha relación, esta deberá ser entregada al Instituto. Ver numeral 6.3.22 Política de cumplimiento de derechos de propiedad intelectual.

La información institucional producto del trabajo, deberá ser respaldada en el DRIVE institucional. El jefe del área deberá garantizar que él tiene acceso a dicha carpeta compartida.

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; 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 con interés de 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 equipo deberá tener instalado un software antimalware propio con su licencia correspondiente.

- Todas las aplicaciones de software, incluyendo el sistema operativo deberán estar debidamente licenciadas y actualizadas.

- El propietario del equipo acepta las directivas de seguridad generadas desde la STRT.

Se deberán 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 lo anterior, se definen las siguientes políticas:

Todos los servicios de tecnología deberán ser solicitados a través del sistema CHIE: Gestión TIC. Esta solicitud deberá ser realizada por el facilitador del área, para ser aprobada por el jefe inmediato. Las solicitudes solamente se pueden realizar por personas y para personas, a condición de tener una vinculación vigente con la Entidad. Cualquier cambio o modificación requerido para un colaborador en cualquiera de los sistemas de información, deberá ser solicitado a través de este sistema.

Se deberán usar los mecanismos de autenticación apropiados para acceder a sistemas, además de aplicaciones críticas (Ej.: corporativas o incluidas en el BIA), tales como: doble factor de autenticación, custodia dual, conjuntamente con la 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 deberá solicitar a cualquier actor (usuario o sistema) que intente autenticarse, como mínimo un nombre de usuario y una contraseña. No usar solo identificadores como documento, correo, userID, APIkey o ClientID.

El sistema deberá garantizar que quien realiza las acciones de registro, autenticación y restablecimiento de contraseña es un humano (usando CAPTCHA seguro).

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

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

Se deberán usar al menos dos (2) mecanismos de autenticación para acceder remotamente a los servicios, como también plataformas en la nube. Ej.: usuario, contraseña y un segundo factor de autenticación.

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

Se deberá 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, podrá 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, e inclusive restringidas, así mismo, evite abrir mensajes de correo con enlaces, e igualmente con archivos adjuntos, con proveniencia de fuentes desconocidas, estos pueden contener programas de “secuestro de datos - ransomware” de igual forma pueden ser phishing, entre otros.

Queda prohibido para los servidores públicos como para los contratistas de prestación de servicios, acceder 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 de T.I., podrá realizar seguimientos para determinar el cumplimiento de los lineamientos expuestos en esta política, mediante las herramientas con las que cuenta.

En caso de que un colaborador, cambie de área, de funciones o de obligaciones contractuales, se deberá hacer la solicitud de retiro de permisos y en la nueva área se creará la solicitud de asignación de nuevos permisos.

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 o revocación de los mismos, deberá realizarse de acuerdo a lo estipulado en el Procedimiento *PR-TI-02 - GESTIONAR USUARIOS TECNOLÓGICOS*, a través del sistema CHIE: Gestión TIC.

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.

Las cuentas de usuario privilegiado están estrictamente delimitadas y restringidas dentro del instituto.

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 será el responsable del uso de dichos privilegios y sus riesgos asociados.

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 y de un elemento activo de red.

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

Las contraseñas de las cuentas de administración asociadas con estas credenciales privilegiadas deberán 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 y también ausencia no programada del titular de dicha cuenta.

Los usuarios privilegiados y cuentas privilegiadas, podrán ser monitoreados periódicamente, además 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 y cuentas privilegiadas se les prohíbe de manera explícita, modificar, 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, de este documento.

Se deberá verificar que los servicios requeridos por las aplicaciones no dependan de la cuenta con privilegios de administrador de dominio. Las aplicaciones 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, razón por la cual se exige a este grupo, confidencialidad y responsabilidad al hacer uso de la misma, 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, esto puede llevar a la apertura de investigación por parte de las autoridades competentes.

