# MANUAL OPERATIVO
# POLITICAS DE SEGURIDAD DE LA INFORMACION

## Control de Versiones

| Versión | Fecha | Descripción Modificación | Folios |
|---|---|---|---|
| 2 | 2019-10-15 | Ajuste de las políticas en redacción y alcance basados en las recomendaciones de la preuaditoria de certificación del SGSI. | 18 |

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 / Héctor Andres Mafla Trujillo, STRT |
| **Validado por** | Isauro Cabrera Vega, OAP Validado el 2019-10-09 |
| **Revisado por** | Hector Pulido Moreno, STRT Revisado el 2019-10-09 Salvador Mendoza Suarez, DTAF Revisado el 2019-10-10 |
| **Aprobado por** | Ligia Stella Rodriguez Hernandez, SGGC Aprobado el 2019-10-15 |

## CONTENIDO


**INTRODUCCIÓN** ..... **3**

**1 OBJETIVO** ..... **4**

**2 ALCANCE** ..... **4**

**3 MARCO NORMATIVO** ..... **4**

**4 TÉRMINOS Y DEFINICIONES** ..... **4**

**5 POLITICA OPERACIONAL** ..... **5**

**6 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN** ..... **5**

*6.1 DIRECTRIZ* ..... *5*

*6.2 RESPONSABILIDADES DE LA GENTE IDU CON EL SGSI* ..... *5*

**6.2.1 RESPONSABILIDADES GENERALES** ..... 5

**6.2.2 RESPONSABILIDADES ESPECÍFICAS** ..... 5

*6.3 POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN* ..... *6*

**6.3.1** POLÍTICA PARA DISPOSITIVOS MÓVILES ..... 6

**6.3.2 POLÍTICA PARA CONEXIÓN REMOTA A LOS SERVICIOS TECNOLÓGICOS** ..... 7

**6.3.3 POLÍTICA DE CONTROL DE ACCESO A LOS SERVICIOS TECNOLÓGICOS** ..... 8

**6.3.4 POLÍTICA DE CONTROLES CRIPTOGRÁFICOS** ..... 9

**6.3.5 POLÍTICA DE GESTIÓN DE LLAVES** ..... 9

**6.3.6 POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA** ..... 10

**6.3.7 POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN** ..... 11

**6.3.8 POLÍTICA DE DESARROLLO Y MANTENIMIENTO SEGURO DE SOFTWARE** ..... 12

**6.3.9 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA RELACIÓN CON PROVEEDORES** ..... 14

**6.3.10 POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO** ..... 16

**6.3.11 POLÍTICA DE USO ACEPTABLE DE LOS ACTIVOS** ..... 17

**6.3.12 POLÍTICA DE INSTALACIÓN Y USO DE SOFTWARE** ..... 17

**6.3.13 POLÍTICA DE COPIAS DE RESPALDO** ..... 17

**6.3.14 POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES** ..... 18

**6.3.15 POLÍTICA GESTIÓN DE SERVIDORES Y EQUIPOS DE RED** ..... 18

**7 REFERENCIAS BIBLIOGRÁFICAS** ..... **18**

## INTRODUCCIÓN

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

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

## 1 OBJETIVO

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

## 2 ALCANCE

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

## 3 MARCO NORMATIVO

- Ley 1341 de 2009, Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
- Ley Estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1273 de 05 de enero de 2009. “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”
- Decreto 1078 de 2015, Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.
- Directiva Distrital 002 de 2002, cuyo asunto es: "formulación de proyectos informáticos y de comunicaciones"
- Directiva Distrital 005 de 2005, Por medio de la cual se adoptan las políticas generales de tecnología de información y comunicaciones aplicables al Distrito Capital.
- Resolución 004 de 2017, Por la cual se modifica la Resolución 305 de 2008 de la CDS.
- Documento CONPES 3854 Política Nacional de Seguridad Digital.
- Resolución IDU 1543 de 2019, "Por la cual se adopta el Manual de Gestión de Políticas de Seguridad de la Información ".
- Resolución interna 1641 de 2019, “Por la cual se adopta el Sistema de Gestión MIPG-SIG del Instituto de Desarrollo Urbano, y se crean los equipos Institucionales”.
- Resolución interna 1909 de 2019, “Por medio de la cual se define la política MIPG-SIG-IDU, se determinan las directrices y objetivos de los Subsistemas de Gestión, y se adopta la versión 4.0 del Manual de Procesos del IDU.”
- NTC/ISO 27001:2013. Sistemas de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

