ALCALDÍA MAYOR
DE BOGOTÁ D.C.

IDPAC

BOGOTÁ

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

	INSTITUTO DISTRITAL DE LA PARTICIPACION Y ACCION COMUNAL		
SISTEMA INTEGRADO DE GESTIÓN			
POLITICA DE SEGURIDAD DE LA INFORMACIÓN			
CÓDIGO:	IDPAC-GTI-OT-04	VERSIÓN	02
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	17/03/2021	26/03/2021	

REGISTRO DE MODIFICACIONES		
VERSIÓN	**FECHA**	**ÍTEM MODIFICADO – DESCRIPCIÓN**
01	22/08/2017	Versión Inicial
02	26/03/2021	Actualización de acuerdo con el marco normativo vigente

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Este documento define las actividades necesarias para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información para el IDPAC, siguiendo la metodología del MINTIC y la alta Consejería Distrital para las TIC, buscando como propósito proteger preservar y administrar la confidencialidad integridad y disponibilidad autenticidad y no repudio de la información. Esta política será aprobada en el Comité creado según resolución 116 de 2017 para tal fin en el Instituto, incluye los dominios sugeridos por la norma técnica internacional ISO 27002:2013, que responden a las necesidades del IDPAC y que contribuyan al alcance de las metas institucionales.

Esta política debe ser aplicada por todos los funcionarios, contratistas, proveedores, y todo personal externo que utilice los servicios de tecnologías de la información que ofrece el IDPAC; deben conocer y aceptar el reglamento vigente para su uso y el desconocimiento del mismo, no exonera de responsabilidad al usuario, ante cualquier acción de amenaza que afecte la seguridad de la información del IDPAC.

La política de privacidad de información del IDPAC se ajusta a la nueva manera de acceso y protección de la información debido a la pandemia del COVID 19, buscando la mejor manera de dar cumplimiento a la legislación de transparencia, acceso a la información pública y a los procesos y personas vinculadas con el manejo que se le da a la información; mediante esta política se busca el fortalecimiento de la información del IDPAC, la privacidad de los datos de funcionarios y ciudadanos acorde con la legislación colombiana.

2. OBJETIVO GENERAL

Regular la 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.

3. OBJETIVOS ESPECIFICOS

- Definir estrategia de uso de la política de seguridad de la información
- Buscar estrategia de continuidad de los procesos frente a los incidentes de la seguridad de la información

- Establecer roles y responsabilidad para la seguridad de la información y seguridad digital en el IDPAC
- Crear lineamientos para la implementación, verificación y cumplimiento de la política de seguridad y privacidad de la información
- Dar lineamientos a los funcionarios contratistas y terceros sobre la información obtenida genera y procesada por el Instituto aplicando las mejores prácticas de seguridad con el objetivo de mitigar el riesgo de acceso uso divulgación, interrupción o destrucción no autorizada de la información que recoge el IDPAC.

4. ALCANCE

La presente Política de Seguridad de la Información se establece en cumplimiento de las disposiciones legales vigentes, con el objeto de implementar una adecuada gestión de la seguridad sobre los activos de información definidos por el IDPAC, debe ser conocida y de obligatorio cumplimiento por parte de funcionarios, contratistas y terceros que acceden al uso de las plataformas y servicios tecnológicos que disponga el Instituto.

Establece los lineamientos requeridos para la implementación de un modelo de seguridad y privacidad de la información, definición de indicadores para su monitoreo, seguimiento y cumplimiento

5. GLOSARIO O DEFINICIÓN DE TÉRMINOS

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 la misma (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 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

Término	Definición
	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.
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.
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.
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

Término	Definición
	Internet, pretende reemplazar la escasez de direcciones que tiene el actual ipv4.
Mecanismos de autenticación	Para efectos del presente Decreto 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	El no repudio o irrenunciabilidad 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	Una 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
Política:	Instrucciones mandatarias que indican la intención y la directriz de la alta gerencia respecto a la operación del IDPAC.
Proactividad	Principio que busca que el Estado y los ciudadanos trabajen de manera conjunta en el diseño de políticas, normas, proyectos y servicios, para tomar decisiones informadas que se anticipen a los acontecimientos, mitiguen riesgos y atiendan a las necesidades específicas de los usuarios, buscando el restablecimiento de los lazos de confianza a través del uso y aprovechamiento de las TIC.
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	Conjunto de elementos interrelacionados o interactuantes (estructura

Término	Definición
de la seguridad de la información - SGSI:	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 gestión del riesgo y de mejora *continua.*
Software utilitario:	Software que está diseñado para realizar una tarea determinada o especifica
Software:	Conjunto de programas, aplicaciones y rutinas que se ejecutan en un computador.
TI	Se refiere a tecnologías de la información
TIC	Se refiere a tecnologías de la información y comunicaciones
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.

6. MARCO NORMATIVO

NORMA	DESCRIPCIÓN
Directiva 05 de 2005	Políticas Generales de Tecnologías de Información y Comunicaciones aplicables a las entidades del Distrito Capital
Resolución 305 de 2008	Por la cual se expiden políticas públicas para las Entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad infraestructura de Datos Espaciales y Software Libre
Ley 1273 de 2009	Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.
Ley 1341 de 2009	Define los principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones – TIC
Decreto 235, Art.	Por el cual se regula el intercambio de información entre Entidades para el

NORMA	DESCRIPCIÓN
1-4 de 2010	cumplimiento de funciones públicas
CONPES 3701 de 2011	Define los lineamientos de política ciberseguridad y ciberdefensa.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales
Decreto 1377 de 2013	Tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales
Ley 1712 de 2014	Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones
Decreto 1074 de 2014	"Por medio del cual se expide el Decreto único Reglamentario del Sector Comercio, Industria y Turismo"
Decreto 1078 de 2015	Se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y Comunicaciones
Decreto 1081 de 2015	Se expide el Decreto Reglamentario Único del Sector Presidencia de la República
Decreto 415 de 2016	Por el cual se adicional el Decreto único Reglamentario del sector de la Función Pública, decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de información y las comunicaciones.
Directiva 3 de 2016	Creación equipo de trabajo de seguridad de la información adscrito a la Dirección General
Resolución 116 de 2017	Por la cual se crea el Comité de Seguridad de la información (CSI) del Instituto de la Participación y la Acción Comunal
CONPES 3854 de 2017	Política Nacional de Seguridad Digital
Decreto 1499 de 2017	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
CONPES 3920 de 2018	Política Nacional de Explotación de datos
Decreto 1008 de 2018	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 1978 de 2019	Se moderniza el sector de las Tecnologías de la Información y las Comunicaciones (TIC),
Directiva 2 de	Simplificación de interacción digital entre los ciudadanos y el Estado.

NORMA	DESCRIPCIÓN
2019	

7. ACERCA DEL IDPAC

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.