6.3.5.3 Cuentas de servicio

Se entiende por cuenta de servicio, aquella que es utilizada por una aplicación informática. En ningún caso, estas aplicaciones podrán utilizar las cuentas de superusuario, root o administrador para su funcionamiento. El equipo de Seguridad de la Información deberá mantener un inventario de estas cuentas.

6.3.5.4 Gestión de información de autenticación secreta de usuarios.

La contraseña **deberá** ser totalmente privada, es personal e intransferible.

La aceptación de credenciales de acceso por parte de los usuarios, es el equivalente a una declaración y aceptación de la obligación, manteniendo la confidencialidad respecto a la información secreta de autenticación.

En términos generales las condiciones que rigen las contraseñas de usuario final en el Instituto de Desarrollo Urbano son:

- **Longitud de las contraseñas:** Se establece que las contraseñas deberán tener una longitud mínima de dieciséis (16) caracteres alfanuméricos.
- **Tiempo de Expiración de la contraseña:** Todas las contraseñas deberán 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 para ingresar al sistema sin ser bloqueado, es decir, son los intentos de un usuario para ingresar. El número máximo de intentos fallidos para ingresar a las aplicaciones es cinco (5) intentos.
- **Memoria de reutilización de las contraseñas:** Este parámetro define cuántas veces deberá 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, así como la fecha actual. Si se supera este valor, se considera la cuenta del usuario como 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 en la cual una sesión de trabajo sea desconectada de forma automática por no registrar ninguna actividad en las aplicaciones. Está configurado para activarse a los tres (3) minutos de inactividad y se protege a través de la contraseña que se deberá ingresar para poder reanudar la sesión.

Las contraseñas para los administradores de la plataforma tecnológica, por ser cuentas de acceso privilegiado deberán tener una longitud mínima de 20 caracteres y cumplir con los demás requisitos ya mencionados.

Las contraseñas de las cuentas de servicios deberán tener una longitud mínima de 50 caracteres y cumplir con los demás requisitos ya mencionados.

Los usuarios no deberán 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, particularmente al personal de mesa de servicios.

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 deberán 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 deberán 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 “auto conexión” 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 cuenten con la funcionalidad técnica para adoptar estas políticas.

6.3.5.5 Revisión de los derechos de acceso de usuarios

Cada jefe de dependencia es responsable de asignar, revisar y actualizar mínimo una vez al año o en los periodos de contratación masiva, los permisos, además de las 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 deberán 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.

6.3.5.6 Retiro o ajuste de los derechos de acceso.

6.3.5.6.1 Ajuste de los derechos de acceso.

Se deberán retirar todos los derechos de acceso a los servicios de TI, cuando un usuario cambia el rol que viene desempeñando, bien sea por: cambio dentro del área, porque pasa a otra área, por cambio de tipo de vinculación, 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.

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

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

Se deberá suspender temporalmente el acceso a los servicios de TI, cuando un contratista de prestación de servicios pide la suspensión de su contrato.

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

Se deberá suspender el acceso a los servicios de TI, a los colaboradores 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, se deberán 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,[6] según los criterios de seguridad de la información y brinda lineamientos, facilitando proteger los activos, fortaleciendo la confidencialidad, disponibilidad e integridad.

[6] 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

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 entre otros, los siguientes algoritmos[7]:

- SHA1[8]
- SHA256
- SHA512
- AES

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 y memorias, entre otros, el medio, además de 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, asimismo divulgada a usuarios no autorizados, proceda inmediatamente a cambiarla en todos los archivos, a razón de haberse 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 deberá 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.

[7] 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, deberá pasar por un proceso de descifrado, el cual utiliza la clave que se empleó para cifrarlo.

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

- 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.
- deberá evitar dejar desprotegidos o fuera del alcance visual estos elementos.

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

- Esta política aplica para transacciones que realiza el IDU a través de sistemas de información, en las cuales se deberá transmitir información pública clasificada o pública reservada; por lo cual deberá ser protegida mediante cifrado a través de la firma electrónica y 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, deberá ser reportada urgentemente por el servidor público responsable, a través de la mesa de servicios a la STRT, a la Oficina de Control Interno Disciplinario (OCDI), 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 de 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 deberá gestionar su suspensión ante el proveedor.

