Manual de Políticas de Seguridad y Privacidad de la Información

2025

Aprobó: Líder de proceso	Aprobó: Jefe Subdirección de Planeación
Ivonne Adriana Martínez Zapata	Andrés Felipe Escobar Leal

Versión	Fecha de actualización	Descripción del cambio
1	28/08/2015	Creación
2	30/01/2020	Se actualiza el código del Manual; se integra el tema de MANTIS y del firewall, se actualizó el nombre de la oficina de manera correcta, se integró la última normatividad en materia de seguridad, se actualizaron los nombres de las personas y se retiró el contenido que habla del comité de sistemas ya que esto no opera actualmente.
3	4/06/2021	Se actualiza el nombre de la jefe de la Oficina Asesora de Planeación
4	28/01/2022	Actualizado de acuerdo con el Manual de Funciones vigente.
5	30/01/2023	Se identifica la línea base de seguridad (GAP) trabajado en unión de la Alta Consejería Distrital TIC.
6	04/04/2025	Se actualiza las políticas y lineamientos de seguridad de acuerdo con las políticas organizaciones, de personas, controles físicos y tecnológicos. Así mismo se actualiza y ajusta redacción del objetivo, alcance, referencia normativa, definiciones, sensibilización, aprobación y sanciones.

CONTENIDO

1. OBJETIVO 7

2. ALCANCE 7

3. REFERENCIA NORMATIVA 7

4. DEFINICIONES Y SIGLAS 8

4.1. DEFINICIONES 8

4.2. SIGLAS 9

5. POLITICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN 9

5.1. ORGANIZACIONALES. 9

5.1.1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 9

5.1.2. CONTACTO CON LAS AUTORIDADES 10

5.1.3. CONTACTO CON GRUPOS DE INTERÉS ESPECIAL 10

5.1.4. INTELIGENCIA DE AMENAZAS 10

5.1.5. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS 11

5.1.6. INVENTARIO DE INFORMACIÓN Y OTROS ACTIVOS ASOCIADOS 11

5.1.7. USO ACEPTABLE DE LA INFORMACIÓN Y OTROS ACTIVOS 11

5.1.8. DEVOLUCIÓN DE LOS ACTIVOS 14

5.1.9. CLASIFICACIÓN DE LA INFORMACIÓN 14

5.1.10. ETIQUETADO DE LA INFORMACIÓN 14

5.1.11. TRANSFERENCIA DE INFORMACIÓN 15

5.1.12. CONTROL DE ACCESO 15

5.1.13. GESTIÓN DE IDENTIDAD 15

5.1.14. INFORMACIÓN DE AUTENTICACIÓN 15

5.1.15. DERECHOS DE ACCESO 16

5.1.16. SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON PROVEEDORES 16

5.1.17. ABORDAR LA SEGURIDAD DE LA INFORMACIÓN DENTRO DE LOS ACUERDOS CON PROVEEDORES 16

5.1.18. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA CADENA DE SUMINISTRO DE LA TECNOLOGIA DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES (TIC) 17

5.1.19. MONITOREO, REVISIÓN Y GESTIÓN DEL CAMBIO DE LOS SERVICIOS DE LOS PROVEEDORES 17

5.1.20. SEGURIDAD DE LA INFORMACIÓN PARA EL USO DE SERVICIOS EN LA NUBE 17

5.1.21. PLANIFICACIÓN Y PREPARACIÓN DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 17

5.1.22. EVALUACIÓN Y DESICIÓN SOBRE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN....18
5.1.23. RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN....18
5.1.24. APRENDIZAJE DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.18
5.1.25. RECOLECCIÓN DE EVIDENCIAS....18
5.1.26. SEGURIDAD DE LA INFORMACIÓN DURANTE LA INTERRUPCIÓN. 18
5.1.27. PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DE LA ACTIVIDAD 18
5.1.28. REQUISITOS LEGALES, ESTATUTARIOS REGLAMENTARIOS Y CONTRACTUALES....18
5.1.29. DERECHOS DE PROPIEDAD INTELECTUAL....19
5.1.30. PROTECCIÓN DE REGISTROS....19
5.1.31. PRIVACIDAD Y PROTECCIÓN DE LA INFORMACIÓN DE IDENTIFICACIÓN PERSONAL IIP 19
5.1.32. REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN 19
5.1.33. CUMPLIMIENTO DE POLÍTICAS, REGLAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN 19
5.1.34. PROCEDIMIENTOS OPERATIVOS DOCUMENTADOS....20
5.2. PERSONAS....20
5.2.1. SELECCIÓN 20
5.2.2. CONDICIONES DE EMPLEO....20
5.2.3. SENSIBILIZACIÓN, EDUCACIÓN Y FORMACIÓN EN TÉRMINOS DE SEGURIDAD DE LA INFORMACIÓN 20
5.2.4. PROCESO DISCIPLINARIO 21
5.2.5. RESPONSABILIDADES TRAS EL CESE O CAMBIO DE EMPLEO....21
5.2.6. ACUERDOS DE CONFIDENCIALIDAD O NO DIVULGACIÓN 21
5.2.7. TRABAJO REMOTO 21
5.2.8. INFORMES DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN 22
5.3. CONTROLES FÍSICOS....22
5.3.1. PERIMETROS DE SEGURIDAD FÍSICA 22
5.3.2. ENTRADA FÍSICA 22
5.3.3. PROTECCIÓN DE OFICINAS, SALAS E INSTALACIONES....22
5.3.4. MONITOREO DE LA SEGURIDAD FÍSICA....23
5.3.5. PROTECCIÓN CONREA LAS AMENAZAS FÍSICAS Y MEDIOAMBIENTALES. 23
5.3.6. TRABAJAR EN ÁREAS SEGURAS....23
5.3.7. ESCRITORIO Y PANTALLAS LIMPIAS 23
5.3.8. UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS 23
5.3.9. SEGURIDAD DE LOS ACTIVOS FUERA DE LAS INSTALACIONES....24

5.3.10. MEDIOS DE ALMACENAMIENTO 24
5.3.11. SERVICIOS PÚBLICOS DE RESPALDO 24
5.3.12. SEGURIDAD DEL CABLEADO 24
5.3.13. MANTENIMIENTO DE EQUIPOS 24
5.3.14. ELIMINACIÓN O REUTILIZACIÓN SEGURA DE LOS EQUIPOS 25
5.4. TECNOLÓGICOS 25
5.4.1. DISPOSITIVOS FINALES DE USUARIO 25
5.4.2. DERECHOS DE ACCESO PRIVILEGIADOS 26
5.4.3. RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN 26
5.4.4. ACCESO AL CÓDIGO FUENTE 27
5.4.5. AUTENTICACIÓN DE SEGURIDAD 27
5.4.6. GESTIÓN DE LA CAPACIDAD 27
5.4.7. PROTECCIÓN CONTRA MALWARE 28
5.4.8. GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS 28
5.4.9. GESTIÓN DE LA CONFIGURACIÓN 28
5.4.10. ELIMINACIÓN DE LA INFORMACIÓN 28
5.4.11. ENMASCARAMIENTO DE DATOS 28
5.4.12. PREVENCIÓN DE LA FUGA DE DATOS 29
5.4.13. COPIA DE SEGURIDAD DE LA INFORMACIÓN. 29
5.4.14. REDUNDANCIA DE LAS INSTALACIONES DE TRATAMIENTO DE LA INFORMACIÓN. 29
5.4.15. ACTIVIDADES DE MONITOREO 29
5.4.16. SINCRONIZACIÓN DEL RELOJ 29
5.4.17. USO DE PROGRAMAS DE UTILIDAD PRIVILEGIOS 30
5.4.18. INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS 30
5.4.19. SEGURIDAD DE LAS REDES 30
5.4.20. SEGURIDAD DE LOS SERVICIOS DE RED 31
5.4.21. SEGREGACIÓN DE REDES 31
5.4.22. CICLO DE VIDA DE DESARROLLO SEGURO 31
5.4.23. REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN 31
5.4.24. ARQUITECTURA DE SISTEMAS SEGUROS Y PRINCIPIOS DE INGENIERIA 32
5.4.25. CODIFICACIÓN SEGURA 32
5.4.26. PRUEBAS DE SEGURIDAD EN EL DESARROLLO Y LA ACEPTACIÓN 32
5.4.27. DESARROLLO TERCERIZADO 33
5.4.28. SEPARACIÓN DE LOS ENTORNOS DE DESARROLLO, PRUEBAS Y PRODUCCIÓN 33

5.4.29. GESTIÓN DEL CAMBIO 33

5.4.30. INFORMACIÓN DE LA PRUEBA 33

5.4.31. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN DURANTE LAS PRUEBAS DE AUDITORÍA 34

6. SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN...34

7. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS 34

8. SANCIONES 34

9. ANEXOS 35

1. OBJETIVO

Establecer las Políticas específicas, lineamientos y controles de la Seguridad y Privacidad de la Información del IDT para proteger y salvaguardar la integridad, disponibilidad y confidencialidad de los activos información, brindando a los usuarios directrices para el buen uso de los servicios, herramientas y manejo de la información, promoviendo la mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI.

