ALCALDÍA MAYOR
DE BOGOTÁ D.C.

IDPAC

BOGOTÁ

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

	INSTITUTO DISTRITAL DE LA PARTICIPACIÓN Y ACCIÓN COMUNAL
SISTEMA INTEGRADO DE GESTIÓN	
Política de seguridad y privacidad de la información	

CÓDIGO:	IDPAC-CENT-PO-01	**VERSIÓN**	03
ELABORÓ	**REVISÓ**	**APROBÓ**	
Luz Marina Díaz	José Antonio Chaparro María Angélica Castro Corredor Silvia Milena Patiño León	Pablo César Pacheco Rodríguez	
Contratista – Secretaria General	Profesional especializado Código 222-04 Contratista – Secretaria General Contratista – Oficina Asesora de Planeación	Secretario General	

REGISTRO DE MODIFICACIONES		
VERSIÓN	**FECHA**	**DESCRIPCIÓN MODIFICACIONES**
01	22/08/2017	Versión Inicial
02	26/03/2021	Actualización de acuerdo con el marco normativo vigente
03	30/12/2022	Se realiza revisión general del documento y se actualiza a partir de los resultados del diagnóstico del Modelo de Seguridad y Privacidad de la Información.

ALCALDÍA MAYOR DE BOGOTÁ D.C.

IDPAC

BOGOTÁ

TABLA DE CONTENIDO

INTRODUCCIÓN

El Instituto Distrital de la Participación y Acción Comunal – IDPAC a través de la Alta Dirección y con el fin de apoyar la implementación del Modelo de Seguridad y Privacidad de la Información define las políticas donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información al interior de la Entidad; definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información.

Conforme a la metodología señalada por el Ministerio de las Tecnologías de la Información y la Comunicación MINTIC y por los lineamientos de la Alta Consejería Distrital para las TIC, que tiene como propósito proteger, preservar y administrar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información. Esta política es aprobada en el marco del Sistema Integrado de Gestión y responde a las necesidades de la entidad.

Mediante la divulgación e implementación de las Políticas de Seguridad y Privacidad de la Información, se pretende garantizar la seguridad contemplando las medidas técnicas, operativas y administrativas que se deben tener en cuenta frente a la seguridad de la información.

El presente documento es dinámico es decir que es susceptible de actualización con el propósito de atender los lineamientos que se emitan por las entidades líderes de las políticas de Gobierno y Seguridad digital.

1. OBJETIVO

GENERAL

Establecer los lineamientos que contribuyan a la adecuada gestión de la seguridad de la información del Instituto de la Participación y Acción Comunal - IDPAC, asegurando el cumplimiento de los principios de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información, con el fin de garantizar la continuidad del negocio frente a posibles incidentes o eventos que puedan poner en riesgo la seguridad de la información.

ESPECÍFICOS

- Definir las pautas de uso y aplicabilidad de las políticas de seguridad y privacidad de la información que deben ser dadas a conocer a los servidores públicos, contratistas, proveedores, grupos de valor y demás partes interesadas que se relacionan con la entidad.
- Generar acciones que contribuyan a minimizar la ocurrencia de eventos, incidentes o riesgos asociados a la seguridad de la información, con el fin de proteger la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica o sus activos.
- Definir los roles y responsabilidades para la seguridad y privacidad de la información, con el fin de minimizar impactos financieros, operativos o legales debido a un uso indebido de la información.
- Crear procedimientos que permitan gestionar la seguridad de la información en cada uno de los procesos definidos en la entidad.

2. ALCANCE

Implementa los lineamientos requeridos para garantizar la seguridad y privacidad de la información por parte de sus funcionarios, contratistas, proveedores, grupos de valor, partes interesadas y la ciudadanía con el fin de dar cumplimiento a las disposiciones dadas en la materia.

3. DOCUMENTOS DE REFERENCIA

- Documento maestro del Modelo de Seguridad y Privacidad de la Información. Versión 4, octubre de 2021. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf
- Roles y responsabilidades del Modelo de Seguridad y Privacidad de la Información. Versión 4, octubre de 2021. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237904_maestro_mspi.pdf

4. DEFINICIONES

Término	Definición
Autenticación	Procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.
Activo	Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) Que tenga valor para la organización.
Análisis de riesgos	Proceso para comprender la naturaleza del riesgo y determinar el nivel de exposición al riesgo.
Articulador	La Agencia Nacional Digital, que será la encargada de

Término	Definición
	proveer y gestionar de manera integral los servicios ciudadanos digitales, además de apoyar técnica y operativamente al Ministerio de Tecnologías de la Información y las Comunicaciones para garantizar el pleno funcionamiento de tales servicios.
Cloud Computing	Concepto tecnológico basado en que las aplicaciones software y los equipos hardware con capacidad de proceso y almacenaje de datos que están ubicados en un Datacenter que permite a los usuarios acceder a las aplicaciones y servicios disponibles a través de Internet - “la Nube” de Internet-, de una forma sencilla y cómoda.
Competitividad	Según este principio el Estado y los ciudadanos deben contar con capacidades y cualidades idóneas para actuar de manera ágil y coordinada, optimizar la gestión pública y permitir la comunicación permanente a través del uso y aprovechamiento de las TIC.
Confidencialidad	Propiedad que determina que la reserva de la información, es decir que no esté disponible ni sea revelada a individuos, entidades, terceros indeterminados o procesos no autorizados.
Control	Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Término	Definición
Criptografía	Técnica de codificar u ocultar mensajes o textos como claves o información que no debe ser vista salvo por la persona a quien está dirigida. Kryptos "ocultar “. Grafos: "escribir “("escritura oculta “) Es el arte o ciencia de cifrar (encriptar) y descifrar (desencriptar) información utilizando técnicas matemáticas
Disponibilidad	Propiedad de que la información sea accesible y utilizable por solicitud de *una entidad autorizada.*
Etiquetar Información	Referenciar registros de información acuerdo a un inventario y clasificación de la información.
Evento de seguridad de la información	Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.
Gestión del riesgo	Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.
Incidente de seguridad de la información	Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las actividades del IDPAC y amenazar la seguridad de la información.
Innovación	En virtud de este principio el Estado y los ciudadanos deben propender por la generación de valor público a través de la introducción de soluciones novedosas que hagan uso de TIC, para resolver problemáticas o necesidades identificadas.