- Si está vigente, pero no se puede reasignar, este deberá ser revocado y la STRT deberá 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, además no pueda ser reutilizado, deberá ser destruido.

- Los contratos de adquisición de certificados de firma digital deberán 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, datos de procesamiento de información no expuestos, con el fin de reducir los riesgos de acceso no autorizado, pérdida, daño de la información durante el trabajo o después de la jornada laboral.

Se entiende por escritorio, el puesto de trabajo, la mesa principal donde se ubica el computador, la sobremesa de la cajonera y los elementos que delimitan estos espacios, utilizados por cada uno de los servidores públicos, así como los contratistas de prestación de servicios.

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

Se deberá configurar en todos los equipos de escritorio el bloqueo de sesión, el cual deberá 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, deberá 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 deberán 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 deberán 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.

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

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

Cuando se envíe a impresión información Clasificada o Reservada, deberá 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 colaborador deberá guardar en un lugar seguro bajo llave, los documentos y medios que contengan información pública clasificada, de modo similar, 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, es decir, la Entidad, 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”.

Los siguientes controles aplican para transferencia de información por medios electrónicos, medios de almacenamiento físico y transferencia verbal:

6.3.9.1 Transferencia de Información por Medios Electrónicos

Si se deberá transferir información PÚBLICA CLASIFICADA o PÚBLICA RESERVADA, esta deberá 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.

Todo archivo que provenga de un correo electrónico o sistema de mensajería deberá ser revisado por un antimalware.

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

Si se va a enviar información PÚBLICA CLASIFICADA o PÚBLICA RESERVADA, siempre se deberá verificar el destinatario.

No se deberá enviar información etiquetada como PÚBLICA CLASIFICADA o PÚBLICA RESERVADA a través de aplicaciones de mensajería instantánea o servicio SMS.

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 esta deba ir firmado electrónicamente, la Subdirección Técnica de Recursos Tecnológicos deberá realizar las configuraciones correspondientes.

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 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 todos los controles existentes.

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

Para los terceros, a quienes se les suministre información PÚBLICA CLASIFICADA o PÚBLICA RESERVADA, en el ejercicio de sus obligaciones contractuales, deberán firmar el *FO-PE-20 COMPROMISO DE INTEGRIDAD TRANSPARENCIA Y CONFIDENCIALIDAD*.

6.3.9.2 Transferencia de Información por Medios Físicos

- Se deberán tener en cuenta los lineamientos sobre retención, disposición de correspondencia y documentación de la Entidad, dados en el MG-DO-01 MANUAL DE GESTIÓN 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 enviada e igualmente recibida en correspondencia, mediante préstamo o transferencia documental a través del proceso Gestión Documental, deberá ser registrada adecuadamente, identificando los contactos apropiados, su autorización relacionados con la transferencia, para facilitar un seguimiento detallado del despacho, entrega y recibo de la misma (cadena de custodia).

Se deberán 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 pudiendo afectar la integridad de la información, tal como exposición al calor, humedad, lluvia o campos electromagnéticos.

Se deberán 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 y obligaciones en caso de incidentes, así como pérdida de medios de almacenamiento.

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 almacenamiento de archivos deberá informar al IDU por medio de oficio, adjuntando el denuncio correspondiente. Será responsabilidad de la Entidad generar nuevamente los documentos, así como la reconstrucción de los mismos, también los soportes correspondientes para volver a hacer el envío de los documentos.

6.3.9.3 Transferencia de Información Verbal

No tener conversaciones verbales confidenciales en lugares públicos o a través de canales de comunicación inseguros, ya que pueden ser escuchadas por personas no autorizadas;

No dejar mensajes que contengan información confidencial en los contestadores automáticos o mensajes de voz, pueden ser reproducidos por personas no autorizadas, almacenados en sistemas comunitarios, inclusive almacenados incorrectamente como resultado de un marcado erróneo. De igual manera, no dejar notas de voz en aplicaciones de mensajería instantánea.