## 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).

## 5 POLITICA OPERACIONAL

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

## 6 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El IDU cuenta con una política general para el sistema integrado de gestión. Es por ello que los subsistemas de gestión poseen una directriz, que hace las veces de Política, la cual fue adoptada mediante Resolución interna 1909 de 2019.

### 6.1 DIRECTRIZ

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

### 6.2 RESPONSABILIDADES DE LA GENTE IDU CON EL SGSI

#### 6.2.1 Responsabilidades generales

Todos los servidores públicos, contratistas de apoyo a la gestión, contratistas de outsourcing, visitantes y terceros que tengan acceso a la información institucional deben cumplir con las políticas descritas en el presente manual y deben acatar las recomendaciones dadas en el documento *RESOLUCIÓN NÚMERO 5044 DE 2019*

#### 6.2.2 Responsabilidades específicas

**Subdirector General de Gestión Corporativa**

Es el líder en la implementación del SGSI, por lo tanto, es responsable de adoptar y promover la apropiación de las presentes políticas.

**Subdirección Técnica de Recursos Tecnológicos**

La STRT debe proveer los recursos de infraestructura tecnológica, los sistemas de información, el personal y los lineamientos necesarios para dar cumplimiento a la seguridad de la información del IDU.

**Subdirección Técnica de Recursos Físicos**

La STRF debe proveer los recursos para el acceso físico, el personal de vigilancia, el manual de vigilancia y demás lineamientos necesarios para apoyar la seguridad física y del entorno del IDU.

**Todos los Jefes de Dependencia**

Sin excepción alguna, deben dar a conocer a todo el personal a su cargo el presente manual de políticas de seguridad de información, señalando el estricto cumplimiento de las mismas en razón de formalizar su compromiso con la seguridad de la información del IDU.

## 6.3 POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

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

### 6.3.1 Política para dispositivos móviles [1]

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

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

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

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

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

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

Si desea conectarse a la red inalámbrica (WIFI) debe:
1. Utilizar la red de Directivos IDU, si usted es jefe de alguna dependencia.

[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

2. Utilizar la red de Funcionarios IDU del instituto, si usted es servidor público o contratista de apoyo a la gestión.
3. Utilizar la red de Visitantes - IDU para cualquier otro caso.

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

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

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

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

Si almacena información del IDU en el dispositivo móvil, se recomienda realizar copia de seguridad de los documentos en algún medio de confianza, con una periodicidad mínima de 30 días.

Cumplir los lineamientos descritos en el documento de DU-TI-06 – *POLITICAS OPERACIONALES DE TIC*, acerca del uso de los dispositivos móviles.

### 6.3.2 Política para conexión remota a los servicios tecnológicos[5]

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

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

[4] Servicio de GOOGLE para dispositivos Android perdidos, mayor información en: HTTPS://SUPPORT.GOOGLE.COM/ACCOUNTS/ANSWER/6160491

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

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

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

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

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

Los usuarios en Teletrabajo y/o de conexión remota, no deben desatender su sesión de trabajo, ni utilizar conexiones inseguras (por ejemplo, conexiones WiFi gratuitas[6] , acceder a conexiones y/o redes públicas). Además, deben cumplir las políticas de seguridad de la información definidas en este documento.

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

### 6.3.3 Política de control de acceso a los servicios tecnológicos

Esta política se refiere al control de acceso de los usuarios autorizados a los sistemas y servicios tecnológicos en relación con el otorgamiento, actualización, revocación y gestión de permisos, teniendo en cuenta que el IDU se basa en dos principios que rigen la política de control de acceso:

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

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

Se deben revisar los accesos y privilegios a:

- La red institucional

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

- Los sistemas de información
- Las carpetas compartidas y
- Los servicios en la nube, como el correo electrónico.

