PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2022

CONTROL DE CAMBIOS

NO. DE ACTA DE APROBACIÓN	FECHA	VERSIÓN	DESCRIPCIÓN
1	31-12-2022	1.0	Adopción mediante Acta Comité de Gestión y Desempeño

AUTORIZACIONES

ELABORÓ:	REVISÓ	APROBÓ
ÁREA TÉCNICA	**OFICINA ASESORA DE PLANEACIÓN**	**LIDER DEL PROCESO**
Nombre: Germán González Rozo José Alfonso Pérez Contreras	**Nombre:** Loren Guisell Díaz Jimenez J Sebastián Moreno S	**Nombre:** Gotardo Antonio Yáñez Álvarez
Firma: Germán GonzáLez Rozo	**Firma:** LorenDiaz	**Firma:**
Cargo: Profesionales Contratistas Tecnología	**Cargo:** Profesionales Oficina Asesora de Planeación	**Cargo:** Subdirector Gestión Corporativa

TABLA CONTENIDO

DERECHOS DE AUTOR

CONTEXTUALIZACIÓN

Con el ánimo de asegurar la integridad, disponibilidad, confidencialidad y privacidad de la información de sus procesos, el Instituto Distrital de Protección y Bienestar Animal, está en el proceso de transformación e implementación del Plan de Seguridad y Privacidad de la información (MSPI), así como el Sistema de Gestión y Seguridad de la Información (SGSI), el cual expresa el compromiso de la alta dirección con la seguridad de la información, así como, la identificación de las reglas y procedimientos que cada usuario que accede o usa los recursos tecnológicos de la entidad y debe conocer para preservar los sistemas y la información que usan.

INTRODUCCIÓN

El Instituto Distrital de Protección y Bienestar Animal, reconoce la importancia y el valor de la información con respecto al funcionamiento eficiente y efectivo de la institución, entendiendo que la información no es sólo crítica para el éxito de la organización, sino estratégica para su supervivencia a largo plazo, por esta razón, se establece el siguiente plan que regula el manejo de la información en el IDPYBA, orientada a definir las medidas que resguarden la confidencialidad, integridad y disponibilidad de la información propia del Instituto Distrital de Protección y Bienestar Animal el acceso a la información en conformidad con la norma ISO 27001: 2013.

Es por ello que se desea mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información (SGSI) que permita lograr niveles adecuados de seguridad para todos los activos de información institucional considerados relevantes, de manera tal de garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados, como parte del proceso de revisión estratégica, o cuando se identifiquen cambios en la entidad, en su estructura, sus objetivos o en alguna condición que la afecte, para asegurar que dichas políticas sigan siendo adecuadas y ajustadas a los requerimientos de la Entidad.

1. OBJETIVO

Orientar y dar lineamientos de seguridad de la información frente al acceso a los activos de información del Instituto Distrital de Protección y Bienestar Animal, entidad adscrita al Sector Ambiente de Bogotá D.C. con el fin de garantizar que los riesgos de seguridad de la información identificados, valorados sean administrados de una forma estructurada, eficiente y adaptada a los cambios que se produzcan en el entorno de las tecnologías de información, velando por principios de Integridad, confidencialidad y disponibilidad de los activos de información a través de mejora continua.

2. OBJETIVOS ESPECÍFICOS

- Establecer para todo el personal del IDPYBA la necesidad de la seguridad de la información y promover la comprensión de sus responsabilidades individuales, mediante campañas de sensibilización sobre el manejo de esta. Para ello se buscará promover y programar acciones continuas de mejoramiento de niveles de cultura en seguridad de la información, buscando lograr una concientización de los funcionarios mencionados anteriormente, minimizando la ocurrencia de incidentes de seguridad de información.
- Determinar frente al acceso a los activos de información y adoptar las medidas esenciales de seguridad de la información necesarias, para proteger al IDPYBA de amenazas que podrían afectar en alguna medida la confidencialidad, integridad y disponibilidad de la información, ocasionando pérdida o mal uso de los activos de

información. Para ello se realizará la valoración y tratamiento de Riesgos de seguridad de la información definido en el Plan de riesgos 2022.

- Cumplir con los requisitos legales vigentes aplicables a la naturaleza de la Entidad en materia de Seguridad de la Información. Diligenciando y desarrollando el Documento de Autodiagnóstico con herramienta MINTIC de Gobierno Digital de acuerdo con los de la Alta consejería para las TICs del Distrito y atender los requerimientos de auditorías.
- Identificar mediante una adecuada evaluación del riesgo, el valor de la información, así como las vulnerabilidades y las amenazas a las que están expuestos los activos de información, como lo siguiere el plan de riesgos.
- Minimizar, gestionar y dar tratamiento a los riesgos de seguridad de la información, para que sean conocidos y según su impacto sean asumidos, transferidos, minimizados y/o eliminados de forma eficiente y adaptada a los cambios que se produzcan en la entidad, el entorno y la tecnología.
- Continuar con el enriquecimiento de políticas y procedimientos específicos a la política de seguridad y privacidad de la información actualizada, con el fin de asegurar su vigencia y eficacia.