Asegúrese de que se implementan los controles adecuados de la sala (por ejemplo: puerta cerrada, evite a los curiosos);

Comenzar cualquier conversación sensible con un descargo de responsabilidad aludiendo a los presentes el nivel de clasificación y cualquier requisito de manejo de lo que están a punto de oír.

En general, cuando sea pertinente, se deberán acordar y especificar el uso de controles adicionales necesarios para el intercambio de información, a través de medios digitales e igualmente físicos

entre la entidad externa, 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 e información definidos que incluyan la verificación del destinatario.

6.3.10 POLÍTICA PARA LOS SISTEMAS DE INFORMACIÓN

Esta política aplica durante la adquisición, desarrollo y mantenimiento de aplicaciones de software, permitiendo 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, similarmente las consideradas 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 equipo de Seguridad de la Información.

Todos los trabajos relacionados con la construcción, mantenimiento de aplicaciones que sean desarrollados por la STRT, se rigen 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.

Se prohíbe el uso total o parcial del código fuente de las aplicaciones desarrolladas internamente y/o adquiridas por el Instituto con fines ajenos a los de la Entidad.

Todos los nuevos desarrollos de software, sus actualizaciones y mantenimientos, deberán contar con funcionalidades que garanticen la seguridad de la información. Estas serán definidas entre el equipo líder del desarrollo, además del equipo de seguridad de la información.

De lo anterior, todos los sistemas de información que vayan a ser desarrollados internamente o sean adquiridos en el mercado, posterior a la publicación de la versión 4 de este Manual, deberán contar con un módulo de autenticación a través del Directorio Activo.

Todos los sistemas de información, antes de salir a producción, deberán pasar por pruebas de seguridad realizadas por el equipo de seguridad de la información, para evitar la exposición de vulnerabilidades.

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 uno de estos elementos: certificación o informe de realización de pruebas de seguridad.

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

Se deberán incluir múltiples factores de autenticación para los procesos sensibles de los sistemas de información, lo cual permitirá reforzar la seguridad del sistema.

Se deberá configurar la comunicación segura entre cliente y servidor de manera que esta se cifre a través de protocolos no vulnerados.

En el IDU no se desarrollarán servicios de tipo pasarela de pagos. En caso de necesitar 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 deberá llevar un control de las versiones del software, así como mantenerlo actualizado desde que se libera una nueva versión.

Se deberán personalizar los errores provocados en los sistemas de información, incluidos los de bases de datos, parametrizar las consultas, filtrar y comprobar el valor de las entradas.

Se deberán 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 deberán 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, además del público reservado, que serán tratados en la aplicación, aplicar controles criptográficos, enmascaramiento u otras medidas de seguridad para garantizar el cumplimiento legal, evitando posibles fugas de información.

Todas las aplicaciones que manejen datos personales deberán realizar la solicitud explícita de autorización de tratamiento de los datos. Además, en la medida de lo posible, resguardar dicha autorización en la base de datos para futuros requerimientos legales.

Para el despliegue de aplicaciones robustas y seguras, se deberá involucrar en la toma de decisiones de desarrollo de software al personal de los equipos de seguridad de la información, arquitectura, infraestructura, además todos los que se consideren necesarios para generar sinergia entre los diferentes equipos.

Todos los contratos suscritos para el desarrollo de soluciones de software deberán 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 deberá usar el formato *FO-PE-20 COMPROMISO DE INTEGRIDAD TRANSPARENCIA Y CONFIDENCIALIDAD.*

No se deberán usar datos reales para hacer pruebas. Si se requiere utilizarlos, estos deberán ser anonimizados 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 expresa del propietario del sistema de información (ver circular 10 de 2024 o la que la reemplace). Esta autorización se deberá expedir cada vez que sea requerida, tomando datos de producción para un ambiente de pruebas. Si esta información se deberá retirar de la entidad, el medio externo deberá estar cifrado, ver numeral 6.3.6 Política de Controles Criptográficos.

