
 ALCALDÍA MAYOR DE BOGOTÁ D.C. BOGOTÁ Municipio Mayor del Departamento de Cundinamarca Bogotá, Colombia	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ INSTITUTO MUNICIPAL DE PROTECCIÓN Y BIENESTAR ANIMAL
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

CONTROL DE CAMBIOS

No. DE ACTA DE APROBACIÓN	FECHA	VERSIÓN	DESCRIPCIÓN
03	25/01/2021	1.0	Adopción de la política
22	28 NOV 2023	2.0	<p>Se modifica el nombre del documento.</p> <p>Se consolidan y agrupan las políticas y lineamientos de seguridad de la información:</p> <p>Se actualiza la política general PA04-PL01 Política seguridad y privacidad de la información, se incluyen y se consolidan en el documento:</p> <p>PA04-PL03 Políticas gestión de seguridad de la Información PA04-PL08 política de bloqueo de sesión, escritorio y pantalla limpia. PA04-PL07 política de protección contra software malicioso PA04-PL06 política de administración de contraseñas</p> <p>Complementariamente se actualizan los lineamientos:</p> <ol style="list-style-type: none"> 1. Premisas de operación, 2. Se amplió los términos y definiciones, 3. Se incluyó las obligaciones generales, 4. se creó el capítulo "políticas específicas de seguridad de la información" en el cual se incluyeron y modificaron las políticas; política específica de seguridad física, política de antivirus que reemplaza la política de protección contra software malicioso ,política de uso de correo electrónico corporativo, política de uso de contraseñas, política específica para dispositivos móviles, política de uso de servicios de red, política específica de teletrabajo, política específica de uso de medios tecnológicos de comunicación y acceso a internet, política específica de uso de controles criptográficos, política específica de desarrollo software seguro, política específica para relaciones con proveedores, política

 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>ALMAYOR</small> <small>Sistema de Planeación de Producción y Bienestar Animal</small>	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ	 <small>INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL</small>	
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA				
	Código: PA04-PL01	Versión: 2.0			

			<p>específica de derechos de uso de propiedad intelectual, política de uso de red privada virtual (VPN), política de control de cambios</p> <p>Alineados con los requisitos de la norma ISO 27001 versión 2013 y Modelo de Seguridad y Privacidad de la Información del MinTIC.</p>
--	--	--	---

AUTORIZACIONES

ELABORÓ:	REVISÓ	APROBÓ
ÁREA TÉCNICA	OFICINA ASESORA DE PLANEACIÓN	LIDER DEL PROCESO
Nombre: Julio César Benavides Carranza José Alfonso Pérez Contreras	Nombre: Sara Sofía Lancheros Ramírez	Nombre: Clara Inés Parra Rojas
Firma: 	Firma: 	Firma: 
Cargo: Contratistas Subdirección de Gestión Corporativa -Gestión Tecnológica	Cargo: Profesional especializada Oficina Asesora de Planeación	Cargo: Subdirectora de Gestión Corporativa




	PROCESO GESTIÓN TECNOLÓGICA		
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

TABLA DE CONTENIDO

INTRODUCCIÓN.....	7
OBJETIVO DE SEGURIDAD DE LA INFORMACIÓN.....	8
PREMISAS DE OPERACIÓN.....	8
No repudio.....	8
Privacidad y Confidencialidad.....	9
Integridad.....	9
Disponibilidad del Servicio e Información.....	10
Registro y Auditoría.....	10
Gestión de Incidentes de Seguridad de la Información.....	11
Capacitación y Sensibilización en Seguridad de la Información.....	11
1. TERMINOS O DEFINICIONES.....	12
2. DESARROLLO.....	15
2.1. PRINCIPIOS DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....	15
2.2..... POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	16
OBJETIVO.....	16
ALCANCE.....	16
POLÍTICA.....	16
2.3..... ORGANIZACIÓN DE LA SEGURIDAD	17
2.3.1. Roles y Responsabilidades.....	17
2.3.2. Contacto con autoridades y grupos de Interés.....	19
2.4..... OBLIGACIONES GENERALES	19
2.5..... POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN	20
2.5.1. POLÍTICA ESPECIFICA PARA CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN.....	20
OBJETIVO.....	20
ALCANCE.....	20
POLÍTICA.....	21
RESPONSABILIDADES.....	21
2.5.2. POLÍTICA ESPECÍFICA DE SEGURIDAD FÍSICA.....	21
OBJETIVO.....	21
ALCANCE.....	21
POLÍTICA.....	22
RESPONSABILIDADES.....	23
2.5.3. POLÍTICA DE ANTIVIRUS.....	24

 ALCALDIA MAYOR DE BOGOTÁ D.C. <small>ASAMBLEA</small> <small>INSTRUMENTO DE PROTECCIÓN Y BIENESTAR ANIMAL</small>	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ <small>INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL</small>
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	



OBJETIVO.....	24
ALCANCE.....	24
POLÍTICA.....	24
RESPONSABILIDADES.....	25
2.5.4. POLÍTICA DE USO DE CORREO ELECTRÓNICO CORPORATIVO.....	25
OBJETIVO.....	25
ALCANCE.....	25
POLÍTICA.....	25
RESPONSABILIDADES.....	26
2.5.5. POLÍTICA DE USO DE CONTRASEÑAS.....	27
OBJETIVO.....	27
ALCANCE.....	27
POLÍTICA.....	27
RESPONSABILIDADES.....	28
2.5.6. POLÍTICA ESPECIFICA PARA DISPOSITIVOS MÓVILES.....	28
OBJETIVO.....	28
ALCANCE.....	28
POLÍTICA.....	28
RESPONSABILIDADES.....	29
2.5.7. POLÍTICA DE USO DE SERVICIOS DE RED.....	30
OBJETIVO.....	30
ALCANCE.....	30
POLÍTICA.....	30
RESPONSABILIDADES.....	30
2.5.8. POLÍTICA ESPECÍFICA DE TELETRABAJO.....	31
OBJETIVO.....	31
ALCANCE.....	31
POLÍTICA.....	31
RESPONSABILIDADES.....	31
2.5.9. POLÍTICA ESPECIFICA DE USO DE MEDIOS TECNOLÓGICOS DE COMUNICACIÓN Y ACCESO A INTERNET.....	32
OBJETIVO.....	32
ALCANCE.....	32
POLÍTICA.....	32
RESPONSABILIDADES.....	33

	PROCESO GESTIÓN TECNOLÓGICA		 
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

2.5.10.	POLÍTICA ESPECÍFICA DE CONTROL DE ACCESO A LA INFORMACIÓN	34
	OBJETIVO	34
	ALCANCE	34
	POLÍTICA	34
	RESPONSABILIDADES	34
2.5.11.	POLÍTICA ESPECÍFICA DE USO DE CONTROLES CRIPTOGRÁFICOS	35
	OBJETIVO	35
	ALCANCE	35
	POLÍTICA	36
	RESPONSABILIDADES	36
2.5.12.	POLÍTICA ESPECÍFICA DE ESCRITORIO Y PANTALLA LIMPIOS	36
	OBJETIVOS	36
	ALCANCE	37
	POLÍTICA	37
	RESPONSABILIDADES	37
2.5.13.	POLÍTICA ESPECÍFICA DE COPIAS DE RESPALDO DE INFORMACIÓN	38
	OBJETIVO	38
	ALCANCE	38
	POLÍTICA	38
	RESPONSABILIDADES	39
2.5.14.	POLÍTICA ESPECÍFICA DE TRANSFERENCIA O INTERCAMBIO DE INFORMACIÓN	
	39	
	OBJETIVO	39
	ALCANCE	40
	POLÍTICA	40
	RESPONSABILIDADES	40
2.5.15.	POLÍTICA ESPECÍFICA DE DESARROLLO SOFTWARE SEGURO	41
	OBJETIVO	41
	ALCANCE	41
	POLÍTICA	42
	RESPONSABILIDADES	42
2.5.16.	POLÍTICA ESPECÍFICA PARA RELACIONES CON PROVEEDORES	44
	OBJETIVO	44
	ALCANCE	44
	POLÍTICA	44

 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>UNIVERSIDAD</small> <small>INSTITUTO DE PROTECCIÓN Y BIENESTAR ANIMAL</small>	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

RESPONSABILIDADES	44
2.5.17. POLÍTICA ESPECÍFICA DE DERECHOS DE USO DE PROPIEDAD INTELECTUAL .	45
OBJETIVO	45
ALCANCE	46
POLÍTICA	46
RESPONSABILIDADES	46
2.5.18. POLÍTICA ESPECÍFICA PARA CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN ..	47
OBJETIVO	47
ALCANCE	48
POLÍTICA	48
RESPONSABILIDADES	48
2.5.19. POLÍTICA DE USO DE RED PRIVADA VIRTUAL (VPN)	49
OBJETIVO	49
ALCANCE	49
POLÍTICA	49
RESPONSABILIDADES	49
2.5.20. POLÍTICA DE CONTROL DE CAMBIOS	49
OBJETIVO	49
ALCANCE	50
POLÍTICA	50
RESPONSABILIDADES	50

	PROCESO GESTIÓN TECNOLÓGICA		
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

INTRODUCCIÓN

De conformidad con lo establecido en el decreto único reglamentario 1078 de 2015, con el decreto 1008 de 2018 de la política de Gobierno Digital, emitidos por el Ministerio de las TIC, con el documento CONPES 3995 de 2020 en donde se establece la política “NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL”, la cual se articula con las políticas institucionales establecidas bajo el marco del decreto 1449 de 2017 cuyo objeto es el Modelo Integrado de Planeación y Gestión, se han adoptado mejores prácticas y se ha establecido un Subsistema de Gestión de Seguridad de la Información (SGSI) articulado con el Modelo de Seguridad y Privacidad de la Información -MSPi como lo establece el Ministerio de las Tecnologías y las Comunicaciones -MinTIC, el cual está conformado por políticas, estándares y lineamientos (técnicos y generales para seguridad de la información), procesos y procedimientos, estructura organizacional y mecanismos de verificación y control; y tiene como propósito garantizar la identificación y clasificación de los activos de información, para identificación de los riesgos de seguridad de la información los cuales tratados y gestionados según su criticidad de forma adecuada.

El Instituto Distrital de Protección y Bienestar Animal IDPYBA, aplicando el modelo de seguridad y privacidad de la información, definen las **POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IDPYBA**, las cuales serán monitoreadas y evaluadas periódicamente con el fin de validar su implementación y requerimiento de modificaciones para el cumplimiento de los objetivos de seguridad, conforme con los requerimientos normativos descritos en la Estrategia de Gobierno específicamente en el Modelo de Seguridad y Privacidad de la información del MinTIC, las normas técnicas: NTC/IEC-ISO 27001:2013 y NTC/IEC-ISO 27001:2022 y mejores prácticas GTC/IEC-ISO 27002, así como en la normatividad colombiana.

El valor de la información va más allá de palabras escritas, números e imágenes, incluido el conocimiento, los conceptos, las ideas y las marcas son ejemplos de formas de información intangibles. En un mundo como el actual que se encuentra interconectado y donde la información, los sistemas, las redes y el personal involucrado se consideran como otro activo importante para cualquier organización, es importante definir lineamientos que permitan y faciliten su protección y prevención contra diversos peligros que puedan afectar la información vista en todas sus representaciones.

Estos activos pueden ser objetos de amenazas deliberadas o accidentales, ocasionadas por ciberdelincuentes, cambios en los procesos, nuevas leyes y reglamentaciones, lo que nos permite hablar de vulnerabilidades inherentes a procesos, sistemas, redes y personas. Por lo que la presencia de riesgos que afecten la información y su seguridad requieren del compromiso entero de la entidad que permitan prevenir y reducir la materialización de estos riesgos.

En consideración a lo expuesto, a continuación, se establecen las Políticas de operación para seguridad y privacidad de la información, establecidas en el marco legal, las cuales se instauran por medio de la definición de procesos, procedimientos, metodologías, herramientas y documentos internos. En el marco de las presentes Políticas de seguridad y privacidad de la información idpyba se define la Política general de Seguridad y Privacidad de la información, la cual ampara las políticas específicas que apoyan en su cumplimiento, directrices que son de obligatorio cumplimiento para todas las áreas, procesos y personal indistinto del tipo de vinculación, para toda la entidad.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. AMBIENTE INALIENABLES INSEPARABLES INDELEGABLES	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

OBJETIVO DE SEGURIDAD DE LA INFORMACIÓN

- Fortalecer la seguridad de la información, garantizando la confianza de los ciudadanos, servidores públicos y terceros partes por medio del seguimiento, actualización, divulgación y el cumplimiento de las políticas, procedimientos e instructivos definidos dentro del Instituto Distrital de Protección y Bienestar Animal – IDPYBA.
- Realizar una adecuada gestión de riesgos de seguridad de la información con el fin de preservar los niveles de confidencialidad, integridad y disponibilidad de los activos de información del Instituto Distrital de Protección y Bienestar Animal - IDPYBA, los cuales se encuentran definidos en la matriz de inventario de activos de información.
- Fortalecer la cultura de seguridad de la información, por medio de la inclusión de buenas prácticas y conciencia en los servidores públicos y terceros en lo concerniente a la seguridad de la información en el Instituto Distrital de Protección y Bienestar Animal - IDPYBA.
- Favorecer con la continuidad del negocio del Instituto Distrital de Protección y Bienestar Animal - IDPYBA, mediante la ejecución de planes y controles asociados a la seguridad de la información que brinden los niveles de riesgos tolerables para la entidad, a través de una adecuada gestión de incidentes de seguridad de la información.

PREMISAS DE OPERACIÓN

Son los lineamientos que deben ser contemplados en la aplicación de las políticas de seguridad de la información o Seguridad Digital, que deben ser acogidos por funcionarios, contratistas y terceras partes, que intervengan para uso y gestión de los activos de información del Instituto Distrital de Protección y Bienestar Animal -IDPYBA, los cuales se describen a continuación:

No repudio

El Instituto Distrital de Protección y Bienestar Animal -IDPYBA a través del proceso de gestión tecnológica se reserva el derecho de auditar las redes y sistemas de información periódicamente para asegurar el cumplimiento de la Política de Seguridad y Privacidad de la Información.