2. ALCANCE

El presente manual de políticas de seguridad y privacidad de la información aplica a todos los funcionarios, contratistas, proveedores, operadores, entes de control, terceros, usuarios y visitantes del Instituto Distrital de Turismo (IDT) que, en el ejercicio de sus funciones, compartan, utilicen, recolecten, procesen, intercambien o consulten los activos de información de forma interna o externa. Su propósito es proteger la información institucional contra daños, pérdidas o modificaciones accidentales o intencionales, estableciendo directrices para el uso adecuado de los sistemas, servicios informáticos y demás activos de información del IDT para el cumplimiento de las labores contractuales y operativas.

3. REFERENCIA NORMATIVA

a. **Ley 1978 de 2019**. por la cual se moderniza el sector de las tecnologías de la información y las comunicaciones -TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones.

b. **Ley 1712 de 2014**. “Por medio de la cual se crea la Ley de Transparencia y el Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”

c. **Ley 1581 de 2012**. “Por la cual se dictan disposiciones generales para la protección de datos personales”

d. **Ley 1273 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.

e. **Ley 594 de 2000**. Ley general de archivos. Por medio de la cual se dicta la ley general de Archivos y se dictan otras disposiciones. Se encuentra reglamentada parcialmente por el decreto 4124 de 2004. En su Artículo 19, establece “Soporte Documental” Las entidades del Estado podrán incorporar tecnología de avanzada en la administración y conservación de sus archivos, empleando cualquier medio técnico, electrónico, informático, óptico o telemático, siempre y cuando cumplan con los requisitos contemplados en la ley.”

f. **Decreto 1008 de 2018**: por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

g. **Decreto 103 de 2015**: por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

h. **Decreto 1377 de 2013**: por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015.

i. **Directiva Presidencial 02 de 2022**: establece los lineamientos de seguridad digital para las entidades del estado colombiano, con un enfoque en la protección de la infraestructura crítica de la información y la gestión adecuada de los activos digitales.

j. **Modelo Integrado de Planeación y Gestión: MIPG**, Es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión Institucional del MEN y sus Entidades Adscritas y Vinculadas, en términos de calidad e integridad del servicio, con el fin de que se entreguen resultados que atiendan y resuelvan las necesidades y problemas de los grupos de valor.

k. **Manual de Gobierno Digital**: Contiene los lineamientos de la estrategia de Integración del Estado.

4. DEFINICIONES Y SIGLAS

4.1. DEFINICIONES

a. **Activo de Información:** se entiende por todo aquel elemento lógico o físico que conforme cualquiera de los sistemas de información de la Entidad. Ej. Información de bases de datos, programas de computación, plataforma tecnológica (procesamiento de datos o comunicaciones), documentos impresos y Recursos Humano y que tienen un valor para la entidad.

b. **Confidencialidad:** Característica de la información que define que esta sea conocida únicamente por usuarios o entidades autorizadas.

c. **Control**: mecanismo para prevenir o minimizar el riesgo, los cuales pueden ser de carácter administrativo, técnico o legal.

d. **Disponibilidad:** Característica de la información que define la accesibilidad cuando se requiere por los usuarios autorizados.

e. **Integridad:** Característica de la información para definir que esta sea completa y exacta en todo momento y no se modifique o altere sin autorización.

f. **Riesgo**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información

g. **Seguridad de la Información:** Salvaguardar la confidencialidad, integridad y disponibilidad de la información.

4.2. SIGLAS

a. **CID:** Confidencialidad, Integridad y Disponibilidad.

b. **IDT**: Instituto Distrital de Turismo.

c. **LAN**: Red de área local

d. **IIP**: Información de Identificación Personal

e. **SIGTI:** Subdirección de Inteligencia y Gestión de Tecnologías de la Información.

f. **SGC**: Subdirección de Gestión Corporativa.

g. **SGSI:** Sistema de Gestión de Seguridad de la Información

h. **SLA:** Acuerdos de Niveles de servicios.

i. **TI:** Tecnologías de la Información

j. **TIC:** Tecnologías de la Información y las Comunicaciones

k. **TRD:** Tablas de Retención Documental

l. **MSPI:** Modelo de Seguridad y Privacidad de la Información

m. **WAN:** Red de área amplia

5. POLITICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

En el marco del modelo de seguridad y privacidad de la información, establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones, el cual se basa en los estándares internacionales definidos en la norma IEC/ISO 27001:2022 se presentan a continuación las políticas específicas, controles y lineamientos para el IDT.

5.1. ORGANIZACIONALES

5.1.1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas generales y específicas de seguridad y privacidad de la información se encuentran definidas en el documento de Política de Seguridad y Privacidad de la Información IDT, publicado en la intranet de la entidad.
En este se establecen los lineamientos generales, objetivos, principios, roles y responsabilidades y desagregación de funciones en términos de la seguridad y privacidad de la información.

Las políticas específicas establecidas en dicho documento hacen referencia a:

- Organización de seguridad de la información
- Talento humano
- Gestión de activos
- Control de acceso
- Criptografía
- Seguridad física y del entorno
- Seguridad de las operaciones
- Seguridad de las comunicaciones
- Adquisición, desarrollo seguro y mantenimiento de sistemas
- Relaciones con los proveedores
- Gestión de incidentes de seguridad de la información
- Seguridad de la información de la gestión de continuidad de negocio
- Cumplimiento

5.1.2. CONTACTO CON LAS AUTORIDADES

El IDT, mediante las diferentes Subdirecciones mantiene contacto con las autoridades pertinentes, atendiendo el procedimiento de gestión de incidentes de seguridad de la entidad. GT-P13 Procedimiento para Gestión de Incidentes de Seguridad de la Información.

5.1.3. CONTACTO CON GRUPOS DE INTERÉS ESPECIAL

La Subdirección de Inteligencia y Gestión de Tecnologías de la Información establece contacto con grupos, foros, asociaciones y entidades, tanto públicas como privadas, que aborden temas actualizados sobre seguridad de la información. Este acercamiento permite implementar acciones de mejora, prevención y corrección, fortaleciendo así la seguridad de la información en la entidad.
La SIGTI tiene contacto con los siguientes grupos de interés

Tabla 1. Grupos de interés

GRUPO DE INTERÉS	CONTACTO
Centro Cibernético de la Policía	https://caivirtual.policia.gov.co
Grupo de Respuesta a Emergencias Cibernéticas de Colombia Colcert	https://www.colcert.gov.co
Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL	https://cc-csirt.policia.gov.co
Contacto con los fabricantes a través de sus canales de alertas de vulnerabilidades y actualizaciones para ambientes de hardware/software	Contacto específico para cada fabricante.
Alta Consejería TIC	https://tic.bogota.gov.co/

5.1.4. INTELIGENCIA DE AMENAZAS

La SIGTI participa en programas de intercambio de información a nivel nacional sobre amenazas en Colombia, lo que fortalece las medidas de defensa y la resiliencia ante ciberataques, posterior a un análisis de su impacto y clasificando los riesgos según su gravedad y probabilidad de ocurrencia en la entidad.

Por su parte, la SIGTI atiende a los comunicados de orden nacional y distrital sobre alertas de amenazas relevantes para las entidades públicas, permitiendo una actualización constante y la toma de decisiones informadas para fortalecer la seguridad, anticipar vulnerabilidades y garantizar la continuidad de las operaciones.

Asi mismo, de manera anual en el Plan Institucional de Capacitación se definen y realizan campañas de sensibilización sobre la adopción de buenas prácticas de seguridad de la información, fomentando un comportamiento responsable en el manejo de los activos de información y promoviendo una cultura de seguridad dentro de la entidad.

5.1.5. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS

La gestión de proyectos considera como componente transversal la seguridad de la información, la cual debe estar incluida desde la etapa inicial y durante la ejecución, identificando y gestionando los posibles riesgos de seguridad digital que se puedan presentar en el proyecto.

5.1.6. INVENTARIO DE INFORMACIÓN Y OTROS ACTIVOS ASOCIADOS

Como lo indica la política de activos de información, estos son identificados, clasificados, valorados, inventariados y actualizados periódicamente por el propietario, de acuerdo con la Guía para la gestión de activos de información (GT-I06) y por medio del Formato Inventario de activos de información (GT-F14).

5.1.7. USO ACEPTABLE DE LA INFORMACIÓN Y OTROS ACTIVOS

Esta política establece el uso aceptable de los activos de información de la entidad y por ende los servidores públicos y contratistas son responsables de reportar cualquier uso no aceptable que evidencie, por medio de la mesa de ayuda.

La entidad establece directrices para el uso adecuado de los activos de información. En este sentido, el Manual de Políticas para la Administración y Uso de las Tecnologías de la Información y la Comunicación (GT-M03) define las normas para el uso responsable de los servicios de internet, correo electrónico, redes y telecomunicaciones, así como el manejo de información.

A continuación se define pautas generales para asegurar la protección de la información de otros servicios de TI.

Servicio de Intranet

El servicio de Intranet hace referencia a la plataforma de comunicación y gestión interna que permite a los servidores y contratistas de la entidad acceder a información, aplicaciones y recursos de manera segura y eficiente.

Acceso y Uso Permitido

- Este servicio debe utilizarse exclusivamente para las actividades propias de la función desarrollada en el IDT.
- El servicio debe ser empleado para una finalidad operativa y administrativa en relación con la entidad.