Término	Definición
Integridad	Propiedad de salvaguardar la exactitud y estado completo de los activos.
Inventario de activos	Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) Dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.
IPV6	Protocolo de comunicación de internet de sexta versión del Protocolo de Internet, pretende reemplazar la escasez de direcciones que tiene el actual ipv4.
Mecanismos de autenticación	Son las firmas digitales o electrónicas que al ser utilizadas por su titular permiten atribuirle la autoría de un mensaje de datos. Lo anterior sin prejuicio de la autenticación notarial.
No repudio	Es un servicio de seguridad que permite probar la participación de las partes en una comunicación.
Plan de Contingencia	Procedimientos alternativos de una Entidad cuyo fin es permitir el normal funcionamiento de esta y/o garantizar la continuidad de las operaciones, aun cuando algunas de sus funciones se vean afectadas por un accidente interno o externo.
Plan de Pruebas de Recuperación	Pruebas de recuperación de copias de respaldo programadas con el fin de verificar la consistencia e integridad de las copias de respaldo.
Plataforma Tecnológica	Es una agrupación de equipamientos técnicos y humanos destinados a ofrecer unos recursos tecnológicos para la realización de las tareas de los usuarios

Término	Definición
Protocolo de comunicación	Conjunto de reglas de internet establecidas que permiten que distintos componentes que conforman un sistema se puedan comunicar entre sí, facilitando el intercambio de información.
Riesgo	Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
Seguridad de la información	Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad.
Servicios ciudadanos digitales	Es el conjunto de soluciones y procesos transversales que brindan al Estado capacidades y eficiencias para su transformación digital y para lograr una adecuada interacción con el ciudadano garantizando el derecho a la utilización de medios electrónicos ante la administración pública. Estos servicios se clasifican en servicios base y servicios especiales.
Sistema de gestión de la seguridad de la información - SGSI	Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de

Término	Definición
	gestión del riesgo y de mejora *continua.*
Software	Conjunto de programas, aplicaciones y rutinas que se ejecutan en un computador.
Software utilitario	Software que está diseñado para realizar una tarea determinada o específica
Trazabilidad	Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.
Usabilidad	La capacidad de un software de ser comprendido, aprendido, usado y ser atractivo para el usuario en condiciones específicas de uso. En el diseño y configuración de los servicios ciudadanos digitales se propenderá porque su uso sea de fácil manejo para todos los usuarios.

5. NORMATIVIDAD

Conforme con lo establecido en la normatividad vigente el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, hace referencia a las siguientes normas, que se deben tener en cuenta para el desarrollo de la apropiación del MSPI en la entidad:

- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan

otras disposiciones en materia de Gestión Documental para todas las entidades del Estado.

- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1083 de 2015 establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital.
- Decreto 728 de 2017. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico

- Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- Decreto 1008 del 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.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

6. ROLES Y RESPONSABILIDADES

- El representante legal del IDPAC es el responsable de coordinar, hacer seguimiento y verificación de la implementación de la Política Seguridad de la Información en cumplimiento de Gobierno Digital. Igualmente, debe garantizar el desarrollo integral de la política como una herramienta transversal que apoya la gestión del IDPAC y el desarrollo de las políticas de gestión y desempeño institucional del Modelo Integrado de Planeación y Gestión.

- El Comité Institucional de Gestión y Desempeño será el responsable de orientar la implementación de la política de Gobierno Digital, conforme a lo establecido en el Modelo Integrado de Planeación y Gestión.

- El Secretario General es responsable de la Seguridad de la Información quien funge como líder de los procesos de Comunicación Estratégica y Nuevas tecnologías y Gestión de Bienes, Servicios e Infraestructura, quien a su vez se apoya en personal a su cargo para la implementación, puesta en marcha, mantenimiento, supervisión y mejora continua. Este rol tiene las siguientes responsabilidades:
  a) Asegurar la implementación, puesta en marcha e implementación de los lineamientos de las políticas de gobierno y seguridad digital.
  b) Velar por la revisión de documentos que soportan los lineamientos de las políticas de gobierno y seguridad digital.
  c) Presentar las necesidades de recursos financieros, tecnológicos y de talento humano para el desarrollo de los proyectos que fortalezcan la gestión de la seguridad de la información con el fin de lograr los objetivos misionales y estratégicos del IDPAC.

Teniendo en cuenta que el nuevo enfoque de Gobierno Digital es el uso de la tecnología como una herramienta que habilita la gestión del IDPAC para la generación de valor público, todas las dependencias son corresponsables en su implementación.

- El Oficial de Seguridad de la Información es aquel funcionario o contratista que implementa y mantiene operativamente el Modelo de Seguridad y privacidad de la información y tendrá las siguientes responsabilidades:

  a) Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación del Instituto para realizar el seguimiento a los

riesgos de seguridad de la información, incluye aspectos relacionados con el ambiente físico, digital y las personas. identificados[1]

b) Elaborar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información.
c) Coordinar las actividades de los colaboradores con responsabilidades críticas en el MSPI y proporcionar apoyo administrativo mediante la realización de informes requeridos.
d) Planear y ejecutar el cronograma de implementación del MSPI, bajo un enfoque orientado a riesgos para darle solución oportuna y escalar al responsable de seguridad de la información en caso de ser necesario.
e) Elaborar documentos que permitan la implementación en el MSPI.
f) Contribuir al enriquecimiento en la gestión del conocimiento en materia de seguridad y privacidad de la información apoyando la documentación de las lecciones aprendidas.
g) Participar en las reuniones de seguimiento y velar por la actualización de los indicadores de gestión del SGSI.

- Responsables críticos de la seguridad digital**,** esta se establece entre servidores públicos y/o contratistas que por sus funciones u obligaciones contractuales gestionan, disponen o supervisan los activos de información críticos del IDPAC, este rol corresponde a Directores, Subdirectores, Gerentes y/o líderes de procesos, jefes de y el responsable de infraestructura y servicios tecnológicos; quienes responderán por:

[1] Guía para la administración del riesgo y el diseño de controles en entidades públicas:

a) El estricto cumplimiento de las políticas de seguridad de la información a título personal, funcionarios y contratistas que conforman sus equipos de trabajo a cargo.
b) Tener en cuenta los requerimientos de seguridad de información que les soliciten y en caso de ser requerido escalarlo al responsable de seguridad de la información.
c) Participar en las reuniones de seguridad de la información cuando sean convocados.
d) Contribuir con el levantamiento de los activos de información.

7. DESCRIPCIÓN

El Instituto Distrital de la Participación y Acción Comunal -IDPAC-, es un establecimiento público del orden distrital, con personería jurídica, autonomía administrativa y patrimonio propio, adscrito a la Secretaría Distrital de Gobierno, el cual surgió de la transformación del Departamento Administrativo de Acción Comunal Distrital -DAACD, ampliando sus funciones y ajustando su estructura a las nuevas necesidades de la ciudad.

El IDPAC, hacen parte del Sector Gobierno de la Alcaldía Mayor de Bogotá D.C., junto con el Departamento Administrativo de la Defensoría del Espacio Público - DADEP (soporte técnico del sector) y la Secretaría Distrital de Gobierno (cabeza del sector) conforme a los Acuerdos 257 de 2006 y 637 de 2016[2]

[2] Acuerdos 257 de 2006 y 637 de 2016

7.1. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Instituto Distrital de la Participación y Acción Comunal - IDPAC, cuenta con medidas de seguridad de la información en los procesos, trámites, servicios, sistemas de información y su infraestructura permitiendo preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos y la información que se administran en este, y en cumplimiento del marco jurídico correspondiente, con el objetivo de proporcionar una experiencia confiable, mediante un servicio seguro.