El uso de los sistemas de información del Instituto Distrital de Protección y Bienestar Animal -IDPYBA debe ser monitoreado con el objetivo de identificar algún intento de intrusión. El monitoreo debe contemplar como mínimo los siguientes puntos:

- Intentos fallidos recurrentes para tener accesos a los sistemas.
- Intentos deliberados para evadir los controles de seguridad establecidos.
- Altas y bajas de usuarios en sistemas sin una solicitud aprobada correctamente.
- Modificaciones en los privilegios de usuarios sin una solicitud aprobada correctamente.

Para tener control, los registros de auditoría deben ser respaldados de forma periódica y se debe proporcionar un reporte periódico mensual de los incidentes de seguridad identificados.

	PROCESO GESTIÓN TECNOLÓGICA		
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

Privacidad y Confidencialidad

El Instituto Distrital de Protección y Bienestar Animal, aplicará la política de Tratamiento y Protección de Datos Personales para toda la información que contenga datos personales los cuales deben ser identificados a través del inventario de Bases de datos personales.

Todo funcionario, contratista, colaborador, pasante y/o tercero que ingrese a la Entidad, debe leer y firmar el compromiso de Acuerdo de Confidencialidad, en el caso que maneje o tenga acceso a la información pública clasificada y/o reservada y tratamiento de datos personales.

Integridad

Todos los sistemas de información del Instituto Distrital de Protección y Bienestar Animal -IDPYBA deben:

- Identificar e informar las fallas para que el encargado de la administración del sistema de información pueda corregir las fallas y evitar afectación en la información.
- Si el sistema operativo donde se aloja el aplicativo requiere actualizaciones, se deben realizar pruebas antes de proceder a la actualización, para evitar fallas en la ejecución de los sistemas de información o aplicativos de la entidad.
- En el proceso de gestión de cambios es necesario incluir las correcciones que se requieran.

Frente a la protección contra código malicioso, todos los sistemas del Instituto Distrital de Protección y Bienestar Animal deben:

- Emplear mecanismos de protección de código malicioso en las estaciones de trabajo, servidores o dispositivos de computación móvil para detectar y erradicar el código malicioso.
- Actualizar los mecanismos de protección de códigos maliciosos (incluidas las definiciones de firmas)
- Configurar mecanismos de protección de código malicioso (por ejemplo, análisis en tiempo real, análisis periódicos, detección de códigos maliciosos) para proteger los sistemas y activos de información de la empresa.

Respecto al monitoreo del Sistema de Información: Todos los sistemas del Instituto Distrital de Protección y Bienestar Animal deben:

- Identificar el uso no autorizado de los activos de información.
- Aumentar el nivel de actividad de monitoreo de activos de información siempre que exista una indicación de un mayor riesgo para los activos de la Entidad, basados en información del CSIRT, u otras fuentes creíbles de información.

Asegurarse que los usuarios de terceros, que requieren información del Instituto Distrital de Protección y Bienestar Animal -IDPYBA que contengan información clasificada o reservada, hayan firmado un acuerdo de confidencialidad de la información o en el caso de contratistas, que el acuerdo este incluido como parte del contrato firmado con El Instituto Distrital de Protección y Bienestar Animal. El acuerdo de confidencialidad debe firmarse antes de intercambiar cualquier tipo

 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>ASISTENTE Oficina General de Planeación y Desarrollo Urbano</small>	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ <small>INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL</small>
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

de información clasificada o reservada y se determinará su vigencia, acorde con el tipo de información que se maneje (incluso después de terminado el vínculo contractual o laboral con la Entidad).

Para los casos en que el Instituto Distrital de Protección y Bienestar Animal, lleve a cabo intercambio de información con otras entidades deben existir procedimientos para garantizar la confidencialidad, integridad y disponibilidad de la información a intercambiar a través de cualquier tipo o infraestructura de comunicaciones, con base en la clasificación de la información, las políticas de seguridad y procedimientos del Instituto Distrital de Protección y Bienestar Animal -IDPYBA.

Disponibilidad del Servicio e Información

Se debe crear y mantener un seguimiento al entorno de disponibilidad de los servicios y los componentes de la infraestructura para garantizar que los requerimientos de disponibilidad futuros puedan ser cubiertos.

El Comité Institucional de Gestión y Desempeño debe definir una estrategia para la continuidad del negocio, así como desarrollar, documentar, probar y mantener el Plan de Continuidad, que conduzca a la restauración de los procesos críticos del negocio y así dar continuidad en el servicio a las partes interesadas.

Dentro del proceso de desarrollo del plan de continuidad se debe hacer énfasis en mantener niveles de seguridad de información acordes con el resultado del análisis de riesgo y su clasificación, dentro de los procesos alternos utilizados antes, durante y después de la contingencia. Los documentos e información necesaria para llevar a cabo el proceso de continuidad del negocio deben ser clasificados como información "confidencial".

La información debe ser copiada y resguardada en un lugar fuera de las instalaciones del Instituto Distrital de Protección y Bienestar Animal.

Registro y Auditoría

Todos los sistemas y/o aplicativos deben generar logs o trazas de auditoría, para los desarrollos de los Sistemas de Información que se generen a partir de la divulgación de esta política, se debe establecer este punto como obligación contractual.

Todos los logs del sistema y de las aplicaciones deben mantenerse en forma segura, de tal forma que evite el acceso no autorizado a esta información y deberán analizarse para determinar si existen intentos de vulneración del sistema.

Las siguientes actividades deberán ser registradas en el momento que sean desarrolladas por un sistema:

- Crear, leer, actualizar o eliminar información.
- Iniciar una conexión de red.
- Aceptar una conexión de red.
- Autenticación y autorización de los usuarios y desconexión de estos.

	PROCESO GESTIÓN TECNOLÓGICA		
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

- Conceder, modificar o revocar derechos de acceso, incluyendo la adición de un nuevo usuario o grupo, cambio en los niveles de privilegios de usuario, cambio de permisos de archivos, cambio de permisos de objetos de base de datos, cambio de reglas en el Firewall y cambios de contraseñas de usuario.

Cambios en la configuración de sistemas, redes o servicios, incluida la instalación de software, parches y actualizaciones, u otros cambios de software instalados. Todos los registros deberán contener los siguientes elementos de forma directa o indirecta:

- Tipo de acción: autorizar, crear, leer, actualizar, eliminar y aceptar.
- Subsistema que realiza la acción.
- Identificadores para el sujeto que solicita la acción.
- Identificadores para el objeto sobre el que se realizó la acción.
- Fecha y hora en que se realizó la acción, incluida la información pertinente sobre la zona horaria.
- Si la acción fue permitida o denegada por mecanismos de control de acceso: Descripción y/o razón de los códigos que indican que la acción fue denegada por el control de acceso, si aplica.


Gestión de Incidentes de Seguridad de la Información

El Instituto Distrital de Protección y Bienestar Animal -IDPYBA cuenta con un procedimiento Incidentes de Seguridad en el que se puede reportar, registrar y dar tratamiento de los incidentes de seguridad de la información.

- Los usuarios deben asegurar que los archivos adjuntos de los correos electrónicos descargados de Internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras.
- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar al Equipo de trabajo de Gestión Tecnológica para que se tomen las medidas correspondientes.
- Equipo de trabajo de Gestión Tecnológica, debe generar y ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades detectadas en la plataforma tecnológica de la entidad.

Capacitación y Sensibilización en Seguridad de la Información

Todos los servidores públicos, contratistas, colaboradores y terceros deben recibir la inducción para tomar conciencia de la Seguridad de la Información y sus responsabilidades. Así como también debe participar en todas las actividades establecidas en el plan de capacitación, sensibilización y comunicación teniendo en cuenta que esto permite fortalecer la cultura de seguridad de la información y disminuir los posibles incidentes de seguridad de la información.



 ALCALDÍA MAYOR DE BOGOTÁ D.C. AMBIENTE Instituto Especial de Protección y Bienestar Animal	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

1. TERMINOS O DEFINICIONES

TERMINO	DEFINICIÓN
ACTIVO	En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.
ACTIVO DE INFORMACIÓN	Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Entidad y, en consecuencia, debe ser protegido.
AMENAZA	causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.
AMENAZA INFORMÁTICA	Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la entidad política del Estado. (Ministerio de Defensa de Colombia).
ANÁLISIS DE RIESGOS	Proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo. " http://www.iso27000.es/glosario.html "
ANONIMIZACIÓN	Método por el cual se pretende mitigar los riesgos que se pueden presentar al momento de compartir un activo de información que contenga datos sensibles o confidenciales permitiendo la divulgación de la información pública contenida y la protección de la información sensible o confidencial.
ÁREA SEGURA	Son lugares donde se encuentra localizada la información crítica para la organización, éstas estarán protegidas por un perímetro de seguridad y por los controles de acceso pertinentes.
AUTENTICIDAD	Es la condición de poder identificar que el generador o receptor (interlocutor) de la información es realmente quien dice ser.
AUTENTICACIÓN	provisión de una garantía de que una característica afirmada por una entidad es correcta.
AUTORIZACIÓN	Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.
AVISO DE PRIVACIDAD	Comunicación, verbal o escrita, en la que el responsable del Tratamiento de la información le informa al Titular de los datos personales la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma en que podrá acceder a estas y las finalidades del Tratamiento que se pretende dar a los datos personales que suministre.
BASE DE DATOS	Conjunto organizado de datos personales que serán objeto de Tratamiento.
BASE DE DATOS PERSONAL O DOMÉSTICA	Conjunto de datos personales que serán objeto de Tratamiento dentro del marco de la vida privada o familiar de las personas naturales
BUEN USO	Se entiende por "buen uso" respecto al cuidado que su personal debe tener con los activos que la organización les entregue para el desempeño de sus funciones. Confidencialidad: es asegurar que la información es accesible sólo para las personas autorizadas para ello.
CAUSAHABIENTE	Persona que es sucesora o heredera del Titular de la información a causa del fallecimiento de este.
CIBERSEGURIDAD	capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.
CONFIDENCIALIDAD	Principio básico que impide la divulgación de información a personas o sistemas no autorizados
CONTROL	es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.
CUSTODIO DE ACTIVO DE INFORMACIÓN	Personal asignado a un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de administrar y hacer efectivo los controles que el propietario del activo haya definido, con base en los controles de seguridad disponibles en la entidad.
DECLARACIÓN DE APLICABILIDAD	Documento que describe los objetivos de control y los controles pertinentes y aplicables para el SGSI de la organización.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p>	PROCESO GESTIÓN TECNOLÓGICA		 <p>BOGOTÁ INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL</p>
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

DERECHOS DE AUTOR	El derecho de autor es la rama de la propiedad intelectual que reconoce, en cabeza de los autores, ciertas prerrogativas morales y patrimoniales sobre sus obras artísticas y literarias que sean originales, y susceptibles de ser divulgadas o reproducidas por cualquier medio. Esta aplica para el desarrollo de software y derecho de uso de licenciamiento según su tipo. "https://propiedadintelectual.unaf.edu.co/acerca-de/derechos-de-autor/"
DISPONIBILIDAD	Principio básico que permite encontrar la información a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones autorizados que tengan acceso a la información y los activos asociados cuando estos sean requeridos.
DISPOSITIVO MÓVIL	Es un dispositivo electrónico portable con capacidades de procesamiento, conexión a Internet, y memoria, diseñado específicamente para acceder a información, administrarla y almacenarla, por ejemplo, un computador portátil de mano, Tablet, celulares de última generación entre otros.
EVENTO DE SEGURIDAD DE LA INFORMACIÓN	ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
GESTIÓN DE RIESGOS	Actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.
IMPACTO	el coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.
INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN	Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
INFORMACIÓN	La información está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.
INFORMACIÓN PÚBLICA	Toda aquella información no catalogada como secreta o reservada, de acuerdo con los establecido en la ley 1581 de 2012.
INFORMACIÓN CONFIDENCIAL RESERVADA (CONOCIMIENTO RESERVADO)	son aquellos documentos cuyo conocimiento está circunscrito al ámbito de la respectiva unidad del órgano a que sean remitidos, en virtud cuando la naturaleza misma de la información requiera ser tratada de manera reservada, de acuerdo con los establecido en la ley 1581 de 2012.
INFORMACIÓN PRIVADA	(solamente a quien le atañe la información debe conocerlo): son aquellos documentos cuyo conocimiento está circunscrito a las autoridades o personas a las que vayan dirigidos y a quienes deban intervenir en su estudio y resolución, de acuerdo con los establecido en la ley 1581 de 2012.
INTEGRIDAD	Principio básico que busca mantener los datos libres de modificaciones no autorizadas.
INVENTARIO DE ACTIVOS	lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc. que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.
IMPACTO	El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.
MIPG	Modelo Integrado de Planeación y Gestión.
NO REPUDIO	También conocido como "no negación", es la condición que evita que se niegue la autoría o recepción de un mensaje o información.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. AMBIENTE Instituto Distrital de Protección y Bienestar Animal</p>	PROCESO GESTIÓN TECNOLÓGICA		 <p>BOGOTÁ INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL</p>
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

POLÍTICA	Toda intención y directriz expresada formalmente por la dirección.
PROPIETARIO DE LA INFORMACIÓN	es la unidad organizacional o proceso donde se crean los activos de información.
PROPIEDAD INTELECTUAL	La propiedad intelectual se relaciona con las creaciones de la mente: invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizados en el comercio. "chrome-extension://efaidnbmninnbpcjpcglclefindmkaj/https://cerlalc.org/wp-content/uploads/documentos-de-interes/odai/ODAI_DOCUMENTOS_DE_INTERES_Que_es_la_propiedad_intelectual_V1.pdf"
RECURSOS TECNOLÓGICOS	son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior del IDPYBA.
RESPONSABLE POR EL ACTIVO DE INFORMACIÓN	es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.
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 consideraciones.
RIESGO DE SEGURIDAD DIGITAL	es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. "Consejo Nacional de Política Económica y Social –Política Nacional de Confianza y Seguridad Digital CONPES 3995 – 2020 - Glosario, edición digital, pág. 42"
SEGURIDAD DE LA INFORMACIÓN	Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de esta.
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI	Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.
SISTEMA DE INFORMACIÓN	es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por el Instituto Distrital de Protección y Bienestar Animal o de origen externo ya sea adquirido por la Entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.
SOFTWARE	También referido a él con la abreviatura SW, es una palabra que proviene del inglés y que da significado al soporte lógico de un sistema informático, es decir, es la parte no física que hace referencia a un programa o conjunto de programas de cómputo que incluye datos, reglas e instrucciones para poder comunicarse con el ordenador y que hacen posible su funcionamiento. Sin Software, los ordenadores serían inútiles, y es desarrollado mediante el uso de distintos lenguajes de programación que consisten en símbolos y reglas semánticas y sintácticas y que definen el significado de sus elementos y expresiones. "https://www.ciset.es/glosario/480-software-concepto-y-tipos"
USUARIOS	funcionarios, contratistas y terceros que tienen acceso a los sistemas de información, servicios de red y a la infraestructura tecnológica que los soporta.
VULNERABILIDAD	debilidad de un activo o control que pueda ser explotado por una o más amenazas.