3. ALCANCE

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

Así también, tendrá como referencia el Modelo de Seguridad y Privacidad de la información (MSPI), basado en el estándar ISO 27001: 2013, y con aplicación a referencia los controles definidos en cada uno de sus dominios.

4. GLOSARIO

- **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) que tenga valor para la organización.
- **Activo de Información:** en relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Activo de información:** conocimiento o datos que tienen valor para el individuo u organización.
- **Acuerdo de Confidencialidad**: documento donde se plasma el compromiso para mantener la confidencialidad de la información de la Entidad, a no divulgar, usar o explotar

la información confidencial a la que tengan acceso en virtud del desarrollo de las funciones desempeñadas en la Entidad.

- **Autenticación:** asegurar que una característica declarada de una Entidad es correcta.
- **Autenticidad**: Propiedad se refiere a que la información provenga de una fuente fidedigna, es decir, que el emisor sea realmente quien envía la información
- **Aceptación de riesgo**: decisión de asumir un riesgo.
- **Adaptabilidad**: define los eventos y bajo qué criterios un sistema debe poder ser monitoreado y revisado para su control posterior.
- **Amenazas:** causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.
- **Análisis de Riesgo**: proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo aceptable.
- **Auditoria:** proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría.
- **Autenticidad:** busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidad.
- **Cifrado:** es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información. Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
- **Ciberseguridad:** capacidad del Estado para minimizar el nivel de riesgo aceptable al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.
- **Confiabilidad de la Información:** garantiza que la fuente de la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- **Confidencialidad:** propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Las políticas:** los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo aceptado.
- **Control:** control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. Declaración de aplicabilidad: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo particular
- **Custodio del activo de información**: es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados. Derechos de Autor: es un conjunto.
- **Dato personal:** es cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

- **Dato público:** es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- **Datos sensibles**: se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.
- **Confidencialidad**: propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- **Dirección IP:** número que identifica, de manera lógica y jerárquica en una red informática a un dispositivo (computadora, tableta, portátil, Smartphone).
- **Disponibilidad**: propiedad de ser accesible y utilizable a demanda por una Entidad autorizada.
- **Incidente de seguridad:** se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información.
- **Información**: es un activo esencial para el negocio de una organización y por consiguiente necesita ser debidamente protegida. La información puede ser almacenada en muchas formas, incluyendo formato digital (por ejemplo, ficheros almacenados en medios electrónicos u ópticos), formato físico (por ejemplo, en papel), así como la información intangible que forma parte del conocimiento de los empleados. La información puede ser transmitida por diferentes medios incluyendo: mensajería, comunicación electrónica o verbal. Independientemente del formato o del medio por el cual se transmite la información, es necesaria siempre una protección adecuada.
- **Integridad**: propiedad de exactitud y completitud de la información.
- **Medios removibles:** dispositivos tecnológicos de almacenamiento de información diseñados para ser extraídos del computador.
- **Mejora Continua:** el objetivo de la mejora continua de un SGSI es aumentar la probabilidad de lograr los objetivos relativos a la preservación de la confidencialidad, disponibilidad e integridad de la información. El foco de la mejora continua es buscar oportunidades para la mejora y no asumir que las actividades de gestión existentes son suficientemente buenas o tan buenas como podrían ser.
- **Política:** declaración de alto nivel que describe la posición de la Entidad sobre un tema específico.
- **Seguridad de la información**: asegura la confidencialidad, integridad y disponibilidad de la información. La seguridad de la Información implica la aplicación y gestión de controles apropiados que involucran la consideración de un amplio rango de amenazas, con el

objetivo de asegurar el éxito empresarial sostenido, así como su continuidad, y minimizar las consecuencias de los incidentes de la seguridad de la información.

- **Vulnerabilidad:** debilidad de un activo o control que pueda ser explotada por una a más amenazas.

5. ESTRATEGIA

Los activos de información del Instituto Distrital de Protección y Bienestar Animal han sido identificados y clasificados, para lo cual se considera dentro del presente plan, realizar la actualización y revisión al interno del Instituto para establecer su grado de criticidad. Así mismo, deben tener un propietario designado, quien tiene la responsabilidad de garantizar que se clasifican adecuadamente, revisar las restricciones de acceso y la seguridad del activo.