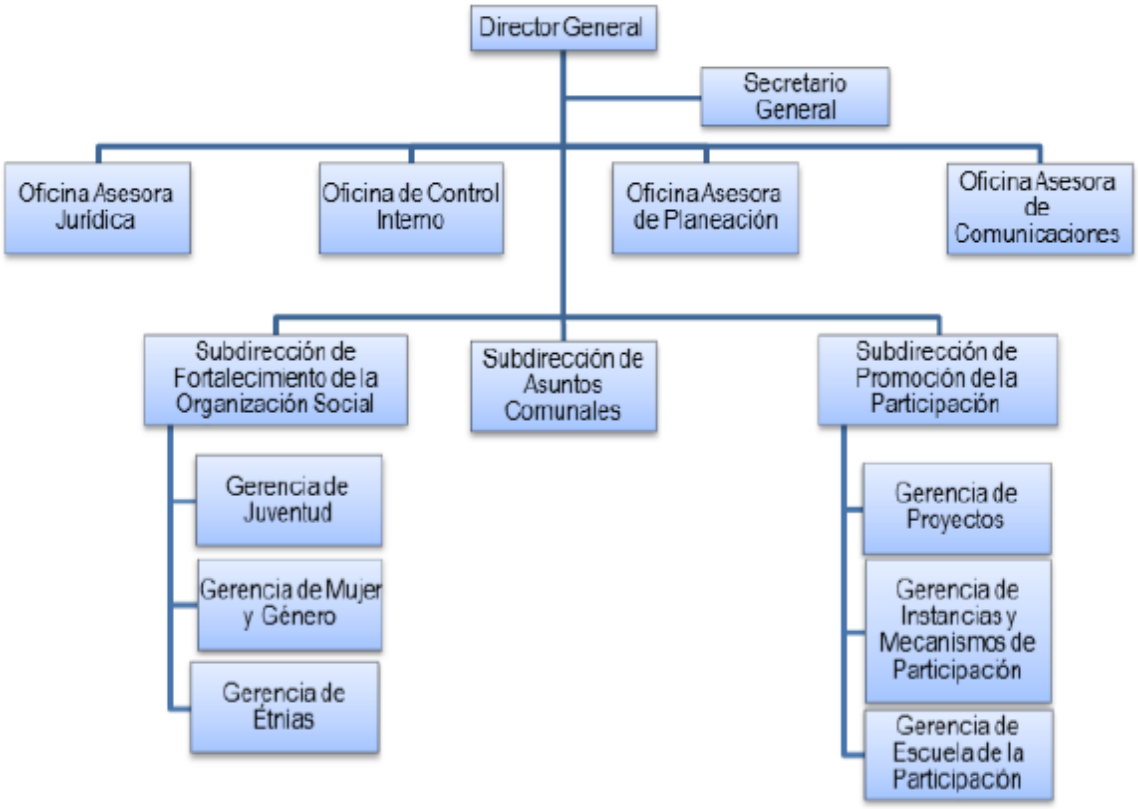
MISIÓN.

Somos una entidad pública, del orden distrital, que genera condiciones innovadoras, institucionales, organizativas y culturales en Bogotá y la región, que incentivan, facilitan y fortalecen la participación y el empoderamiento ciudadano como forma de mejorar el bienestar de los ciudadanos y sus comunidades.

VISIÓN.

En el 2030, el IDPAC será reconocido local, nacional e internacionalmente, como la entidad líder en la promoción e investigación de la participación ciudadana en el Distrito Capital, así como en producción de técnicas y metodologías de fortalecimiento organizativo, que aportan a la cultura democrática, inclusiva, intercultural y con equidad de género y a incrementar la capacidad de incidencia de la ciudadanía en la gestión pública y el control social.

ORGANIGRAMA.



Fuente: Elaboración propia

8. DOMINIOS POLÍTICAS DE SEGURIDAD

8.1. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración del INSTITUTO DISTRITAL DE LA PARTICIPACIÓN Y LA ACCIÓN COMUNAL - IDPAC con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos del IDPAC y apoyan la implementación del Sistema de Gestión de Seguridad de la Información - SGSI, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

EL INSTITUTO DISTRITAL DE LA PARTICIPACIÓN Y LA ACCIÓN COMUNAL - IDPAC, para asegurar la dirección estratégica, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales del IDPAC
- Cumplir con los principios de seguridad de la información
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del IDPAC
- Garantizar la continuidad del negocio frente a incidentes.

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

A continuación, se establecen las políticas de seguridad que soportan el SGSI de EL INSTITUTO DISTRITAL DE LA PARTICIPACIÓN Y LA ACCIÓN COMUNAL - IDPAC:

- EL INSTITUTO DISTRITAL DE LA PARTICIPACIÓN Y LA ACCIÓN COMUNAL - IDPAC implementa, opera y mejora de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la misión del Instituto y a los requerimientos regulatorios que le aplican a su naturaleza.

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

- EL INSTITUTO DISTRITAL DE LA PARTICIPACIÓN Y LA ACCIÓN COMUNAL - IDPAC busca proteger la información generada, procesada o resguardada por los procesos en cumplimiento de su misionalidad y activos de información que hacen parte de los mismos.

- EL INSTITUTO DISTRITAL DE LA PARTICIPACIÓN Y LA ACCIÓN COMUNAL - IDPAC busca proteger la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de ésta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- EL INSTITUTO DISTRITAL DE LA PARTICIPACIÓN Y LA ACCIÓN COMUNAL - IDPAC busca proteger su información de las amenazas originadas por parte del personal.

- EL INSTITUTO DISTRITAL DE LA PARTICIPACIÓN Y LA ACCIÓN COMUNAL - IDPAC busca proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- EL INSTITUTO DISTRITAL DE LA PARTICIPACIÓN Y LA ACCIÓN COMUNAL - IDPAC busca controlar la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- EL INSTITUTO DISTRITAL DE LA PARTICIPACIÓN Y LA ACCIÓN COMUNAL - IDPAC busca implementar control de acceso a la información, sistemas y recursos de red.

- EL INSTITUTO DISTRITAL DE LA PARTICIPACIÓN Y LA ACCIÓN COMUNAL - IDPAC busca garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- EL INSTITUTO DISTRITAL DE LA PARTICIPACIÓN Y LA ACCIÓN COMUNAL - IDPAC busca garantizar a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- EL INSTITUTO DISTRITAL DE LA PARTICIPACIÓN Y LA ACCIÓN COMUNAL - IDPAC busca garantizar la disponibilidad de sus procesos y la continuidad de su operación basado en el impacto que pueden generar los eventos.

- EL INSTITUTO DISTRITAL DE LA PARTICIPACIÓN Y LA ACCIÓN COMUNAL - IDPAC busca garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, trae consigo, las consecuencias legales que apliquen a la normativa del IDPAC, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

8.2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Objetivo: Establecer un marco de gestión para dar continuidad, mejorar y controlar la implementación y operación de seguridad de la información dentro del Instituto.

Esta política debe ser asumida y aplicada por todos los servidores públicos, contratistas y particulares que tengan acceso y uso de los activos de información del IDPAC con la responsabilidad de cumplir con las normas, procedimientos y estándares referentes a la seguridad de la información.

Mediante la Resolución 123 de 2018 se estableció que el Comité Institucional de Gestión y Desempeño del Instituto Distrital de la Participación y Acción Comunal, es la máxima Autoridad de Seguridad de la Información y por tanto el responsable de generar, modificar y aprobar las políticas específicas de seguridad de la información aplicables al interior del Instituto, así como sus procesos, procedimientos, controles y directrices para el adecuado uso y administración de los activos de información, asegurando los recursos adecuados y promoviendo una cultura activa de seguridad de la información en el IDPAC.

Los directores y demás directivos que integran el Comité de seguridad de la información son los responsables de hacer cumplir las políticas y directrices de seguridad de la información establecidas en el IDPAC.

Las auditorías y seguimientos a los sistemas de información deben ser programadas conjuntamente con las auditorías que realiza la Oficina de Control Interno y las externas que programe el IDPAC.

Los usuarios de los activos de información deben notificar al Comité Institucional de Gestión y Desempeño - CIGD, Secretario General, al jefe inmediato o al encargado del área las inconsistencias, anomalías e incidentes de seguridad, tales como:

- Eventos adversos o anormales en computadores, sistemas de información asignados, redes de datos, equipos de comunicación.

- Cuando exista sospecha o conocimiento de información confidencial o reservada que ha sido revelada, modificada, alterada o borrada sin autorización.