En la entidad comprobamos y ponemos a prueba todas las etapas de desarrollo, pruebas y producción y realizamos evaluación constante del mismo, en cumplimiento de la Estrategia de Gobierno Digital y la Política Nacional de Seguridad Digital con el objetivo de analizar los riesgos de seguridad digital a los cuales se encuentra expuesto el portal web y lograr su adecuada mitigación.

El Instituto Distrital de la Participación y Acción Comunal - IDPAC, se compromete a adoptar una política de confidencialidad y protección de datos, con el objeto de proteger la privacidad de la información personal de la ciudadanía y grupos de valor.

7.2. POLITICAS ESPECÍFICAS

7.2.1. Política de Gestión de Activos

El Instituto Distrital de la Participación y Acción Comunal – IDPAC, a través del proceso de Comunicación Estratégica y Nuevas Tecnologías, establecerá y divulgará los lineamientos específicos para la identificación, clasificación, valoración, rotulado y buen uso de los activos de información, con el fin de garantizar su protección.

Los lineamientos se impartirán, teniendo en cuenta los siguientes literales:

a) Inventario de Activos

Los activos de información físicos y lógicos del Instituto Distrital de la Participación y Atención Ciudadana – IDPAC, serán identificados y clasificados para establecer los mecanismos de protección necesarios de acuerdo a su valor, junto con el proceso de Gestión Documental y la normatividad vigente (Ley 1581 de 2012, Ley 1712 de 2014, Decreto 103 de 2015) que proveen los criterios, instrumentos y mecanismos para la identificación y actualización del inventario de activos de información que permita clasificar, etiquetar y definir la propiedad de estos.

b) Propiedad de los Activos

Los activos de información mantenidos en el inventario son de propiedad del Instituto Distrital de la Participación y Acción Comunal - IDPAC y administrados, custodiados y publicados por el proceso de Gestión Documental.

c) Uso Aceptable de los Activos de Información

El acceso a los activos de información (documentos físicos y digitales, así como a los sistemas de gestión de documentos e información) es controlado incluye

restricción o permisos y niveles de acceso segregado para servidores públicos, contratistas y terceros de acuerdo con sus funciones, obligaciones contractuales y responsabilidades. Los permisos deben ser determinados por los propietarios de la información, dueños de los aplicativos, supervisores de contrato y/o el comité de Gestión y Desempeño – CIGD, en información documentada como contratos, convenios, normatividad, legislación y otros; estos controles deben ser gestionados por los responsables asegurando su trazabilidad.

d) Clasificación y Etiquetado de la Información

La información del IDPAC reciba los niveles de protección adecuados, ya que con base en su valor y de acuerdo con otras características particulares requiere un tipo de manejo especial, dando cumplimiento a los cuatro (4) puntos principales descritos en el ítem 8 de la tabla 2 de la guía controles del Anexo A del estándar ISO/IEC 27001:2013.

Los activos de información se clasifican de acuerdo con los principios fundamentales de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad, conforme a la evaluación que se realice sobre las características de su valor relativo, su privacidad, la sensibilidad, el nivel de riesgo a que está expuesta y/o los requerimientos legales de retención.

- **Clasificación de acuerdo con la confidencialidad**[3] Se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o

[3] Ley 1581 de 2012, Decreto 1377 de 2013, Ley 1712 de 2014, Decreto 103 de 2015.

procesos no autorizados. En el IDPAC se definen cuatro (4) niveles alineados con los tipos de Información declarados en la ley 1712 del 2014, así:

1. **Información pública reservada:** Información disponible sólo para un proceso de la entidad y que, en caso de ser conocida por terceros sin autorización, puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
2. **Información pública clasificada:** Información disponible para todos los procesos del IDPAC y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de esta. Esta información es propia del IDPAC o de terceros y puede ser utilizada por todos los funcionarios para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
3. **Información pública**: Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos del instituto.
4. **No clasificada**: Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información pública reservada.

El Etiquetado de activos de información, será aplicado de acuerdo con el esquema de clasificación de la información aprobado por la entidad, lo anterior teniendo en cuenta las Tablas de Retención Documental aprobadas para las diferentes dependencias y las siguientes pautas generales:

- Se deben etiquetar todos los Activos de Información que estén clasificados según el esquema de clasificación en Confidencialidad, Integridad y disponibilidad.

- Se debe etiquetar el nivel de clasificación con relación a la Confidencialidad, la Integridad y la Disponibilidad.
- Si un Activo de Información en formato impreso no se encuentra etiquetado debe ser tratado en todos sus niveles (Confidencialidad, Integridad y Disponibilidad) como NO CLASIFICADA.
- Cada Activo de Información debe ser etiquetado teniendo en cuenta el esquema de clasificación.

e) Categorización de los Activos de Información Según confidencialidad.

Principio que se le debe dar a la existencia de información que puede o debe ser divulgada o no. Dando alcance a los criterios de clasificación de la información definidos en la Ley 1712 de 2014, la entidad aplicará los siguientes criterios a los activos de información: pública, reservada, privada o confidencial, semi-privada o interna.

f) Almacenamiento de Información.

Los equipos de cómputo que almacenen información reservada, privada o confidencial deben estar protegidos con mecanismos de seguridad para evitar que ante la pérdida del equipo una persona no autorizada pueda acceder a la información allí almacenada. Así mismo si son reasignados a usuarios diferentes, se debe borrar la información del disco duro de forma segura, de acuerdo con los lineamientos estipulado en la Ley 1712 de 2014 por la cual se crea la ley de transparencia.

g) Gestión de Soportes Extraíbles

La gestión de medios extraíbles se realizará de acuerdo con el esquema de clasificación adoptado por el IDPAC. Los equipos de cómputo que tienen autorizado el uso de puertos para conexión USB y unidades reproductoras de CD/DVD, deben cumplir los siguientes requisitos:

- Tener configurada en la herramienta de antivirus institucional, el bloqueo de la reproducción automática de archivos ejecutables
- Tener habilitado el escaneo automático de virus.
- Tener los permisos necesarios para poder ejecutar estos dispositivos en los computadores que se requieran.

h) Impresión de Información.

Los documentos que se impriman y/o digitalicen en equipos del IDPAC deben ser de carácter institucional.

La información clasificada reservada, privada o confidencial debe ser enviada a la impresora y recogida inmediatamente, evitando que personal no autorizado tenga acceso a ésta.

Los funcionarios y contratistas no deben divulgar información reservada, privada o confidencial a terceros sin la autorización por parte de los responsables de la información y la firma de un acuerdo de confidencialidad.

i) Soportes Físicos en Tránsito

Los medios que contienen información deben estar protegidos contra el acceso no autorizado, mal uso o corrupción durante el transporte. Se debe implementar la utilización de protocolos de seguridad para la encriptación de las claves de acceso.