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.

Para el caso de requerirse acceso mediante conexión remota, debe realizarse siguiendo la Política para conexión remota a los servicios tecnológicos

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

El acceso a servicios de red se debe llevar a cabo de acuerdo a lo estipulado en la presente política y en el capítulo servicios de red del documento *DU-TI-06 - Políticas Operacionales de TIC*.

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

### 6.3.4 Política de controles criptográficos

Esta política aplica para los activos de información que se identifican como públicos clasificados o públicos reservados [7] según los criterios de seguridad de la información y brinda lineamientos que permitan proteger a los activos, fortaleciendo la confidencialidad, disponibilidad e integridad.

En este procedimiento se pude utilizar cualquier software de compresión que deberían tener instalado en sus equipos de cómputo. Para proteger el activo, se debe dar clic derecho sobre la carpeta o archivo a comprimir, seleccionar la opción añadir al archivo e ingresar una clave, que no debe olvidar, ya que no podrá volver a abrir el archivo contenedor de la información.

### 6.3.5 Política de gestión de llaves

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

Se le entregará un token o certificado de firma electrónica por solicitud expresa a cada ordenador del gasto con su respectivo certificado de función pública, para que, en su calidad de funcionario

[7] 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

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.

Cada ordenador del gasto que cuenta con firma electrónica y realiza transacciones a través del Sistema de Información de Acompañamiento Contractual (SIAC) y el Sistema de Información administrativo y Financiero (STONE), es el responsable de resguardar su clave privada, el token y cumplir las especificaciones de seguridad dadas por el proveedor del servicio[8].

La divulgación, extravío o sospecha de interceptación de la clave privada asignada a la firma electrónica, debe ser reportada urgentemente por el funcionario público responsable a través de la mesa de servicios a la STRT y a su vez a las Oficinas de Control Disciplinario (OCD) y a la Dirección Técnica Administrativa y Financiera (DTAF) 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 el token (certificado de función pública) que se le ha asignado, estar atento a su vencimiento y a la realización de las diligencias a que haya lugar para su renovación estos son personales e intransferibles, pues son elementos que le permiten identificarse ante un sistema de información.

### 6.3.6 Política de escritorio y pantalla limpia

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

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

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

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

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

[8] Recomendaciones de seguridad, Certicámara.

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

Los servidores públicos y contratistas de apoyo a la gestión del IDU, deben conservar su escritorio libre de información propia de la Entidad, que pueda ser accedida, copiada o utilizada por terceros o por personas no autorizadas.

Cuando se envíe a impresión información sensible, debe retirarse inmediatamente de la impresora.

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

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*.

### 6.3.7 Política de transferencia de información

Esta política busca mantener la seguridad de los datos y aplica para toda la información que se transfiera e intercambie a través de los diferentes canales de comunicación de la Entidad, entre los usuarios del IDU y los receptores internos o externos de la Entidad, por lo cual se brindan los siguientes lineamientos:

Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o daño físico durante el transporte.

Sera responsabilidad del área propietaria de la información, cuando realice intercambio de información con entidades externas, suscribir acuerdos de transferencia, contratos interadministrativos u otro que establezca el uso y confidencialidad de la información con el fin de proteger su integridad y disponibilidad, conforme al nivel de confidencialidad de la misma.

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

Se deben establecer acuerdos de confidencialidad donde se indiquen los requisitos fundamentales por los cuales no se debe divulgar la información; además, que reflejen las obligaciones particulares de la contraparte para la protección de la información.

Para los terceros a quienes que se les suministre información durante el tiempo de permanencia en las instalaciones de la entidad y/o en el ejercicio de su labor deben firmar el *FO-TI-04 - ACUERDO DE CONFIDENCIALIDAD CON TERCEROS (FO-TI-04)*.