El Comité Institucional de Gestión y Desempeño - CIGD revisa anualmente la presente Política, a efectos de mantenerla actualizada. Así mismo efectúa toda modificación que sea necesaria en función a posibles cambios que afecten su definición, como, cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, cambios estructurales del IDPAC, entre otros.

Cualquier usuario de los servicios tecnológicos del IDPAC puede identificar la necesidad de modificar la Política de Seguridad de la Información, comunicando las inquietudes y/o sugerencias al Comité Institucional de Gestión y Desempeño - CIGD, responsable por el mantenimiento de la misma.

Los funcionarios, Contratistas, y Proveedores del IDPAC deben aceptar los acuerdos de confidencialidad, las políticas y controles de seguridad definidos por el IDPAC, los cuales reflejan los compromisos de protección y buen uso de la información y activos de acuerdo con los criterios establecidos en la normatividad vigentes y la política de Seguridad de la Información.

8.2.1 ASIGNACIÓN DE RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN

El uso de activos de la información será autorizado por los directores o Jefes de áreas responsables de las dependencias involucradas, considerando su propósito y uso, conjuntamente con los Responsables de la Seguridad de la Información, a fin de garantizar que se cumplan todas las Políticas, directrices y requerimientos de seguridad pertinentes.

8.2.2 CONTACTO CON GRUPOS DE INTERÉS ESPECIAL

El IDPAC podrá compartir experiencias y cooperar en materia de seguridad, con entidades territoriales y nacionales del Estado, previa firma de un convenio o acuerdo de confidencialidad de los temas de seguridad tratados.

Se mantendrán los contactos apropiados con los grupos de interés especial como la Alta Consejería Distrital de TIC, Comisión Distrital de Sistemas, Ministerio de TIC, Policía y demás entes de seguridad especializados y asociaciones profesionales para que puedan ser

contactados de manera oportuna en el evento en que se presente un incidente de seguridad de la información.

8.3. GESTIÓN DE ACTIVOS

Objetivo: Identificar los activos del IDPAC y definir las responsabilidades de protección adecuados.

Los propietarios responsables de los Activos de Información, tienen la responsabilidad de colaborar en la vigilancia del cumplimiento de la Política de Seguridad de la Información dentro de su área y para poder realizarlo debe conocer el valor de su información, los usuarios que deben tener acceso a ella y los privilegios en su uso.

El Comité Institucional de Gestión y Desempeño - CIGD es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que se procesa.

8.3.1 INVENTARIO DE ACTIVOS DE LA INFORMACIÓN

Los activos de información físico 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 a 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 los activos.

8.3.2 PROPIEDAD DE LOS ACTIVOS DE INFORMACIÓN

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.

8.3.3 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 funcionarios, contratistas y terceros de acuerdo con sus funciones 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 seguridad de la información con los periodos de inicio y fin claramente establecidos, en información documentada como contratos, convenios, normatividad, legislación y otros; estos controles deben ser gestionados por los responsables asegurando su trazabilidad.

8.3.4 CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN

Objetivo: Asegurar que la información del IDPAC reciba los niveles de protección adecuados, ya que con base en su valor y de acuerdo a 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 a 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, sensibilidad, el nivel de riesgo a que está expuesta y/o requerimientos legales de retención.

Clasificación de acuerdo con la confidencialidad

Se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o 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:

- **INFORMACION PUBLICA RESERVADA:** Información disponible sólo para un proceso del IDPAC 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.
- **INFORMACION PUBLICA 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 la misma. Esta información es propia del IDPAC o de terceros y puede ser utilizada por todos los funcionarios del instituto para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
- **INFORMACION PÚBLICA** Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera del IDPAC, sin que esto implique daños a terceros ni a las actividades y procesos del instituto.

- **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 PUBLICA RESERVADA.

Etiquetado de activos de información

Los procedimientos para el etiquetado de los activos información serán aplicados de acuerdo con el esquema de clasificación de la información aprobada por el IDPAC, lo anterior teniendo en cuenta las Tablas de Retención Documental aprobadas para las diferentes áreas y las siguientes pautas generales:

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

8.3.5 CATEGORIZACIÓN DE LOS ACTIVOS DE INFORMACIÓN SEGÚN LA 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, el IDPAC aplicará los siguientes criterios a los activos de información: *Pública*, *Reservada*, *Privada o Confidencial*, *Semi-privada o Interna.*

8.3.6 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 a los lineamientos estipulado en la Ley 1712 de 2014 por la cual se crea la ley de transparencia.

8.3.7 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.

8.3.8 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.

8.3.9 DIVULGACIÓN DE INFORMACIÓN A TERCEROS.

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

8.3.10 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 del IDPAC 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.

8.3.11 DEVOLUCIÓN DE LOS ACTIVOS DE INFORMACIÓN

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

8.4. CONTROL DE ACCESO

Objetivo: Limitar y controlar el acceso y uso de los activos de información a funcionarios, contratistas y terceros que estén vinculados al IDPAC.

El Instituto Distrital de la Participación y la Acción Comunal implementa y mantiene controles de acceso físico y lógico sobre las instalaciones, infraestructura, 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, circuito 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 al personal autorizado

8.4.1 GESTIÓN DE ACCESO DE USUARIO.

Registro de usuario.

El acceso a los Activos de Información del IDPAC, debe ser gestionado mediante un procedimiento formal de creación, modificación y eliminación de cuentas de usuario.

Se asigna una cuenta única o identificador de usuario mediante la cual se pueda realizar el registro de acceso a los activos de información.

El nivel de acceso otorgado debe ser el adecuado para el propósito de la función del usuario y coherente con la Política de Seguridad del IDPAC, por ejemplo, que no comprometa la separación de tareas.

Únicamente el responsable de la información, puede autorizar la creación, modificación y eliminación de cuenta de usuario.

Las áreas del IDPAC deben realizar revisiones periódicas con el objeto de cancelar cuentas de usuario redundantes o inactivas y remitirlas al proceso de Gestión de Tecnologías de la Información al responsable de manejo de accesos y cuentas de usuario.

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.

Gestión de contraseñas de usuario.

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.

Se configurarán 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.

Revisión de los derechos de acceso de usuario

Los responsables de activos deben revisar los derechos, autorizaciones y privilegios de acceso de los usuarios a 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 en el IDPAC.

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 IDPAC-GTI-PR-19 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.

Retirada o adaptación de los derechos de acceso

Los privilegios otorgados a las cuentas de usuario de funcionarios del IDPAC serán suspendidos en el momento de retiro de su empleo y para para el caso de contratistas y proveedores las contraseñas deben contar con vigencias establecidas y una vez expiradas surtir las fases de deshabilitación y eliminación, previo cumplimiento de requisitos legales o vigencias contractuales o por solicitud de los jefes de áreas o Supervisores de los contratos. En ningún caso se habilitarán usuarios y contraseñas a personas que no tengan ningún tipo de vinculación con el IDPAC.

8.4.2 CONTROL DE ACCESO A LA INFORMACIÓN.

Objetivo: Limitar y controlar el acceso y uso de los activos de información a funcionarios y contratistas y terceros que estén vinculados al IDPAC.

El IDPAC 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 implantación 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 áreas seguras tienen la obligación de vigilar y garantizar que se cumplan las medidas de seguridad definidas.

Los directores y Jefes de área como 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.

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 del negocio del IDPAC, 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 del IDPAC 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 del IDPAC, 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 del IDPAC 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:

  - ✓ Utilizar el Correo electrónico para cualquier propósito personal, comercial o financiero no referente al IDPAC.
  - ✓ No se debe participar en la propagación de “cartas en cadenas”, ni en esquemas piramidales de índole político, religioso o temas similares.
  - ✓ 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.