- Los usuarios son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información del IDT.
- El servicio solo puede ser accedido por servidores o contratista del IDT, por medio de un usuario y contraseña previamente activada por la mesa de ayuda la entidad.
- Los servicios a los que un determinado usuario pueda acceder desde la Intranet dependerán del rol que desempeña el usuario en la entidad y para los cuales este formal y expresamente autorizado.

Uso Prohibido

- La cuenta de acceso al servicio de intranet no debe suministrarse o compartirse con otras personas o exhibirse en público.

Disposiciones generales

La Subdirección de Inteligencia y Gestión de Tecnologías de la Información es el encargado de proporcionar el servicio de acceso institucional a Intranet, en su rol de custodio de este. Para tal fin asigna una cuenta de usuario que tendrá asociados unos privilegios específicos y una clave de acceso.

La Oficina Asesora de comunicaciones junto con la Subdirección de Planeación son los propietarios de la Intranet, por ende son quienes administran y autorizan la información a disponer en el sitio.

Todo usuario es responsable de informar los contenidos o accesos a servicios que no le estén autorizados o no correspondan a sus funciones o actividades dentro de la entidad a través de la mesa de ayuda.

El requerimiento para publicar información en la Intranet debe atender a los procedimientos definidos por los propietarios y administradores del servicio.

Ante la ocurrencia de eventos o incidentes que afecten los servicios y recursos tecnológicos con los que dispone e IDT y que puedan comprometer la seguridad de la información de la entidad, podrá realizar actividades de revisión, escaneo y análisis a estos recursos o servicios tecnológicos, con el fin investigar o dar solución al incidente.

Redes Sociales

El servicio de redes sociales en la entidad tiene como objetivo gestionar la comunicación digital y la interacción con ciudadanos o usuarios a través de plataformas como Facebook, X, Instagram y YouTube.

Acceso y Uso Permitido

- Los servidores públicos y contratistas son responsables de evitar prácticas o usos que pongan en riesgo la seguridad de la información en las redes sociales.
- Toda comunicación realizada a través de este servicio puede ser monitoreada por el administrador del sistema o por las instancias de vigilancia y control competentes.
- La entidad proporciona acceso a estas herramientas como apoyo a diversas actividades institucionales; no obstante, su uso debe ser responsable, adecuado y moderado.

Uso Prohibido

- Está prohibido compartir o publicar información que afecte la integridad moral de personas o instituciones.
- El uso de las redes sociales debe estar exclusivamente relacionado con las actividades del IDT; cualquier otro propósito no está permitido.
- No se permite la descarga, difusión o distribución de material obsceno, degradante, terrorista, abusivo o calumnioso a través del servicio de redes sociales.
- Los servidores públicos y contratistas del IDT no pueden crear cuentas, abrir grupos ni publicar información escrita o audiovisual en nombre de la entidad. Cualquier iniciativa en este sentido debe ser consultada con la Oficina Asesora de Comunicaciones.
- No está permitido crear o vincular cuentas personales de redes sociales utilizando el correo electrónico institucional.

Disposiciones generales

La Oficina Asesora de Comunicaciones son los propietarios, administradores y responsables de las redes sociales del IDT.

La Oficina Asesora de Comunicaciones establece los lineamientos para la adecuada administración, interna y externa, de los canales sociales digitales del Instituto Distrital de Turismo, por medio del Manual Gestión de la Comunicación en Redes Sociales (CO-M03).

Recursos Tecnológicos

Los recursos tecnológicos proporcionan a los servidores públicos y contratistas las herramientas necesarias para el desempeño de sus funciones, garantizando eficiencia, seguridad y continuidad en las operaciones de la entidad.

Acceso y Uso Permitido

- Las configuraciones en los componentes de red solo pueden ser realizadas por los administradores designados en la SIGTI, utilizando exclusivamente las herramientas autorizadas para este propósito.
- Cuando un colaborador se ausente de su puesto de trabajo o se retire de las instalaciones, debe bloquear la sesión de su estación de trabajo para evitar accesos no autorizados a la información.
- Todo software instalado en los equipos de cómputo de la entidad debe estar autorizado y contar con su respectiva licencia de uso. La instalación solo puede ser realizada por la Mesa de Ayuda, el único equipo autorizado para esta tarea.

Uso Prohibido

- Los usuarios no están autorizados para modificar la configuración de las estaciones de trabajo, incluyendo conexiones de red, usuarios locales, papel tapiz y protector de pantalla institucional. Cualquier ajuste en estos aspectos debe ser realizado exclusivamente por la SIGTI.
- Está prohibido alterar o desactivar los controles de seguridad implementados en los equipos de cómputo.

- Los recursos tecnológicos deben utilizarse exclusivamente para las actividades de la entidad y no pueden emplearse para fines personales, ilícitos o no autorizados.

Disposiciones generales

- La SIGTI define el software y las aplicaciones permitidas para su instalación en las estaciones de trabajo de los usuarios, restringe la configuración de los equipos y supervisa el cumplimiento del licenciamiento del software y sus aplicaciones asociadas.

- Una vez se de baja a una licencia de un software se debe desinstalar y velar por que no sea utilizada.

5.1.8. DEVOLUCIÓN DE LOS ACTIVOS

Todo activo de propiedad del IDT, asignado a un servidor público, contratista o tercero, debe ser devuelto al finalizar el contrato o en caso de cambio de cargo. Esto incluye documentos institucionales, equipos de cómputo (hardware y software), dispositivos móviles, tarjetas de acceso, manuales, tarjetas de identificación y cualquier información almacenada en dispositivos móviles o extraíbles.

Para el traslado de equipos de cómputo al almacén, su reasignación a otro servidor público o su baja del inventario se debe solicitar a la mesa de ayuda un respaldo de la información contenida en el equipo. Posteriormente, se procede con el borrado seguro de los datos.

Cada servidor o contratista al que se le haya asignado un token debe llevarlo consigo en todo momento para su uso en los sitios autorizados. Además, es responsable de su correcto uso y disponibilidad, debiendo devolverlo a su jefe cuando corresponda.

5.1.9. CLASIFICACIÓN DE LA INFORMACIÓN

La clasificación de los activos de información se establece conforme a la Ley 1712 de 2014 sobre transparencia y acceso a la información pública. Esta normativa determina que la información producida por las entidades del Estado es de naturaleza pública y, en sus artículos 18 y 19, la clasifica en Pública, Pública Clasificada y Pública Reservada,

El nivel de clasificación se determina basado en la Confidencialidad como principio rector en la selección, estableciendo un nivel de bajo para la información Pública, nivel medio para la información Pública Clasificada y Alto para la Información Pública Reservada.

Los lineamientos para esta clasificación están definidos en la Guía para la Gestión de Activos de Información (GT-I06). Los líderes de proceso son responsables de clasificar los activos dentro de su ámbito de gestión.

La SIGTI brinda apoyo a los líderes de proceso, proporcionándoles la metodología de clasificación y asesorándolos en su correcta aplicación.

5.1.10. ETIQUETADO DE LA INFORMACIÓN

Los activos de información sujetos a etiquetado son aquellos que, conforme a la Ley 1712 de 2014, pueden clasificarse como Públicos Clasificados o Públicos Reservados. Estos deben llevar una etiqueta que indique el nivel de clasificación determinado por su propietario.

Por otro lado, los activos de tipo software, hardware, servicios, intangibles, componentes de red y personas pueden contener activos de información, pero no están sujetos a clasificación según la ley, por lo que no requieren etiquetado.

Cada área del IDT, en su calidad de propietaria de activos de información, es responsable de etiquetar aquellos activos de información que hayan sido clasificados.

5.1.11. TRANSFERENCIA DE INFORMACIÓN

El IDT debe establecer políticas y procedimientos formales para la transferencia de información con otras entidades y terceros.

La transmisión de información debe realizarse exclusivamente a través de los canales oficiales designados por la entidad.

Está prohibido enviar información Pública Clasificada o Pública Reservada mediante redes WiFi públicas, gratuitas o sin contraseña, ya que estas conexiones son inseguras y vulnerables a interceptaciones.

5.1.12. CONTROL DE ACCESO

El propietario de los activos de información es responsable de definir, autorizar, restringir y revisar periódicamente el acceso a los aplicativos o sistemas de información, conforme al perfil o rol asignado a cada usuario.

La SIGTI, previa solicitud de las áreas y en cumplimiento del Procedimiento de Gestión de Usuarios y Creación de Contraseñas (GT-P15), se encarga de otorgar o cancelar las credenciales de acceso a los servicios de red, correo y sistemas de información.

Las credenciales de acceso son personales e intransferibles. Su correcta administración y uso son responsabilidad exclusiva del servidor público o contratista al que han sido asignadas.

5.1.13. GESTIÓN DE IDENTIDAD

La SIGTI, a través de la Mesa de Ayuda, activa o elimina las cuentas de usuario conforme al Procedimiento de Gestión de Usuarios y Creación de Contraseñas (GT-P15), garantizando así el acceso autorizado a los servicios de TI de la entidad.

5.1.14. INFORMACIÓN DE AUTENTICACIÓN

Los servidores públicos, contratistas y pasantes de la entidad deben mantener la confidencialidad de su información de autenticación. No está permitido divulgar, compartir ni registrar por escrito sus credenciales en ningún medio físico. Además, deben cambiar su contraseña ante cualquier evento que pueda comprometer la seguridad de la información.

