**MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | INSTITUTO DISTRITAL DE LA PARTICIPACION Y ACCION COMUNAL | | |
| SISTEMA INTEGRADO DE GESTIÓN | | | | |
| MANUAL DE SEGURIDAD DE LA INFORMACIÓN | | | | |
| CÓDIGO: | IDPAC-GTI-MN-01 | | VERSIÓN | 01 |
| ELABORÓ | REVISÓ | | APROBÓ | |
| Maribel Ardila Flórez  Contratista | José Antonio Chaparro Gómez  Profesional especializado 222 – 04 | | Comité Institucional de Gestión y Desempeño | |
| FECHA | FECHA | | FECHA | |
| 16/12/2020 | 18/03/2021 | | 26/03/2021 | |

|  |  |  |
| --- | --- | --- |
| **REGISTRO DE MODIFICACIONES** | | |
| **VERSIÓN** | **FECHA** | **ÍTEM MODIFICADO – DESCRIPCIÓN** |
| 01 | 26/03/2021 | Versión Inicial |

**TABLA DE CONTENIDO**

[1 INTRODUCCION 4](#_Toc69506325)

[2 OBJETIVO 4](#_Toc69506326)

[3 ALCANCE 4](#_Toc69506327)

[4 GLOSARIO Y DEFINICIÓN DE TÉRMINOS 4](#_Toc69506328)

[5 ROLES Y RESPONSABILIDADES 6](#_Toc69506329)

[6 POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 7](#_Toc69506330)

[6.1 Dispositivos Móviles 7](#_Toc69506331)

[6.2 Seguridad de los Recursos Humanos 7](#_Toc69506332)

[6.3 Gestión de Activos 8](#_Toc69506333)

[6.4 Control de Acceso 8](#_Toc69506334)

[6.5 Seguridad Física y del Entorno 9](#_Toc69506335)

[6.6 Controles Criptográficos 9](#_Toc69506336)

[6.7 Seguridad en las Operaciones 10](#_Toc69506337)

[6.8 Seguridad de las Comunicaciones 10](#_Toc69506338)

[6.9 Políticas Adquisición, Desarrollo y Mantenimiento de Sistemas 11](#_Toc69506339)

[6.10 Relaciones con los Proveedores 11](#_Toc69506340)

[6.11 Gestión de Incidentes de Seguridad 11](#_Toc69506341)

[6.12 Cumplimiento 11](#_Toc69506342)

[7 Apoyo 12](#_Toc69506343)

[7.1 Toma de conciencia 12](#_Toc69506344)

[7.2 Comunicación 12](#_Toc69506345)

[7.3 Seguimiento, medición, análisis y evaluación 12](#_Toc69506346)

# INTRODUCCION

Este documento pretende establecer los principios orientadores de seguridad y privacidad de la información que buscan garantizar la disponibilidad, integridad, confidencialidad, privacidad, continuidad, autenticidad y no repudio de la información del IDPAC, así como dar lineamientos para la aplicación de mecanismos que impidan la vulneración de la seguridad y privacidad de la información. Con ello se busca la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información – SGSI, teniendo en cuenta que la amenaza se encuentra en cualquiera de sus estados del ciclo de vida (creación, procesamiento, almacenamiento, transmisión, utilización o destrucción), con lo que se puede llegar a tener impactos a nivel legal, de imagen, operacional, en el cumplimiento de la misión y los objetivos estratégicos del IDPAC.

# OBJETIVO

Establecer e integrar los lineamientos de seguridad de la información con la estrategia organizacional del IDPAC, enmarcados en la implementación de un Sistema de Gestión de Seguridad de la Información para apoyar los objetivos del instituto a través de identificación y valoración de los riesgos y el fortalecimiento de la seguridad de la información en la protección de su confidencialidad, integridad, disponibilidad, privacidad, continuidad, autenticidad y no repudio y por el cumplimiento de la normatividad vigente aplicable.