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 del IDPAC 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 área de Tecnologías de la Información y previo análisis y verificación de la situación de vulnerabilidad del IDPAC.

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 TIC, 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.

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 el IDPAC, para su acceso deben contar con la cuenta de usuario con sus permisos establecidos de acuerdo al perfil del usuario.

Acceso a sistemas de información y aplicaciones

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

En el caso que entes externos requieran acceso a información crítica del IDPAC, se deben suscribir acuerdos de confidencialidad para la salvaguarda de la información.

Aislamiento de sistemas sensibles.

Según las necesidades del IDPAC, 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).

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 área de TI tendrá acceso a esta información y harán uso de la misma. Estos accesos deben ser controlados y supervisados

8.5. CRIPTOGRAFÍA

Objetivo: Asegurar el acceso, uso adecuado y efectivo de la información para proteger la confidencialidad, autenticidad y/o integridad de la información.

La política sobre uso, protección y duración de las claves criptográficas se realiza a través del directorio activo durante todo su ciclo de vida.

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.

8.6. SEGURIDAD FÍSICA Y DEL ENTORNO

Objetivo: Evitar el acceso físico no autorizado, daños e interferencia para la información del IDPAC y a las instalaciones de procesamiento de información.

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.

Deben existir procedimientos especiales para mantener la seguridad en los momentos de mantenimiento de equipos, cuando la información o los equipos que la contienen deben salir del IDPAC o cuando se eliminan o dan de baja los equipos tecnológicos y cuando se realiza ingresos de personal a las áreas restringidas.

8.6.1 ÁREAS SEGURAS

Perímetro de seguridad física.

Todas las áreas o dependencias administrativas y operativas del IDPAC deben contar con un croquis actualizado de las instalaciones eléctricas y de comunicaciones de los equipos de cómputo en red (planos de cableado estructurado), los cuales deben estar compendiados y disponibles en su respectivo cuarto de equipos y comunicaciones. Identificando áreas seguras, con acceso restringido a personal no autorizado.

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.

Seguridad de oficinas, despachos e instalaciones

Todas las oficinas donde se procese y almacene información deben tener acceso restringido al personal no autorizado.

Las puertas y ventanas de las áreas seguras deben permanecer cerradas y periódicamente se debe inspeccionar las áreas protegidas desocupadas, además se agregará protección externa a las ventanas que presenten riesgos especiales.

Protección contra las amenazas externas y de origen ambiental.

La Secretaría General en cabeza del área de Tecnologías de la Información 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 del IDPAC 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 en cabeza de TI, debe monitorear las variables de temperatura y humedad de las áreas de procesamiento de datos.

El IDPAC 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.

Trabajo en áreas seguras.

Son áreas seguras las áreas de archivo documental, sitio donde se ubican equipos de cómputo de tratamiento de información sensible y/o critica, las áreas de informática y sistemas del IDPAC, como centro de datos internos o externos, centros de cableados, cuartos de Unidades de poder no interrumpida – UPS, laboratorio de soporte. En estas áreas se debe incrementar la seguridad estableciendo directrices y controles para la protección de los activos de información aquí ubicados.

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.

Para el uso de auditorios y salas de reuniones, el uso de los equipos de cómputo diferentes a los del IDPAC tendrán acceso restringido y autorizado por el área de Tecnologías de la información.

8.6.2 SEGURIDAD DE LOS EQUIPOS.

Emplazamiento y protección de equipos.

Los equipos que hacen parte de la infraestructura tecnológica del IDPAC deben ser ubicados y protegidos adecuadamente para reducir los riesgos de las amenazas ambientales, pérdida, daño, robo o acceso no autorizado de los mismos

Cada usuario es responsable del cuidado del hardware y software suministrado por el IDPAC, 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 área de Recursos Físicos, 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.

Seguridad del cableado.

El cableado de energía eléctrica y de comunicaciones, deberán cumplir con los estándares vigentes y 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

Mantenimiento de los equipos.

Con el fin de garantizar un correcto funcionamiento y disponibilidad de los equipos de cómputo del IDPAC, se debe realizar mantenimiento preventivo y correctivo, mediante la contratación de firmas especializadas que presten este tipo de servicio o en su defecto por el personal soporte técnico del IDPAC, quienes deben tener a su disposición las herramientas necesarias para efectuar dichos mantenimientos.

- **Mantenimiento Preventivo y correctivo**

  El mantenimiento preventivo de equipos de cómputo se realizará según la política establecida en el IDPAC, mínimo cada seis meses.

La Secretaria General a través del personal de soporte o del proveedor del servicio de mantenimiento mantendrá una hoja de vida 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 los técnicos de sistemas del IDPAC realicen dentro de las instalaciones del IDPAC y en horas laborales mantenimiento preventivo o correctivo de equipos que no son propiedad del Instituto.

- Solicitud de Mantenimiento

Para el mantenimiento correctivo, o solicitud de mantenimiento preventivo el usuario del equipo de cómputo, debe realizar solicitud al área de soporte técnico de Sistemas utilizando la Mesa de Ayuda.

La Secretaria General en cabeza de TI debe definir los acuerdos de niveles de servicio operativo que se deben cumplir para la atención y solución del requerimiento de los servicios de mantenimiento.

Seguridad de los equipos fuera de las instalaciones.

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

Mantener pólizas de seguros con una adecuada cobertura para proteger los recursos informáticos fuera de las instalaciones del Instituto.

En caso de pérdida o robo de un equipo portátil o cualquier medio que contenga información relacionada con el IDPAC, se debe realizar inmediatamente el respectivo reporte al área correspondiente y se deberá poner la denuncia ante la autoridad competente.

Retirada de materiales propiedad del IDPAC

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

Reutilización o eliminación segura de dispositivos de almacenamiento

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 sea eliminado o sobrescrito de forma segura antes de su reutilización o eliminación definitiva

8.7. ADMINISTRACION DEL RIESGO

El IDPAC implementa la administración del riesgo en sus etapas de contexto, información general, identificación, análisis, valoración de controles, manejo, monitoreo y seguimiento con base en los lineamientos establecidos en la Guía de Administración de Riesgo creada en el Instituto (IDPAC-PE-GU-01 Guía Para la Administración del Riesgo) y así evitar o mitigar riesgos mediante actividades de control para el cumplimiento de los objetivos del IDPAC.

De acuerdo a la Guía de Administración de Riesgo del IDPAC, la evaluación del riesgo se calcula con base en variables cuantitativas y cualitativas de acuerdo a la siguiente gráfica:

COLOR	ZONA DE RIESGO
B	Baja
M	Moderada
A	Alta
E	Extrema

8.8. SEGURIDAD DE LAS OPERACIONES

Objetivo: Asegurar operaciones correctas y seguras en el procesamiento de información.

La Secretaría General en cabeza del área de Tecnologías de la información es la encargada de la operación y administración de la plataforma tecnológica que apoya los procesos del IDPAC, asignará funciones 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.

8.8.1 RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIÓN

Documentación de Procedimientos de operación

Se 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.

Gestión de cambios

La Secretaría General en cabeza del área de Tecnologías de la información establecerá, coordinará y controlará los cambios realizados en los activos de información, asegurando que los cambios efectuados sobre la plataforma tecnológica, serán debidamente autorizados por las áreas correspondientes.

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 los mismos, ni de la información que soportan.

La Secretaría General en cabeza del área de Tecnologías de la información evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.

Se debe garantizar que todo cambio realizado sobre la plataforma tecnológica del IDPAC, quede formalmente documentado desde su solicitud hasta su implantación cumpliendo con el procedimiento correspondiente.