Las contraseñas deben ser seguras y difíciles de predecir. Se prohíbe el uso de claves secuenciales, fácilmente deducibles o que contengan información personal. Deben ser alfanuméricas, incluir mayúsculas, minúsculas y caracteres especiales, y tener una longitud mínima **de ocho (8) caracteres**.

Las cuentas corporativas no pueden utilizarse para registrarse en formularios o páginas web ajenas a los fines de la entidad, con el objetivo de evitar su inclusión en listas de correos fraudulentos o publicitarios. Asimismo, las contraseñas utilizadas para autenticación en los sistemas de información y servicios de la entidad no deben emplearse en cuentas personales.

Cualquier sospecha o indicio de uso indebido de una cuenta o contraseña asignada debe reportarse de inmediato a la mesa de ayuda de la entidad.

Los servidores públicos, contratistas y pasantes deben cambiar las contraseñas la primera vez que usen las cuentas asignadas

El IDT cuenta con un sistema de directorio activo que garantiza la calidad de las contraseñas, asegurando el cumplimiento de requisitos de longitud y complejidad. Además, este sistema mantiene un historial de contraseñas utilizadas por los usuarios, evitando su reutilización.

5.1.15. DERECHOS DE ACCESO

Los propietarios de los activos de información son los responsables de establecer los roles de acceso, para facilitar la administración de usuarios e indicar al custodio que en de acuerdo con el sistema de información, o servicio puede ser las diferentes subdirecciones las restricciones o acceso por rol se deben asignar, así mismo deberán informar al custodio las novedades que conlleven a la inactivación o cancelación de acceso.

Con el objetivo de garantizar la seguridad de los activos de información, se implementa el formato "Devolución de Inventarios y Cancelación de Servicios" (GB-F09). Este documento funciona como un paz y salvo, permitiendo que servidores públicos y contratistas obtengan los vistos buenos de las áreas responsables para la verificación, entrega de bienes y cancelación de accesos al momento de su retiro.

5.1.16. SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON PROVEEDORES

En los contratos o acuerdos con terceros que impliquen el intercambio, uso o procesamiento de información de la entidad, se establecen Acuerdos de Confidencialidad para garantizar su adecuado manejo. Estos acuerdos forman parte integral de los documentos que formalizan la relación comercial y deben definir con claridad el tipo de información que será compartida entre las partes.

La Subdirección Jurídica es responsable de incluir en los contratos con terceros y proveedores los requisitos legales y regulatorios relacionados con la protección de datos personales, derechos de propiedad intelectual y derechos de autor.

5.1.17. ABORDAR LA SEGURIDAD DE LA INFORMACIÓN DENTRO DE LOS ACUERDOS CON PROVEEDORES

Las condiciones de seguridad de la información que deben cumplir los proveedores son definidas en el pliego de condiciones, documento que forma parte integral del expediente contractual y que, por lo tanto, debe ser firmado por ambas partes.

5.1.18. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA CADENA DE SUMINISTRO DE LA TECNOLOGIA DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES (TIC)

En los procesos de contratación para la adquisición de recursos tecnológicos, se consideran aspectos de seguridad en la cadena de suministro de productos y servicios de tecnologías de la información y la comunicación. Los requisitos de seguridad se especifican en la ficha técnica del objeto a contratar. Además, se exigen pólizas de cumplimiento y garantías sobre los servicios y/o productos contratados, basadas en los niveles de servicio establecidos.

5.1.19. MONITOREO, REVISIÓN Y GESTIÓN DEL CAMBIO DE LOS SERVICIOS DE LOS PROVEEDORES

Según la criticidad de la información, los sistemas y la valoración de riesgos, se deben gestionar los cambios necesarios con los proveedores, incluyendo el mantenimiento o mejora de los procesos y controles de seguridad. Estos cambios deben realizarse en coordinación con la SIGTI, garantizando que la gestión de cambios se lleve a cabo sin afectar la operación ni la prestación del servicio.

5.1.20. SEGURIDAD DE LA INFORMACIÓN PARA EL USO DE SERVICIOS EN LA NUBE

El IDT debe definir en los contratos con los proveedores Acuerdos de Niveles de servicios (SLA) esperados, tiempos de respuesta ante incidentes y medidas de protección de datos con los proveedores que suministran el servicio de nube.

Se deben identificar y analizar los riesgos asociados al almacenamiento, procesamiento y transmisión de la información en la nube.

Se debe asegurar que los proveedores de servicios en la nube cumplan con estándares de seguridad reconocidos, como ISO 27001, NIST, o SOC 2, y con la normativa legal vigente, así como asegurar que el servicio en la nube cumpla con la normativa de protección de datos aplicable, como la Ley 1581 de 2012.

El proveedor del servicio debe suministrar mecanismos de autenticación robustos, como autenticación multifactor (MFA), y establecer permisos según los roles de los usuarios autorizados por el IDT.

El proveedor debe realizar seguimiento continuo del uso de los servicios en la nube, identificando accesos indebidos o actividades sospechosas.

La entidad debe establecer con el proveedor estrategias de respaldo y recuperación ante desastres para asegurar la disponibilidad y continuidad del servicio.

5.1.21. PLANIFICACIÓN Y PREPARACIÓN DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La entidad cuenta con el Procedimiento para la Gestión de Incidentes de Seguridad de la Información (GT-P13), el cual establece que la mesa de ayuda es la primera instancia encargada de atender estos incidentes. En caso de ser necesario, se realiza la escalación correspondiente para su adecuada gestión. El objetivo es mitigar posibles daños y adoptar las medidas necesarias para proteger los activos de información de la

entidad.

5.1.22. EVALUACIÓN Y DESICIÓN SOBRE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

La Subdirección de Inteligencia y Gestión de TI evalúa los eventos de seguridad para determinar si califican como incidentes. En caso de ser necesario, se realiza el reporte al CSIRT, permitiendo así iniciar las investigaciones correspondientes y tomar las acciones legales pertinentes.

5.1.23. RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La SIGTI gestiona oportunamente los incidentes de seguridad de la información, realizando un análisis previo, recopilando evidencia y registrando cada acción tomada para garantizar una solución efectiva. Todo esto se lleva a cabo conforme a lo establecido en el Procedimiento para la Gestión de Incidentes de Seguridad de la Información (GT-P13).

5.1.24. APRENDIZAJE DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Entidad dispone de un procedimiento para documentar las lecciones aprendidas, permitiendo generar una base de conocimientos sobre los incidentes analizados y resueltos. Esto facilita una respuesta rápida en caso de que se repitan y contribuye a la implementación de medidas para reducir, controlar o prevenir futuros incidentes.

5.1.25. RECOLECCIÓN DE EVIDENCIAS

La recolección de evidencia se realiza siguiendo los lineamientos de la Guía 13 de Evidencia Digital del Ministerio de Tecnologías de la Información y las Comunicaciones, tomando como referencia, cuando corresponda, el Manual Único de Cadena de Custodia de la Fiscalía General de la Nación.

5.1.26. SEGURIDAD DE LA INFORMACIÓN DURANTE LA INTERRUPCIÓN.

Ante eventos imprevistos que afecten la disponibilidad de los controles de seguridad de la información, la SIGTI implementa el Procedimiento de Recuperación de Información (GT-P02), asegurando la continuidad de la seguridad de la información conforme a los criterios establecidos.

5.1.27. PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DE LA ACTIVIDAD

Se ha establecido el Plan de Contingencia Tecnológica (GT-PR02), el cual define las estrategias y acciones necesarias para garantizar la continuidad de los servicios de Tecnologías de la Información (TI) en caso de incidentes que puedan afectar su disponibilidad, integridad o confidencialidad.

5.1.28. REQUISITOS LEGALES, ESTATUTARIOS REGLAMENTARIOS Y CONTRACTUALES

Las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, se identifican y establecen en el normograma de la Entidad.

5.1.29. DERECHOS DE PROPIEDAD INTELECTUAL

El software utilizado en la entidad cuenta con las licencias correspondientes y su asignación es gestionada exclusivamente a través de la mesa de ayuda.

Está estrictamente prohibido almacenar, descargar desde Internet, intercambiar, utilizar, copiar, reproducir o instalar software no autorizado, así como cualquier tipo de contenido protegido por derechos de propiedad intelectual (música, videos, documentos, textos, fotografías, gráficos y otras obras), sin la debida licencia o autorización legal. Esta restricción busca garantizar el cumplimiento de la legislación sobre derechos de autor.

Se permite el uso de documentos, datos y textos de carácter público, siempre y cuando se cite adecuadamente al autor, con el fin de preservar los derechos morales e intelectuales de las obras o referencias utilizadas.

Control Interno verifica anualmente el cumplimiento de las normativas relacionadas con los derechos de autor en el uso del software.

En los documentos contractuales se especifican los derechos de autor, diferenciando entre los derechos patrimoniales y morales, para asegurar el cumplimiento normativo y la protección de la propiedad intelectual.

5.1.30. PROTECCIÓN DE REGISTROS

La definición de los lineamientos sobre la retención, almacenamiento y los periodos de retención de los registros se definen en las tablas de retención documental la cual lidera la Subdirección Corporativa, pero se establecen con cada una de las dependencias.