# ALCANCE

El presente Manual de Seguridad y Privacidad de la Información se establece en cumplimiento de las disposiciones legales vigentes, cubriendo todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios, contratistas y terceros que laboren o tengan relación con el IDPAC, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

# GLOSARIO Y DEFINICIÓN DE TÉRMINOS

| **Término** | **Definición** |
| --- | --- |
| **Activo** | Se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tienen un valor para la entidad. |
| Administración de Riesgos: | Se entiende por administración de riesgos, como el proceso de identificación, control, minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar la información o impactar de manera considerable la operación. Dicho proceso es cíclico y deberá llevarse a cabo en forma periódica. |
| Amenaza: | Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad. |
| Alta Dirección: | Persona o grupo de personas que dirigen y controlan al más alto nivel una entidad (Director, Secretario General y Direcciones). |
| Autenticación | Proceso que tiene por objetivo asegurar la identificación de una persona o sistema. |
| Autenticidad | Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades. |
| Cifrado | Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo. |
| Comité de Seguridad de la Información | El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del MINTIC, destinado a apoyar el cumplimiento de las normas, procesos y procedimientos de seguridad de la información |
| Confiabilidad de la Información | Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones. |
| Confidencialidad | Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma. |
| Control | Son todas aquellas políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. |
| Disponibilidad | Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran. |
| Dispositivos móviles | Equipo celular smartphone, equipos portátiles, tablets, o cualquiera cuyo concepto principal sea la movilidad, el cual permite almacenamiento limitado, acceso a internet y cuenta con capacidad de procesamiento. |
| Evaluación de Riesgos | Se entiende por evaluación de riesgos a la valoración de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operación de la entidad. |
| Incidente de Seguridad | Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información. |
| Información | Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro. |
| Integridad | Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento. |
| Legalidad | Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la entidad. |
| Medio removible | Los dispositivos de almacenamiento removibles son dispositivos de almacenamiento independientes del computador y que pueden ser transportados libremente. Los dispositivos móviles más comunes son: Memorias USB, Discos duros extraíbles, DVD y CD. |
| Mesa de Servicios | Constituye el único punto de contacto con los usuarios finales para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Es a través de la gestión proactiva de la Mesa de Servicios que la Oficina de Tecnologías de la Información recolecta las necesidades que tienen dependencias en cuanto a los recursos tecnológicos. |
| No repudio | El emisor no puede negar que envió porque el destinatario tiene pruebas del envío. El receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor pueda negar tal envío. |
| Plan de Continuidad de Negocio | Actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles predefinidos después de un incidente que afecte la continuidad de las operaciones. |
| Plan de tratamiento de riesgos | Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. |
| Propietario del riesgo | Persona o proceso con responsabilidad y autoridad para gestionar un riesgo. |
| Oficial de Seguridad de la información | Es la persona que cumple la función de supervisar el cumplimiento de la Política, coordinar el Comité de Seguridad de la Información y de asesorar en la materia a los integrantes de la entidad que así lo requieran. |
| Riesgo | Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. |
| Sistema de Información | Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales. |

# ROLES Y RESPONSABILIDADES

**Líder de Seguridad de la Información:** Es la persona, área o comité encargado de diseñar y presentar para aprobación, políticas, normas y procedimientos que fortalezcan la seguridad de la información, y someterlos a decisión del Comité Institucional de Gestión y Desempeño del IDPAC, realizando la implementación y seguimiento de los mismos.

**Líder o responsable de protección de datos personales**: Es la persona, área o comité encargado de establecer lineamientos para la protección de los datos personales tratados en el IDPAC.

**Comité Institucional de Gestión y Desempeño:** Comunicar a los funcionarios, contratistas y/o particulares que participan en actividades de forma directa o indirecta con el IDPAC, la importancia de satisfacer los requisitos de seguridad digital.

**Líderes de proceso**: persona, área o comité encargado de identificar e inventariar los nuevos activos digitales de información del IDPAC y los riesgos cibernéticos asociados.