	PROCESO GESTIÓN TECNOLÓGICA		
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

2. DESARROLLO

2.1. PRINCIPIOS DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



La gestión de la información se fundamenta en los (3) tres pilares de Seguridad de la Información que son: confidencialidad, integridad y disponibilidad. La seguridad de la información son un conjunto de protocolos, controles y procedimientos que resguardan el acceso a la información, destinados a reducir o mitigar los riesgos informáticos, teniendo como base los lineamientos y buenas prácticas establecidas en la norma ISO 27001: 2013 y articulado con el Modelo de Seguridad y Privacidad de la Información -MSPI.

- **La confidencialidad**, requiere que la información sea accesible de forma única a las personas que se encuentran autorizadas. Es necesario acceder a la información mediante autorización y control.
- **La integridad**, supone que la información se mantenga inalterada ante accidentes o intentos maliciosos. Sólo se podrá modificar la información mediante autorización.

El objetivo de la integridad es prevenir modificaciones no autorizadas de la información.

- **La disponibilidad**, supone que el sistema informático se mantenga trabajando sin sufrir ninguna degradación en cuanto a accesos. Es necesario que se ofrezcan los recursos que requieran los usuarios autorizados cuando se necesiten. La información deberá permanecer accesible a elementos autorizados.

El objetivo es necesario prevenir interrupciones no autorizadas de los recursos informáticos.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>AMBIENTE INICIATIVA LEY 1614 de Protección y Bienestar Animal</small>	PROCESO GESTIÓN TECNOLÓGICA		 INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

2.2. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

OBJETIVO

La política de seguridad de la información tiene por objetivo establecer los lineamientos generales con el propósito de preservar los niveles de confidencialidad, integridad y disponibilidad de los activos de información, que dependen o usan las tecnologías de la información y las comunicaciones del Instituto Distrital de Protección y Bienestar Animal -(en adelante IDPYBA), entidad adscrita al Sector Ambiente de Bogotá D.C., conforme a los controles de seguridad y privacidad determinados en la entidad para prevenir o mitigar eventos o incidentes de seguridad de la información.

ALCANCE

La política general de seguridad de la información aplica a todos los funcionarios, contratistas y terceros del Instituto Distrital de Protección y Bienestar Animal -IDPYBA. De igual manera la presente política aplica a todos los procesos de la entidad bajo el marco de gestión establecido en el Modelo Integrado de Planeación y Gestión –MIPG¹.

Dicha política permitirá un manejo adecuado de la confidencialidad, integridad y disponibilidad de los activos de información, mediante una gestión continua del riesgo, la adopción de buenas prácticas en el uso de estos y la mejora de las competencias de los funcionarios y contratistas de la entidad basado en la norma ISO 27001:2013, mediante la ejecución de planes de trabajo independientes para los temas de seguridad y de privacidad de la información.



Esta política deberá contar con procedimientos asociados, mecanismos de control.

POLÍTICA

El Instituto Distrital de Protección y Bienestar Animal -IDPYBA consiente de los riesgos actuales decidió adoptar el modelo de gestión de seguridad y privacidad de la información sugerido, antes denominado Subsistema de Gestión de Seguridad de la Información establecido por el Ministerio de las Tecnologías de la Información -MinTIC, mediante la política de “Estrategia de Gobierno Digital” impulsado por la Alta Consejería Distrital para las TIC, el cual permite identificar y minimizar los riesgos a que está expuesta la información, los procesos y elementos asociados a ella.

El Instituto Distrital de Protección y Bienestar Animal (IDPYBA) logrará la protección y manejo adecuado de la información de los ciudadanos del Distrito Capital, que se encuentre bajo su responsabilidad y custodia, de igual manera con la información

¹ Decreto 1499 de 2017, “Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 33 de la Ley 1753 de 2015”.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>ASISTENTE INSTITUCIONAL DEL GOBIERNO MUNICIPAL</small>	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

generada en el desarrollo de su misionalidad, que soportan los procesos de la entidad y apoyan la adopción e implementación del Modelo de Seguridad y Privacidad de la Información.

Para la gestión estratégica y operacional de la seguridad y privacidad de la información, se alinea con las siguientes premisas:

- Disminuir el riesgo de los procesos misionales de la entidad.
- Atender los principios de seguridad de la información.
- Atender los principios de la función administrativa.
- Fortalecer la confianza de los funcionarios y terceros (proveedores y contratistas).
- Apoyar las iniciativas y proyectos de innovación con tecnología.
- Proteger y salvaguardar los activos de información.
- Fortalecer la cultura de seguridad de la información en los funcionarios y terceros (proveedores, contratistas y practicantes) del IDPYBA
- Garantizar la continuidad de la seguridad de la información crítica del negocio frente a incidentes.
- Implementar el sistema de gestión de seguridad de la información ajustado a las necesidades y dimensión de la entidad.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

Los servidores públicos, proveedores y terceras partes son responsables por el adecuada gestión y aseguramiento de la información utilizada en el desarrollo de sus actividades, en el cumplimiento de los lineamientos, requisitos, controles y buenas prácticas de seguridad de la información definidas por la entidad, así como la prevención, identificación y reporte de cualquier evento o incidente relacionado con la seguridad de la información.

2.3. ORGANIZACIÓN DE LA SEGURIDAD



2.3.1. Roles y Responsabilidades

Dentro del Modelo de Gestión de Seguridad y Privacidad de la Información, el Equipo de trabajo de Gestión Tecnológica será el encargado de efectuar el seguimiento y actualización de las Políticas Específicas del Subsistema de Gestión de Seguridad de la información – SGSI o también denominado Modelo de Seguridad y Privacidad de la Información -MSPI, para el Instituto Distrital de Protección y Bienestar Animal – IDPYBA.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CORPORACIÓN INSTRUMENTO LEGISLATIVO DE PROTECCIÓN Y BIENESTAR ANIMAL</p>	PROCESO GESTIÓN TECNOLÓGICA		 <p>BOGOTÁ INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL</p>
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

Definiendo un punto de partida para la gestión de seguridad de la información, se establecen principios que soportan la seguridad de la información:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, proveedores, o terceros.
- El Instituto Distrital de Protección y Bienestar Animal (IDPYBA) protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes).
- El Instituto Distrital de Protección y Bienestar Animal (IDPYBA) protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- En ninguna circunstancia se podrá divulgar la información clasificada como CONFIDENCIAL o RESERVADA a personas no autorizadas o en espacios públicos o privados. Esta restricción se debe cumplir inclusive después de la terminación del vínculo laboral y contractual y debe estar incluida en los Acuerdos de Confidencialidad establecidos por la Entidad.
- Todos los activos de información del deben tener un propietario, custodio y deben estar debidamente identificados.
- Los propietarios de los activos de información son los responsables de aplicar y velar por el cumplimiento de los controles que garanticen la disponibilidad, confidencialidad e integridad de la información de los activos.
- Se deben definir e incluir los roles y privilegios de la plataforma tecnológica y sistemas de información, con el fin de crear el procedimiento de solicitud, modificación, eliminación y/o inactivación de usuarios privilegiados.
- La mesa de servicios designada para tal fin debe informar a través de los mecanismos de comunicación seleccionados, que el usuario fue creado y que fueron asignados los privilegios solicitados.
- Se debe capacitar a todos los Colaboradores y terceros solicitantes de accesos a componentes tecnológicos y sistemas de información sobre el uso y la responsabilidad que tienen al ser autorizados.
- El Instituto Distrital de Protección y Bienestar Animal (IDPYBA) protegerá su información de las amenazas originadas por parte del personal.
- El Instituto Distrital de Protección y Bienestar Animal (IDPYBA) implementará control de acceso a la información, sistemas y recursos de red.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>AMBIENTE</small> <small>PLAN DE ORDENAMIENTO TERRITORIAL</small> <small>BOGOTÁ 1988</small>	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	


- El Instituto Distrital de Protección y Bienestar Animal (IDPYBA) velará 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.

2.3.2. Contacto con autoridades y grupos de Interés

- El Instituto Distrital de Protección y Bienestar Animal (IDPYBA), mantiene contacto con las autoridades competentes para el cumplimiento de la ley, organismos de control y autoridades de supervisión correspondientes.
- El Equipo de trabajo de Gestión Tecnológica, junto con el Oficial de Seguridad mantienen contacto con grupos de interés, con el fin de tener información actualizada referente a seguridad de la información, como advertencias, actualizaciones, vectores de ataque y vulnerabilidades de Software.

2.4. OBLIGACIONES GENERALES

- Los funcionarios, contratistas, proveedores, usuarios o terceras partes son responsables por el manejo adecuado y aseguramiento de la información utilizada en el desarrollo de sus actividades y obligaciones contractuales.
- Las partes interesadas mencionadas, deberán cumplir con los lineamientos, requisitos y buenas prácticas de seguridad de la información que adopte la entidad y que harán parte de la documentación de la gestión de seguridad, previniendo, detectando y reportando cualquier incidente que afecte la seguridad de la información.
- Todos los sistemas de información Instituto Distrital de Protección y Bienestar Animal – IDPYBA. deben implementar reglas de acceso, de tal manera que exista segregación de funciones, entre quien administre, opere, mantenga y audite, y todo aquel que tenga acceso al sistema de información, así como quien otorgue privilegios de estos.
- Todo aquel que tenga acceso a la información del Instituto Distrital de Protección y Bienestar Animal – IDPYBA. debe tener sus funciones definidas con el fin de reducir el uso no autorizado, indebido o accidental a los activos de información, que para su nivel de confidencialidad este restringido a quien no está autorizado.
- Todos los sistemas de información del Instituto Distrital de Protección y Bienestar Animal – IDPYBA. deben implementar seguimiento a sus acciones dentro del sistema de información, mediante el uso de control de cambios, que para tal efecto el Equipo de trabajo de Gestión Tecnológica tenga en su mapa de procesos, con el fin de verificar, controlar, y auditar los cambios que se realicen en el desarrollo de los sistemas de información, independiente cual sea su modalidad de creación, así como todo lo concerniente con la creación, modificación y asignación de permisos para manejo de bases de datos, ambientes de prueba, producción y afectación a la infraestructura tecnológica del Instituto Distrital de Protección y Bienestar Animal – IDPYBA.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. ASISTENTE Vicerrectoría de Planeación y Gestión Pública	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

2.5. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

2.5.1. POLÍTICA ESPECÍFICA PARA CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

OBJETIVO


Identificar lineamientos para la gestión de activos de Información en el Instituto Distrital de Protección y Bienestar Animal - IDPYBA, mediante la comprensión de los procesos que la componen, para definir el nivel de criticidad, sensibilidad y reserva de la información, para clasificar la información y definir la sensibilidad y criticidad de acuerdo los principios de seguridad de la información como son: Confidencialidad, Integridad y Disponibilidad, garantizando que los activos de información reciban una adecuada valoración y protección.

ALCANCE

Aplica a todos los funcionarios y contratistas que cuenten con activos de información identificados en del Instituto Distrital de Protección y Bienestar Animal - IDPYBA. Para la identificación de los activos de información se debe tener presente, la información, sistemas de información, Bases de datos, software, hardware, personas o lugares para la operación o aquella información estratégica requerida para lograr los objetivos misionales de la entidad.

Inicia con la identificación, valoración, revisión, aprobación y ubicación del inventario de activos de información de la entidad, dentro de los activos a identificar se pueden encontrar:

- La sede electrónica del IDPYBA y los contenidos que residen en ellos;
- La información que se transmite a través de los diferentes servicios del IDPYBA;
- Servicios de interacción con la comunidad, servicios de transacciones en línea, servicios de recaudo o registro de información, entre otros.
- Sistemas de información que apoyan los servicios del IDPYBA;
- La plataforma tecnológica que soporta los diferentes servicios y sistemas de información (hardware, software, comunicaciones, bases de datos, etc.) del IDPYBA.
- La infraestructura tecnológica de seguridad en la cual esta soportados los servicios e información del IDPYBA;
- Los documentos físicos requeridos para llevar a cabo el desarrollo de las actividades para el cumplimiento de los objetivos misionales del IDPYBA.
- Los activos de información a los que se refiere el Decreto 103 de 2015 que reglamenta la Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información).

 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>ALCALDÍA MAYOR DE BOGOTÁ D.C.</small> <small>VEREDAS: CENTRO DE PROTECCIÓN Y BIENESTAR ANIMAL</small>	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ <small>INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL</small>
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

POLÍTICA

El Instituto Distrital de Protección y Bienestar Animal - IDPYBA, garantiza la identificación de los activos de información definiendo el nivel de criticidad, sensibilidad y brinda los controles adecuados encaminados a la preservación de los principios de seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

RESPONSABILIDADES

Los responsables de la información serán los jefes de Área, subdirectores (as) encargados de clasificarla, de acuerdo con su grado de sensibilidad y criticidad; mantener actualizada la clasificación realizada y de definir los niveles que podrán tener permisos de acceso a la información.

El custodio de la información se encarga de mantener las medidas de protección establecidas por los responsables.

Cada responsable de la Información supervisará que el proceso de clasificación y rotulado de información de su área de competencia sea cumplido de acuerdo con lo establecido en la presente Política.