Los funcionarios, contratistas y proveedores de la entidad tienen la obligación de proteger las unidades de almacenamiento físicas y lógicas que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información de valor para el IDPAC.

j) Devolución de los Activos de Información.

Los funcionarios y contratistas deberán devolver todos los activos producto del desarrollo de la organización que esté a su cargo a la terminación de su empleo, contrato o acuerdo.

7.2.2. Política de Control de Acceso.

El Instituto Distrital de la Participación y la Acción Comunal – IDPAC, implementa y mantiene controles de acceso físico y lógico a las instalaciones, infraestructura, distintos sistemas y servicios de información, que incluyen, selección y contratación de personas con la validación de antecedentes penales y legales, identificación de personal, manejo de usuarios y contraseñas, manejo de control de accesos biométricos y sistemas de vigilancia física, circuitos cerrados de video vigilancia y monitoreo, controlando las amenazas físicas externas y velando por

proveer las condiciones medioambientales requeridas para el funcionamiento de la plataforma tecnológica, esto con el fin de asegurar que los activos de información sean preservados, protegidos y estén disponibles para el personal autorizado.

Los lineamientos se impartirán, teniendo en cuenta los siguientes literales:

a) Gestión de Usuario.

El acceso a los activos a la información debe ser gestionados a través de la implementación de actividades que contemplen la solicitud formal, creación, modificación y eliminación de cuentas de usuario.

b) Registro de Usuario.

El administrador asigna una cuenta única o identificadora de usuario mediante la cual se pueda realizar el registro de acceso a los activos de información, la creación de cuentas de usuario para aplicaciones y en los sistemas operacionales de los equipos de cómputo, se controlan con el objetivo de establecer los permisos mínimos necesarios para que los funcionarios, contratistas, cumplan con sus funciones u obligaciones pactadas.

El nivel de acceso otorgado debe ser acorde para al rol con el propósito de la función del usuario y coherente con esta política de seguridad y privacidad de la información, por ejemplo, que no comprometa la separación de tareas, al acceder a los diferentes sistemas operativos de la entidad.

Únicamente el personal asignado con el rol de administrador será el responsable de realizar la creación, modificación y activación o desactivación de las cuentas de usuario.

Los responsables de cada dependencia o líder de proceso deben realizar la revisión y reporte periódico con el objeto de cancelar cuentas de usuarios redundantes o inactivos y remitirlas al proceso de Gestión de Bienes, Servicios e Infraestructura responsable del manejo de accesos y cuentas de usuario.

c) Pasos para crear, actualizar, eliminar, activar o inactivar.

La solicitud se realiza a través de la herramienta de mesa de ayuda, - GLPI, en caso de no encontrarse disponible se gestiona a través del correo electrónico institucional.

Para la creación de cuentas de usuario de sistemas de información se debe validar la existencia del usuario del dominio de la Entidad.

La solicitud debe contener la siguiente información:

- Tipo de vinculación con la Entidad: funcionario o contratista.
- Nombres y apellidos completos del funcionario o contratista a quien se le asignara la cuenta de usuario.
- Número de Identificación.
- Dependencia donde estará asignado o donde desarrollará sus actividades.
- Número de acto administrativo o número de contrato.
- Fecha de iniciación del contrato y fecha de terminación del contrato (contratistas) o de vinculación del funcionario.

d) Gestión de Derechos o Privilegios.

Se limita y controla el acceso y uso de activos de información mediante la asignación de permisos, roles y privilegios a las cuentas de usuario, el acceso y uso inadecuado de la información o cualquier recurso informático del IDPAC genera un impacto negativo en la administración de la información.

e) Gestión de Contraseñas de Usuario.

La Secretaria General a través del proceso de Gestión de Bienes, Servicios e Infraestructura, establecerá la administración de la seguridad de los activos de Información, en las políticas contenidas en este documento; así mismo, la apropiación de las buenas prácticas en el uso de las herramientas informáticas que apoyen el proceso.

Mediante la difusión y verificación del cumplimiento del uso de contraseñas para los usuarios estándar y para los usuarios con privilegios de administrador de los diferentes sistemas de información, se debe tener en cuanta:

- Evitar el riesgo de pérdida de las credenciales de acceso de los usuarios internos a los diferentes sistemas de información a los que se les asigna acceso.
- Evitar el riesgo asociado a la ausencia de un administrador con privilegios a los sistemas de información, bases de datos, aplicativos, elementos de infraestructura tecnológica.

- Garantizar la disponibilidad, confidencialidad e integridad de los activos de información de la entidad minimizando el riesgo que se pueda generar por la fuga o pérdida de alguna credencial de acceso.
- Normalizar la creación de usuarios acorde con los roles y perfiles para el acceso a la información.

Lo anterior, aplica para todos los servidores públicos de la entidad, es decir funcionarios (carrera administrativa y provisionales), funcionarios de libre nombramiento y remoción, contratistas y demás personal que tenga asignado un usuario y contraseña para el ingreso los diferentes sistemas de información, bases de datos, equipos de cómputo o aplicativos que soliciten la autenticación. Así mismo, se comprometen dentro de sus funciones u obligaciones contractuales a preservar la confidencialidad de la información y asumen las responsabilidades de seguridad y privacidad de la información, con el fin de salvaguardar la información cumpliendo los acuerdos de confidencialidad.

Se define un estándar de contraseñas dentro la política de seguridad y privacidad de la Información, que aplique de manera transversal a los sistemas de Información con parámetros de acceso garantizando las mejores prácticas para la asignación de contraseñas, cumpliendo como mínimo con los siguientes requisitos:

- El administrado de cada sistema de información es responsable de asegurar que se solicite las credenciales de acceso (usuario y contraseña) para permitir el acceso.

- El administrador de cada sistema es responsable de asegurar que el mismo usuario solicite el cambio de contraseña cada vez que esta es reestablecida manualmente a un usuario.
- Los usuarios son responsables de asegurar la privacidad de las contraseñas asignadas para acceder a los sistemas de información.
- Las credenciales de acceso para los diferentes sistemas de información son de uso personal e intransferible.
- El administrador de cada sistema es responsable de asegurar que las contraseñas que se transmitan a través de redes públicas estén protegidas contra acceso no autorizado mientras se encuentren en tránsito.
- El usuario de los sistemas de información de solicitar el establecimiento de la contraseña y remplazarla por una contraseña segura, debe cumplir con lo siguiente:
  a) La longitud de la contraseña debe ser mínimo de 8 caracteres.
  b) La contraseña debe estar compuesta por una combinación de letras mayúsculas, minúsculas, caracteres numéricos y símbolos especiales como los siguientes: @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /.
  c) No repetir los mismos caracteres en la misma contraseña. (ej.: “111222”).
  d) No enviar nunca la contraseña por correo electrónico o en un mensaje de texto.
  e) No deben usarse palabras o nombres comunes.
  f) No debe haber una relación obvia con el usuario, sus familiares, nombre de la entidad, abreviaciones relacionadas a la entidad, ciudad, país, año, fecha de nacimiento, el grupo de trabajo u otras asociaciones parecidas, ya que pueden ser identificadas de manera fácil a través de un ataque de ingeniería social.

g) Si hay indicios para creer que una contraseña ha sido comprometida, debe cambiarse inmediatamente.
h) No deben usarse contraseñas que sean idénticas o similares a contraseñas previamente empleadas.
i) No se debe almacenar la contraseña en la computadora.
j) Las aplicaciones deben almacenar las contraseñas en forma cifrada.