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

Se prohíbe de manera expresa, la ejecución de conjuntos de comandos, despliegue de aplicaciones que extraigan la estructura, listados de objetos y 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 revelar o extraer sin autorización del código fuente de las aplicaciones de software (adquiridas, o desarrolladas), de módulos parciales y 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, además de las actas de aceptación de los productos así mismo los servicios pasados al ambiente de producción.

Los programas, herramientas de des-compilación 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, gráficos de los sistemas de información, incluyendo el código fuente, la topología de las redes y los diagramas de ubicación de equipos de cómputo (servidores o de usuario final).

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

Todos los cambios a los sistemas de información deberán 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 deberán 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, asegurando que el producto realizado cumpla con características de seguridad, 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 deberá 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 e incidentes de seguridad con la información a la que tengan acceso los proveedores, estos deberán reportarlo de inmediato al equipo 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 donde se prevea que se va a intercambiar información etiquetada como pública clasificada o pública reservada, se deberá realizar una reunión entre las partes, acordándose el protocolo de intercambio de información. En dicha reunión estará un representante del Equipo de Seguridad de la Información y en ella el proveedor deberá definir un responsable de la custodia de dicha información. deberá hacer parte integral del contrato, un documento en el cual se establezcan las responsabilidades de cada parte frente a la información de acceso por los proveedores. Si este caso se presenta, se deberá hacer una identificación de los activos de información, datos e información a los que se vaya a tener acceso, al mismo tiempo, 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 deberán 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 tener presente el cumplimiento que se deberá dar a estas situaciones.

Se deberá dar a los contratistas y a los proveedores de servicio, una indicación clara de los requisitos institucionales que deberán cumplir, tales como los controles de acceso, lógicos y físicos.
Los propietarios de los diferentes sistemas de información deberán mitigar los riesgos de seguridad, con referencia al acceso de los proveedores; es decir, se deberá aplicar la política de control de acceso, ver numeral 6.3.5 Política de gestión de acceso de usuarios e indicar claramente a la STRT los roles y permisos que deberá 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 10 de 2024 (o la que la reemplace) y el inventario de activos de información, para determinar la propiedad de la información.

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.

El propietario de cada sistema de información deberá definir y aplicar mecanismos para verificar, inclusive mantener la integridad de la información a la que tengan acceso los proveedores.

El IDU podrá realizar pruebas de selección al personal dispuesto por 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 deberán realizar actividades de toma de conciencia a los colaboradores 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 deberá estar justificada adecuadamente.

Los contratos relacionados con adquisición de servicios deberán contar con acuerdos de nivel de servicio - ANS, que garanticen una disponibilidad mínima, satisfaciendo las necesidades del IDU.

Los proveedores deberán disponer al menos, de un plan de continuidad de negocio, para afectar lo menos posible la disponibilidad de los servicios de TI de la Entidad.

Cuando sea necesario, se deberán definir las condiciones aplicables sobre la propiedad intelectual del producto o servicio contratado. Ver el numeral 6.3.22 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, procediendo a otorgarla o denegarla. En cualquier situación, dicho acceso será gestionado por la STRT, en este sentido sólo podrá tener por finalidad, dar cumplimiento estricto al objeto del contrato.

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, permitiendo verificar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información, cabe destacar, la ratificación de los 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, además validar la configuración de los equipos instalados, así como también de reportar las debilidades u oportunidades de mejora al proveedor del servicio a través de los procedimientos internos establecidos para estos efectos.

Para los proveedores relacionados 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 adquiridos, se deberán comunicar entre las partes, establecer y documentar procedimientos para la gestión de incidentes de seguridad, además la STRT podrá solicitar informes relacionados con las mediciones de incidentes de algún período, información totalmente 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 deberá contar con un área de recepción y/o vigilancia para controlar el acceso físico a las instalaciones del IDU. Asimismo, se deberá controlar el acceso a las áreas seguras.

Se deberán 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.

La última persona que salga de la oficina o área segura deberá ser quien vele por la seguridad física y ambiental, realizando el cierre de las ventanas, igualmente las puertas del área e informar al personal de vigilancia la ausencia de personas en este espacio.