2.5.2. POLÍTICA ESPECÍFICA DE SEGURIDAD FÍSICA

OBJETIVO

Prevenir acerca de accesos no autorizados, daños o robos a los activos de información del Instituto Distrital de Protección y Bienestar Animal - IDPYBA. Proteger los equipos de procesamiento de información crítica del IDPYBA ubicándolos en áreas seguras y resguardadas por un perímetro de seguridad definido, con medidas y controles de acceso apropiados. Igualmente, contemplar la protección de este en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros. Controlar los factores ambientales que podrían afectar el correcto funcionamiento de los equipos informáticos que contienen la información del IDBYBA Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

ALCANCE

Aplica a todos los recursos físicos y control asociados a los activos de información del Instituto Distrital de Protección y Bienestar Animal - IDPYBA. Referentes a instalaciones, equipos de cómputo, cableado, expedientes, medios de almacenamiento, entre otros. Los cuales deben contar con mecanismos de protección física y ambiental, y controles de acceso apropiados para la protección de la información de la entidad.



 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>AMBOGOTÁ</small> <small>INSTRUMENTO DE POLÍTICAS DE SEGURIDAD Y BIENESTAR ANIMAL</small>	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ	<small>INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL</small>
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA			
	Código: PA04-PL01	Versión: 2.0		

POLÍTICA

Son todos aquellos sitios en donde se encuentren sistemas de procesamiento de información, equipos de cómputo, almacenamiento, comunicaciones y expedientes, los cuales serán protegidos de accesos no autorizados, mediante el uso de controles lógicos o físicos, para prevenir intrusiones u otro tipo de amenazas que puedan afectar su normal operación.

Los aspectos de la seguridad física a considerar son:

- Las medidas de seguridad que se deban tomar dependerán directamente del valor de los activos de información, su nivel de confidencialidad, y los valores requeridos de disponibilidad.
- El sitio donde se ubiquen los recursos informáticos debe ser protegidos de accesos no autorizados, empleando mecanismos de control (tarjetas, vallas, alarmas, cerraduras, claves de acceso, personal de seguridad, etc.)
- Los requerimientos de tipo ambiental deben ser especificados por los diferentes fabricantes de los equipos.
- Debe existir un área de recepción que solo permita la entrada de personal autorizado por un funcionario de la entidad, previa autorización de esta vía correo electrónico y/o autorización escrita.
- El equipamiento de soporte como impresoras y fotocopiadoras debe ser instalado adecuadamente en lugares acondicionados para tal fin, para evitar solicitudes de acceso que podrían comprometer la información.
- Las áreas seguras contarán con equipos contra incendio, detección de humo, control de humedad, todo esto de acuerdo con la infraestructura que posea el Instituto Distrital de Protección y Bienestar Animal - IDPYBA
- Los Backups de información se mantendrán en sitios alejados de los procesamientos principales.
- En las áreas donde se manipule algún tipo de activo de información, no se permite fumar, tomar ningún tipo de bebidas o consumir alimentos, todo ello para evitar la pérdida de disponibilidad o integridad de la información.
- Los equipos deben ser protegidos de fallas de potencia u otras anomalías de tipo eléctrico.
- Los sistemas de abastecimiento de potencia deben cumplir con las especificaciones de los fabricantes.
- El cableado de la red eléctrica y datos debe ser instalado y mantenido por personal calificado con el fin de garantizar su integridad.
- Todo elemento que ingrese debe ser examinado por la compañía de seguridad rigurosamente con el fin de identificar material peligroso y que coincida con su respectiva autorización de ingreso.
- Las áreas de descargue deben estar debidamente identificadas para evitar el acceso a las instalaciones por parte de terceros.
- Los materiales que deban entrar a las instalaciones deben ser examinados debidamente en la zona de descargue, para evitar la entrada de elementos peligrosos a las áreas internas.
- El material entrante o saliente debe ser registrado, con el fin de mantener el listado de inventario actualizado.
- El uso de equipos de procesamiento de la información o software, fuera de las instalaciones del Instituto Distrital de Protección y Bienestar Animal - IDPYBA, debe ser autorizado por el

	PROCESO GESTIÓN TECNOLÓGICA		
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

Propietario de la Información de donde el funcionario o colaborador dependa. Esto aplica para computadores personales, agendas electrónicas, teléfonos móviles, etc.

- Se deben cumplir los lineamientos aplicables a la entidad de acuerdo con la normatividad técnica colombiana sobre gestión documental, descritas en el Modelo de Seguridad y Privacidad de la Información -MSPI.

RESPONSABILIDADES

El(la) Jefe(a) de la subdirección Corporativa definirá las medidas de seguridad física y ambiental para el resguardo de los activos, en función a un análisis de riesgos y controlará su ejecución.

El Oficial de Seguridad y/o el personal responsable del Equipo de Gestión Tecnológica, definirán las medidas de seguridad a implementar en áreas protegidas y coordinarán su implementación. El personal responsable del equipo de trabajo de Gestión Tecnológica controlará el mantenimiento de los equipos informáticos de acuerdo con las indicaciones de proveedores tanto dentro como fuera de las instalaciones del Instituto Distrital de Protección y Bienestar Animal - IDPYBA.

La instalación o reubicación de equipos de procesamiento o de telecomunicaciones, es responsabilidad única y exclusiva del o quien el delegue. Por lo tanto, los usuarios deben abstenerse de realizar modificaciones en los equipos, infraestructura de red o eléctrica sin autorización del Jefe(a) de la Oficina Asesora de Planeación y/o Equipo de trabajo de Gestión de la Tecnología.

Los jefes de área definirán los niveles de acceso físico del personal del Instituto Distrital de Protección y Bienestar Animal – IDPYBA a las áreas protegidas que estén bajo su responsabilidad.

El uso de equipos de procesamiento de la información o software, fuera de las instalaciones del Instituto Distrital de Protección y Bienestar Animal - IDPYBA, debe ser autorizado por el responsable de los activos de información de donde el funcionario, contratista o tercera parte dependa.

El proceso de bienes, servicios o infraestructura o el que haga sus veces garantizará que todo personal interno y externo que ingrese a un área definida como segura, deberá poseer una identificación a la vista que claramente lo identifique como tal y estas identificaciones serán intransferibles.

El ingreso a las áreas seguras debe ser autorizado por el jefe de área correspondiente y será monitoreada mediante registros de acceso y salida, los visitantes siempre deberán estar acompañados por personal del IDPYBA.

Los funcionarios y colaboradores o terceras partes no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica, a menos que se tenga la autorización correspondiente.

El Equipo de trabajo de Gestión Tecnológica velará por que los medios de almacenamiento de información que se den de baja sean donados o se encuentren en obsolescencia, previamente la información almacenada en estos tenga el respectivo respaldo y estos sean formateados a bajo nivel o de manera segura, a través del uso de herramientas especiales que garanticen y verifiquen que no quede información remanente, para su posible reúso, donación, o destrucción según sea el caso.

 ALCALDIA MAYOR DE BOGOTÁ D.C. <small>CONSEJO DE INSTITUCIONES DE PROMOCIÓN Y DEFENSA JURÍDICA</small>	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ <small>INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL</small>
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

2.5.3. POLÍTICA DE ANTIVIRUS

OBJETIVO

Establecer los lineamientos y controles para el correcto funcionamiento del antivirus y otros recursos de protección en el Instituto Distrital de Protección y Bienestar Animal - IDPYBA.

ALCANCE

Se aplica a los servidores, estaciones de trabajo y equipos de cómputo del Instituto Distrital de Protección y Bienestar Animal - IDPYBA, incluyendo dispositivos portátiles que puedan prestar servicio fuera de las instalaciones de la entidad.

POLÍTICA



Los equipos integrados en el dominio del Instituto Distrital de Protección y Bienestar Animal – IDPYBA deberán tener instalado un antivirus y antispyware, gestionado centralizadamente, el cual se actualizará automáticamente de forma periódica.

Los usuarios deberán ejercer buenas prácticas de uso en los equipos de cómputo, tales como:

- Ejecutar el antivirus al usar dispositivos como USB, CD, DVD, discos externos u otros.
- Verificar a través del software antivirus los archivos de cómputo que sean proporcionados por personal externo o interno como programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos.
- No utilizar las facilidades de los navegadores WEB para ejecutar aplicaciones directamente.
- Abstenerse de escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para auto replicarse, dañar, o impedir el funcionamiento de cualquier recurso de procesamiento, archivos de sistema, o software.
- Abstenerse de conectar equipos personales que no contengan antivirus instalado y actualizado, a la red del Instituto Distrital de Protección y Bienestar Animal – IDPYBA.
- Al producirse un incidente se desconectará la estación de la red y se avisará inmediatamente de la presencia del malware para ser eliminado.

Asimismo, la Subdirección de Gestión Corporativa ejercerá los siguientes controles:

- Monitorear por medio de software especializado y actualizado los computadores y medios informáticos en búsqueda de archivos sospechosos o no autorizados.
- Configurar las aplicaciones de correo electrónico y herramientas de oficina para evitar que se ejecute contenido activo, código móvil y macros automáticamente.
- Al producirse un incidente se gestionará la eliminación del malware.

	PROCESO GESTIÓN TECNOLÓGICA		
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

RESPONSABILIDADES

El Oficial de Seguridad de la Información y/o el personal responsable del Equipo de trabajo de Gestión Tecnológica, tendrá a su cargo la definición de controles para la detección, prevención y protección de la información contra software malicioso con el fin de determinar la seguridad de los datos.

Los usuarios y terceras partes deberán cumplir con la Política.

El Oficial de Seguridad y/o el personal responsable de Gestión Tecnológica definirá las medidas de seguridad a implementar en la gestión de la consola de antivirus y coordinará su implementación. El personal responsable de Gestión Tecnológica controlará la instalación y administración del antivirus en los equipos informáticos en las instalaciones del Instituto Distrital de Protección y Bienestar Animal – IDPYBA.

2.5.4. POLÍTICA DE USO DE CORREO ELECTRÓNICO CORPORATIVO

OBJETIVO

Establecer los lineamientos generales para que los servidores públicos y terceros de la entidad, utilicen apropiadamente el correo electrónico a fin de utilizar el recurso de forma racional y como potenciador de las actividades del Instituto Distrital de Protección y Bienestar Animal - IDPYBA.

ALCANCE


La política aquí descrita aplica a todos los servidores públicos y terceros el Instituto Distrital de Protección y Bienestar Animal - IDPYBA, que tengan acceso a la información digital albergada en el correo electrónico corporativo de la entidad.

POLÍTICA

El Instituto Distrital de Protección y Bienestar Animal - IDPYBA, asigna a funcionarios y contratistas una cuenta de correo electrónico corporativa para ejercer sus funciones según las capacidades de la infraestructura del IDPYBA.

La información contenida en el buzón de correo se considera privada, por lo tanto, debe ser manejada como una comunicación directa entre el remitente y su destinatario, los usuarios no deben utilizar los sistemas de correo electrónico del Instituto Distrital de Protección y Bienestar Animal - IDPYBA. para transmitir:

- Correos electrónicos no solicitados, sin relación con las actividades El Instituto Distrital de Protección y Bienestar Animal - IDPYBA, que puedan ofender o causar inconvenientes a quienes lo reciban. Esto incluye el uso de listas de correo, cuando el e-mail enviado no está relacionado con el propósito para el cual la lista de correo utilizada fue creada (SPAM).

 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE AMBIENTE Y ORDENAMIENTO TERRITORIAL</small> <small>INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL</small>	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ <small>INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL</small>
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

- Correos electrónicos no solicitados requiriéndole a otros usuarios en el Instituto Distrital de Protección y Bienestar Animal - IDPYBA o cualquier lugar que continúe reenviando el mismo a otros.
- Correos electrónicos pretendiendo ser de una persona diferente del usuario que realmente envía el correo.
- Material, el cual pueda considerarse sexista, racista, homofóbico, xenofóbico, pornográfico, pedófilo o similarmente discriminatorio y/o ofensivo.
- Material que condene o promueva, directa o indirectamente, actividades criminales o que puedan dañar las actividades del Instituto Distrital de Protección y Bienestar Animal - IDPYBA.
- Texto o imágenes las cuales sean propiedad intelectual de terceros, sin el permiso escrito para dicha divulgación por parte del responsable.
- Material que pueda ser utilizado para vulnerar la seguridad de los equipos de cómputo o para facilitar el acceso no autorizado a las mismas.
- Material que contenga datos personales, a menos que se cuente con autorización expresa para tal fin.

Asimismo, los usuarios deberán ejercer buenas prácticas de uso en las cuentas de usuario asignadas, tales como:

- Depurar continuamente su buzón de correo, con el fin de mantener siempre espacio disponible para enviar y recibir nuevos mensajes, cada buzón de correo tendrá un espacio limitado de almacenamiento.
- Tener claves de acceso seguras y no entregar la contraseña a personas no autorizadas, teniendo en cuenta que la cuenta de correo utiliza la misma contraseña que la de red.
- Abstenerse de abrir correos de remitentes desconocidos o sospechosos y no activar ningún tipo de enlace ni ejecutar archivos adjuntos.
- Reportar posibles anomalías o irregularidades en mensajes recibidos, comunicándose con la Subdirección de Gestión Corporativa y/o Equipo de Gestión Tecnológica mediante la Mesa de Ayuda.
- Abstenerse de interceptar o revelar comunicaciones electrónicas no autorizadas.
- Utilización de un lenguaje apropiado, evitando palabras ofensivas o discriminatorias.
- Cada usuario es responsable de la información enviada, reenviada o eliminada desde su cuenta de correo
- Abstenerse de enviar información confidencial a personal no autorizado. Los usuarios de datos deben asumir que ningún correo electrónico es seguro.
- Considerar la compresión de los archivos adjuntos, a fin de reducir el uso de ancho de banda.

El Instituto Distrital de Protección y Bienestar Animal - IDPYBA se reserva el derecho a pedir las claves de encriptación, en caso de haber sido utilizadas, de acceder y navegar a los contenidos del correo electrónico de los usuarios de acuerdo con sus obligaciones legales y para legitimar los propósitos con los cuales se utiliza el sistema.

RESPONSABILIDADES

El Oficial de Seguridad de la Información y/o el personal responsable del Equipo de trabajo de Gestión Tecnológica definirán y harán seguimiento a los controles a implementar.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>ALPHENITO</small> <small>PERMANENTE</small> <small>PERMANENTE</small>	PROCESO GESTIÓN TECNOLÓGICA		 
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

Los usuarios en general y las terceras partes tendrán la obligación de cumplir lo establecido en la presente Política.