Una vez asignado el usuario a funcionarios, contratistas y/o terceros, se garantiza el cambio de contraseña en el momento del primer ingreso al sistema.

Finalmente, se configuran los sistemas de información de tal manera que las contraseñas sean fuertes, no repetibles en un periodo determinado o en cambios anteriores, bloqueo de cuentas después de intentos fallidos y solicitud automática de cambio de clave después de transcurrido un periodo de tiempo determinado.

f) Revisión de los Derechos de Acceso de Usuario

Los responsables de activos deben revisar los derechos, autorizaciones y privilegios de acceso de los usuarios con intervalos regulares. Cualquier desviación será tratada como un incidente en seguridad de la información, dejando la trazabilidad del ejercicio de esta actividad, las que serán objeto de revisiones por parte de la entidad.

g) Gestión de Derechos de Acceso con Privilegios Especiales

El uso de las claves de usuarios administradores de plataformas tecnológicas, tienen un control especial, éstas se deben cambiar obligatoriamente cada mes y tener una codificación especial definida en el procedimiento “Gestión de cuentas

de usuario", estas cuentas deben ser conocidas únicamente por el responsable de la administración de bases de datos, directorio activo, activos de seguridad y demás plataformas de administración de los recursos de TI.

h) Retirada o Adaptación de los Derechos de Acceso

Los privilegios otorgados a las cuentas de usuario de funcionarios serán suspendidos en el momento de retiro de su empleo y para el caso de contratistas y proveedores las contraseñas deben contar con vigencias establecidas y una vez expiradas surtir las fases de deshabilitar y/o eliminar, previo cumplimiento de requisitos legales o vigencias contractuales o por solicitud de los jefes de dependencia o supervisores de los contratos. En ningún caso se habilitarán usuarios y contraseñas a personas que no tengan algún tipo de vínculo con la entidad.

i) Control de Acceso a la Información

La entidad establece entornos con controles de acceso que aseguran el perímetro de oficinas, recintos, como en entornos abiertos para evitar el acceso no autorizado a ellos, controlando las amenazas físicas externas y velando por proveer las condiciones medioambientales requeridas para el funcionamiento de la plataforma tecnológica y la preservación de sus activos de información.

Así mismo, se exige a los proveedores de servicios de tecnología, el cumplimiento de la implementación y efectividad de mecanismos de seguridad física, controles de acceso físico y condiciones medioambientales con que éste debe contar.

Los funcionarios y contratistas responsables de las dependencias seguras tienen la obligación de vigilar y garantizar que se cumplan las medidas de seguridad definidas.

Los responsables de la información, colaborarán en la definición de los controles de acceso a los activos de información, y ayudarán a monitorear que los activos de información sean accedidos únicamente por los usuarios autorizados.

j) Control de Acceso a las Redes del IDPAC.

El acceso a las redes se permite como una herramienta de trabajo que facilita a los colaboradores realizar las actividades propias de la misionalidad, por lo que el uso adecuado de este recurso se debe controlar, verificar y monitorear. El uso de este recurso debe atender las siguientes reglas:

- Se prohíbe el uso de este recurso para el acceso a páginas relacionadas con pornografía, sustancias alucinógenas, armas, terrorismo, racismo, alcohol, web proxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.
- Se prohíbe el uso de este recurso para el intercambio no autorizado de información de propiedad de la entidad o de sus funcionarios.
- Los usuarios son responsables de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra los activos de información, contra terceros, la legislación vigente o los lineamientos de seguridad de la información.
- La creación de recursos y acceso a los mismos debe ser únicamente relacionado con la misionalidad de la entidad o necesidades de alguna de sus

áreas, previa autorización del encargado y donde se especifique claramente el objeto del requerimiento.

- La creación de acceso a través de VPN, controles remotos o cualquier medio de control externo, debe ser vigilado, monitoreado, contar con claves de acceso y todos los mecanismos de seguridad implementados por el área de Tecnologías de la Información.
- El correo electrónico es un medio exclusivo de comunicación institucional, están completamente prohibidas las siguientes actividades:
    a) Utilizar el correo electrónico para cualquier propósito personal, comercial o financiero no referente a la entidad.
    b) No se debe participar en la propagación de “cartas en cadenas”, ni en esquemas piramidales de índole político, religioso o temas similares.
    c) Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para el Instituto.

Los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de acceso a la cuenta de correo asignado por el Instituto.

El uso de internet es estrictamente de carácter institucional, estos servicios se monitorean permanentemente o por solicitud de los órganos de control para verificar su adecuada utilización.

Ningún equipo de cómputo o de comunicaciones que no sea de propiedad de la entidad debe ser conectado a la red institucional. En caso de ser necesario el acceso a internet para este tipo de equipos se ha dispuesto una red WiFi de uso exclusivo para visitantes y ciudadanos.

Solo se instalarán computadores personales u otros dispositivos con la autorización de la Secretaría General en cabeza del Proceso de Gestión de Bienes, Servicios e Infraestructura y previo análisis y verificación de la situación de vulnerabilidad de la entidad.

Los encargados del soporte técnico deben desconectar aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad a ser investigado.

La Secretaria General a través del proceso de Gestión de Bienes, Servicios e Infraestructura, es responsable del monitoreo, diseño de mecanismos e implementación de protocolos de seguridad y reporte de incidentes en el uso de internet y red wifi.

El IDPAC considera el abuso en la utilización de recursos informáticos como una falta disciplinaria.

No se realizará ningún tipo de intervención en elementos informáticos tales como computadores, tables, celulares que no sean propiedad del IDPAC.

k) Control de Acceso a las Aplicaciones y a la Información. Restricción del Acceso a la Información.

Todas las aplicaciones y bases de datos que se utilicen en la entidad, para su acceso deben contar con la cuenta de usuario, sus permisos de acuerdo con el perfil.

l) Acceso a Sistemas de Información y Aplicaciones

El acceso a la información en producción, debe hacerse únicamente a través de los aplicativos y sistemas autorizados. En ningún caso la información puede ser accedida directamente.