### 6.3.8 Política de desarrollo y mantenimiento seguro de software

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

Los desarrollos nuevos o modificaciones a las aplicaciones actualmente instaladas en producción cuya responsabilidad de administración, desarrollo, mantenimiento y mejora corresponden a la STRT, deben ser formalmente solicitados y autorizados por los directivos o "líderes de proceso", ante la STRT, mediante el formato de *FO-TI-06 - SOLICITUD REQUERIMIENTOS APLICACIONES*, el cual será sometido a un proceso de verificación para aprobación o rechazo. La respuesta a esta solicitud será informada al solicitante para que tome las medidas pertinentes.

Los criterios de inicio de cualquier solicitud aprobada, serán priorizados y corroborados por el (la) Subdirector(a) Técnico(a) de Recursos Tecnológicos, quien notificara formalmente sobre las decisiones tomadas al grupo de trabajo correspondiente.

Todos los trabajos relacionados con la construcción o mantenimiento de aplicaciones son desarrollados por la STRT, los cuales se rigen por los principios de construcción de aplicaciones seguras adoptadas por el Instituto en el procedimiento “Desarrollo de Soluciones" (PR-TI-04).

Para garantizar la debida aplicación de estos principios, se facilitarán al grupo de trabajo de desarrollo o mantenimiento de aplicaciones, todos los elementos (de hardware, software y formación) y ambiente de trabajo más adecuado para el cumplimento de estas labores.

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

Las áreas solicitantes de nuevos desarrollos o modificaciones a desarrollos de software ya existentes, deben asignar a funcionarios idóneos para colaborar en la identificación de requerimientos para la solución requerida, así como para la realización y aprobación de los resultados de las pruebas funcionales.
Se prohíbe el intento de acceso y/o uso, tanto de los recursos físicos, como tecnológicos asignados al grupo de trabajo de la STRT, a personal no autorizado. Esta prohibición se extiende al intento de uso total o parcial de código fuente de las aplicaciones desarrolladas y/o adquiridas por el Instituto.

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

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

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

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

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

Se debe configurar la comunicación segura entre cliente y servidor de manera que esta se cifre, sobre todo cuando se trata de envíos de formularios, por ejemplo, para autenticarse en aplicaciones web.
Se debe llevar un control de las versiones del software, así como mantenerlo actualizado desde que se libera una nueva versión. Ya que, al cabo de un tiempo el sistema se podría volver vulnerable ante exploits públicos que faciliten atacarlo.
Se deben realizar pruebas de seguridad en las aplicaciones, teniendo en cuenta las recomendaciones del proyecto abierto de seguridad de aplicaciones web en ingles denominado **OWASP** (acrónimo de Open Web Application Security Project), aunque las siguientes recomendaciones pueden cambiar con el tiempo es necesario que se consulte la guía de OWASP y se realicen las pruebas recomendadas. A la fecha se recomienda atender las siguientes recomendaciones para evitar que las aplicaciones tengan vulnerabilidades de tipo Cross-Site Scripting (XSS):

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

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

Se deben ocultar los errores provocados por consultas en bases de datos (BBDD), parametrizar las consultas, filtrar y comprobar el valor de las entradas, además de restringir al máximo los permisos del usuario con el que la aplicación se conecta a la BBDD, con esto se evitará la presencia de vulnerabilidades de tipo SQL INJECTION.

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

Identificar y proteger los datos de carácter público clasificado y público reservado [9] que serán tratados en la aplicación, aplicarle controles criptográficos, enmascaramiento, u otras medidas de seguridad para garantizar el cumplimiento legal y evitar posibles fugas de información.

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

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

Se deben cumplir a cabalidad los lineamientos descritos en el documento *DU-TI-06 - POLÍTICAS OPERACIONALES DE TIC* acerca de: Protección del código fuente, desarrollo seguro, realización de pruebas de calidad, datos de prueba e ingeniería de reversa.