**Responsable de Tecnologías de la Información**: persona, área o comité encargado de participar en la elaboración del cronograma de capacitación de seguridad digital en la entidad. Implementar las mejorar identificadas en la plataforma de seguridad que estén relacionadas con hardware, software, canales de comunicaciones de datos o infraestructura de tecnologías de la Información.

**Partes interesadas** (funcionarios, contratistas y proveedores): cumplir con las políticas de seguridad y privacidad de la información y cláusulas establecidas en el Modelo de Seguridad y Privacidad de la Información - MSPI.

# POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## Dispositivos Móviles

El IDPAC establece y mantiene las condiciones para el uso seguro de los dispositivos móviles institucionales (portátiles, teléfonos, tabletas, entre otros) que se requieren para la prestación de los servicios ofrecidos por el Instituto, entre las que se encuentran; establecer contraseñas de acceso robustas, cifrar la información almacenada y mantener el dispositivo móvil con el sistema operativo siempre actualizado y con un antivirus activo.

Es responsabilidad de los servidores públicos y contratistas del IDPAC al que se le asignó el dispositivo móvil evitar la instalación de programas desde fuentes desconocidas, evitar el uso de redes inalámbricas públicas, y mantener desactivadas las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados. Así mismo, deben evitar conectar los dispositivos móviles institucionales a puertos USB de computadores, terminales, y demás sitios de acceso público.

Los servidores públicos y contratistas deben notificar al personal de soporte técnico del área de TI los dispositivos móviles institucionales que tengan asignados con sospecha de infección por malware para el proceso de análisis, evaluación y tratamiento

## Seguridad de los Recursos Humanos

El área de Talento Humano debe realizar la contratación de personal en el IDPAC, para lo que debe hacer verificaciones de los antecedentes (Procuraduría General de la Nación, Contraloría General de la República, Policía, Consejo Superior de la Judicatura, entre otros) de los candidatos al cargo, la formación académica, experiencia y demás información que se requiera, de acuerdo a las leyes, reglamentos del Instituto y ética pertinente.

Los acuerdos contractuales entre la Entidad y los servidores públicos o contratistas deberán especificar entre sus disposiciones la obligatoriedad del cumplimiento de los lineamientos de seguridad de la información establecidos en la Entidad.

El proceso de Gestión de Talento Humano realiza la desvinculación, licencias, vacaciones o cambio de labores de los servidores públicos y el proceso de Gestión contractual define las funciones para los contratistas llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin. Así mismo, los directores, jefes, supervisores de contrato o líderes están obligados a informar la desvinculación o cambio de labores de acuerdo con los procedimientos establecidos por el IDPAC, esta información debe ser entregada oportunamente al proceso de Gestión de Tecnologías de la información.

El IDPAC debe incorporar los roles y responsabilidades en seguridad de la información dentro de las funciones y obligaciones contractuales de los funcionarios, contratistas y terceros.

El incumplimiento o la violación de las políticas de seguridad de la información del IDPAC por parte de los funcionarios, contratistas o terceros, estará sujeto a las investigaciones contractuales, disciplinarias, civiles y/o penales a que haya lugar, por los daños y perjuicios causados a la Entidad o a terceros.

## Gestión de Activos

El IDPAC establece los métodos de identificación, clasificación y valoración de activos de información, así como la definición de la asignación de responsabilidades, manteniendo mecanismos acordes para el control de riesgos de la información.

Cada activo de información del Instituto debe tener un responsable que debe velar por su seguridad, garantizando que todos los activos de información reciban un apropiado nivel de protección con base en su valor de confidencialidad, integridad, disponibilidad, riesgos identificados y/o requerimientos legales de retención.

Es responsabilidad del líder de proceso, jefe de área o Director, la identificación y reporte de nuevos activos de información, así mismo mantener actualizada la valoración de estos.

Los servidores públicos y contratistas del IDPAC deben hacer la devolución de los activos de información asignados a su cargo una vez finalice la relación contractual con la Entidad.