En el evento en el que entes externos requieran acceso a información crítica de la entidad, se deberán suscribir acuerdos de confidencialidad para la salvaguarda de la información.

m) Aislamiento de Sistemas Sensibles.

Según las necesidades de la entidad, se debe aislar los computadores donde se procese la nómina, procesos disciplinarios, evaluaciones para la selección de contratistas o donde se autoricen o se realicen pagos en línea, así como la información de carácter sensible perteneciente a las Juntas de Acción Comunal (JAC).

n) Control de Acceso al Código Fuente de los Programas

El acceso a los archivos de código fuente de las aplicaciones de software es limitado, únicamente al personal autorizado por la Secretaria General a través del Proceso de Gestión de Bienes, Servicios e Infraestructura tendrá acceso a esta información y harán uso de esta. Estos accesos deben ser controlados y supervisados.

7.2.3. Política de Criptografía

La entidad asegura el acceso, uso adecuado y efectivo de la información para proteger la confidencialidad, autenticidad y/o integridad de la información, así mismo busca garantizar el secreto en la comunicación entre dos entidades (personas, organizaciones, entre otros.)

Esta política, sobre uso, protección y duración de las claves criptográficas se realiza a través del directorio activo durante todo su ciclo de vida, por lo cual se deben utilizar controles criptográficos en los siguientes casos:

- Para la protección de claves de acceso a sistemas, datos y servicios.
- Para la transmisión de información clasificada, fuera del ámbito del IDPAC.
- Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el responsable de la Información y el responsable de Seguridad de la información.
- Asegurar que la información que se envía es auténtica en dos aspectos: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado no haya sido modificado en su tránsito.
- Método criptográfico que asocia la identidad de una persona a un mensaje o documento.
- La firma digital también se utiliza como una forma de garantizar la integridad del documento o mensaje.
- La firma digital se basa en el hecho de que un documento cifrado utilizando la llave privada de una persona sólo puede ser descifrado utilizando la llave pública asociada a esa misma persona.

- La firma digital es un digesto del documento, el cual se cifra utilizando la llave privada del firmante.

a) Controles Criptográficos Política de Uso de dos Controles Criptográficos.

Se utilizan controles criptográficos en los siguientes casos:

- Para los sitios web de uso externo, como por ejemplo portal web institucional.
- Para la protección de claves de acceso a sistemas, datos y servicios.
- Para la transmisión de información clasificada como crítica o sensible, fuera del ámbito de la entidad.
- Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el propietario de la Información y el responsable de Seguridad Informática.

b) Regulación de los controles criptográficos

- Los controles criptográficos serán utilizados en cumplimiento a todos los acuerdos pertinentes, normas internas política de seguridad y privacidad de la información, así mismo como el uso de firma digital, uso de correo electrónicos entre otros y los reglamentos.

7.2.4. Política de Seguridad Física y del Entorno

El Instituto debe contar con protecciones físicas y ambientales para los activos críticos, incluyendo perímetros de seguridad, controles de acceso físicos,

controles especiales en áreas de mayor sensibilidad, seguridad de los equipos, en el suministro eléctrico y cableado, detección y extinción de incendios, condiciones ambientales de operación y sistemas de contención.

a) Perímetro de Seguridad Física.

La entidad debe contar con un plano actualizado de las instalaciones eléctricas y de comunicaciones de los equipos de cómputo en red (planos de cableado estructurado), los cuales deben estar disponibles en su respectivo cuarto de equipos y comunicaciones, identificando áreas seguras, con acceso restringido a personal no autorizado.

b) Controles Físicos de Entrada.

Todos los funcionarios y contratistas deben portar el carnet en lugar visible, permitiendo con esto, una mejor identificación y control de las personas que ingresan a las áreas de cómputo y/o de archivo documental restringidas y que puedan tener acceso a cualquier elemento de TI.

c) Seguridad de Oficinas, Despachos e Instalaciones

Todas las dependencias donde se procese y almacene información deben tener acceso restringido al personal no autorizado. Las puertas y ventanas deben permanecer cerradas y periódicamente se debe inspeccionar las áreas protegidas desocupadas, además se agregará protección externa a las ventanas que presenten riesgos especiales.

d) *Protección Contra las Amenazas Externas y de Origen Ambiental.*

La Secretaría General debe garantizar la adopción de los controles necesarios para asegurar que los suministros de electricidad, así, como las redes de comunicaciones se encuentran protegidos.

Los equipos de cómputo se instalarán en lugares adecuados, lejos de polvo y tráfico de personas, garantizando las condiciones para su adecuado funcionamiento.

Los equipos servidores y equipos activos de red deben estar protegidos en un ambiente de acceso restringido con las condiciones ambientales adecuadas y con la protección de cambios de voltaje respectivas.

La Secretaría General, debe monitorear las variables de temperatura y humedad de las áreas de procesamiento de datos.

La entidad, mantendrá póliza de seguros de los recursos informáticos en funcionamiento, se debe incluir en la póliza colectiva de seguros el riesgo ante posibles pérdidas de información, por daños irrecuperables en los medios de información.

e) *Trabajo en Áreas Seguras.*

Son áreas seguras las dependencias de archivo documental, sitio donde se ubican equipos de cómputo de tratamiento de información sensible y/o critica,

como centro de datos internos o externos, centros de cableados, cuartos de unidades de poder no interrumpida – UPS, laboratorio de soporte. En estas dependencias se debe incrementar la seguridad estableciendo directrices y controles para la protección de los activos de información aquí ubicados.

f) Áreas de Acceso Público de Carga y Descarga.

En áreas de atención directa al público, zonas de almacén y recibo de insumos, radicación y puntos en los que las personas no autorizadas puedan estar, los equipos de cómputo deben estar aislados o instalados de manera que el público no tenga acceso directo a ellos.

7.2.5. Política de Seguridad de los Equipos.

Los equipos que hacen parte de la infraestructura tecnológica de la entidad, deben ser ubicados y protegidos adecuadamente para reducir los riesgos de las amenazas ambientales, pérdida, daño, robo o acceso no autorizado de los mismos. Así mismo se debe tener en cuenta los siguientes lineamientos:

a) Emplazamiento y Protección de Equipos.

Cada usuario es responsable del cuidado del hardware y software suministrado por la entidad, dichos equipos no deberán ser prestados a personas ajenas no autorizadas para su uso y no deberán salir de las instalaciones sin previa autorización del jefe inmediato y firmada por el Proceso de Gestión de Bienes, Servicios e Infraestructura, en consecuencia, cada usuario responderá por los daños y perjuicios técnicos y legales ocasionados por su mala utilización. La

detección de este uso indebido puede ocasionar la inhabilitación temporal o definitiva del activo de información para el usuario responsable.

b) Seguridad del Cableado.

El cableado de energía eléctrica y de comunicaciones, deberán cumplir con los estándares vigentes, deberán estar resguardados del paso de personas o máquinas y libres de cualquier interferencia eléctrica o magnética. Se debe tener un circuito independiente según los estándares que rigen la materia para las instalaciones eléctricas que alimenten elevadores, aspiradoras, cafeteras, motores y otros.

c) Mantenimiento de los Equipos.