5.1.31. PRIVACIDAD Y PROTECCIÓN DE LA INFORMACIÓN DE IDENTIFICACIÓN PERSONAL IIP

El IDT cuenta con una política de protección de datos personales en cumplimiento de la Ley 1581 de 2012, la cual establece el régimen general de Protección de Datos Personales. Esta política está disponible para consulta en la página web de la entidad.
Se deben definir y formalizar condiciones contractuales y medidas de seguridad con los proveedores o entidades externas autorizadas para el tratamiento de los datos personales bajo custodia del IDT, garantizando así su adecuado manejo y protección.

5.1.32. REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN

Control interno de manera anual realiza la auditoría interna al Modelo de Seguridad y Privacidad de la Información, en el marco del cumplimiento de las políticas de gobierno y seguridad digital.

5.1.33. CUMPLIMIENTO DE POLÍTICAS, REGLAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN

La Entidad establece directrices claras para garantizar el cumplimiento de las políticas, normas y estándares

de seguridad de la información, como lo que se define en la Política de Seguridad y Privacidad de la Información IDT, el Manual de Políticas para la Administración y Uso de las Tecnologías de la Información y la Comunicación (GT-M03) y en el presente documento.

La SIGTI debe diligenciar la Matriz de Declaración de aplicabilidad (SOA), con el fin de revisar la implementación de controles de seguridad en la entidad.

5.1.34. PROCEDIMIENTOS OPERATIVOS DOCUMENTADOS

La entidad cuenta con procedimiento de las actividades operaciones, en lo que refiera a TI, e relacionan los procesos propios de configuración, instalación, accesos, bakup, recuperación entre otros con el fin de conocer las acciones a seguir frente a cualquier eventualidad que afecte los servicios de TI, evaluar procesos de mejora y generar instrucciones claras para una buena conducta en términos de seguridad de la información.

5.2. PERSONAS

5.2.1. SELECCIÓN

Servidores Públicos

Los procesos de vinculación en la Entidad son regulados por la normativa vigente, la cual permite garantizar la idoneidad, así como el cumplimiento de las políticas de seguridad de la información. El proceso de vinculación del personal se divide en tres grupos: carrera administrativa, provisionalidad y Libre nombramiento y remoción, ver Procedimiento para la provisión del Talento Humano en empleos de carrera administrativa (TH-P02).

Contratistas

Por medio de la Subdirección Jurídica se realiza el proceso de vinculación de los contratistas, definido en el Procedimiento de Prestación de servicios profesionales y de apoyo a la gestión (JC-P10) y Manual de Contratación (JC-M01) a través de los cuales se busca garantizar el personal idóneo para ejercer el rol y a su vez proteger los activos de información a los que pueda tener acceso para el desarrollo de sus funciones.

5.2.2. CONDICIONES DE EMPLEO

Los servidores públicos, contratistas y pasantes del IDT deben cumplir con los requerimientos de seguridad de la información y estos deben hacer parte integral de los contratos o documentos de vinculación a que haya lugar.

5.2.3. SENSIBILIZACIÓN, EDUCACIÓN Y FORMACIÓN EN TÉRMINOS DE SEGURIDAD DE LA INFORMACIÓN

El IDT promueve espacios de capacitación y socialización dirigidos a servidores públicos y contratistas, con el propósito de fortalecer sus conocimientos y habilidades para un desempeño eficiente, garantizando la protección de los recursos e información de la Entidad.

Los planes de capacitación, socialización y comunicación del SGSI están alineados con los procesos de

Gestión del Talento Humano y Comunicaciones.

La Entidad define anualmente un plan de comunicaciones que establece los procesos de formación, entrenamiento y sensibilización en Seguridad de la Información.

5.2.4. PROCESO DISCIPLINARIO

Todos los incidentes de seguridad de la información ocurridos en la entidad deben ser gestionados adecuadamente para identificar sus causas y responsables. A partir del análisis de los reportes y la evaluación de la gravedad de cada incidente, se adoptarán las acciones necesarias y se realizarán los trámites correspondientes ante las instancias competentes.

Las violaciones a las Políticas de Seguridad serán sancionadas conforme al Código Disciplinario Único, aplicando las medidas administrativas, disciplinarias o penales que correspondan según la normativa vigente de la Entidad.

5.2.5. RESPONSABILIDADES TRAS EL CESE O CAMBIO DE EMPLEO

Los servidores públicos y contratistas deben cumplir con las responsabilidades y deberes de seguridad de la información establecidos en la Entidad, en donde se incluyen aquellos que permanecen válidos después de la terminación o cambios en el contrato.

5.2.6. ACUERDOS DE CONFIDENCIALIDAD O NO DIVULGACIÓN

Se debe firmar Acuerdos de Confidencialidad con servidores públicos, contratistas, pasantes y terceros, en el momento de la posesión para el caso de los servidores públicos de carrera y provisionales y para contratistas, pasantes y terceros al momento de firmar el Contrato. En estos acuerdos deben quedar especificadas las responsabilidades para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información. Lo anterior puede establecerse dentro del contrato.

5.2.7. TRABAJO REMOTO

La entidad establece la Política Interna de Teletrabajo (TH-P05), en la cual el proceso de talento humano define los lineamientos para que los servidores puedan acceder a esta modalidad.

Mediante el Procedimiento para la selección y seguimiento de la modalidad de teletrabajo en el IDT (TH-P04), la entidad establece los pasos a seguir que inicia con la postulación del servidor público de planta a la modalidad de teletrabajo y termina con la negativa o aprobación de la solicitud y su seguimiento mensual hasta el fin de la vigencia acordada o la reversión de la resolución de la solicitud de teletrabajo según sea el caso.

Para esto y en complemento al procedimiento, el IDT ha generado los siguientes formatos TH-F54 Formato Reversibilidad del Teletrabajo, TH-F53 Formato Evaluación y Avance del Teletrabajo, TH-F52 Formato Compromiso del Teletrabajo, TH-F51 Formato Planificación y Seguimiento del Teletrabajo, TH-F50 Formato Aprobación del Teletrabajo y TH-F49 Formato Postulación Para Teletrabajo.

Los servidores a los que se les autorice el teletrabajo deben proveer su equipo de cómputo, así como una conexión a internet segura y debe tener instalado un antivirus actualizado.

Las solicitudes de acceso remoto se deben realizar a través de la mesa de ayuda, con la autorización del jefe inmediato, donde se justifique las razones laborales por la cual se requiere este permiso y la SIGTI autorizará de acuerdo con los recursos disponibles en la entidad. El acceso se otorgará por un tiempo limitado y atendiendo lo solicitado por el jefe.

5.2.8. INFORMES DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

Cada servidor público, contratista y pasante de la entidad tiene el deber de informar de manera inmediata cualquier evento, incidente o vulnerabilidad relacionada con la seguridad de la información a través de la mesa de ayuda.

La entidad por medio de la alta consejería TIC, realiza de manera anual un análisis de vulnerabilidades a los sitios web de la entidad.

5.3. CONTROLES FÍSICOS

5.3.1. PERIMETROS DE SEGURIDAD FÍSICA

La entidad cuenta con los siguientes controles periféricos de seguridad:

Externos:

- Recepción en la entrada del edificio, personal a cargo del control de acceso físico de las personas que ingresan a la Entidad.
- Zonas de parqueadero, servicio de vigilancia, tarjeta de acceso y cámaras de seguridad.
- Zona de despacho y descarga, servicio de vigilancia, tarjeta de acceso y cámaras de seguridad.

Internos:

- Acceso controlado a los diferentes pisos y a la Dirección General
- Centros de cableado con acceso biométrico.

5.3.2. ENTRADA FÍSICA

El acceso a la entidad para para servidores y contratistas es a través de huella.

Todo visitante debe registrarse en la recepción del edificio, dejando constancia de la fecha y hora de ingreso y salida. Además, su acceso deberá contar con la autorización del funcionario a quien va a visitar.

Las áreas seguras, dentro de las cuales se encuentran el Centro de Cómputo cuenta con control de acceso biométrico y registro de ingreso y salida, cuenta con acceso restringido del SIGTI. El acceso por parte de proveedores o personal externo previamente autorizado y se registra en la bitácora del Centro de Datos.

5.3.3. PROTECCIÓN DE OFICINAS, SALAS E INSTALACIONES

La entidad centraliza el control de acceso con un responsable del IDT, quien reporta a recepción y servicio de vigilancia, la autorización de acceso o habilitación de huella, para los servidores y contratistas.

Los visitantes deben ser autorizados para ingresar al IDT previamente mediante correo electrónico, cuando se encuentren en las oficinas o áreas donde se maneje información, deben estar acompañados de un servidor.

5.3.4. MONITOREO DE LA SEGURIDAD FÍSICA

Las instalaciones cuentan con sistema de video vigilancia en cada piso, en los ascensores y puertas de acceso, el cual es monitoreado en la recepción.

5.3.5. PROTECCIÓN CONREA LAS AMENAZAS FÍSICAS Y MEDIOAMBIENTALES.

Las instalaciones están protegidas frente a siniestros ocasionados por el ser humano o desastres naturales, como incendios, inundaciones, terremotos y explosiones, mediante pólizas de seguro y controles implementados por la Subdirección Corporativa. Además, en cada piso se dispone de extintores para una respuesta inmediata ante emergencias.

5.3.6. TRABAJAR EN ÁREAS SEGURAS

Restricción de acceso a los centros de cableados y de datos, por medio de un sistema biométrico.

Registro de visitantes, proveedores o personal externo que realice labores puntuales en zonas restringidas y siempre acompañadas de un servidor o contratista de la entidad.