## Control de Acceso

El IDPAC define los lineamientos para asegurar un acceso controlado, físico o lógico, a la información y plataforma tecnológica, considerándolas importantes para el sistema de gestión de seguridad de la información.

El IDPAC establece procedimientos para la creación de datos de acceso, suministro de accesos a la información, revisión periódica de los accesos otorgados, y desactivación o eliminación de las cuentas de usuario una vez finalizada la relación contractual.

Todos los servidores públicos y contratistas con acceso a un sistema de información o a la red informática institucional, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña y serán responsables de las acciones realizadas por el usuario que les ha sido asignado.

## Seguridad Física y del Entorno

Las oficinas administrativas, áreas de procesamiento de información, equipos tecnológicos y de soporte, información de medios físicos entre otros, son esenciales para el cumplimiento de los objetivos del IDPAC, por tanto, se mantienen y establecen controles para resguardar la seguridad de las instalaciones y el acceso a las áreas y ambientes de trabajo.

Los equipos de cómputo que pasen a un estado de retiro o se requieran para la reutilización, deberán cumplir los siguientes lineamientos:

1. Al momento de retirar un equipo de cómputo y llevarlo al almacén, el área responsable del activo debe informar al proceso de Gestión de TI si requiere que se realice una copia de respaldo de la información almacenada.
2. Cuando se hace entrega de un computador a un funcionario o contratista del IDPAC, el proceso de Gestión de TI realiza el alistamiento, creación de perfiles y permisos, así como la revisión de contenido de información almacenada y software instalado, el cual debe estar debidamente licenciado.

Para todos los usuarios de equipos de cómputo del IDPAC, es obligatorio que las sesiones sean cerradas al finalizar las actividades y realizar un correcto apagado.

Las áreas dentro de las cuales se encuentran el centro de datos, centros de cableado y áreas de almacenamiento de información de TI, deben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para su protección.

Las claves son de uso personal e intransferible, por esa razón el uso de las credenciales asignadas, las sesiones abiertas que se dejen en ausencia del puesto de trabajo, la información almacenada en el equipo asignado y la obligación de acatar las políticas de actualización y cambios de contraseñas, es responsabilidad del usuario.

El proceso de Gestión de TI realiza seguimiento a los accesos de los usuarios, con el fin de minimizar los riesgos de pérdida de integridad, disponibilidad y confidencialidad de la información.

Todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas suministradas de acceso a la red, sistemas de información, aplicaciones, entre otros.

## Controles Criptográficos

El IDPAC asegura el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la integridad y el no repudio de la información, por lo cual establece técnicas criptográficas y cifrado como son: Cifrado de la información cuando se requiere trasferir o almacenar información sensible o crítica, uso de protocolos seguros para las redes Wifi, uso de protocolo HTTPS con un nivel de cifrado actualizado.

El acceso remoto a la red y los sistemas de información del IDPAC desde una red externa, se realiza a través de conexiones seguras.

## Seguridad en las Operaciones

El IDPAC garantiza que las operaciones tecnológicas se gesten de forma correcta y se brinde seguridad a las instalaciones de procesamiento de información.

Los cambios en los recursos tecnológicos en el IDPAC deben ser tratados a través de un proceso establecido, con el fin de minimizar los riesgos de alteración de los sistemas de información.

Según la clasificación de la información del IDPAC, se establecen las medidas de respaldo de la información, a través de mecanismos como cintas, SAN, NAS o en la nube.

Los responsables de TI definen pruebas de restauración que permitan validar la integridad y disponibilidad de la información almacenada, garantizando la confiabilidad del proceso ejecutado para copias de respaldo.

El proceso de Gestión de TI es el encargado de aplicar los parches, controles o remediaciones derivadas de la ejecución de pruebas periódicas de análisis de vulnerabilidades o liberadas por lo fabricantes de software.

## Seguridad de las Comunicaciones

El Proceso de Gestión de TI realiza el bloqueo a las páginas de contenido para adultos, mensajería instantánea y demás páginas que no sean de uso institucional, mediante los recursos que posee el IDPAC para la realización de esta tarea.