Con el fin de garantizar un correcto funcionamiento y disponibilidad de los equipos de cómputo de la Entidad, se deben realizar mantenimientos preventivos y correctivos por parte del personal de soporte técnico o en su defecto mediante la contratación de firmas especializadas que presten este tipo de servicio.

d) Mantenimiento Preventivo y Correctivo.

La Secretaría General a través del personal de soporte o del proveedor del servicio de mantenimiento mantendrá una hoja de vida o historial de cada equipo, que contemple las revisiones efectuadas, cambio de piezas, modificaciones realizadas, fecha de vencimiento de la garantía, contrato de mantenimiento vigente y ubicación actual.

Está prohibido que el personal de soporte realicen dentro de las instalaciones del IDPAC y en horas laborales mantenimiento preventivo o correctivo de equipos que no son propiedad del Instituto.

e) Solicitud de Mantenimiento

Para la solicitud de mantenimiento, el usuario del equipo de cómputo debe registrar a través de la mesa de ayuda un soporte, el cual es atendido por el personal designado para tal fin, para ello el proceso de Gestión de Bienes, Servicios e Infraestructura definirá los acuerdos de niveles de servicio.

f) Seguridad de los Equipos Fuera de las Instalaciones.

El uso del equipo destinado al procesamiento de información fuera de las instalaciones de la entidad, será autorizado por la Secretaría General. En el caso de que en el mismo se almacene información clasificada, deberá ser aprobado además por el responsable de esta.

En caso de pérdida o robo de un equipo o cualquier medio que contenga información relacionada de la entidad, se debe realizar inmediatamente el respectivo reporte al proceso de Gestión de Bienes, Servicios e Infraestructura y se deberá interponer la denuncia ante la autoridad competente.

g) Retiro de equipos de propiedad del Instituto

Ningún activo de información debe ser retirado de una sede del IDPAC sin autorización formal. El personal de vigilancia será el encargado de controlar la

salida del recurso con la debida verificación, registro y autorización respectiva de cada uno de los elementos retirados.

h) Reutilización o eliminación segura de dispositivos de almacenamiento.

La Secretaría General mediante el proceso de Gestión de Bienes, Servicios e Infraestructura, debe garantizar la extracción y Backup de la información de cada uno de los equipos tecnológicos que contengan información; toda vez que estos pueden hacer parte de los activos de información.

Todos los elementos del equipo que contienen los medios de almacenamiento deben ser verificados para garantizar que los datos sensibles y el software con licencia sean eliminados o sobrescrito de forma segura antes de su reutilización o eliminación definitiva.

7.2.6. Seguridad de las operaciones

La Secretaría General es la encargada de la operación y administración de la plataforma tecnológica que apoya los procesos de la entidad, para ello asigna responsabilidades específicas a sus funcionarios y/o contratistas, quienes actuarán como responsables de garantizar la adecuada operación y administración de dicha plataforma, manteniendo actualizada la documentación de los procesos operativos para la ejecución de dichas actividades.

a) *Responsabilidades y documentación de procedimientos de operación*

El Instituto debe proveer a los funcionarios y/o contratistas de manuales de configuración y operación de los sistemas operativos, servicios de red, bases de datos y sistemas de información (comunicaciones y servicios como correo, intranet, WEB) así como todos los componentes de la plataforma tecnológica del Instituto.

Se debe garantizar la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica que apoya los procesos del IDPAC.

b) *Gestión de Cambios*

La Secretaría General, establecerá, coordinará y controlará los cambios en los activos de información, asegurando que los mismos sobre la plataforma tecnológica se encuentran debidamente autorizados por las dependencias correspondientes, evaluando el posible impacto operativo de los cambios previstos y su correcta implementación.

Los responsables de los activos de información deben solicitar formalmente los requerimientos de nuevas funcionalidades, servicios o modificaciones sobre sus sistemas de información.

El Comité Institucional de Gestión y Desempeño – CIGD, controlará que los cambios en los componentes de producción y de comunicaciones no afecten la seguridad de estos, ni de la información que soportan.

El Instituto a través del Proceso de Comunicación Estratégica y Nuevas Tecnologías, definirá los instrumentos para el registro de cambios y solicitudes de modificación de la plataforma tecnológica, igualmente se deben conservar los soportes documentales de las actividades desarrolladas.

c) Separación de Tareas

La asignación de tareas de operación y apoyo a la gestión estarán separadas del seguimiento y verificación de seguridad, con el fin de reducir el riesgo de modificaciones no autorizadas, mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas. Por ejemplo:

- Los roles y responsabilidades asociadas a la gestión operativa y de seguridad de la información, en ningún caso serán prestadas o ejecutadas por el mismo funcionario o contratista.
- El desarrollador de aplicaciones no podrá ser administrador de bases de datos en producción, ni administrador de aplicaciones o sistemas de información.
- Los funcionarios o contratistas con funciones u obligaciones contractuales operativas o de soporte en plataformas tecnológicas no tendrán a su cargo responsabilidades de auditoría de seguridad de la información o de control interno.

d) Separación de Entornos de Desarrollo Prueba y Producción

Los ambientes de desarrollo, las pruebas y producción deberán estar separados para reducir los riesgos de acceso no autorizado o cambios en el entorno operativo.

Se deben garantizar los recursos necesarios que permitan la separación de ambientes de desarrollo, pruebas y producción, así como de la independencia de los funcionarios o contratistas que ejecutan dichas labores.

e) Planificación y Aceptación del Sistema.

La Secretaría General, efectúa el monitoreo de las necesidades de capacidad de los sistemas en producción y proyecta futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuado, para ello tomará en cuenta además de los nuevos requerimientos de tecnología informática, las tendencias actuales y proyectadas en el procesamiento de la información. Así mismo, informará los eventos que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento.

f) Protección contra el código malicioso y descargable.

La entidad garantiza la adquisición de uno o varios antivirus debidamente licenciados con la funcionalidad de actualización permanente, de sus bases de virus y como medida preventiva todo medio de almacenamiento, como cintas, discos duros removibles, dispositivos con conexión USB, discos compactos, que

ingresen a la entidad, los cuales deben ser revisados y/o vacunados antes de su uso.

Todos los equipos de cómputo, deben tener habilitado la solicitud de clave de administrador cuando se intente realizar la instalación de un programa ejecutable, estas claves deben ser cambiadas periódicamente y no deben ser conocidas por los usuarios estándar del Instituto.

Si un usuario sospecha de una infección por un virus en el computador, debe desconectar el cable de red y avisar a soporte técnico a través de la mesa de ayuda para que sea revisado inmediatamente.