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, deberán portar el carné 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 carné, deberá 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, deberán ser registradas en la recepción de la respectiva sede y deberán portar en un lugar visible el distintivo para ser identificado como tal.

El IDU deberá contar con un Circuito Cerrado de Televisión - CCTV para el monitoreo del perímetro interno y externo.

Las áreas seguras de acceso restringido[9] deberán contar con cerramiento físico y control de acceso al espacio físico, que permita el ingreso solamente al personal autorizado.

1. 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.

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

Se deberá 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, encender elementos que produzcan humo, vapor como cigarrillos, tabaco, cigarrillos electrónicos o algún dispositivo similar.

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

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

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.

La finalidad del uso de los activos de información corresponde al cumplimiento de los objetivos misionales de la entidad, enmarcados en los planes institucionales, obligaciones y responsabilidades formalmente documentados a los vínculos laborales o de contratación con el IDU.

Está estrictamente prohibida la utilización de los activos de información del IDU, con fines personales o en atención de cualquier fin distinto de la vinculación establecida formalmente con el Instituto de Desarrollo Urbano - IDU.

Se deberá recordar la naturaleza de los activos de información: son aquellos elementos que pueden almacenar, contener, procesar, transmitir o dar tratamiento a los datos de valor para la Entidad; en este sentido toda la Gente IDU deberá cumplir con esta política, la cual incluye:

a. Registrar y mantener actualizado su inventario de activos de información particular en el Sistema de Información CHIE Módulo SGSI.

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

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

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 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.

6.3.14 USO DE LOS DISPOSITIVOS DE ALMACENAMIENTO EXTRAÍBLES

Se entiende por dispositivo de almacenamiento extraíble, cualquier elemento tecnológico que permita contener archivos. 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.

En el IDU, la utilización de dispositivos de almacenamiento extraíble es prohibida. Por necesidad del servicio, el jefe inmediato gestionará la excepción.

Los puertos USB en todos los equipos de cómputo institucionales deberán 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, por tiempo limitado, 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, además del consentimiento informado.

Para ampliar la información al respecto, remítase al instructivo IN-TI-05 USO ADECUADO DE LOS MEDIOS REMOVIBLES DE ALMACENAMIENTO DE INFORMACIÓN.

6.3.15 POLÍTICA DE INSTALACIÓN Y USO DE SOFTWARE

Esta política brinda lineamientos en relación con el uso de software e instalación controlada de aplicaciones, ya que una instalación no controlada puede conducir a introducir 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 deberán cumplir a cabalidad las siguientes políticas:

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 deberá aplicar el principio de menor privilegio.

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

Cada colaborador será responsable de cualquier efecto NO deseado, al realizar una instalación por su cuenta de un programa NO autorizado ni licenciado.

Solamente se instalará software licenciado por el IDU en los equipos que sean de propiedad del instituto.

En cuanto al software de tipo utilitario, está restringido exclusivamente a los técnicos y profesionales de la Subdirección Técnica de Recursos Tecnológicos, para realizar diagnósticos e intentar solucionar los casos asignados.

No se autoriza por ningún motivo el uso de estos programas utilitarios a usuarios finales de ninguna dependencia o proceso del Instituto.

Cuando sea requerido el uso de un programa utilitario sobre un elemento crítico de la plataforma de servidores, así mismo de los elementos activos de red, las actividades ejecutadas se deberán presentar a la mesa de trabajo de gestión de cambios (como cambio planeado o de emergencia) y se deberán conservar de manera especial los registros automáticos (logs) del periodo durante el cual ocurrieron dichas acciones.

Se deberán eliminar, al mismo tiempo desinstalar dichas herramientas utilitarias de los equipos (servidores, de usuario final o de gestión de red) una vez se hayan concluido las acciones para las cuales se tuvo que recurrir a ellas.