El IDPAC debe crear o tener un formato estandarizado de control de cambios y solicitudes de modificación de la plataforma tecnológica y de las solicitudes de digitalización de las soluciones.

Mientras se establece que el cambio está en producción de manera satisfactoria se debe mantener documentadas las actividades y el seguimiento que contenga toda la información relevante de cada cambio implementado.

Segregación de tareas

La asignación de tareas de operación y apoyo a la gestión estarán separadas del seguimiento y verificación de seguridad, a 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:

- Las funciones operativas y de soporte del proceso de Gestión de Tecnologías de la Información y las funciones 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 operativas o soporte en plataformas tecnológicas no tendrán a su cargo funciones de auditoría de seguridad de la información o de control interno.
- El interventor de un contrato no debe ser el mismo que autoriza el pago.

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

8.8.2 PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA.

Gestión de capacidades.

La Secretaría General en cabeza del área de Tecnologías de la información 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.

Aceptación del sistema.

La Secretaria General y el Responsable de Seguridad de la Información definirán los criterios de aprobación de los nuevos sistemas de información, actualizaciones y nuevas versiones.

8.8.3 PROTECCIÓN CONTRA EL CÓDIGO MALICIOSO Y DESCARGABLE.

Se implementa una plataforma de antivirus debidamente licenciada 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 al IDPAC, deben ser revisados y/o vacunados antes de su uso.

Todos los equipos de cómputo del IDPAC 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 del área de TI 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 del área de TI.

Los funcionarios, contratistas y/o terceros que tienen vínculo con el IDPAC no deben utilizar software obtenido externamente desde Internet o de una persona u organización diferente al área de TI del IDPAC, el incumplimiento de esta política acarreará 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 área de TI.

8.8.4 COPIAS DE SEGURIDAD.

Se establecen directrices y controles para 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.

El IDPAC cuenta con políticas de backup para asegurar la estabilidad e integridad de la información, con el fin de:

- Salvaguardar los activos de información
- Evitar la pérdida de datos en el caso de una eliminación accidental o corrupción de datos, error del sistema, o de desastre.
- Permitir la restauración oportuna de información y procesos del instituto, en caso fortuito y así garantizar su integridad y usabilidad en caso de ser requerido.

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

Es responsabilidad de los líderes de proceso y/o jefes de área identificar claramente la información crítica a su cargo, identificar los riesgos y generar el plan de continuidad en el cual debe estar incluida la solicitud de respaldo al administrador de copias de seguridad.

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.

El área de Tecnologías de la información 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.
- El área de TI, cuenta 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.

Todos los funcionarios, contratistas y terceros vinculados con el IDPAC son responsables de realizar los respaldos de información almacenada en los equipos asignados.

8.9. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTOS DE SISTEMAS DE INFORMACIÓN

Objetivo: Garantizar que la seguridad informática es una parte integral de los sistemas de información a través de su ciclo de vida.

Se establecen los procedimientos correspondientes para la adquisición de sistemas de información o aplicación de software y para el desarrollo o mantenimiento de software en el IDPAC. Para el caso del desarrollo del software subcontratado por el instituto, se implementan las supervisiones y metodologías correspondientes.

La Secretaría General en cabeza del área de Tecnologías de la información como encargada de los sistemas de información brinda la custodia y realiza copias de los archivos fuente de las aplicaciones que son propiedad del IDPAC.

Todos los desarrollos de software y las nuevas aplicaciones que se implementen en el IDPAC deben estar autorizados por el área de TI con el visto bueno de la Dirección General y/o la Secretaria General.

Los controles y directrices que brinden seguridad y protección al desarrollo y mantenimiento de software harán parte del subsistema de seguridad de la información.

8.9.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN.

Análisis y especificación de los requisitos de seguridad.

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.

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 del mismo 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.

8.9.2 TRATAMIENTO CORRECTO DE LAS APLICACIONES

Validación de los datos de entrada.

Se identifica cada uno de los flujos de entrada de datos y se verifica que el tipo de datos sea el esperado. Los controles y su tratamiento serán documentados.

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.

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

Validación de los datos de salida.

Se establecen mecanismos como casos de prueba, con el fin de verificar la salida esperada de datos en informes, reportes o consultas, por el proceso o los usuarios.

8.9.3 SEGURIDAD EN LA NUBE

El IDPAC como plataforma de servicios en la nube posee Azure con servidores en varios sistemas operativos, servidores de datos y servidores de archivos, se tiene una amplia gama de opciones de seguridad controladas por el IDPAC. 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.

8.9.4 CONTROLES CRIPTOGRÁFICOS.

Política de uso de los controles criptográficos.

Se utilizan controles criptográficos en los siguientes casos:

- Para los sitios web de uso externo, como por ejemplo página 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 del IDPAC
- 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.

8.9.5 SEGURIDAD DE LOS ARCHIVOS DE SISTEMA.

Control del software en producción.

Todo sistema de información y aplicaciones implementadas en el IDPAC tendrán un líder técnico responsable designado formalmente por la Secretaria General.

Los desarrolladores software encargados del desarrollo y mantenimiento de aplicaciones no podrán acceder a los ambientes de producción.

El IDPAC 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 áreas funcionales. 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.

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 idénticos procedimientos 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.

Control de acceso al código fuente de las aplicaciones de software.

La Secretaría General en cabeza del área TI define e implementará la herramienta para control del código fuente de las aplicaciones de software.

Se designa un responsable para la administración del código fuente de los programas, quién no debe cumplir con funciones de desarrollo, mantenimiento o implementación de aplicaciones.

El administrador del código fuente de los programas no debe realizar modificaciones sobre los programas fuentes bajo su custodia.

Se define o actualizará el procedimiento de gestión del código fuente hasta su despliegue en producción, para así evitar su alteración o modificación sin los accesos permitidos.

Se establece que todo programa objeto o ejecutable en producción tenga un único código fuente asociado que garantice su origen.

Se prohíbe el acceso a todo operador y/o usuario de aplicaciones a las herramientas que permitan la generación o gestión de los programas fuentes.

Los programas fuentes contarán con copias de respaldo periódicas, cumpliendo los requisitos de seguridad establecidos por el IDPAC.

8.9.6 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE.

Procedimientos de control de cambios.

Todo cambio deberá ejecutarse conforme al procedimiento de control de cambios que, establecido por el IDPAC, con el fin de minimizar los riesgos de alteración de los sistemas de información.

Se debe actualizar la documentación de usuario final o técnica para cada cambio implementado que implique modificaciones en la estructura de la base de datos, cambio de modelo operativo, adición de nueva funcionalidad, entre otros.

Cuando se cambien las plataformas de operación o sistemas operativos, las aplicaciones y sistemas de información deberán ser revisadas y probadas para asegurar que no hay impacto negativo en las operaciones del IDPAC o de la seguridad de la información.

Desarrollo tercerizado

La Secretaría General en cabeza del área TI 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, dada la proliferación del "outsourcing", es especialmente importante clarificar los derechos generados por proveedores en desarrollo de este tipo de contratos.

Pruebas de funcionalidad durante el desarrollo de los Sistemas

Las pruebas de la funcionalidad se deben llevar a cabo durante el desarrollo del sistema.

Pruebas de aceptación del sistema

Se debe cumplir con los formatos y el procedimiento del sistema de calidad para la realización y documentación de las pruebas.

Protección de los datos de prueba

Los datos de prueba deben seleccionarse cuidadosamente, en caso que éstos sean datos reales deben ser protegidos y controlados.

8.10. RELACIÓN CON LOS PROVEEDORES

Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores

8.10.1 SEGURIDAD DE LA INFORMACIÓN EN RELACIÓN CON LOS PROVEEDORES

Política de seguridad de la información para las relaciones con proveedores
Se acordará con el proveedor y se documentaran los requerimientos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de información del IDPAC.