Los usuarios son responsables por la adecuada administración del correo electrónico y la herramienta de almacenamiento en la nube que use la entidad.

2.5.5. POLÍTICA DE USO DE CONTRASEÑAS

OBJETIVO

Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas.

ALCANCE

Esta política aplica a todos los servidores públicos y terceros que tengan acceso, por medio de un usuario previamente establecido a la red de datos del Instituto Distrital de Protección y Bienestar Animal - IDPYBA.

POLÍTICA

El Instituto Distrital de Protección y Bienestar Animal - IDPYBA, establece a funcionarios y contratistas acceso a una cuenta de correo electrónico y sistemas de información corporativos para ejercer sus funciones, el usuario deberá crear una contraseña teniendo en cuenta las siguientes recomendaciones:

- No contener el nombre de cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres consecutivos.
- Tener una longitud mínima de 8 caracteres.
- Incluir caracteres de tres de las siguientes categorías:
 - Mayúsculas (de la A a la Z)
 - Minúsculas (de la a a la z)
 - Dígitos de base 10 (del 0 al 9)
 - Caracteres no alfanuméricos (¡por ejemplo!, \$, #, %)
- No repetir las últimas 3 contraseñas utilizadas anteriormente.
- No usar contraseñas por defecto o iguales al nombre de usuario o del perfil del usuario, nombres de familiares, amigos, mascotas, número de teléfono, números de documentos.
- No escribir la contraseña en papel o documentos electrónicos.
- No utilizar la misma contraseña para usos personales o formularios electrónicos.
- No revelar la contraseña de acceso a terceros de ningún sistema de información del Instituto Distrital de Protección y Bienestar Animal - IDPYBA (aplicativos, Internet, correo o ingreso a la red).
- En caso de olvido de la contraseña, se deberá gestionar el cambio de esta por medio de la mesa de ayuda.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE PLANEACIÓN Y POLÍTICAS PÚBLICAS</small>	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ <small>INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL</small>
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

RESPONSABILIDADES

El Oficial de Seguridad de la Información y/o el responsable del Equipo de Gestión Tecnológica estarán a cargo de la definición de procedimientos para el control de acceso a los sistemas de información.

El personal responsable del Equipo de Gestión Tecnológica implementará las normas y procedimientos definidos.

Los usuarios y terceras partes deberán cumplir todas las directrices asociadas con esta política.

Los servidores públicos y terceros de la entidad tendrán la responsabilidad de mantener las contraseñas de aplicativos, internet, correo electrónico o ingreso a la red en estricta confidencialidad.

2.5.6. POLÍTICA ESPECIFICA PARA DISPOSITIVOS MÓVILES

OBJETIVO

Garantizar los niveles de seguridad de los activos de información para el uso óptimo de los dispositivos móviles (ejemplo: equipos portátiles, teléfonos celulares, tabletas, tarjetas inteligentes entre otros) que administren, transmitan, almacenen o procesen información definidos por el Instituto Distrital de Protección y Bienestar Animal - IDPYBA.


ALCANCE

Esta política aplica a todos los servidores públicos y terceras partes a los cuales se le haya asignado dispositivos y/o equipos móviles propiedad del Instituto Distrital de Protección y Bienestar Animal - IDPYBA, que tengan acceso a la red de información o cualquier servicio de tecnologías de la información y comunicaciones de la entidad.

POLÍTICA

El Equipo de trabajo de Gestión Tecnológica en coordinación con el Oficial de Seguridad de la Información, establecerán lineamientos y mecanismos de seguridad lógicos para preservar los niveles de seguridad de los activos de información, requeridos para permitir el acceso a los mismos a través de los dispositivos de tecnología móviles (equipos portátiles, teléfonos celulares, tabletas, tarjetas inteligentes entre otros), con el fin de salvaguardar la información administrada, transmitida, almacenada o procesada por éstos. Así mismo, se establecerán los controles de seguridad de la información de acuerdo con la identificación y valoración de los riesgos de seguridad de la información.

Los controles dispuestos por el IDPYBA deben ser de estricto cumplimiento por parte de los servidores públicos y terceras partes que hagan uso de estos y que a través de estos ingresen a la información, tecnologías de la información y comunicaciones o servicios de la entidad.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>AMBOGOTÁ</small> <small>VENECIA CAPITAL DE INNOVACIÓN</small> <small>BOGOTÁ PRIMERA</small>	PROCESO GESTIÓN TECNOLÓGICA		 
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

RESPONSABILIDADES

- El uso de dispositivos móviles para la realización o ejecución de las actividades de un proceso en el Instituto Distrital de Protección y Bienestar Animal – IDPYBA, debe ser definido por el propietario de la información, en el cual se identifiquen los riesgos que puedan afectar la información ocasionados por uso de mismo.
- Asegurarse del registro de los dispositivos móviles, las restricciones de instalación de software y sus versiones, así como los requisitos de conexiones a servicios de información, controles de acceso, configuración de cifrado y protección contra software malicioso, todo esto antes de ser entregado al servidor público que los requiera para su trabajo.
- Garantizar la configuración de borrado remoto, así como deshabilitar y cerrar todas las sesiones que el dispositivo móvil pueda tener configuradas.
- El uso de dispositivos móviles debe ser restringido y solamente usado para los casos específicos que se requieran por la labor que realiza un servidor público, teniendo en cuenta los requisitos legales, seguros y otros requisitos de seguridad para los casos de robo o pérdida de este.
- Todo servidor público que bajo su responsabilidad cuente con un dispositivo móvil o varios debe ser debidamente informado de las responsabilidades de seguridad de este o estos dispositivos, así como de los mecanismos establecidos para informar inmediatamente al responsable de comunicar a las aseguradoras y al Equipo de trabajo de Gestión Tecnológica en caso de pérdida del dispositivo.



Para los casos de dispositivos móviles personales que se usan para realizar labores de la entidad, es importante considerar la separación entre el uso privado de la de uso para labores contractuales, esto incluye el uso de software y la protección de datos del Instituto Distrital de Protección y Bienestar Animal - IDPYBA.

El Equipo de trabajo de Gestión Tecnológica debe garantizar conexiones seguras para accesos remotos donde se usen dispositivos móviles ya sean de propiedad de la entidad o dispositivos móviles personales usados para realizar labores contractuales en la entidad.

Por su parte el servidor público, contratista, pasante y tercera parte debe:

Cuando use un dispositivo móvil, debe firmar un acuerdo de confidencialidad y un acuerdo de usuario final en el que reconozca sus deberes, así como el desistimiento de la propiedad de los datos almacenados en el mismo, con el fin de permitir el borrado seguro y remoto de la información de la organización en el caso de robo pérdida, o cuando ya no se posee autorización para usar el servicio teniendo en cuenta la legislación sobre privacidad de la información.

Junto con el Equipo de trabajo de Gestión Tecnológica se debe pactar una periodicidad de copias de respaldo de la información que pueda estar almacenada en el dispositivo móvil, así como la definición de protocolos de almacenamiento seguro ya sea en unidades de almacenamiento compartidas en la red, nube, de forma remota o interna en las instalaciones del IDPYBA.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. AMBIENTE Instituto Distrital de Protección y Bienestar Animal	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

2.5.7. POLÍTICA DE USO DE SERVICIOS DE RED

OBJETIVO

Establecer los lineamientos que se deben tener en cuenta para el uso de los servicios de red por servidores públicos y terceras partes de la entidad, preservando las características de seguridad de los activos de información del Instituto Distrital de Protección y Bienestar Animal – IDPYBA.

ALCANCE

Aplica a todas las formas de acceso para aquellos a quienes se les haya concedido permisos sobre el uso de servicios de red.

POLÍTICA

El Instituto Distrital de Protección y Bienestar Animal – IDPYBA controlará el acceso a los servicios de red para que los usuarios que tengan acceso a las redes y a sus servicios no comprometan la seguridad de estos.

La Subdirección de Gestión Corporativa, concederá el acceso a los servicios y recursos de red, de acuerdo previa solicitud formal, especialmente a las aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo; por ejemplo: áreas públicas o externas que están fuera de la administración y del control de seguridad del Instituto Distrital de Protección y Bienestar Animal – IDPYBA.

Para ello del Instituto Distrital de Protección y Bienestar Animal – IDPYBA documentará los procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán: |

- Identificar las redes y servicios de red a los cuales se concedió el acceso.
- Establecer controles y procedimientos de gestión para salvaguardar el acceso a las conexiones y servicios de red.

RESPONSABILIDADES

El Oficial de Seguridad de la Información y/o el responsable del Equipo de trabajo de Gestión Tecnológica estarán a cargo de la definición de normas y procedimientos para el uso de servicios de red.

El personal responsable del Equipo de trabajo de Gestión Tecnológica implementará las reglas y procedimientos determinados.

Los Usuarios y Terceras Partes deberán cumplir todas las normas asociadas con esta política.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>ALMAYOR</small> <small>MAYORAL OFFICE OF BOGOTÁ</small> <small>BOGOTÁ PERÚ</small>	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

2.5.8. POLÍTICA ESPECÍFICA DE TELETRABAJO

OBJETIVO

Garantizar los niveles de seguridad de los activos de información definidos por el Instituto Distrital de Protección y Bienestar Animal – IDPYBA al momento de realizar actividades de teletrabajo.

ALCANCE

Esta política aplica a todos los servidores públicos y terceros del Instituto Distrital de Protección y Bienestar Animal – IDPYBA que estén autorizados para efectuar el desarrollo de actividades mediante teletrabajo.

POLÍTICA

El Equipo de trabajo de Gestión Tecnológica en coordinación con el Oficial de Seguridad de la Información, establecerán mecanismos de seguridad física y lógica para preservar los niveles de seguridad de los activos de información, requeridos para efectuar actividades de teletrabajo, por parte de servidores públicos y terceros autorizados por la entidad.

RESPONSABILIDADES

- Se debe identificar la seguridad física existente en el lugar donde se ejercerá el teletrabajo y su entorno físico, los requisitos de seguridad en las comunicaciones teniendo en cuenta las necesidades de acceso remoto a los sistemas de información de la entidad y a la sensibilidad de la información a la que se tendrá acceso.
- El Equipo de trabajo de Gestión Tecnológica es el encargado de definir los canales de comunicación y mecanismos de acceso a la información que el teletrabajador utilizará, teniendo en cuenta los requisitos de seguridad y protección de la información que transita por estos medios.
- Es necesario identificar las amenazas que corresponden al acceso no autorizado a información o recursos del IDPYBA por parte de otras personas que usan el mismo equipo de cómputo del teletrabajador ejemplo familias o amigos.
- Es indispensable la definición de requisitos de protección contra software malicioso en el equipo de cómputo, ya sea móvil o de escritorio con el cual se realizará las labores de teletrabajo, así como la responsabilidad del Equipo de trabajo de Gestión Tecnológica de definir la protección o el acceso seguro a la información de forma remota.
- Se debe tener clara la clasificación de la información y mantener la protección de esta, a través de la definición de permisos de control de acceso remoto y horarios permitidos para este acceso.
- Se debe informar al teletrabajador sobre las reglas de acceso a la información evitando el uso del dispositivo, por parte de personas ajenas al Instituto Distrital de Protección y Bienestar Animal - IDPYBA, con el fin de proteger la información que pueda llegar a ser almacenada en el equipo de teletrabajo o los mecanismos de acceso configurados en el mismo.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. ASISTENTE Instituto Distrital de Protección y Bienestar Animal	PROCESO GESTIÓN TECNOLÓGICA		
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

2.5.9. POLÍTICA ESPECIFICA DE USO DE MEDIOS TECNOLÓGICOS DE COMUNICACIÓN Y ACCESO A INTERNET

OBJETIVO

Establecer los lineamientos generales para el uso adecuado de Internet y/o activos de información por parte de los funcionarios, colaboradores y terceras partes, para impedir errores, pérdidas, alteraciones o uso inadecuado de la información en las aplicaciones web del Instituto Distrital de Protección y Bienestar Animal - IDPYBA.

ALCANCE

Aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre el uso de Internet en el Instituto Distrital de Protección y Bienestar Animal - IDPYBA.

POLÍTICA



El acceso a Internet es suministrado a los funcionarios y terceras partes del Instituto Distrital de Protección y Bienestar Animal – IDPYBA, es únicamente para desarrollo de las actividades relacionadas con las funciones o actividades designadas. La utilización del software de navegación web designado por el Instituto Distrital de Protección y Bienestar Animal – IDPYBA, deberá estar configurado con las directivas determinadas.

El acceso a Internet debe ser realizado a través de los canales de acceso provistos por el Instituto Distrital de Protección y Bienestar Animal - IDPYBA. En caso de necesitar una conexión a Internet especial, ésta debe ser solicitada y aprobada por el equipo de trabajo de Gestión Tecnológica y el Oficial de Seguridad de la Información.

Los usuarios que requieran acceso a través de protocolo FTP deberán ser explícitamente autorizados a este tipo de acceso, por el Oficial de Seguridad de la Información y/o el personal responsable del Equipo de trabajo de Gestión Tecnológica. De igual manera, los usuarios del servicio de Internet están sujetos al monitoreo de las actividades que realizan en la red.

Se restringe el acceso a Internet para los usuarios, siempre que cumplan con los siguientes propósitos:

- Acceso a sitios que puedan considerarse por su contenido sexista, racista, homofóbico, xenofóbico, pornográfico, pedofílico o similarmente discriminatorio y/u ofensivo.
- Acceso a sitios que reproduzcan en forma no autorizada material protegido por los derechos de autor.
- Acceso a sitios que proporcionen instrucciones o claves para utilizar o acceder a software, servicios o sitios en forma ilegal (piratería).
- Acceso a sitios de juegos en red u online.
- Descarga de software sin autorización.
- Descarga de archivos de audio o video sin autorización.

	PROCESO GESTIÓN TECNOLÓGICA		
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

Se restringe el acceso a Internet para los usuarios, siempre que cumplan con los siguientes propósitos, salvo expresa autorización:

- Acceso para audio o video en línea (TV, Radio, música, etc.).
- Acceso a redes sociales autorizadas.
- Realizar ataques sobre otros sitios, usuario o servidores.
- Brindar servicios externos desde el puesto de trabajo.