5.3.7. ESCRITORIO Y PANTALLAS LIMPIAS

Los servidores públicos, contratistas y pasantes deben conservar su escritorio libre de información propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

Al imprimir documentos que contengan información pública clasificada y publica reservada, estos deben ser retirados de la impresora inmediatamente. Así mismo, no se deberá reutilizar papel que contenga dicha información.

En horarios no hábiles o cuando los sitios de trabajo se encuentren desatendidos, toda información clasificada o reservada debe resguardarse bajo llave. Esto aplica a documentos impresos, discos compactos, dispositivos USB y otros medios de almacenamiento removibles.

Cada vez que los funcionarios se retiren del lugar de trabajo deben bloquear los equipos de cómputo.

Para fortalecer la seguridad de los equipos, todos los computadores de la entidad deben contar con un protector de pantalla activado automáticamente tras un máximo de tres (3) minutos de inactividad.

5.3.8. UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS

Existe la prohibición de comer, consumir líquidos y fumar dentro o cerca de los centros de cómputo o de cableado, además de contar con un sistema de registro de acceso por parte del personal autorizado.

Las condiciones ambientales del centro de cómputo se garantizan por medio del uso del aire acondicionado

permitiendo las condiciones ideales de humedad, minimizando los escenarios que puedan afectar negativamente las instalaciones de los centros de cómputo o de cableado.

5.3.9. SEGURIDAD DE LOS ACTIVOS FUERA DE LAS INSTALACIONES

Los servidores públicos y contratistas con equipos portátiles asignados, al retirarlos de la oficina no deben dejarlos desatendidos en lugares o sitios públicos, en los cuales puedan ser sustraídos, ni conectarlos a redes públicas o desprotegidas.

Los equipos de cómputo de la entidad al ser retirados, se conservan las políticas de no tener privilegios de usuario administración, y contar con antivirus.

5.3.10. MEDIOS DE ALMACENAMIENTO

Los equipos de cómputo deben ser retirados de la Entidad con la autorización formal, de acuerdo con lo establecido por la Subdirección Corporativa.

5.3.11. SERVICIOS PÚBLICOS DE RESPALDO

La infraestructura tecnológica (hardware y comunicaciones) cuenta con medidas de protección eléctrica como UPS y planta eléctrica,

5.3.12. SEGURIDAD DEL CABLEADO

El acceso a los centros de cableados es controlado de manera biométrica, cuya autorización es limitada para el SIGTI.

Mediante una bitácora se registra el acceso y las actividades que se realicen en el centro de cableado.

El cableado eléctrico y de red, deben estar separados y protegidos de interceptaciones de acuerdo con la normativa vigente.

5.3.13. MANTENIMIENTO DE EQUIPOS

El mantenimiento a los equipos se debe realizar de manera periódica, en donde se lleve un registro de las actividades realizadas y debe realizarse únicamente por la SIGTI.

El soporte y mantenimiento de los activos de TI que soportan los sistemas de información de la entidad, su funcionamiento, disponibilidad y actualización es responsabilidad de la Subdirección de Inteligencia y Gestión Tecnológica.

El Instituto Distrital de Turismo no se hará responsable de mantenimiento, soporte o licenciamiento de los equipos o software que no hacen parte del Inventario oficial de la entidad, y que sean utilizados dentro de las instalaciones.

Subdirección de Inteligencia y Gestión Tecnológica debe gestionar los elementos necesarios para adelantar el plan de soporte y mantenimiento de los activos tecnológicos de la entidad.

5.3.14. ELIMINACIÓN O REUTILIZACIÓN SEGURA DE LOS EQUIPOS

Se debe realizar una copia de respaldo de la información institucional a los equipos de cómputo que sean reasignados o dados de bajo por obsolescencia o falla, posteriormente se debe realizar un proceso de borrado seguro de la data.

La disposición final de los equipos de cómputo se realiza con base en el concepto técnico de la SIGTI y es gestionada por la Subdirección Corporativa, encargada de ejecutar el procedimiento.

5.4. TECNOLÓGICOS

5.4.1. DISPOSITIVOS FINALES DE USUARIO

Todos los dispositivos de cómputo de la entidad deben contar con antivirus actualizado y software licenciado.

Los equipos de cómputo de la entidad deben contar con una autenticación por medio de credenciales y con permisos de administrador restringidos,

Los dispositivos finales deben ser utilizados exclusivamente para actividades laborales autorizadas por la entidad.

Los dispositivos móviles personales de servidores públicos y contratistas que tengan acceso al correo institucional y a los servicios corporativos en la nube (deben contar obligatoriamente con un mecanismo de bloqueo de acceso, como un patrón de movimiento, código de desbloqueo o contraseña.

Los servidores públicos que deseen conectar sus dispositivos personales a la red de la entidad deberán aceptar las políticas de monitoreo del dispositivo móvil, garantizando en todo momento el respeto a su privacidad.

Los dispositivos móviles personales de colaboradores y visitantes deberán conectarse exclusivamente a la red de "Visitantes", siguiendo los lineamientos de la política de seguridad de la información y previa solicitud a la mesa de ayuda.

Los computadores portátiles personales de servidores públicos y contratistas no pueden ser incluidos en el dominio idt.gov.co. No obstante, pueden acceder a los servicios de la red inalámbrica para conexión a internet, previa solicitud a la mesa de ayuda.

Los demás lineamientos del bueno uso de los equipos de cómputo se establecen Manual Políticas administración y Uso de TI V6 (GT-M03).

El Instituto Distrital de Turismo a través de hará la Subdirección de Inteligencia y Gestión Tecnológica la entrega oficial del equipo de cómputo en funcionamiento, con el respectivo software instalado, de acuerdo con la actividad del usuario. Si el usuario es trasladado del Área con sus elementos tecnológicos, es responsabilidad de éste avisar al Área de Subdirección de Inteligencia y Gestión Tecnológica para realizar dicho movimiento o para revisar los equipos y diligenciar el concepto técnico en caso de que el equipo sea asignado a otro usuario, con la debida autorización del jefe de área tanto en la asignación como en el evento de un traslado, de acuerdo con el documento institucional vigente.

Los usuarios de los equipos de cómputo de El Instituto Distrital de Turismo no deben por ningún motivo desarrollar, comprar, distribuir, instalar o ejecutar software malicioso que afecte el normal funcionamiento y/o cause cualquier tipo de daño a los activos de infraestructura tecnológica.

En el evento en que un usuario requiera ingresar un equipo de cómputo ajeno a la entidad a la red de datos, debe solicitar a Subdirección de Inteligencia y Gestión Tecnológica las credenciales de acceso previo concepto técnico de la viabilidad sobre el activo tecnológico.

5.4.2. DERECHOS DE ACCESO PRIVILEGIADOS

Se deben asignar controles de acceso para los servicios de TI y sistemas de información, por parte de los propietarios, asignado derechos de acceso según el rol desempeñado en la solución de TI.

Las cuentas con privilegios elevados serán asignadas exclusivamente a personal técnico y administrativo autorizado de la SIGTI. El acceso de usuario administrador para los equipos de cómputo de la entidad solo está autorizado para el equipo de mesa de ayuda y para los quienes equipos de comunicaciones y servidores está autorizado para los especialistas que pertenecen a la SIGTI y tienen entre sus funciones la administración de estos.

El acceso privilegiado solo será concedido a personal autorizado cuya función lo requiera.

Se aplicará el principio de mínimos privilegios, otorgando solo los accesos indispensables para el desempeño de las funciones.

De acuerdo con las políticas de control de acceso, se debe asignar los derechos de acceso, determinado los accesos de privilegiado para los servicios y sistemas de información de la Entidad.

Los derechos de acceso privilegiado serán revocados de inmediato ante cambios de función, desvinculación o cuando dejen de ser necesarios.

Cualquier modificación en los accesos privilegiados debe ser gestionada a través de la mesa de ayuda.
Los usuarios con acceso privilegiado son responsables del uso adecuado de sus credenciales y del cumplimiento de las políticas de seguridad.

5.4.3. RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN

El acceso a la información se otorga según el principio de mínimo privilegio, permitiendo únicamente el acceso necesario para el desempeño de funciones específicas.

Se implementan controles de acceso basados en roles para restringir el acceso a datos sensibles o información clasificada o reservada.

El acceso a información clasificada o reservada está restringido a personal autorizado.

La transferencia de información clasificada y reservada debe realizarse mediante canales seguros.

5.4.4. ACCESO AL CÓDIGO FUENTE

El acceso al código fuente se otorga únicamente a personal autorizado, según su rol y funciones dentro de la entidad, mediante la autenticación de dominio principalmente. Solo los desarrolladores y administradores autorizados podrán realizar modificaciones al código fuente.

El acceso a los códigos fuentes de un programa en específico se asigna a los desarrolladores relacionados con el proyecto y las demás personas no tendrán acceso, incluso desarrolladores de otros proyectos.

5.4.5. AUTENTICACIÓN DE SEGURIDAD

Se debe restringir los intentos de accesos fallidos a los servicios de TI de la entidad, incluyendo los sistemas de información, bloqueando temporal o definitivamente las credenciales y por medio de la mesa de ayuda se podrán habilitar nuevamente, después de validar que el usuario está autorizado.