De igual forma se debe incluir un acuerdo formal de Niveles de Servicios en Seguridad de la Información, en el que se detallen los compromisos en el cuidado de los activos de información del IDPAC y las sanciones en caso de incumplimiento. Cuando la supervisión sea contratada, se debe estipular esta obligación en los Contratos.

Tratamiento del riesgo dentro de acuerdos con proveedores
Todos los requerimientos de seguridad de la información pertinentes serán establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proporcionar los componentes de infraestructura de tecnología para la información del IDPAC.

Cadena de suministro en tecnologías de la información y comunicaciones
Incluir los requerimientos para los acuerdos con proveedores para abordar los riesgos de la seguridad de la información asociada con los servicios de las tecnologías de información y comunicación y de la cadena de suministro de productos.

8.10.2 GESTIÓN DE LA PRESTACIÓN DE SERVICIOS POR PROVEEDORES

Seguimiento y revisión de los servicios de proveedores
Cada servicio que un proveedor preste al IDPAC deberá tener con un supervisor encargado de revisar y auditar el proceso llevado a cabo para la ejecución del servicio prestado.

Gestión de cambios en los servicios prestados por proveedores
Los cambios en la prestación de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora de las actuales políticas de seguridad de información, procedimientos y controles, se gestionarán, teniendo en cuenta la criticidad de la información, sistemas y procesos que intervienen y reevaluación de los riesgos.

8.11. GESTIÓN DE INCIDENTES DE SEGURIDAD

Objetivo: Garantizar un enfoque coherente y eficaz para la gestión de incidentes en la seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades.

La priorización del tratamiento de los incidentes se realiza conforme a la criticidad de la Información.

Todo funcionario y contratista del IDPAC es responsable del reporte oportuno de debilidades e incidentes de seguridad que detecte o que sean de su conocimiento.

El Responsable de Seguridad de la Información tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados, así como su comunicación al Comité de Seguridad de la Información y a los propietarios de la información.

El Comité de Seguridad efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

El Responsable de Seguridad de la Información junto con la Secretaría General en cabeza del área TI son los responsables de establecer el proceso, procedimientos e instructivos para la Gestión de Incidentes de Seguridad de la Información

8.11.1 GESTIÓN DE INCIDENTES Y MEJORAS DE SEGURIDAD DE LA INFORMACIÓN

Notificación de eventos y puntos débiles de seguridad de la información.

Las incidencias pueden provenir de diversas fuentes tales como usuarios, gestión de aplicaciones, soporte técnico, entre otros. Toda persona del IDPAC deberá reportar de manera oportuna las debilidades e incidentes de seguridad que detecte o que sean de su conocimiento.

Responsabilidades y procedimientos.

La responsabilidad y el procedimiento de manejo para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información está en cabeza de la Secretaria General a través del área TI. El procedimiento debe contemplar el reporte, registro,

clasificación, diagnóstico, resolución y cierre del incidente, así como el monitoreo y seguimiento del incidente.

Aprendizaje de los incidentes de seguridad de la información.

La solución de un incidente se registrará en una base de conocimientos de errores conocidos, con el fin de que pueda ser consultada y sirva de apoyo oportuno cuando un incidente se presente de manera recurrente o de pistas de solución en incidentes similares. La recurrencia de un incidente deberá ser tratada como un problema. Así como para reducir la probabilidad o el impacto de los incidentes en el futuro.

Recopilación de evidencia

Se deberá registrar las pistas de auditoría y evidencias para análisis de problemas internos, uso como evidencia en relación con una probable violación contractual o infracción normativa, o en marco de un proceso judicial y negociación de compensaciones por parte de los proveedores de software y de servicios.

Respuesta a vulnerabilidades e Incidentes Relativos a la Seguridad

El IDPAC desarrollará un procedimiento formal de comunicaciones, que incluya el reporte, verificación, escalamiento, seguimiento, acciones de mejoras y cierre de vulnerabilidades, riesgos o incidente de seguridad que se detecten o sucedan.

Todo funcionario y contratista debe conocer el procedimiento de comunicación de incidentes de seguridad, y debe informar de los mismos tan pronto hayan tomado conocimiento de su ocurrencia.

Documentación de los Incidentes

El IDPAC deberá documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Identificará aquellos que sean recurrentes, con su respectivo de nivel de impacto. Esto será evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

8.12. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Objetivo: Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres y asegurar su recuperación oportuna.

Los directores, Jefes de área y el responsable de Seguridad de la Información deben identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades del IDPAC, evaluando los riesgos para determinar el impacto de dichas interrupciones, Identificar los controles preventivos y elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades.

Para los procesos críticos del IDPAC, se debe contar con instalaciones alternas y con capacidad de recuperación, que permitan mantener la continuidad del negocio aún en caso de desastre en las instalaciones de los lugares de operación. El plan de continuidad debe considerar los siguientes aspectos:

- Plan de contingencia. Se describen las acciones a tomar cuando ocurre un incidente que interrumpe las operaciones del negocio, proporcionando mecanismos alternos y temporales para continuar con el procesamiento.
- Plan de recuperación. Se describen las acciones a seguir para trasladar las actividades del negocio a un centro alterno de recuperación.
- Plan de retorno. Se describen las acciones a seguir para regresar las operaciones normales a las instalaciones originales.
- Programación de pruebas. Se describe la periodicidad en que el plan de continuidad debe ser probado.
- Actualización periódica. El plan debe actualizarse cuando cambios realizados en el ambiente operativo impacten su funcionalidad.
- Consideraciones de seguridad. Es importante que el plan sea diseñado para mantener los controles de seguridad establecidos por la Organización, aun cuando se opere en modalidad de contingencia. Es responsabilidad del responsable de la seguridad de la información asegurar que estas consideraciones sean efectivamente contempladas en el plan.

8.12.1 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

El IDPAC debe contar con un procedimiento de gestión de la continuidad del negocio, que contemple la implementación y actualización de planes de contingencia para garantizar que las operaciones del IDPAC puedan restablecerse dentro de plazos aceptables, ante la eventual ocurrencia de interrupciones de actividades

La Secretaría General en cabeza del área TI desarrollará un plan de contingencias informáticas y de comunicaciones, el cual debe estar ajustado a los estándares nacionales e internacionales.

Planificación de la continuidad de la seguridad de la información y Análisis de riesgos

Se debe realizar análisis de riesgos enfocado específicamente a valorar el impacto de incidentes que comprometen la continuidad del negocio, teniendo en cuenta que este impacto será mayor cuanto más dure el incidente. Igualmente se debe definir los pasos a seguir para realizar el análisis de riesgos.

Implantación de la continuidad de la seguridad de la información

Se debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.

Verificación, revisión y evaluación de la continuidad de la seguridad de la información

El Comité de Seguridad de Información establecerá y hará seguimiento al cronograma de pruebas periódicas de cada plan de contingencia, para minimizar el riesgo de fallas por cambios en la infraestructura, por errores o malas apreciaciones y definiciones

Redundancias

Las instalaciones para el procesamiento de información deben contar con la suficiente redundancia para satisfacer los requisitos de disponibilidad.

8.13. CUMPLIMIENTO

Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y de los requisitos de seguridad.

El Comité de Seguridad de la Información debe garantizar el cumplimiento de las directrices definidas en la presente Política de Seguridad de la Información.

Los directores y Jefes de área velarán por la correcta implementación y cumplimiento de la Política de Seguridad de la Información y los controles y directrices de seguridad que harán parte del Subsistema de Seguridad de la Información, dentro de la dependencia de su responsabilidad.