Los usuarios no podrán transferir o publicar información de propiedad del Instituto Distrital de Protección y Bienestar Animal – IDPYBA, sin previa autorización y con la utilización de los canales establecidos por el IDPYBA para el fin requerido. igualmente, no podrán bajo ninguna circunstancia utilizar el acceso a Internet para monitorear, interceptar información de otros usuarios a menos que hayan sido autorizados para hacerlo.

Los usuarios del servicio deben asumir que ninguna conexión a Internet es segura, y no deberán enviar información que consideren confidencial a través de este medio.

El acceso a cualquier recurso disponible a través de Internet que no sea el de navegación de sitios, deberá solicitarse en forma justificada para su debida aprobación.

Se permite a los usuarios acceder a Internet para los siguientes usos:

- Acceso a sitios sobre noticias (diarios, radios, agencias, etc.).
- Acceso a Sistemas Bancarios.
- Acceso a Sistemas de Pago Electrónico de servicios.
- Acceso a Sistemas de información sobre transportes, mapas, espectáculos, hotelería.
- Acceso a sitios de capacitación, educación, tecnología.
- Acceso a redes sociales autorizadas.
- Acceso a sitios de clientes, proveedores o similares.

RESPONSABILIDADES

El Oficial de Seguridad de la Información y/o el responsable del Equipo de trabajo de Gestión Tecnológica estarán a cargo de la definición de normas y procedimientos para el servicio de Internet.

El personal responsable del Equipo de trabajo de Gestión Tecnológica implementará las normas y procedimientos definidos.

Los Usuarios y Terceras Partes deberán cumplir todas las directrices asociadas con esta política.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>ALCALDÍA MAYOR DE BOGOTÁ D.C.</small> <small>SECRETARÍA DE SEGURIDAD Y PROTECCIÓN</small> <small>SECRETARÍA DE SEGURIDAD Y PROTECCIÓN</small>	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

2.5.10. POLÍTICA ESPECÍFICA DE CONTROL DE ACCESO A LA INFORMACIÓN

OBJETIVO

Establecer los lineamientos generales para gestionar el acceso a la información y/o activos de información del Instituto Distrital de Protección y Bienestar Animal - IDPYBA.

ALCANCE

Esta política aplica para todos los servidores públicos y terceros cuenten con acceso a los activos de información del Instituto Distrital de Protección y Bienestar Animal - IDPYBA.

POLÍTICA

El Instituto Distrital de Protección y Bienestar Animal - IDPYBA, establece los controles de seguridad necesarios que permitan definir los accesos a los activos de información, con el fin de preservar los niveles de confidencialidad de la información a la cual se haya concedido acceso. Por lo anterior, se establecerán las responsabilidades por parte de los servidores públicos y terceros mediante la celebración de contratos y/o acuerdos de confidencialidad, conforme a los lineamientos establecidos por la entidad.

RESPONSABILIDADES

- El Equipo de trabajo de Gestión Tecnológica, es quien regula el control de acceso a través de usuario y contraseña, acceso a nivel de red, sistema operativo, sistemas de información y servicios tecnológicos, con la finalidad de mitigar riesgos asociados al acceso a la información, salvaguardando la integridad, disponibilidad y confidencialidad de esta en El Instituto Distrital de Protección y Bienestar Animal - IDPYBA.
- La creación, reactivación o desactivación de usuarios de la red o sistemas de información, al igual que los roles y permisos otorgados, los realizará el Equipo de trabajo de Gestión Tecnológica a solicitud del Coordinador del grupo de Gestión de Talento Humano o su delegado, el Coordinador del proceso Contractual o su delegado, de acuerdo con lo establecido por los propietarios de la información a la que tendrá acceso el usuario.
- Las contraseñas serán de uso personal e intransferible, se considera un activo de información de carácter reservado por lo que no debe ser divulgada a ningún otro usuario, incluidos los jefes inmediatos o alguna autoridad dentro de la entidad.
- Se debe acceder a los sistemas de información o dispositivos de red a través de la cuenta de usuario asignada, la cual debe cumplir con los controles y estándares de seguridad definidos.
- Se debe socializar con los servidores públicos, contratistas y terceras partes las reglas de control de acceso definidas por el Instituto Distrital de Protección y Bienestar Animal – IDPYBA y las políticas de control de acceso, así como las responsabilidades que se tienen frente a los medios

 ALCALDÍA MAYOR DE BOGOTÁ D.C. AVANZANDO JUNTAMENTE <small>VEREDAS UNIDAS POR PROGRESAR SERVICIO PÚBLICO</small>	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

físicos y lógicos que permitan el acceso a la información y las consecuencias de no aplicar estos requisitos de seguridad.

- La definición de los roles para el control del acceso a la información debe ser acordé a la identificación y clasificación de la información, tanto en los sistemas de información, redes, unidades de almacenamiento compartidas, como en el acceso físico a áreas restringidas o donde se encuentra información confidencial o reservada.
- Se debe mantener un registro de todos los eventos significativos concernientes al uso y gestión de autenticación e identificación de usuarios y sus acciones dentro de la red.
- Se debe estipular la periodicidad con la que los usuarios deben cambiar su contraseña, así como definir los parámetros de seguridad en la creación de contraseñas.
- Se debe estipular e implementar un proceso formal para el registro y cancelación total o temporal de usuarios y sus permisos de acceso.
- El acceso a los códigos fuente de los aplicativos o sistemas de información debe ser controlado con el fin de reducir potenciales riesgos de corrupción en los mismos y en la manipulación de la información, así como definir un registro de auditoría de todos los accesos y generar copias de respaldo sujetas a cambios realizados.
- se debe evitar el uso no autorizado de fotocopiadoras o cualquier tipo de tecnología que permita reproducir información. Por ejemplo, escáner, cámaras digitales para reproducir información catalogada como pública reservada o pública clasificada.
- Si se debe imprimir información en impresoras conectadas a la red y debe garantizarse que esta información será impresa bajo la vigilancia de la persona autorizada y llevar un control de esta.

2.5.11. POLÍTICA ESPECÍFICA DE USO DE CONTROLES CRIPTOGRÁFICOS

OBJETIVO

Salvaguardar los activos de información del Instituto Distrital de Protección y Bienestar Animal – IDPYBA en cuanto a pérdida de la confidencialidad, autenticidad o integridad mediante la adopción de controles criptográficos.

ALCANCE

Esta política aplica a todos los servidores públicos y terceras partes que mediante el ejercicio de sus actividades y los niveles de clasificación de la información requieran ejecutar actividades de cifrado de información.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>ASISTENTE SOCIAL</small> <small>Unidad Organizacional de Innovación y Tecnología Social</small>	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ <small>INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL</small>
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

POLÍTICA

El Equipo de trabajo de Gestión Tecnológica con el apoyo del Oficial de Seguridad de la Información, serán los responsables de definir los mecanismos de cifrados más convenientes frente a las necesidades de la entidad. Estas medidas de seguridad se determinarán con base en el análisis de riesgos y los requisitos de seguridad. Los usos de las herramientas de cifrado de la información serán autorizadas de acuerdo con los roles o responsabilidades de los servidores públicos del Instituto Distrital de Protección y Bienestar Animal - IDPYBA.



RESPONSABILIDADES

- Se debe definir por parte de la dirección el enfoque y uso de los controles de cifrado de información para el Instituto Distrital de Protección y Bienestar Animal - IDPYBA, incluyendo los principios bajo los cuales se debe proteger la información de la entidad.
- De acuerdo con la valoración de riesgos, la identificación y valoración de los activos de información sea esta confidencial o reservada o contenga datos sensibles, se debe establecer los mecanismos de cifrado necesarios para garantizar su protección en el acceso, almacenamiento y transferencia de la información.
- Se debe establecer un responsable de la implementación de la presente política para la gestión de las llaves, incluida su generación y teniendo en cuenta las normas o lineamientos a adoptar de forma efectiva en toda la entidad mediante soluciones adecuadas a las necesidades del IDPYBA.
- La implementación de los controles de cifrado puede ser usada para proteger la confidencialidad, la integridad, el no repudio y la autenticidad de la información.
- Las llaves de cifrado deben ser definidas con un ciclo de vida que incluya la generación de la clave, su almacenamiento, archivo, recuperación, distribución, retiro y destrucción.
- Todas las llaves o claves de cifrado deben ser protegidas contra la modificación no autorizada, pérdida uso y divulgación no autorizadas, además los equipos usados para generar estas llaves deben estar protegidos físicamente siendo ubicados en áreas de acceso restringido.
- Es necesario realizar copias periódicas del respaldo de las llaves y archivarlas, así como registros de auditorías de las actividades relacionadas con la gestión de las llaves con el fin de reducir la posibilidad de uso inapropiado.

2.5.12. POLÍTICA ESPECÍFICA DE ESCRITORIO Y PANTALLA LIMPIOS

OBJETIVOS

Garantizar que los servidores públicos y terceros de la entidad mantengan su puesto de trabajo y pantalla del computador libre de documentos y/o información sensible para el Instituto Distrital de

	PROCESO GESTIÓN TECNOLÓGICA		
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

Protección y Bienestar Animal – IDPYBA, con el fin de prevenir la pérdida, daño, robo o compromiso de la información durante y fuera de las horas laborales en los puestos de trabajo y equipos de cómputo de los servidores públicos y colaboradores de la entidad.

ALCANCE

Esta política aplica a todos los servidores públicos y terceros del Instituto Distrital de Protección y Bienestar Animal – IDPYBA, que cuenten con acceso a la información tanto digital como física de la entidad.

POLÍTICA

Los servidores públicos y terceras partes deberán acoger los lineamientos determinados por del Instituto Distrital de Protección y Bienestar Animal – IDPYBA, para garantizar los niveles de seguridad de los activos de información que tienen a su cargo. Para ello se deberá contemplar:

- Almacenar los documentos y elementos de almacenamiento externos (CD, DVD, USB, entre otros.), así como la información física en sitios seguros, por ejemplo: cajones o gabinetes bajo llave o archivadores. Esto con el fin de prevenir el acceso no autorizado, pérdida o daño de la información a cargo.
- Durante los periodos de tiempo en los cuales cesan las actividades en el equipo de cómputo, la sesión se debe bloquear, para evitar accesos no autorizados a la información contenida en el equipo.
- De utilizar medios de impresión o copiado de documentos, la información debe retirarse inmediatamente por el servidor público responsable y así mismo, se deberá evitar reutilizar papel que contenga información confidencial.
- De acuerdo con los niveles de clasificación de la información, los archivos o carpetas deberán ser almacenados en ubicaciones que impidan el fácil acceso por parte de terceros, así mismo, se deberá evitar guardarlos en el escritorio del perfil de usuario o carpetas del sistema operativo del equipo de cómputo.

RESPONSABILIDADES

- Se debe tener en cuenta la clasificación de la información, los requisitos legales y contractuales y los riesgos identificados en Instituto Distrital de Protección y Bienestar Animal – IDPYBA, para determinar la información sensible o crítica que se puede encontrar en papel o en medio de almacenamiento digital y que debería ser almacenada y protegida cuando no sea requerida, especialmente cuando el puesto de trabajo se encuentre desatendido (libre o desocupado).
- Todo el personal tenga acceso a la red, al ausentarse del puesto de trabajo debe asegurarse de bloquear su equipo de cómputo y evitar así el acceso a la información Y el uso de los recursos o sistemas de información por personal no autorizado.
- Se deben conservar sobre el escritorio únicamente los documentos necesarios para realizar sus actividades, si el responsable de esta documentación debe ausentarse de su puesto de trabajo,

 ALCALDIA MAYOR DE BOGOTÁ D.C. <small>ADMINISTRACIÓN</small> <small>INSTITUTO Distrital de Protección y Bienestar Animal</small>	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

toda información identificada como pública reservada o pública Clasificada, así como los documentos que contengan información sensible deben ser guardados de forma segura, de igual forma se debe realizar esta actividad al terminar la jornada laboral.

- Los usuarios no deberán almacenar en el escritorio del sistema operativo de sus estaciones de trabajo, documentos, accesos directos a los documentos o a sistemas de información sensibles.
- Los usuarios son responsables por la custodia y las acciones que se realicen a través de los activos informáticos asignados. Por lo tanto, es importante que permanezca en el sitio de trabajo cuando se realice cualquier mantenimiento o actualización a los activos de información.

2.5.13. POLÍTICA ESPECÍFICA DE COPIAS DE RESPALDO DE INFORMACIÓN

OBJETIVO

Garantizar la gestión, realización, administración y custodia de las copias de respaldo, con el fin de preservar las características de seguridad de la información en el Instituto Distrital de Protección y Bienestar Animal - IDPYBA.


ALCANCE

La presente política debe ser cumplida por los servidores públicos y terceros que realicen la gestión de las copias de respaldo (usuarios, Bases de Datos, Aplicativos, Configuraciones, correo, sistemas de información y replicación de datos entre otros) del Instituto Distrital de Protección y Bienestar Animal - IDPYBA.

POLÍTICA

La información necesaria para el cumplimiento de los objetivos estratégicos del Instituto Distrital de Protección y Bienestar Animal – IDPYBA, deberá estar respaldada y ser tratada conforme a los niveles de clasificación de la información y riesgos asociados, de acuerdo con los lineamientos legales, técnicos y administrativos establecidos por la entidad.