### 6.3.9 Política de seguridad de la información para la relación con proveedores

Esta política busca controlar que toda relación con proveedores, y en particular con aquellos que tienen acceso a la información institucional, para que ella esté suficientemente protegida con base en clausulas, acuerdos y contratos correspondientes. Esta protección debe contemplarse antes, durante y a la finalización del servicio, por lo cual se establecen los siguientes lineamientos:

Se debe incluir en los contratos de obra, suministro y prestación de servicios, cláusulas de confidencialidad y no divulgación y de cumplimiento a las políticas de seguridad de la información del IDU. La aplicación de las clausulas será responsabilidad del área que lo requiera, además, la redacción estandarizada y el resguardado de los contratos y acuerdos adicionales ya formalizados será responsabilidad del jefe de área.

Se debe entregar el presente manual de políticas de seguridad de la información a los proveedores del IDU para que tengan presente el cumplimiento que se debe dar a estas.

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

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

Los propietarios de los diferentes sistemas de información deben mitigar los riesgos de seguridad con referencia al acceso de los proveedores y/o contratistas a ellos; es decir que deben aplicar la

[9] Instructivo Identificación de activos de información y uso del módulo de apoyo a la gestión de activos de información (IN-TI-13) Tabla 4. Clasificación frente a confidencialidad Disponible en: HTTP://INTRANET/MANUALPROCESOS/GESTION_TIC/04_INSTRUCTIVOS_GUIAS_CARTILLAS/INTI13_USO_DEL_MODULO_DE_APOYO_A_LA_GESTION_DE_ACTIVOS_DE_INFORMACION_V_2.0.PDF

política de control de acceso e indicar claramente a la STRT los roles y permisos que debe tener cada usuario en cada sistema de información.

En las situaciones en que se requiera contratar servicios de tratamiento o resguardo de activos de información, tales como servicios de hosting, infraestructura, plataforma tecnológica, centros de datos y procesamiento, almacenamiento de información física o digital, entre otros, se deberá verificar que el proveedor cuenta con mecanismos y controles de seguridad adecuados, los que deberán tener, al menos, el mismo estándar existente en el IDU.

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.

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

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

Cuando se requiera elaborar un contrato particular con proveedores que tenga relación con servicios de tratamiento, manipulación, transmisión o almacenamiento de activos de información, ya sea en formato físico o digital, se deberán incorporar cláusulas de seguridad que permitan verificar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información, derechos de auditar los procesos involucrados en el contrato, los procedimientos aplicados frente a incidentes de seguridad, cláusulas de confidencialidad y no divulgación de información, 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 activos de información tipo software, será requisito base implementar configuraciones que cumplan con el estándar de seguridad establecido por la STRT, para lo cual, en caso necesario, deberán considerar ajustes en el acceso a los equipos, el monitoreo de capacidad, la sincronización de hora, el registro de auditoría y los servicios de nombre de dominio (DNS). La STRT tendrá la responsabilidad de verificar y validar la configuración de los equipos instalados, así como también de reportar las debilidades y oportunidades de mejora al proveedor del servicio a través de los procedimientos internos establecidos para estos efectos.

Para el intercambio de información con los proveedores, se deberán implementar estándares y procedimientos formales asociados al intercambio de información, que permitan garantizar razonablemente la seguridad en el acceso y la transferencia de información, considerando la

aplicación de cifrado en las comunicaciones y la validación de identidad. Para los casos en que existan proveedores que requieran acceder a información pública clasificada y/o publica reservada a partir de una solicitud específica, se deberá hacer entrega en medios en los que se pueda aplicar criptografía basada en herramientas con cifrado robusto, para lo cual puede contactar a la STRT quien asesorará a los servidores públicos y/o contratistas de apoyo a la gestión de la mejor forma posible y segura para transferir información.

Para los proveedores que tengan relación con almacenamiento, comunicación, infraestructura, plataforma o software que sean entregados al IDU en la modalidad de servicio, también conocidos como servicios en la nube, además de los equipos tecnológicos que sean adquiridos o sistemas de información que sean desarrollados por terceros y sobre los cuales existan garantías del fabricante, se deberán comunicar entre las partes, establecer y documentar procedimientos para la gestión de incidentes de seguridad, y además la STRT, podrá solicitar informes relacionados con las mediciones de incidentes de algún período, información que deberá estar disponible durante la vigencia del contrato entre el proveedor y el IDU. El procedimiento de seguridad para la gestión de incidentes en cada caso deberá señalar, la persona de contacto, así como el número telefónico y/o correo electrónico al cual habrá que dirigir las solicitudes.