Las situaciones o acciones que violen la presente Política, controles y directrices deben ser detectadas, registradas, analizadas, resueltas y reportadas de manera inmediata a través de los canales señalados para el efecto.

8.13.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES.

Identificación de la legislación aplicable

En el numeral 4. Marco legal de la presente política, se encuentra relacionada la legislación aplicable a la seguridad de la información.

Derechos de propiedad intelectual

El IDPAC solo podrá autorizar para la realización de sus actividades el uso software licenciado, software desarrollado en el IDPAC o software declarado como de libre uso, así mismo, uso de material documental, el producido por el Instituto mismo o el producido por el titular cuando medie autorización de éste, en los términos y condiciones acordados y lo dispuesto en la normatividad vigente. Los funcionarios únicamente podrán utilizar material o software autorizado por el IDPAC.

Se debe establecer en los contratos de trabajo de empleados y en los contratos de realizados con proveedores y contratistas, cláusulas respecto a la propiedad intelectual respecto, al material y productos generados en el desarrollo de la misionalidad del instituto.

Protección de los documentos de la organización.

Los documentos críticos del IDPAC deben ser protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de conformidad con los requisitos de legalidad, reglamentarios, contractuales y comerciales. Para cada uno de ellos se debe detallar los períodos de retención y el tipo de medios de almacenamiento y se debe cumplir con los lineamientos y directrices fijadas por el IDPAC y por el Archivo General de la Nación.

Protección de datos y privacidad de la información de carácter personal

Los funcionarios y contratistas del IDPAC deben conocer las restricciones al tratamiento de los datos y de la información personal registrada en el Instituto, conforme a lo estipulado en la normatividad interna y en la Ley Estatutaria 1581 de 17 de octubre 2012, por la cual se dictan disposiciones para la protección de datos personales: "T*odas las personas tiene el derecho constitucional a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma".*

Prevención del uso indebido de recursos de tratamiento de la información

Los funcionarios y contratistas del IDPAC deben conocer y respetar el alcance preciso del uso adecuado de los recursos informáticos.

Regulación de los controles criptográficos

Los controles criptográficos serán utilizados en cumplimiento a todos los acuerdos pertinentes, la legislación y los reglamentos.

8.13.2 REVISIONES DE LA SEGURIDAD DE LA INFORMACIÓN

Revisión independiente de la seguridad de la información

El enfoque del IDPAC para la gestión de seguridad de la información y su aplicación (es decir, los objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) debe ser revisada de forma independiente a los de demás procesos del Instituto a intervalos planificados o cuando se produzcan cambios significativos.

Cumplimiento de las políticas y normas de seguridad

La Secretaría General en cabeza del área de Tecnologías de la información deberá comprobar periódicamente el cumplimiento de los procesos y procedimientos de la información relacionados con la seguridad de la información e informar el cumplimiento al Comité de Seguridad de la Información, quien tomará las medidas según sea el caso para la mejora continua.

Comprobación del cumplimiento

Los Activos de información deben ser revisados regularmente para cerciorarse que se da cumplimiento a las políticas y normas de seguridad de la información del IDPAC.

Las situaciones o acciones que quebranten la presente Política deben ser detectadas, registradas, analizadas, resueltas e informadas al comité de Seguridad de la Información y a las áreas responsables por su tratamiento de manera inmediata.

9. MIGRACIÓN IPV4 A IPV6.

Con el fin de dar cumplimiento debe atenderse lo dispuesto por el MinTIC en la Guía de Transición a IPv6, Circular No.0002 de 2011,"(https://www.mintic.gov.co/portal/604/articles-5932_documento.pdf)";la Resolución 2710 de 2017, las recomendaciones o mejores prácticas del IPv6 Fórum, del Internet Government Forum (IGF), de los RIRs, LACNIC, de los fabricantes de las tecnologías y las RFCs de la IETF, por este motivo el IDPAC requiere de una asesoría técnica especializada de acompañamiento y orientación para la transición de IPV4 a IPv6 de conformidad con lo dispuesto por el MINTIC aplicado a la infraestructura tecnológica del IDPAC.

El IDPAC debe Realizar un diagnóstico, plan de implementación y monitoreo del proceso de transición de IPv4 a IPv6 a fin de generar mecanismos de direccionamiento IP de acceso seguro y uso eficiente de las infraestructuras de información.

10. POLITICA GOBIERNO DIGITAL

Objetivo: Establecer lineamientos para el uso y aprovechamientos de las tecnologías de la información y las comunicaciones para generar un entorno de confianza digital del IDPAC ante la ciudadanía basados en innovación, competitividad, proactividad y seguridad de la información.

10.1. IMPLEMENTACION

La implementación de la política de Gobierno Digital en el IDPAC se desarrollará conforme a principios, elementos y estándares establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones que permitirán el logro de sus propósitos a partir del aprovechamiento de las TIC, como mejorar la relación con otras entidades públicas y fortalecer la relación con la ciudadanía en un entorno confiable y de calidad.

10.2. INSTITUCIONALIDAD

El representante legal del IDPAC es el responsable de coordinar, hacer seguimiento y verificación de la implementación de la Política 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 tendrá la responsabilidad de liderar la implementación de la Política de Gobierno Digital y las demás áreas del IDPAC serán corresponsables de la implementación de la Política de Gobierno Digital en los temas de su competencia.

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 áreas o dependencias son corresponsables en su implementación.

El Secretario General del IDPAC hará parte del Comité Institucional de Gestión y Desempeño y responderá directamente al representante legal.

10.3. PROPOSITOS

Los propósitos de la Política de Gobierno Digital en el IDPAC se obtendrán a partir del desarrollo de los componentes y los habilitadores transversales, estos propósitos son:

- Habilitar y mejorar la provisión de servicios digitales de confianza y calidad.

- Lograr procesos internos, seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información.
- Tomar decisiones basadas en datos a partir del aumento el uso y aprovechamiento de la información.
- Impulsar el desarrollo del IDPAC para la solución de retos y problemáticas sociales a través del aprovechamiento de las TIC.

10.4. SEGUIMIENTO Y EVALUACION

El seguimiento y evaluación de esta política se adelantará a través de indicadores de cumplimiento e indicadores de resultado definidos por el IDPAC y con mediciones internas para realizar seguimiento al uso y aprovechamiento de las TIC tanto en su gestión interna como en la entrega de servicios digitales a usuarios, ciudadanos y grupos de interés. Estas mediciones deben estar orientadas a establecer aspectos como: ahorro en términos de tiempos y recursos, disminución de costos, nivel de satisfacción de usuarios internos y externos, tasas de uso de procesos, trámites y servicios digitales vs. Presenciales

Se debe hacer el reporte oficial de la implementación de la política de Gobierno Digital a través del Formulario Único de Reporte de Avance en la Gestión - FURAG, en los tiempos determinados por el DAFP

10.5. ZONAS DE ACCESO PÚBLICO A INTERNET INALÁMBRICO PARA EL FORTALECIMIENTO DEL MODELO DE GOBIERNO DIGITAL

Objetivo: fortalecer el modelo de Gobierno Digital del IDPAC, a través de la regulación de zonas de acceso público y gratuito a Internet inalámbrico, en las instalaciones del Instituto.

10.5.1 IMPLEMENTACION

El Instituto Distrital de la Participación y Acción Comunal - IDPAC implementará zonas de acceso público y gratuito a Internet inalámbrico, en los espacios dispuestos para atención al público en sus instalaciones, con las condiciones técnicas, operativas y de seguridad que así lo permitan, cumpliendo con los requisitos técnicos establecidos por el MINTIC para este fin.