Cuando se reciba un correo sospechoso por el nombre, la extensión de éste, el remitente o con otras características anormales, se recomienda no hacer la apertura o descarga de los archivos adjuntos y mucho menos su ejecución, para estos casos se debe solicitar la revisión inmediata a soporte técnico.

Los funcionarios, contratistas y/o terceros que tienen vínculo con la entidad no deben utilizar software obtenido externamente desde Internet o de una persona u organización diferente a la entidad, el incumplimiento de esta política acarreará las sanciones correspondientes y el software será desinstalado inmediatamente del equipo donde se encuentre.

En caso de necesitar la instalación de algún software adicional de protección y detección de código malicioso, se debe contar con la autorización del Proceso de Gestión de Bienes, Servicios e Infraestructura.

g) Copias de seguridad.

Con el fin de tener directrices y controles que permitan realizar y administrar las copias de seguridad que aseguren la disponibilidad, integridad y confidencialidad de las bases de datos que contienen la información institucional, configuraciones y parámetros de aplicaciones de software, sistemas de información y demás servicios, esta tarea debe realizarse diariamente y de forma automática.

Se deben realizar pruebas periódicas de recuperación de la información respaldada y documentar sus resultados, con el fin de garantizar la integridad de la información resguardada.

Se deben asignar los niveles de protección física y ambiental adecuada a la información de respaldo según las normas aplicadas y las especificaciones dadas por el fabricante de los medios de almacenamiento.

Finalmente, el proceso de gestión de Bienes, Servicios e Infraestructura debe:

- Actualizar periódicamente las configuraciones de los Servidores para la correcta ejecución de las copias de respaldo.
- Efectuar las copias de información de los Servidores, cada vez que se realice un cambio significativo en los Sistemas Operativos o configuraciones Básicas.
- Realizar una copia de respaldo incremental diaria de los Servidores de Base de Datos, servidores Web, Sistemas de Información misionales, Aplicaciones, Desarrollo y dispositivos de red.
- Realizar un respaldo semanal y uno mensual de los Servidores de Base de Datos, servidores Web, Sistemas de Información, Aplicaciones, Desarrollo y dispositivos de red.

- Realizar las copias de respaldo en horario no hábil, lo cual será verificado a través de Procesos Automáticos. Una vez se verifique la correcta ejecución de las copias de respaldo, se debe retirar la cinta de Backup del robot de cintas. Los dispositivos magnéticos que contienen información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra almacenada.
- El sitio alterno donde se almacenan las copias de respaldo debe contar con los controles de seguridad necesarios, para cumplir con las medidas de protección y seguridad física apropiados.
- Conservar los medios de almacenamiento de información en un ambiente que cuente con las especificaciones emitidas por los fabricantes o proveedores.
- Contar con un responsable para gestionar la entrega o retiro de las cintas de Backup del sitio externo.
- Las cintas de Backup con la Información actualizada, no deben permanecer más de una semana fuera del sitio externo.

h) Adquisición, Desarrollo y Mantenimientos de Sistemas de Información

La Secretaría General, a través del proceso de Comunicación Estratégica y Nuevas Tecnologías, brinda la custodia y realiza copias de los archivos fuente de las aplicaciones que son propiedad de la entidad.

Todos los desarrollos de software y las nuevas aplicaciones estarán aprobados desde la alta dirección los cuales tendrán el seguimiento de su cumplimiento desde la Dirección General y/o la Secretaria General. En todo desarrollo e

implementación y mantenimiento de los sistemas de información o aplicaciones de software, se identifican, especifican y analizan los requerimientos de seguridad.

i) Análisis y especificación de los requisitos de seguridad.

Con base en el análisis y clasificación del riesgo del sistema y durante la fase de diseño del proyecto, los requerimientos de seguridad deben ser definidos formalmente por parte del "usuario" del sistema o un representante de este y las medidas de seguridad deben ser definidas a partir de los requerimientos de seguridad ya establecidos.

Se debe realizar las pruebas de aceptación, de escenario, de regresión, exploratorias, de función con el fin de validar que las aplicaciones desarrolladas al interior del IDPAC cumplan con todos los requerimientos solicitados.

j) Control del procesamiento interno.

En el diseño de los sistemas de información y aplicaciones se contemplará la implementación de controles para la verificación de requisitos previos al procesamiento de información, estos controles son adicionales a los controles manuales ya establecidos en los sistemas de información.

Todo procesamiento de información contará con mecanismos de recuperación ante fallas, con el fin de garantizar su integridad en los sistemas y aplicaciones afectadas, dejando el respectivo registro de trazabilidad de las operaciones realizadas.

k) Integridad de los mensajes.

Se identifican los requisitos para asegurar la autenticidad y protección de la integridad del contenido de los mensajes en las aplicaciones, los cuales hacen referencia al estado y finalización de transacciones, petición de datos, solicitud de acciones al usuario, petición de claves, confirmaciones, errores, resultados de validaciones, entre otros; se identificarán e implantarán los controles apropiados.

l) Seguridad en la nube

La entidad cuenta con la plataforma de servicios en la nube “Azure” con servidores en varios sistemas operativos, servidores de datos y servidores de archivos, se tiene una amplia gama de opciones de seguridad, para lo cual se deben llevar a cabo las siguientes pruebas de seguridad:

- Pruebas de penetración, detección de intrusiones, auditorías y registro.
- Control en la ubicación de los datos
- Verificación de Acceso a los datos y bajo qué términos.

m) Seguridad de los Archivos de Sistema.

La entidad, debe contar con un administrador de despliegues de aplicaciones, quién coordina la implementación de ajustes y nuevas funcionalidades, para asegurar que los sistemas en producción sean los probados y autorizados por los responsables de las dependencias solicitantes. El administrador no podrá ser un desarrollador, ni tendrá acceso al código fuente de las aplicaciones, en cumplimiento de la política de segregación de tareas y funciones.

Se cuenta con la documentación de seguridad que contemple registro de auditoría de las actualizaciones realizadas, retención de las versiones previas del sistema como medida de contingencia y pruebas a realizarse, entre otros.

n) Protección de los datos de prueba del sistema.

Las pruebas de los sistemas se podrán efectuar sobre datos extraídos del ambiente de producción. En el ambiente de pruebas se aplicarán procedimientos idénticos de control de acceso a los realizados en el ambiente de producción.

Toda copia de información o bases de datos de producción para la realización de pruebas debe contar con la autorización de su propietario donde se especifique la fecha de vencimiento de uso; una vez finaliza esa fecha, la información será eliminada inmediatamente.

o) Desarrollo tercerizado

La Secretaría General en cabeza del proceso de Comunicación Estratégica y Nuevas tecnologías debe contar con un responsable de autorizar la creación, adaptación o adquisición de software.

Los contratos de consultoría, y en general todo tipo de contratos de servicios deben contener provisiones a este respecto. De igual manera, para los servicios de “outsourcing”, es especialmente importante definir los derechos generados por proveedores en desarrollo de este tipo de contratos.