Así mismo, este proceso asegura la protección de las redes y la trasferencia de información e implementa y mantiene la separación de las redes virtuales para garantizar la confidencialidad de la información en la red de telecomunicaciones de la Entidad.

Para dar cumplimiento a lo señalado se deben firmar acuerdos de confidencialidad y de no divulgación entre el IDPAC y entidades externas, con las cuales se intercambie información e implementa controles de seguridad al monitoreo de la red.

La transferencia de información deberá realizarse protegiendo la confidencialidad, integridad y disponibilidad de los datos de acuerdo con la clasificación del involucrado.

## Políticas Adquisición, Desarrollo y Mantenimiento de Sistemas

El IDPAC garantiza que los sistemas de información estén asociados a lineamientos, procesos, buenas prácticas y demás requisitos que sirvan para regular los desarrollos de software internos en un ambiente controlado, así mismo, se identifican y gestionan los posibles riesgos referentes a seguridad de la información durante todo el ciclo de vida del software.

El IDPAC establece controles técnicos para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información que son públicos mediante herramientas de seguridad perimetral de proveedores o de forma local.

Los datos de pruebas que se utilicen durante todo el ciclo de vida de los sistemas de información deben ser seleccionados, utilizados y eliminados de forma segura.

El IDPAC cuenta con una metodología de desarrollo seguro de software.

## Relaciones con los Proveedores

El IDPAC controla las relaciones con proveedores, y en particular aquellos que tienen acceso a la información. La información está suficientemente protegida con base a los acuerdos y contratos correspondientes. Esta protección debe contemplarse antes, durante y con posterioridad a la culminación del servicio.

Cualquier cambio que se realice con algún proveedor crítico de TI o de los procesos misionales, debe aplicarse mediante el procedimiento de gestión de cambios establecido en el IDPAC.

El IDPAC realiza revisiones periódicas al cumplimiento de las Políticas de Seguridad y Privacidad de la Información a los Proveedores.

## Gestión de Incidentes de S**eguridad**

El IDPAC debe asegurarse que todos los servidores públicos y contratistas conozcan y apliquen el procedimiento correspondiente para actuar ante cualquier incidente en materia de seguridad de la información. Por lo tanto, se deben establecer los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.

El IDPAC cuenta con una bitácora de los incidentes de seguridad de la información reportados y atendidos.

## Cumplimiento

El IDPAC asegura el conocimiento y cumplimiento de las obligaciones legales en materia de seguridad de la información. Por lo anterior, garantiza el respeto de los derechos de propiedad intelectual de terceros controlando la adquisición y uso del software en la Entidad.

El IDPAC cuenta con una política para gestionar la protección de datos personales.

# Apoyo

## Toma de conciencia

Será responsabilidad del proceso de gestión de TI y Recursos Humanos, incorporar la aplicación de las políticas de seguridad de la información en su plan de capacitación institucional, y velar por la correcta inducción de los funcionarios nuevos en materia de seguridad de la información.

## Comunicación

El IDPAC debe establecer los canales accesibles para la comunicación permanente de todas las políticas, procedimientos u otros documentos que hagan parte del Modelo de Seguridad y Privacidad de la Información (MSPI), algunos de estos, usados para la comunicación formal en el Instituto son: Correo Electrónico, intranet, portal web, comunicación impresa, charlas, DCRadio, DCTv y capacitaciones.

## **Seguimiento, medición, análisis y evaluación**

Se deben establecer los indicadores de medición de los Objetivos de Seguridad y Privacidad de la Información, así como la imperatividad de realizar revisiones periódicas del cumplimiento de las políticas de Seguridad y Privacidad de la Información y la respuesta a los incidentes de seguridad de la información reportados por el IDPAC.

Las actualizaciones necesarias del modelo MSPI se adelantarán de acuerdo a la normatividad vigente aplicada.