Las copias de respaldo serán realizadas conforme al procedimiento definido por el Instituto Distrital de Protección y Bienestar Animal – IDPYBA y estas serán almacenadas en áreas seguras, para garantizar el acceso no autorizado y la integridad y seguridad de estas.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>ALCALDÍA DE PROTECCIÓN Y BIENESTAR ANIMAL</small>	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	


RESPONSABILIDADES

- Se deben realizar copias de respaldo a los sistemas de información, a la información, las aplicaciones y las configuraciones de servidores ya sean éstos virtuales físicos y poner a prueba regularmente las copias realizadas.
- De acuerdo con las necesidades de las áreas o procesos se deben definir los intervalos de tiempo en los que se realizarán las copias de respaldo de información, así como la verificación de estas en compañía del propietario o responsable de la información a la que se le realizó la copia de respaldo.
- Teniendo en cuenta los tiempos estipulados en las tablas de retención documental, las definiciones de conservación de la información y los requisitos legales se deben retener y proteger las copias de respaldo.
- Las copias de respaldo y sus pruebas de restauración deben ser documentadas con el fin de garantizar las pruebas de ejecución.
- Las copias de respaldo deben ser almacenadas en lugares remotos y a una distancia prudente que permitan mitigar los riesgos de pérdida de información en el caso de eventos que afecten las instalaciones del IDPYBA.
- Se debe garantizar la protección física de las copias de respaldo, así como de los medios en los que se realizan estas copias.
- Las copias de respaldo que contengan información de carácter pública reservada o pública clasificada deberán ser protegidas por medio de cifrado.
- Las copias de respaldo de sistemas y servicios deberán ser probadas con mayor regularidad con el fin de asegurarse que cumplen con los requisitos de los planes de contingencia y continuidad de la operación, para los casos de sistemas y servicios críticos del Instituto Distrital de Protección y Bienestar Animal – IDPYBA, lo dispuesto para las copias de respaldo debe abarcar toda la información de sus sistemas, aplicaciones y datos necesarios para recuperar la operación de forma completa en caso de desastre.

2.5.14. POLÍTICA ESPECÍFICA DE TRANSFERENCIA O INTERCAMBIO DE INFORMACIÓN

OBJETIVO

Salvaguardar las características de seguridad de los activos de información del Instituto Distrital de Protección y Bienestar Animal – IDPYBA, durante su transferencia a nivel interna y externa.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. AMARILLA INSTITUTO LOCAL DE PROTECCIÓN Y BIENESTAR ANIMAL	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

ALCANCE

La política aquí descrita debe ser adoptada por todos los servidores públicos y terceras partes que realicen transferencia de información de forma interna o externa en el desempeño de sus funciones.

POLÍTICA

El Instituto Distrital de Protección y Bienestar Animal – IDPYBA, garantiza la transmisión o transferencia de la información, de acuerdo con los niveles de clasificación y las políticas de seguridad de la información de la entidad.

Para el intercambio de información con otras organizaciones o partes externas se establecerán contratos o acuerdos externos, en los cuales se determinen los controles frente a la transmisión o transferencia y tratamiento, teniendo en cuenta los niveles de clasificación de la información. De igual manera, se firmarán acuerdos de confidencialidad que garanticen la protección de la información durante y después del tiempo de ejecución de las actividades establecidas.

RESPONSABILIDADES

- Se debe definir con cada proceso y área la información que requieren transferir como parte del ejercicio y ejecución de sus responsabilidades dentro del IDPYBA y determinar los mecanismos de actualización de esta información. En caso de eliminar privilegios de transferencia, crear nuevos privilegios para la transferencia y determinar los requisitos legales o de temporalidad en la transferencia de la información.
- Se debe contar con mecanismos tecnológicos que permitan proteger la información que se transfiere contra cualquier tipo de interceptación, copiado, modificación, enrutado y destrucción.
- Por medio del uso de aplicaciones o de arquitectura segura que permita detectar el intento de instrucción o ejecución de software malicioso se debe proteger la información que se transfiere o comparte con terceros.
- Los usuarios deben evitar dejar mensajes o información confidencial en mensajes de voz configurados en buzones empresariales, máquinas contestadoras o teléfonos celulares, esto con el fin de evitar que personas no autorizadas puedan tener acceso a esta información ya sea por escuchas mal intencionadas o errores en la marcación.
- Se debe sensibilizar a los servidores públicos, contratistas o terceras partes que presten servicios a la entidad sobre conversaciones confidenciales en lugares públicos o mediante canales de comunicación no seguros.
- Se debe contar con acuerdos de transferencia de la información ya sea con empresas prestadoras de servicio de mensajería electrónica o física, donde se especifiquen las responsabilidades del acceso a la información no autorizado o divulgación de esta, así como la reserva de la información a la que pueden tener acceso por la prestación de sus servicios.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>ALCALDÍA DE PROTECCIÓN Y BIENESTAR ANIMAL</small>	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

- La información que viaja a través de la mensajería electrónica debe ser protegida contra el acceso no autorizado, modificación o posible denegación del servicio de forma proporcional al esquema de clasificación de la información adoptado por el Instituto Distrital de Protección y Bienestar Animal - IDPYBA.
- Se debe garantizar la Anonimización de la información de carácter reservado o confidencial al momento de compartir el contenido de un activo de información Con cualquier entidad o persona.
- Se deben definir los requisitos de uso de firmas electrónicas para garantizar el no repudio de la información transmitida o recibida a través de medios de mensajería electrónica.
- Para la transferencia de información electrónica, el Equipo de trabajo de Gestión Tecnológica en coordinación con El Oficial de Seguridad de la Información, establecerán los canales de comunicación que brinden niveles de seguridad adecuados para la transferencia de información, adicionalmente, se tendrán presentes los riesgos de seguridad, así como los niveles de clasificación de la información antes del envío de esta.
- El intercambio de la información se llevará a cabo según los acuerdos establecidos, los cuales deben tener definido como mínimo: las responsabilidades y procedimientos para la transferencia de información que permita garantizar la trazabilidad y no repudio, el responsable y proceso a seguir en caso de presentarse un incidente de seguridad y los niveles de clasificación de la información a ser intercambiada y tratada por las partes.
- Se deben establecer acuerdos de confidencialidad y no divulgación con los terceras partes ya sean estos públicos, privados de naturaleza jurídica o personal que puedan acceder a la información del IDPYBA y puedan de forma directa o indirecta transferir o compartir esta información.



2.5.15. POLÍTICA ESPECÍFICA DE DESARROLLO SOFTWARE SEGURO

OBJETIVO

Definir los lineamientos generales para el desarrollo o adquisición de software a la medida en el Instituto Distrital de Protección y Bienestar Animal - IDPYBA, estableciendo los controles de seguridad adecuados para su protección.

ALCANCE

La política aquí descrita debe ser adoptada por los servidores públicos y terceras partes del Instituto Distrital de Protección y Bienestar Animal – IDPYBA, que efectúen actividades relacionadas con el desarrollo o adquisición de software a la medida.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>ALCALDÍA MAYOR DE BOGOTÁ D.C. - INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL - Secretaría Técnica</small>	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

POLÍTICA

Los contratos de desarrollo de software se realizarán conforme a la Ley 23 de 1982, las obras literarias (dentro de las que se encuentra el software), artísticas y científicas creadas por servidores públicos y particulares contratados mediante prestación de servicios por la Entidad, desarrolladas en cumplimiento de las obligaciones constitucionales y legales del cargo que fungen y/o de las que se establezcan en el contrato, son de propiedad del Instituto Distrital de Protección y Bienestar Animal - IDPYBA, en virtud de la presunción legal de cesión de derechos patrimoniales vigente en el ordenamiento nacional. Lo que significa que, los servidores públicos preservan los derechos morales como autores de las obras, aunque no puedan utilizarlos para explotarlos en detrimento de los derechos y deberes del Instituto Distrital de Protección y Bienestar Animal - IDPYBA.

Con el fin de que todas las licencias sobre software adquiridas por del Instituto Distrital de Protección y Bienestar Animal – IDPYBA, gocen de un medio de prueba y publicidad legítimo, seguro y que garantice la autenticidad de la titularidad de estas, del Instituto Distrital de Protección y Bienestar Animal – IDPYBA, registrará los actos y contratos suscritos al respecto.

Dentro del ambiente de pruebas, no se permite el uso de información sensible de producción, en caso de que sea estrictamente necesario, se deberá realizar el ofuscamiento de los datos o enmascaramiento de datos para garantizar la protección de la información. Una vez dicha información no sea requerida, la misma deberá eliminarse de manera segura.

En los casos de adquisición de software a la medida, el Instituto Distrital de Protección y Bienestar Animal – IDPYBA, determinará dentro de los contratos definidos con el proveedor, la propiedad de la licencia y los derechos intelectuales de los códigos fuente, así como las condiciones de uso, de la misma manera cualquier desarrollo se le deberá exigir soporte IPv6 nativo en coexistencia con IPv4.


RESPONSABILIDADES

- Antes de iniciar el desarrollo de software, el grupo técnico que lidere el desarrollo del software, el Equipo de trabajo de Gestión Tecnológica y/o el oficial de seguridad de la información, así como las partes interesadas, acordarán una metodología de desarrollo, identificando detalladamente la estructura de trabajo, responsables, cronograma, alcance, requisitos a cumplir, procesos afectados y requerimientos.
- El grupo técnico que lidere el desarrollo del software, el Equipo de trabajo de Gestión Tecnológica junto con el oficial de seguridad de la información, establecerán criterios de aceptación de seguridad para la aprobación del software. La aceptación del software se establecerá a través de los resultados obtenidos de las pruebas planteadas, las cuales tendrán dentro de sus parámetros, la validación de vulnerabilidades, códigos maliciosos, puertas traseras, entre otras.
- Dentro de los requisitos a tener presentes para el desarrollo de software con respecto a la seguridad de la información, es importante determinar: controles para proteger la confidencialidad, disponibilidad e integridad de la información, métodos de autenticación, cifrado de datos, control de roles y privilegios, pistas de auditoría, gestión de sesiones, datos históricos,

 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>ALCALDÍA MAYOR DE BOGOTÁ D.C.</small> <small>PROCESO DE GESTIÓN TECNOLÓGICA</small>	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

manejo apropiado de errores, seguridad en las comunicaciones, codificación segura, mecanismos de protección de datos personales, entre otras.

- Antes, durante y después del desarrollo de software, se deberá efectuar un análisis de riesgos donde se determine el impacto y afectación de la materialización de los riesgos a la entidad. Así mismo, se determinarán los controles de seguridad necesarios para la mitigación de estos.
- El grupo técnico que lidere el desarrollo del software, el Equipo de trabajo de Gestión Tecnológica junto con el oficial de seguridad de la información, deberán llevar a cabo revisiones y auditorías informáticas a los desarrollos realizados, con el fin de validar el cumplimiento de los requisitos de seguridad y calidad definidos.
- El grupo técnico que lidere el desarrollo del software y el responsable del Equipo de trabajo de Gestión Tecnológica verificarán y controlarán las versiones del software desarrollado con los respectivos documentos de soporte. Esto con el adecuado control y funcionamiento en el ciclo de vida de este.
- Los usuarios deberán utilizar diferentes perfiles para el ambiente de desarrollo, de pruebas y de producción; así mismo, se deberá asegurar que cada usuario cuente únicamente con los privilegios necesarios en cada ambiente para el desarrollo de sus funciones.
- Los servidores públicos o terceros que realicen actividades de desarrollo de software no podrán realizar pruebas, instalaciones o desarrollos de hardware o software directamente sobre el entorno de producción, con el fin de evitar problemas de disponibilidad, integridad o confidencialidad de la información, todo esto debe quedar documentado en control de cambios.
- El grupo técnico que lidere el desarrollo del software y el Equipo de trabajo de Gestión Tecnológica, deberán restringir el acceso a los compiladores, editores, utilidades de los sistemas y otras herramientas de desarrollo desde los sistemas del ambiente de producción y a cualquier usuario que no lo requiera para el desarrollo de su labor.
- El grupo técnico que lidere el desarrollo del software y el Equipo de trabajo de Gestión Tecnológica deberán verificar periódicamente las versiones instaladas tanto en ambiente de pruebas como en producción, con el fin de que las mismas correspondan a las últimas versiones aprobadas.
- El grupo técnico que lidere el desarrollo, prueba y producción, deberá contar con auditoría sobre las bases de datos, diferentes credenciales de acceso y separación de roles, con el fin de evitar la pérdida de confidencialidad de estas.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. INSTRUMENTO DE POLÍTICAS Y BIENESTAR ANIMAL	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ	INSTRUMENTO DE POLÍTICAS Y BIENESTAR ANIMAL
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA			
	Código: PA04-PL01	Versión: 2.0		

2.5.16. POLÍTICA ESPECÍFICA PARA RELACIONES CON PROVEEDORES

OBJETIVO

Establecer los lineamientos generales para preservar los niveles de seguridad y privacidad de la información y activos de información permitidos para gestión con proveedores.

ALCANCE

La política aquí descrita debe ser adoptada por todos los servidores públicos y terceras partes del Instituto Distrital de Protección y Bienestar Animal – IDPYBA, que tengan relación con proveedores y que éstos accedan a activos de información propiedad de la entidad.

POLÍTICA

El Instituto Distrital de Protección y Bienestar Animal - IDPYBA, suministrará los procedimientos y controles adecuados para la preservación de las características de seguridad de los activos de información que van a ser consultado y/o gestionados por los proveedores que tiene vinculación con la entidad.

Los servidores públicos responsables de los activos de información del Instituto Distrital de Protección y Bienestar Animal - IDPYBA, en ningún caso otorgarán acceso a los activos y/o áreas críticas de la entidad a los proveedores, hasta no haber realizado la formalización de la relación contractual conforme lo establecido en el Manual de Contratación, la firma de los acuerdos de intercambio de información y la identificación y evaluación de los riesgos.

Los acuerdos de intercambio de información con proveedores estarán encaminados al cumplimiento de las regulaciones legales, propiedad intelectual y protección de datos personales. Así mismo establecerán las consideraciones de seguridad y reserva de la información y las responsabilidades por el mal uso o divulgación de esta.

RESPONSABILIDADES

- Se deben identificar y documentar los diferentes tipos de proveedores con los que la entidad cuenta actualmente por ejemplo proveedores en servicios de tecnología, almacenamiento, mensajería, servicios de aseo y vigilancia, entre otros a quienes el Instituto Distrital de Protección y Bienestar Animal – IDPYBA, les permitirá acceso a sus instalaciones y/o a su información.
- El responsable del activo de información antes de otorgar los accesos a los proveedores deberá validar que se encuentren firmados y formalizados los acuerdos de confidencialidad y/o el acto administrativo que determine los fines de uso, las condiciones de tratamiento de la información, así como la debida definición de los controles requeridos para preservar las características de seguridad de los activos de información.
- Los propietarios de la información que pretendan intercambiar la misma, son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de esta; por

	PROCESO GESTIÓN TECNOLÓGICA		
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	


su parte, los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad de acuerdo con la reglamentación vigente y los lineamientos determinados por el Instituto Distrital de Protección y Bienestar Animal - IDPYBA.