Se debe bloquear la visualización de la contraseña mientras se esta digitando, con el fin de evitar pueda ser vista por personal no autorizado.

Se deben finalizar las sesiones inactivas después de un periodo de tiempo establecido con el propietario del activo de información.

La Subdirección de Inteligencia y Gestión Tecnológica a través del medio institucional vigente, establecerá los niveles de protección de la Información institucional digital, de acuerdo con su clasificación, roles y responsabilidades asignados a los usuarios del sistema, permitiendo el acceso a los servicios y sistemas informáticos través de la asignación de un identificador y contraseña inicial, previa autorización formal del jefe de área.

Cada funcionario o contratista cuyas funciones requieran de acceso a sistemas de información o correo electrónico, deberá asignársele un usuario y contraseña.

Las credenciales son personales e intransferibles.

Deben utilizarse esquemas de seguridad para la creación de contraseñas (uso de Mayúsculas, Minúsculas, Caracteres, Números).

Las cuentas de usuario, funcionarios y contratistas, que se desvinculen de la entidad, o que se les terminen sus contratos de prestación de servicios, se desactivaran de inmediato.

Es responsabilidad del Director General, Subdirectores, Jefes de Oficina y Asesores de las diferentes dependencias informar oportunamente a Subdirección de Inteligencia y Gestión Tecnológica la creación, modificación y eliminación de las cuentas de usuarios.

5.4.6. GESTIÓN DE LA CAPACIDAD

Se debe monitorear al menos dos veces al año la capacidad de los recursos de TI, en lo que refiere a memoria, procesamiento y almacenamiento.

5.4.7. PROTECCIÓN CONTRA MALWARE

La SIGTI implementa mecanismos de seguridad, incluyendo un sistema de detección y prevención de intrusos, herramientas anti-spam y soluciones de control de navegación, con el propósito de reducir riesgos asociados a virus y software malicioso.

Asimismo, implementa y gestiona un sistema antivirus en todas las estaciones de trabajo y servidores de la entidad, asegurando el análisis, detección y, cuando sea posible, la eliminación de virus o código malicioso.

5.4.8. GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS

La gestión de las vulnerabilidades técnicas se realizar desde diferentes estrategias, el escaneo de portales web por medio de la alta consejería TIC, con los reportes de los fabricantes y los reportes de los usuarios.

Las mediaciones a las que haya lugar cuando se identifican las vulnerabilidades, se evalúan, priorizan y gestionan desde la SIGTI.

5.4.9. GESTIÓN DE LA CONFIGURACIÓN

Definir y documentar configuraciones base para cada tipo de activo tecnológico, siguiendo mejores prácticas y normativas de seguridad.

Implementar controles para asegurar que solo personal autorizado pueda realizar cambios en la configuración de los servicios de TI.

Establecer un proceso formal para solicitar, evaluar, aprobar e implementar cambios en la configuración de los servicios de TI.

Implementar configuraciones seguras desde la instalación inicial de los sistemas, reduciendo vulnerabilidades desde su despliegue.

Revisar y actualizar periódicamente las configuraciones base según la evolución de amenazas y necesidades operativas

5.4.10. ELIMINACIÓN DE LA INFORMACIÓN

Utilizar herramientas de borrado seguro para eliminar archivos y registros electrónicos de manera irreversible.

Aplicar sobre escritura de datos para discos duros, unidades SSD y otros dispositivos de almacenamiento.

Destruir medios físicos que contengan información clasificada, reservada o confidencial cuando sea necesario.

5.4.11. ENMASCARAMIENTO DE DATOS

Limitar la exposición de datos sensibles, incluyendo datos personales o de interés personal.

Implementar técnicas de enmascaramiento adecuadas según el tipo de dato, cuando se considere necesario, como sustitución de datos reales por valores ficticios, pero estructuralmente similares, aleatorización de valores para evitar su correlación con los datos originales, truncamiento o reducción de datos para eliminar información crítica sin afectar su funcionalidad.

5.4.12. PREVENCIÓN DE LA FUGA DE DATOS

Identificar y clasificar la información según la ley 1712 de 2014 en pública, pública clasificada y pública reservada.

Etiquetar la información pública clasificada y pública reservada.

Establecer restricciones en el acceso a la información pública clasificada y pública reservada.

Los servidores o contratistas no podrán compartir, descargar, almacenar en sus equipos personales o tomar pantallazos de la información pública clasificada y pública reservada.

5.4.13. COPIA DE SEGURIDAD DE LA INFORMACIÓN.

La SIGTI realiza las copias de seguridad de acuerdo con la criticidad de los activos de información y lo requerido por los propietarios de los sistemas de información o servicios de TI. Para ello cuenta con un procedimiento definido para su realización y recuperación de información.

Los servidores públicos y contratistas son responsables de respaldar su información y de verificar que los respaldos se realicen correctamente. Estos deben almacenarse en medios digitales dispuestos por la entidad, como la aplicación Google Drive.

5.4.14. REDUNDANCIA DE LAS INSTALACIONES DE TRATAMIENTO DE LA INFORMACIÓN.

La entidad propende por la migración de los servicios críticos a la nube, con el fin que frente a un desastre o materialización de un evento desafortunado que afecte el centro de datos ubicado en las instalaciones de la entidad, se pueda habilitar o dar continuidad a los servicios sin afectar la operación.

Establecer procedimientos de recuperación ante desastres (DRP).

5.4.15. ACTIVIDADES DE MONITOREO

Configurar alertas automáticas para eventos sospechosos, intentos de acceso no autorizado o actividades inusuales.

Implementar herramientas y soluciones de monitoreo que permitan la recolección y análisis en tiempo real de eventos de seguridad.

5.4.16. SINCRONIZACIÓN DEL RELOJ

Todos los relojes de la infraestructura de procesamiento de información deben estar sincronizados con la hora legal colombiana.

5.4.17. USO DE PROGRAMAS DE UTILIDAD PRIVILEGIOS

Las herramientas usadas por el personal de mesa de ayuda o de TI para atender los requerimientos e incidentes, asi como para configurar equipos o programas son de uso exclusivo de este personal, es decir es restringido para los demás servidores y contratistas de la entidad.

5.4.18. INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS

La instalación de software en sistemas operativos solo podrá ser realizada por personal autorizado y delegado por la Subdirección de Inteligencia y Gestión de TI, mediante herramientas de gestión centralizada.

Se debe mantener un inventario actualizado del software instalado en cada sistema operativo.

Se deben aplicar actualizaciones y parches de seguridad en los sistemas operativos y el software instalado de manera periódica.

Antes de instalar actualizaciones, se debe evaluar su impacto en la estabilidad del sistema y en las aplicaciones institucionales.

Se deben implementar controles para evitar la instalación de software no autorizado o que comprometa la integridad del sistema.

Se debe definir el versionamiento de los sistemas operativos y software autorizado en la entidad.

5.4.19. SEGURIDAD DE LAS REDES

La SIGTI proporciona e implementa un control perimetral de las redes, mediante un firewall que filtra todas las conexiones desde la de WAN hacia la red LAN y permite bloquear tráfico malicioso.

Implementar cifrado en las comunicaciones sensibles, como VPNs seguras para acceso remoto y protocolos seguros (TLS, SSH, IPsec).

Aplicar segmentación de red para limitar el acceso según el principio de mínimos privilegios, asegurando que los usuarios y dispositivos solo accedan a los recursos necesarios.

Restringir el acceso de dispositivos externos o no autorizados mediante listas de control de acceso (ACL) y soluciones de administración de acceso a la red (NAC).

Restringir el acceso a la red Wi-Fi institucional mediante autenticación centralizada y segmentación de redes para invitados.

Implementar controles de filtrado de contenido web y aplicaciones a través del firewall, con el objetivo de restringir el acceso únicamente a sitios y aplicaciones previamente autorizados, garantizando así un uso seguro y adecuado de los recursos tecnológicos.

El usuario autenticado en la red de datos del IDT, renuncia a los derechos de privacidad respecto al uso de la información

5.4.20. SEGURIDAD DE LOS SERVICIOS DE RED

Es necesario realizar un monitoreo continuo del tráfico de red para asegurar su disponibilidad, abordando de manera proactiva el mantenimiento y las oportunidades de mejora.

Los acuerdos contractuales con los proveedores de servicios de red deben incluir compromisos claros sobre niveles de servicio y requisitos de seguridad, asegurando el cumplimiento de los estándares establecidos por la entidad.

La entidad cuenta con un canal de red Backup con el fin de asegurar el servicio de internet en la sede principal.

El Instituto Distrital de Turismo es responsable de suministrar y administrar la infraestructura de Datos y Comunicaciones necesaria para el cumplimiento de su gestión, y podrá a través de Subdirección de Inteligencia y Gestión Tecnológica realizar monitoreo y seguimiento de las comunicaciones electrónicas, hasta donde sea permitido por las disposiciones legales, procurando respetar la autonomía y privacidad del usuario.

Los usuarios de la red de datos no deberán intentar acceder a la configuración de los activos de IT, o intentar acceder a información considerada confidencial que esta almacenada en bases de datos o cualquier otro medio digital.

5.4.21. SEGREGACIÓN DE REDES

Las redes locales On-Premise, como la red de usuarios, la red WAN, la red de servidores y las conexiones VPN, deben estar segmentadas y protegidas mediante firewalls para restringir el acceso no autorizado.