El uso de programas utilitarios no debería omitir los controles de autenticación y restricciones de acceso del elemento que está siendo atendido. En caso de cambios ocurridos, los elementos se deberán restaurar a su situación original una vez concluyan las tareas de atención

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 (backups, del inglés), es minimizar la posibilidad de pérdida de archivos e 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, estas son administradas por la Subdirección Técnica de Recursos Tecnológicos.

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

La información institucional deberá ser respaldada en el DRIVE institucional. El jefe de cada área deberá garantizar que él tiene acceso a dicha carpeta compartida.

6.3.16.1 COPIAS DE RESPALDO DE INFORMACIÓN CENTRALIZADA

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

Las copias de respaldo deberán tener en cuenta los lineamientos sobre retención, 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 deberán realizar copias de respaldo de los equipos activos de red, 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 2.7.48 - Programar copia de respaldo total de servidor de aplicaciones.

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

Posterior a los seis (6) meses citados en el caso anterior o 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 CONSERVACIÓN.*

La periodicidad de las copias de respaldo deberá ser definida por los propietarios de los sistemas de información, ver circular interna 10 de 2024.

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

6.3.16.2 COPIAS DE RESPALDO DE INFORMACIÓN EN EQUIPOS DE USUARIO FINAL

El colaborador será el responsable de la toma de copias de respaldo de su trabajo, para lo cual la frecuencia de generación de estas dependerá de la dinámica de cada proceso y cada persona. Por lo anterior, se deberá generar al menos una copia de seguridad al mes.

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

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

P

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, además de los 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, e igualmente de las demás aplicaciones corridas en el servidor.

Se deberá aplicar en lo que corresponda el procedimiento PR-TI-17 – GESTIÓN DE SERVIDORES.

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, 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, intentar obtener información a través del protocolo SNMP o cualquier otro protocolo similar, de cualquiera de los dispositivos conectados a la red corporativa, 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, notificaciones manuales o de algún sistema y dispositivo que indiquen mal uso del activo de información, así como de la estación de trabajo por parte del usuario.

Uso de la Web

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

Está totalmente prohibido instalar y usar programas para realizar descargas de software desde Internet hacia los computadores institucionales. Así mismo, queda totalmente prohibido el uso de software para intercambio de archivos, música u otros, como Emule, Ares, Kazaa, Torrent o 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, además 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 colaborador 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 deberá utilizarse para enviar y 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 deberán enviar archivos por correo electrónico, cuyo fin sea dejar evidencia del cumplimiento de alguna actividad y proceso, se sugiere calcular la función de resumen[10] 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 tal forma se pueda asegurar que la información recibe un nivel apropiado de protección, de acuerdo con la confidencialidad de la misma.

[10] 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.

Los principios aplicables para la clasificación de la información están expresados en la Circular Interna 216 de 2023 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, etiquetado de la información física o digital que se deberán adoptar al interior de cada proceso, 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) e igualmente 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 o detección de intrusos, herramienta anti-spam y un sistema firewall. Además de estos, se deberán aplicar los siguientes lineamientos:

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 estar en contacto con entidades, organismos o grupos de interés que generen alertas frente a nuevas amenazas y vulnerabilidades.

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

La Gente IDU, al mismo tiempo los 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 deberán tener antivirus y contar con las medidas de seguridad apropiadas. Ver el numeral 6.3.3 Política de seguridad para dispositivos identificados como no pertenecientes de la entidad.

Se deberán hacer revisiones, además de análisis periódicos en búsqueda de malware en las estaciones de trabajo y servidores. La actividad deberá ser programada de forma automática con una periodicidad semanal.

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

La Entidad deberá 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 se deberán descargar programas (software), archivos de sitios desconocidos, e igualmente con mala reputación, ni del correo, cuando se trata de remitentes desconocidos o el contenido es sospechoso, ver numeral 6.3.14 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 debido en caso de sospecha de malware.

6.3.21 REGISTROS DE EVENTOS AUTOMÁTICOS DE LOS ELEMENTOS DE TI

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 deberá formular y aplicar una metodología de rotación de logs, de acuerdo con la capacidad de los recursos involucrados.