### 6.3.10 Política de seguridad física y del entorno

Esta política busca prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las áreas seguras del IDU, de acuerdo con las siguientes consideraciones:

- Las áreas seguras deben contar con cerramiento físico y control de acceso para el ingreso.
- Se debe contar con un área de recepción y/o vigilancia para controlar el acceso físico a las áreas seguras e instalaciones del IDU.
- Se debe cumplir los lineamientos estipulados en el *MG-RF-03 - MANUAL DE SEGURIDAD Y VIGILANCIA* para el control de acceso físico a las diferentes sedes y áreas del IDU.
- Se debe diligenciar y resguardar el contenido del formato *FO-RF-06 - PLANILLA DE CONTROL DE PERSONAS QUE INGRESAN A ÁREAS RESTRINGIDAS*.
- La última persona que salga de la oficina o área segura, debe ser quien vele por la seguridad física y ambiental, realizando el cierre de las ventanas y puertas del área e informar al personal de vigilancia que no queda nadie en este espacio.

El acceso al IDU por medio de autenticación biométrica o tarjeta de aproximación debe realizarse de acuerdo a lo estipulado en el *MG-RF-03 - MANUAL DE SEGURIDAD Y VIGILANCIA*.

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

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

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

Las áreas restringidas deben tener un control de acceso al espacio físico, que permita el ingreso solamente al personal autorizado.

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

### 6.3.11 Política de uso aceptable de los activos

Esta política busca implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información:

La información institucional en medios físicos se debe manejar de acuerdo con los lineamientos del proceso Gestión Documental, en particular lo indicado en el Manual de Gestión Documental – MG-DO-01 y en el Programa de Gestión Documental – DU-DO-01.

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

Todos los activos de información se deben clasificar y etiquetar de acuerdo con su confidencialidad, siguiendo los lineamientos indicados en la Circular 06 de 2019.

Se deben cumplir a cabalidad los lineamientos descritos en el documento *DU-TI-06 - POLÍTICAS OPERACIONALES DE TIC*.

### 6.3.12 Política de instalación y uso de software

Esta política brinda lineamientos en relación al uso de software e instalación controlada de aplicaciones, ya que una instalación no controlada puede conducir a que se introduzcan vulnerabilidades y posteriormente a fuga de información, pérdida de integridad u otros incidentes de seguridad, e inclusive a la violación de derechos de propiedad intelectual, para lo cual se deben cumplir a cabalidad los lineamientos descritos en el documento *DU-TI-06 - POLÍTICAS OPERACIONALES DE TIC*, en particular los relacionados con Instalación de aplicaciones de software y Utilitarios de administración.

### 6.3.13 Política de copias de respaldo

Esta política busca proteger la información del IDU contra la pérdida de datos, información e imágenes de los sistemas, para lo cual se deben cumplir a cabalidad los lineamientos descritos

en el documento de *DU-TI-06 - POLÍTICAS OPERACIONALES DE TIC*, acerca de, Copias de Seguridad, Protección de los datos y archivos digitales y Protección del código fuente.

### 6.3.14 Política de Privacidad y protección de datos personales

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

### 6.3.15 Política gestión de servidores y equipos de red

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

Se debe hacer de manera periódica o cuando se apliquen cambios, una copia de respaldo de los parámetros de los equipos activos de red o seguridad perimetral.

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

## 7 REFERENCIAS BIBLIOGRÁFICAS

● NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27001 Tecnologías de la información. Técnicas de seguridad. Sistema de Gestión de la Seguridad de la Información. Editada por el ICONTEC en Bogotá 2013-12-20.

● GUIA TÉCNICA COLOMBIANA GTC-ISO/IEC 27002 Tecnologías de la información. Técnicas de seguridad. Código de práctica para controles de seguridad de la información. Editada por el ICONTEC en Bogotá 2015-07-29.