Las redes LAN e inalámbricas deben ser segmentadas a través de VLANs, lo que permite aislar el tráfico y aplicar controles de acceso específicos para cada segmento.

Se debe contar con un segmento de red exclusivo para los servidores On-Premise, gestionado a través del firewall, donde el acceso esté restringido y autorizado únicamente con parámetros específicos como dirección IP y puerto.

5.4.22. CICLO DE VIDA DE DESARROLLO SEGURO

Es necesario definir e implementar controles y requisitos de seguridad en todas las etapas del ciclo de vida del desarrollo de software, cuando la entidad tercerice o desarrolle in house.

Los propietarios de los sistemas de información son responsables de llevar a cabo las pruebas necesarias para verificar el cumplimiento de los requisitos de seguridad antes de su implementación en producción. Estas pruebas deben estar debidamente documentadas y contar con la aprobación formal que certifique el correcto funcionamiento del cambio, ajuste o nuevo desarrollo, asegurando que cumple con todas las especificaciones requeridas.

5.4.23. REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN

Incorporar requisitos de seguridad en todas las fases del ciclo de vida del desarrollo y adquisición de

software, hardware y servicios tecnológico.

Propender porque cualquier cambio en los sistemas de información sea evaluado en términos de impacto en la seguridad antes de su implementación.

Asegurar el cumplimiento de normativas nacionales en materia de protección de datos y seguridad de la información, en todo el ciclo de vida del desarrollo o adquisición del software.

5.4.24. ARQUITECTURA DE SISTEMAS SEGUROS Y PRINCIPIOS DE INGENIERIA

Adoptar el enfoque de seguridad por diseño, asegurando que los controles de seguridad sean parte integral del desarrollo de sistemas y no una adición posterior.

Utilizar metodologías seguras de codificación para prevenir vulnerabilidades como inyecciones de código, desbordamiento de búfer y ataques de denegación de servicio.

Aplicar revisiones de código y pruebas de seguridad antes de la implementación de nuevos sistemas o actualizaciones

5.4.25. CODIFICACIÓN SEGURA

Seguir las mejores prácticas de codificación segura definidas por OWASP, NIST y estándares de la industria.

Utilizar librerías y frameworks confiables y mantenerlos actualizados para evitar vulnerabilidades conocidas.

Gestionar errores y excepciones de manera controlada, evitando exponer información confidencial en mensajes de error.

Llevar a cabo revisiones de código y pruebas de penetración para identificar y mitigar vulnerabilidades antes del despliegue en producción

5.4.26. PRUEBAS DE SEGURIDAD EN EL DESARROLLO Y LA ACEPTACIÓN

Incorporar pruebas de seguridad desde las primeras etapas del desarrollo, asegurando que los controles sean evaluados de manera continua.

Realizar análisis de riesgos de seguridad antes del inicio del desarrollo para identificar posibles vulnerabilidades y establecer estrategias de mitigación.

Ningún sistema podrá ser implementado en producción sin haber superado las pruebas de seguridad definidas.

Se deben establecer criterios de aceptación claros que incluyan el cumplimiento de estándares y normativas de seguridad aplicables (ISO/IEC 27001, OWASP, NIST, entre otros) o de acuerdo a los lineamientos de MINTIC.

5.4.27. DESARROLLO TERCERIZADO

Los contratos de desarrollo de software con terceros deben especificar de manera clara los alcances de las licencias, la titularidad del código fuente y los derechos de propiedad intelectual. Asimismo, deben incluir los requisitos contractuales relacionados con la calidad y seguridad del software desarrollado.

Se deben establecer acuerdos de confidencialidad con los proveedores para proteger la información confidencial.

Incluir compromisos del proveedor en cuanto a la aplicación de prácticas de desarrollo seguro, gestión de vulnerabilidades y pruebas de seguridad antes de la entrega del producto.

Todos los procesos del Instituto Distrital de Turismo deberán informar a la Subdirección de Inteligencia y Gestión de Tecnologías de la Información sobre sus proyectos de adquisición de sistemas de información, con el fin de verificar los requisitos de la infraestructura tecnológica, que no existan soluciones similares y asesorar en la mejor solución.

5.4.28. SEPARACIÓN DE LOS ENTORNOS DE DESARROLLO, PRUEBAS Y PRODUCCIÓN

Establecer ambientes separados de Desarrollo, Pruebas y Producción, dentro de la infraestructura de Desarrollo de Sistemas de Información.

Solo personal autorizado debe tener acceso a los entornos de prueba y producción, asegurando que los desarrolladores no puedan realizar modificaciones directas en producción.

5.4.29. GESTIÓN DEL CAMBIO

Todos los cambios deben ser categorizados para determinar su impacto y criticidad.

Todo cambio debe ser solicitado formalmente mediante un registro en el sistema de gestión de cambios, especificando su objetivo, alcance y posible impacto.

Se debe realizar un análisis de riesgos y plan de mitigación antes de la aprobación del cambio.

Ningún cambio puede implementarse en producción sin la aprobación formal del área responsable y el equipo de TI si este es custodio de activos de información.

5.4.30. INFORMACIÓN DE LA PRUEBA

No se debe usar datos reales de producción en entornos de prueba, salvo que se apliquen técnicas de enmascaramiento, anonimización o cifrado que protejan la información.

En caso de requerir datos reales, se debe contar con la aprobación formal del área propietaria y la responsable de seguridad de la información y TI.

Los datos utilizados en pruebas deben ser eliminados o depurados al finalizar el ciclo de validación, evitando su almacenamiento innecesario.

En caso de realizar pruebas en entornos de terceros, se deben establecer acuerdos de confidencialidad y seguridad para proteger los datos utilizados.

5.4.31. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN DURANTE LAS PRUEBAS DE AUDITORÍA

Toda auditoría que requiera pruebas en los sistemas de información debe ser aprobada previamente por el área propietaria y de la SIGTI si esta es custodio del sistema de información.

Se deben restringir las pruebas en bases de datos o sistemas en producción para evitar alteraciones en la operación.

6. SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN

El Instituto Distrital de Turismo implementará un Plan de Comunicación en Seguridad de la Información, liderado por la Subdirección de Inteligencia y Gestión de Tecnologías de la Información. Este plan se elaborará anualmente y establecerá los medios y estrategias para difundir recomendaciones y buenas prácticas en seguridad de la información a todos los servidores y contratistas de la entidad.

El objetivo es socializar las políticas institucionales de seguridad de la información y fortalecer las capacidades en todas las áreas y procesos.

El Instituto Distrital de Turismo a través de las áreas de Gestión de Talento Humano y Gestión Jurídica y Contractual, incluirá dentro de las inducciones las temáticas de seguridad de la información, con el objetivo de que cualquier servidor y contratista que se vincule a la entidad tenga pleno conocimiento de las políticas de seguridad de seguridad de la información, La Subdirección de Inteligencia y Gestión de Tecnologías de la Información apoyará dichas inducciones.

7. 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 anualmente o cuando existan incidentes de seguridad de la información o se produzcan cambios estructurales considerables, esto con el fin de asegurar su vigencia y aplicabilidad dentro del Instituto Distrital de Turismo.

8. SANCIONES

La falta de conocimiento de los presentes lineamientos no libera al personal del Instituto Distrital de Turismo 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.

a. Se aplicarán sanciones de acuerdo con el Código Único Disciplinario.
b. Pueden aplicarse sanciones de tipo penal según sea el caso y la gravedad de este, si así lo consideran los entes investigativos y judiciales correspondientes.

c. La Subdirección de Inteligencia y Gestión de Tecnologías de la Información será el encargado de recopilar y entregar a la Oficina de Control Disciplinario Interno las evidencias de incumplimiento de los lineamientos, informes de impactos y consecuencias y cualquier otro insumo requerido para formalmente manejar la investigación inicialmente a nivel interno, así mismo, La Subdirección de Inteligencia y Gestión de Tecnologías de la Información será el encargado de registrar y gestionar el Incidente de seguridad derivado con el incumplimiento de las políticas.
d. Facultase a la Subdirección de Inteligencia y Gestión Tecnológica para hacer seguimiento, monitoreo y control sobre el uso de los sistemas informáticos por parte del talento humano de la entidad, y la aplicación de las políticas de seguridad de la información dispuestas en la presente política y demás disposiciones legales vigentes y reglamentarias sobre la materia.
e. Todo usuario que incurra en delitos informáticos contemplados en la ley 1273 de 2009, será objeto de investigación técnica por parte de la Subdirección de Inteligencia y Gestión Tecnológica, quienes notificaran los resultados de la investigación a la Oficina de Control Disciplinario Interno, para que adelante las investigaciones que en derecho correspondan, y como resultado de un procedimiento acorde con la Ley vigente en materia disciplinaria, se impongan las sanciones a que haya lugar.
f. El desarrollo de la investigación técnica, disciplinaria u otra a que haya lugar, no exime al contratista, servidor público o tercero, del cumplimiento de sus obligaciones o funciones.
g. Acción de no repudio. El contratista, servidor público o tercero que por descuido o que de alguna manera exponga, revele, divulgue o distribuya a terceros su contraseña, equipo, activos de infraestructura tecnológica o información confidencial bajo su responsabilidad, no estará exento de la responsabilidad de los eventos que bajo esta circunstancia se realicen en contra de la seguridad informática de la entidad.

9. ANEXOS

No aplica.