Se deberá 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 deberán 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 súper–usuario de los elementos de configuración monitoreados, solamente podrán eliminar y remover los archivos de log, una vez hayan sido respaldados.

Está estrictamente 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 deberá definir el espacio máximo asignado a cada elemento de la plataforma para el almacenamiento de sus logs.

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

Se deberá 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, MaríaDB), para lo cual se podrán utilizar herramientas como el SIEM.

Se deberán conservar los archivos de logs respaldados por un periodo no menor a diez (10) años, en copias externas.

6.3.22 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 deberán cumplir las siguientes políticas:

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 colaboradores.

Para ceder los derechos de uso, en cualquier caso, se deberá firmar un 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 al propietario de los derechos de autor sobre las obras creadas por empleados, funcionarios públicos, e igual manera a los contratistas de prestación de servicios, en cumplimiento de las obligaciones constitucionales y legales de su cargo, en el marco del contrato de prestación de servicios, serán de propiedad de la entidad pública correspondiente u del contratante[11].

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 o monitoreo, 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 deberá recordar que los monitoreos de la red efectuados por personas no autorizadas representan una seria amenaza a la disponibilidad, integridad, 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, aplicando las medidas disciplinarias estipuladas para estos casos, así mismo 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, específicamente en su Artículo 269C: Interceptación de datos informáticos y extensivamente en su Artículo 269F: Violación de datos personales.

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

6.3.23 GESTIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Cada vez que se detecta un evento, incidente o debilidad relacionados con seguridad de la información por parte de un funcionario, contratista o terceras partes, se deberá reportar a la STRT por cualquiera de los medios dispuestos para tal fin.

Será responsabilidad de la STRT seguir los procedimientos establecidos (PRTI22_GESTION_DE_INCIDENTES_DE_SEGURIDAD_DE_LA_INFORMACION_V_3 y PRTI22_PROCEDIMIENTO_DE_GESTION_DE_EVENTOS_E_INCIDENTES_D_V3) para la gestión de los incidentes que puedan presentarse.

6.3.24 SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN

El Instituto de Desarrollo Urbano, definirá un “Plan de Comunicación en Seguridad de la Información” a través de su oficina de comunicación interna y externa y la STRT , donde se planificará ANUALMENTE la manera en que se comunicarán recomendaciones o tips de seguridad de la información por los diferentes medios institucionales a todos sus funcionarios y contratistas de prestación de servicios, con el fin de socializar las políticas institucionales o las buenas prácticas en seguridad de la información que se desean socializar para aumentar las capacidades de todas las áreas y procesos de la entidad. La creación de los contenidos se hará con apoyo de la STRT y/o el Oficial de Seguridad de la Información.

6.3.25 CAPACITACIONES EN SEGURIDAD

El Instituto de Desarrollo Urbano, a través de sus áreas de Talento Humano y Gestión Corporativa, incluirá dentro de sus capacitaciones e inducciones las temáticas de seguridad de la información, con el objetivo de que cualquier funcionario y/o contratista que se vincule a la entidad tenga pleno conocimiento de las políticas de seguridad de la información, la STRT y/o el Oficial de Seguridad de la Información apoyará en dichas inducciones.

7 SANCIONES

La falta de conocimiento de los presentes lineamientos no libera al personal de Instituto de Desarrollo Urbano de las responsabilidades establecidas en ellos por el mal uso que hagan de los recursos de TIC o por el incumplimiento de los lineamientos aquí descritos.

Cualquier violación a las políticas de seguridad de la información del Instituto de Desarrollo Urbano podrá conllevar el traslado de un informe a la Oficina de Control Disciplinario Interno.

8 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 responsabilidad y consentimiento informado que para el efecto publique la STRT.

9 APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

Las políticas aquí definidas se harán efectivas a partir de su aprobación por la Alta Dirección y serán revisadas por lo menos anualmente, cuando existan incidentes de seguridad de la información o cuando se produzcan cambios estructurales considerables, esto con el fin de asegurar su vigencia y aplicabilidad dentro del Instituto de Desarrollo Urbano