- Se deben identificar y definir los requisitos mínimos de seguridad de la información para cada uno de los tipos de acceso que puedan tener los proveedores con base en las necesidades y requisitos de la entidad y su perfil de riesgo frente al acceso a la información de la entidad.
- De acuerdo con los servicios y obligaciones que el proveedor contraiga con el Instituto Distrital de Protección y Bienestar Animal – IDPYBA, se deberán firmar acuerdos de confidencialidad que incluyan al personal contratado por el proveedor. Donde se incluya el manejo de incidentes y contingencias asociadas al acceso que el proveedor pueda tener incluidas las responsabilidades de la entidad.
- Se debe identificar los riesgos de seguridad por la gestión de transacciones el uso de instalaciones de procesamiento de información y cualquier otro mecanismo de administración, acceso o almacenamiento Por parte del proveedor.
- Se deben definir los acuerdos de nivel en la prestación del servicio y la prioridad que estos deben tener de acuerdo con los riesgos de disponibilidad identificados por el Instituto Distrital de Protección y Bienestar Animal - IDPYBA, con el fin de mantener la continuidad de la operación.
- Para los servicios esenciales contratados con proveedores se debe contar con una planeación de adquisición de servicios que mantenga la continuidad de este, sin que se presenten espacios de tiempo en los que estos servicios no se presten a la entidad.
- En caso de presentarse y/o identificar una amenaza que pueda llegar a afectar la seguridad de la información, se deberá reportar al Oficial de Seguridad de la Información y/o el Equipo de trabajo de Gestión Tecnológica a través de los canales de comunicación establecidos por la entidad.

2.5.17. POLÍTICA ESPECÍFICA DE DERECHOS DE USO DE PROPIEDAD INTELECTUAL

OBJETIVO

Efectuar el cumplimiento de las disposiciones normativas y contractuales con el fin de evitar sanciones administrativas al Instituto Distrital de Protección y Bienestar Animal – IDPYBA y/o a funcionarios y colaboradores que incurran en responsabilidad civil o penal como resultado de su incumplimiento.

	PROCESO GESTIÓN TECNOLÓGICA		 
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

ALCANCE

Esta Política se aplica a todo el personal del Instituto Distrital de Protección y Bienestar Animal - IDPYBA. asimismo, se aplica a los activos de información del Instituto Distrital de Protección y Bienestar Animal – IDPYBA

POLÍTICA

El Instituto Distrital de Protección y Bienestar Animal – IDPYBA, será titular de los derechos de Propiedad Intelectual que recaigan sobre las obras e invenciones producidas en el ejercicio de su función, y en las cuales hubieren participado trabajadores, que desempeñen cargos o actividades inventivas o creativas. El software es considerado una obra intelectual que goza de la protección de la Ley 23 de Propiedad Intelectual.

La explotación de la propiedad intelectual sobre los programas de software incluirá, entre otras formas, los contratos de licencia para su uso o reproducción, los productos de software se suministran normalmente bajo acuerdos de licencia que limiten el uso de los productos al equipo específico y su copia a la creación de copias de resguardo solamente.

Se garantizará la protección de la propiedad intelectual de software de acuerdo con el marco legal de productos de información y de software, así como el mantenimiento de las licencias.

El Instituto Distrital de Protección y Bienestar Animal – IDPYBA, conservará pruebas y evidencias de propiedad de licencias, discos maestros, manuales, entre otros, de igual manera se implementarán controles para evitar el exceso del número máximo permitido de usuarios y se verificará en los equipos propiedad del IDPYBA o estén bajo contrato de arrendamiento, se instalen productos con licencia y software autorizado.

RESPONSABILIDADES

- El Instituto Distrital de Protección y Bienestar Animal - IDPYBAD, será titular de los derechos de Propiedad Intelectual que recaigan sobre las obras e invenciones producidas en el ejercicio de su función, y en las cuales hubieren participado trabajadores, que desempeñen cargos o actividades inventivas o creativas. El software es considerado una obra intelectual que goza de la protección de la Ley 23 de Propiedad Intelectual.
- La explotación de la propiedad intelectual puede definirse en ARTÍCULO 2º.- Adicionado por Art. 67, Ley 44 de 1993.:
"1. Los derechos de autor recaen sobre las obras científicas literarias y artísticas las cuales se comprenden todas las creaciones del espíritu en el campo científico, literario y artístico, cualquiera que sea el modo o forma de expresión y cualquiera que sea su destinación , tales como: los libros, folletos y otros escritos; las conferencias, alocuciones, sermones y otras obras de la misma naturaleza; las obras dramáticas o dramático-musicales; las obras coreográficas y las pantomimas; las composiciones musicales con letra o sin ella; las obras cinematográficas, a las cuales se asimilan las obras expresadas por procedimiento análogo a la cinematografía,

	PROCESO GESTIÓN TECNOLÓGICA		
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

inclusive los videogramas; las obras de dibujo, pintura, arquitectura, escultura, grabado, litografía; las obras fotográficas o las cuales se asimilan las expresadas por procedimiento análogo a la fotografía a; las obras de arte aplicadas; las ilustraciones, mapas, planos croquis y obras plásticas relativas a la geografía, a la topografía, a la arquitectura o a las ciencias y, en fin, toda producción del dominio científico, literario o artístico que pueda reproducirse, o definirse por cualquier forma de impresión o de reproducción, por fonografía, radiotelefonía o cualquier otro medio conocido o por conocer (ARTÍCULO 2º.- Adicionado por Art. 67, Ley 44 de 1993.).



2. los programas de software incluirán, entre otras formas, los contratos de licencia para su uso o reproducción, los productos de software se suministran normalmente bajo acuerdos de licencia que limiten el uso de los productos al equipo específico y su copia a la creación de copias de resguardo solamente.”

- Se garantizará la protección de la propiedad intelectual de software de acuerdo con el marco legal de productos de información y de software, así como el mantenimiento de las licencias.
- EL IDPYBA conservará pruebas y evidencias de propiedad de licencias, discos maestros, manuales, entre otros, asimismo se implementarán controles para evitar el exceso del número máximo permitido de usuarios y se verificará que en los equipos para funcionamiento de la entidad se instalen productos con licencia y software autorizado.
- El jefe o coordinador del equipo de trabajo de Gestión Tecnológica y la oficina Jurídica analizarán los términos y condiciones de las licencias y definirán los procedimientos correspondientes para salvaguardar la propiedad intelectual.
- La jefe o equipo de trabajo de Gestión Tecnológica mantendrá control sobre las licencias que sean instaladas en los equipos de cómputo, estaciones de trabajo y servidores de la entidad.
- El equipo de trabajo de Gestión Tecnológica verificará el tipo de software y determinará la viabilidad para su uso en los activos de información.

2.5.18. POLÍTICA ESPECÍFICA PARA CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

OBJETIVO

- Establecer los niveles de criticidad, sensibilidad y reserva de la información del Instituto Distrital de Protección y Bienestar Animal - IDPYBA, para garantizar la confidencialidad, integridad y disponibilidad de los activos de información del IDPYBA. Igualmente, clasificar la información para establecer su sensibilidad y criticidad de acuerdo con la confidencialidad, integridad y disponibilidad, garantizando que los activos de información reciban un adecuado nivel de protección.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. MAYORÍA PÁBULO LOPEZ DE FIGUEROA BERNARDO FERRAZ	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ	INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA			
	Código: PA04-PL01	Versión: 2.0		

ALCANCE

Se aplica a todos los activos de información identificados en el Instituto Distrital de Protección y Bienestar Animal - IDPYBA. La identificación de los activos de información debe tener presente, la información, sistemas de información, software, hardware, personas o lugares para la operación o aquella información estratégica requerida para lograr los objetivos misionales de la entidad. Dentro de los activos de información a identificar se pueden encontrar:

- Portal web del IDPYBA y los contenidos que alojados en los mismos;
- La información que se transmite a través de los diferentes servicios del IDPYBA;
- Los servicios de interacción con la comunidad, servicios de transacciones en línea, servicios de recaudo o registro de información, entre otros.
- Los sistemas de información que apoyan los servicios del IDPYBA;
- La infraestructura tecnológica que soporta los diferentes servicios, información y sistemas de información (hardware, software, comunicaciones, bases de datos, etc.) del IDPYBA;
- La infraestructura tecnológica de seguridad implementada por el IDPYBA;
- Los documentos físicos requeridos para efectuar el desarrollo de las actividades operaciones para el cumplimiento de los objetivos misionales del IDPYBA.
- Los activos de información a los que se refiere el Decreto 103 de 2015 que reglamenta la Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información).

POLÍTICA


El Instituto Distrital de Protección y Bienestar Animal – IDPYBA, garantiza la identificación de los activos de información precisando el nivel de criticidad, sensibilidad y establece los controles idóneos para la preservación de las características de su seguridad (Confidencialidad, Integridad y Disponibilidad).

RESPONSABILIDADES

Los responsables de la información como: Jefes de Área, Subdirectores (as), asesores (as) son los encargados de clasificarla, de acuerdo con el nivel de sensibilidad y criticidad; mantener actualizada la clasificación efectuada, y de definir los niveles y encargados que podrán tener permisos de acceso a la información.

El custodio de la información se encarga de mantener las medidas de protección establecidas por los responsables.

Cada responsable de la Información supervisará el proceso de clasificación y rotulado de información que se establezca para el área sea cumplido de acuerdo con lo establecido en la presente Política.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. AMBIENTE HUMANISMO SUSTENTABILIDAD</p>	PROCESO GESTIÓN TECNOLÓGICA		 <p>BOGOTÁ INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL</p>
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

2.5.19. POLÍTICA DE USO DE RED PRIVADA VIRTUAL (VPN)

OBJETIVO

Determinar los lineamientos generales que se deben tener en cuenta para preservar las características de seguridad de la información cuando se realizan conexiones por medio de redes privadas virtuales conocidas como VPN (por sus siglas en inglés: Virtual Private Network).

ALCANCE

Aplica a todas las formas de uso de redes privadas virtuales conocidas como VPN para el Instituto Distrital de Protección y Bienestar Animal – IDPYBA.

POLÍTICA

El Instituto Distrital de Protección y Bienestar Animal – IDPYBA establecerá el acceso por VPN con los protocolos determinados y acogiendo los siguientes controles:

- Uso de encriptación acorde a la criticidad del acceso, y acorde a lo establecido en las políticas relacionadas.
- Establecer niveles de servicio que contemplen los tiempos de mantenimientos y Backup.
- Registrar las acciones de inicio y final de conexión con los datos correspondientes al usuario, dirección IP.
- Disponer de estadísticas periódicas de utilización por usuario.

RESPONSABILIDADES

El Oficial de Seguridad de la Información y/o el responsable del Equipo de trabajo de Gestión Tecnológica estarán a cargo de la definición de normas y procedimientos de uso de VPN.

El personal responsable del Equipo de trabajo de Gestión Tecnológica implementará los procedimientos para la conexión y trabajo con la VPN.

El Oficial de Seguridad de la Información y/o el responsable del equipo de trabajo de Gestión Tecnológica antes de otorgar los accesos remotos por VPN, deberá validar que tenga previa autorización del jefe de área donde se determine los fines de uso, las condiciones para el uso de la VPN, así como la debida definición de los controles necesarios para preservar las características de seguridad de los activos de información.

2.5.20. POLÍTICA DE CONTROL DE CAMBIOS

OBJETIVO

Instituir los lineamientos para salvaguardar los niveles de seguridad de la información (confidencialidad, integridad y disponibilidad) de los recursos de procesamiento de información, comunicaciones, y

 ALCALDÍA MAYOR DE BOGOTÁ D.C. ALTERNATIVAS SOLUCIÓN LIDERAZGO PARTICIPACIÓN Bogotá Princesa	PROCESO GESTIÓN TECNOLÓGICA		 BOGOTÁ INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL
	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDPYBA		
	Código: PA04-PL01	Versión: 2.0	

servicios que trabajen con información sensible para el Instituto Distrital de Protección y Bienestar Animal – IDPYBA.

ALCANCE

Aplica a funcionarios del Equipo Gestión Tecnológica, Gestión Documental, Terceras Partes y sistemas de información, por medio de normas, procedimientos, documentación y plataformas técnicas del Instituto Distrital de Protección y Bienestar Animal – IDPYBA.

Los casos en los que no fuera posible la aplicación de la presente política se considerarán como excepciones.

POLÍTICA

Los servicios prestados por terceras partes se deben gestionar de acuerdo con una evaluación de riesgos de seguridad Digital, para mejorar el servicio, implementar nuevas tecnologías, cambios de proveedor y otros.

Se controlará que los cambios en los recursos de procesamiento y de comunicaciones no afecten la seguridad de estos, ni de la información que soportan. Se evaluará el posible impacto operativo de los cambios previstos y se verificará su correcto desarrollo. Todo cambio deberá ser evaluado anticipadamente en aspectos técnicos y de seguridad.

La modificación, actualización o eliminación de los datos operativos serán realizadas a través de los sistemas que procesan dichos datos y de acuerdo con el esquema de control de accesos implementado en los mismos.

Los servidores propietarios y/o encargados de los recursos de procesamiento y de comunicaciones, deberán realizar las solicitudes de cambio por medio de la mesa de ayuda y de acuerdo con los procedimientos, formatos, guías, manuales establecidos para tal fin.

RESPONSABILIDADES

- El(la) Subsector(a) de Gestión Corporativa, el Oficial de Seguridad de la Información y/o el responsable del Equipo de trabajo de Gestión Tecnológica definen y aprueban las normas y procedimientos para la gestión del cambio, el personal responsable del equipo de Gestión Tecnológica y los responsables de los activos implementan los cambios.
- Los usuarios y terceras partes deberán cumplir con los lineamientos establecidos en esta política.
- Los servidores públicos, contratistas y/o terceras partes encargados de los recursos de procesamiento y de comunicaciones, deberán velar porque la información sea almacenada conforme a los lineamientos establecidos, antes de realizarse algún cambio que pueda afectar la información contenida en los recursos descritos anteriormente y de acuerdo con las necesidades del Instituto Distrital de Protección y Bienestar Animal – IDPYBA.