10.5.2 CONEXIÓN AL SERVICIO DE ACCESO A INTERNET

La conexión al servicio de acceso a Internet inalámbrico deberá estar disponible, como mínimo, durante los horarios de atención al público previstos por el IDPAC
En caso de que la conexión deba suspenderse, se indicará a los usuarios, señalando igualmente la fecha y hora a partir de la cual se reanudará la conexión.

10.5.3 SEÑALIZACIÓN

Las zonas de acceso público a Internet inalámbrico del IDPAC deberán contar con una adecuada señalización incluyente que tenga en cuenta las capacidades físicas y cognitivas de los usuarios, de manera que debe permitir y facilitar tanto la ubicación del punto, como las instrucciones para la conexión al servicio, de forma visual y táctil.

Sin perjuicio de lo anterior, la red para el acceso a Internet de que trata el presente capítulo deberá denominarse "Zona Wifi GRATIS para la gente"

10.6. LINEAMIENTOS GENERALES EN EL USO Y OPERACIÓN DE LOS SERVICIOS CIUDADANOS DIGITALES

Objetivo: establecer los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

10.6.1 DISPOSICIONES GENERALES

La prestación de los servicios ciudadanos digitales en el IDPAC se orientará por los principios: accesibilidad inclusiva, escalabilidad, gratuidad, libre elección y portabilidad, privacidad por diseño y por defecto, usabilidad, seguridad y circulación restringida de la información.

10.6.2 CARACTERÍSTICAS DE LOS SERVICIOS CIUDADANOS DIGITALES

Los servicios ciudadanos digitales que presta el IDPAC se caracteriza por brindar las capacidades necesarias para garantizar el adecuado flujo de información e interacción entre los sistemas de información con otras entidades, permitiendo el intercambio, la integración y la compartición de la información, con el propósito de facilitar el ejercicio de sus funciones constitucionales y legales, acorde con los lineamientos del marco de interoperabilidad,

utilizando mecanismos de autenticación y permitiendo la verificación de atributos digitales de una persona en el momento de adelantar trámites y servicios a través de medios digitales en las plataformas del IDPAC.

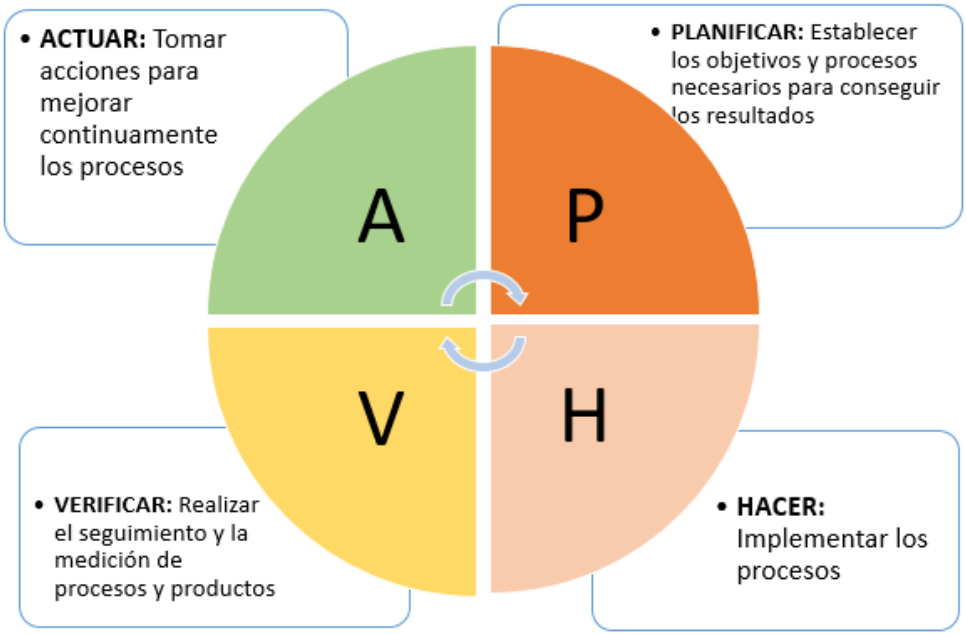
11. PLAN DE CAPACITACIÓN Y SENSIBILIZACIÓN

El recurso humano del IDPAC es necesario sensibilizarlo o capacitarlo sobre la importancia de la preservación de la disponibilidad, integridad y confidencialidad de la información de acuerdo a los siguientes criterios:

- Establecer la metodología que les permita evidenciar cuales son las necesidades de capacitación para la entidad.
- Incluirlo en el Plan institucional de capacitación de la entidad 2020-2023 IDPAC GTH-OT-01, dando alcance al numeral (d) de su eje temático Transformación digital: Este eje temático está relacionado con la forma en cómo las entidades reorganizan sus estrategias y métodos de trabajo con el fin de obtener mayores beneficios por medio de la digitalización de sistemas, procesos y la implementación de las tecnologías de la información y la comunicación.
- Construir materiales para sensibilización y entrenamiento.
- Evaluar, medir y cuantificar, si el programa implementado genera impacto en el desarrollo de las actividades de la Entidad.

El programa debe contar con el apoyo y los recursos necesarios por parte de la Alta Dirección para su ejecución, implementación y definición de técnicas que permitan su difusión y comunicación.

12. MEJORA CONTINUA.



El ciclo de mejoramiento continuo PHVA (Planear, hacer, actuar y verificar), le asegura al IDPAC que el modelo de seguridad y privacidad de la información esté expuesto a revisiones continuas cuando existan cambios importantes o para mejorar su efectividad dependiendo de las mediciones realizadas en su ciclo de vida. Se cuenta, entonces, con un ciclo que permite establecer, implementar, operar, supervisar, revisar, mantener y mejorar el MSPI.

La aplicación de esta fase, le permitirá al IDPAC a partir de los resultados obtenidos en la Gestión, corregir de ser necesario, los errores cometidos, así como mejorar las acciones realizadas en los diferentes procesos, llevando a cabo el plan de mejoramiento continuo de seguridad y privacidad de la información.

12.1. NO CONFORMIDADES Y ACCIONES CORRECTIVAS

- En caso de presentarse no conformidades en las auditorías realizadas, el IDPAC debe llevar a cabo las acciones necesarias para controlarlas y corregirlas y se deben incluir como acciones a la cuales se les haga el seguimiento correspondiente en el plan de mejoramiento institucional, con el propósito de evaluar la eficacia en el cumplimiento

de las actividades formuladas en este proceso y coordinar con la oficina de Control Interno dicho seguimiento llevando a cabo la verificación de las acciones para que sean incluidas en el informe definitivo presentado por la Oficina de control Interno.

- Evaluar y revisar la razón de la no conformidad, con el fin de eliminar las causas de las mismas y evitar que se vuelvan a presentar estas no conformidades. Es importante, que se verifique si existen no conformidades similares en auditorías previas.
- Comparar las no conformidades presentadas con las acciones correctivas tomadas; esto, con el fin de asegurar que no se vuelvan a presentar y evaluar la efectividad de las acciones correctivas aplicadas.
- Implementar las acciones que sean necesarias.
- Evaluar la efectividad de las acciones correctivas tomadas.
- Realizar los cambios en el sistema que sean necesarios.

El IDPAC documenta de la siguiente manera de acuerdo a las auditorías externas e internas que se realicen al proceso de Gestión de Tecnologías donde se deben incluir las revisiones y los seguimientos a la política de seguridad y privacidad de la información.

- Evidencia de las no conformidades y acciones correctivas llevadas a cabo.
- Resultados de las acciones correctivas ejecutadas.
- Revisiones periódicas de la efectividad de las acciones correctivas y del plan de mejoramiento.