Estos activos se pueden categorizar según la siguiente clasificación:

Confidencia: es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado.

Privada: es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos

Pública: información conocida y utilizada por cualquier persona., que un sujeto obligado genere, obtenga, adquiera, o controle.

Con el fin de propender por una cultura sólida en seguridad y privacidad de la información, el Instituto Distrital de Protección y Bienestar Animal definirá y ejecutará periódicamente programas de sensibilización y capacitación en seguridad de la información de acuerdo con las necesidades identificadas.

6. POLITICAS

El instituto Distrital de Protección y Bienestar Animal establece una política general la cual se diseña desde la Subdirección de Gestión Corporativa (SGC), área encargada de la seguridad de la información TIC y varias políticas generales en cumplimiento con el MSPI, teniendo en cuenta los siguientes criterios:

- **Creación de políticas**

El instituto Distrital de Protección y Bienestar Animal deben ser creadas por el área encargada de la seguridad y privacidad de la información y respaldadas por la Alta Dirección de la entidad con la asesoría de las áreas técnicas responsables de los temas asociados a las mismas. Estas políticas deben definir claramente roles y responsabilidades en el SGC y con los propietarios de la información y responsables de riesgos.

- **Aprobación de políticas**

El instituto Distrital de Protección y Bienestar Animal, las políticas relacionadas con la seguridad y privacidad de la información deben ser aprobadas por el Comité Institucional de Gestión y Desempeño. Con base en las recomendaciones de la Subdirección de Gestión Corporativa, la Oficina Asesora de Planeación, Asesor de Control Interno y demás interesados en la seguridad y privacidad de la información.

- **Actualización de políticas**

Las políticas de seguridad y privacidad de la información se deben revisar periódicamente o si ocurren cambios significativos. Cualquier requerimiento de modificación, cambio o actualización de las políticas de seguridad y privacidad de la información, debe ser dirigida a la Comité Institucional de Gestión y Desempeño con base en las recomendaciones del área de la seguridad y privacidad de la información.

- **Nivel de cumplimiento de la política**

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

Participar en las auditorías internas y externas de la norma ISO 27001:2013

7. LINEAMIENTOS GENERALES PARA LAS POLÍTICAS ESPECIFICAS Y PROTOCOLOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Seguridad de la Información:

La 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, entidad adscrita al Sector Ambiente de Bogotá D.C. (IDPYBA), conforme a los controles de seguridad y privacidad determinados en la entidad.

Procedimientos:

Los procedimientos lineamientos e instructivos, constituyen una base importante para la preservación de la seguridad y privacidad de la información. Se han diseñado procedimientos, lineamientos e instructivos, que cubren las políticas de seguridad y privacidad de la información. A continuación, se indican:

- Política de Seguridad de la Información
- Política de Riesgos + Seguridad Digital
- Política de seguridad de la información en la gestión de proyectos
- Política de administración de contraseñas

- Política de Control de acceso
- Política de Protección contra Software Malicioso
- Política de Bloqueo de Sesión, Escritorio y Pantalla limpia
- Acuerdo Confidencialidad Reserva Manejo Información

Acuerdo de confidencialidad y Transferencia de Información con terceros

Protección De Datos Personales:

Establecer criterios generales para la recolección, almacenamiento, uso, circulación y supresión de los datos personales y niveles de seguridad y privacidad adecuados en las bases de datos y activos de información que intervengan en el tratamiento de dichos datos, para evitar posibles adulteraciones, pérdidas, consultas, usos o accesos no autorizados.

Gestión De Riesgos:

El objetivo es brindar principios y directrices genéricos para gestionar el riesgo para identificar y establecer controles efectivos que garanticen la confidencialidad, integridad y disponibilidad de la información.

Así mismo, para la evaluación de riesgos en seguridad de la información se ha clasificado sus activos de información por proceso a los cuales se les ha identificado los riesgos teniendo en cuenta que la Entidad debe preservar la Confidencialidad, Integridad y Disponibilidad de la información.

- Acceso no autorizado a la información.
- Divulgación de información sensible.
- Denegación del servicio.
- Daño de la información.
- Ataques externos o internos.
- Pérdida o robo de la información.
- Modificación no autorizada.

8. ALCANCE DE LA ESTRATEGIA DE SEGURIDAD DE INFORMACIÓN

Los contenidos del presenta plan son aplicables a los activos de información de todos los procesos del Instituto Distrital de Protección y Bienestar Animal, consta de las políticas, procedimientos y controles para la preservación de confidencialidad, integridad y disponibilidad de la información, en concordancia con el plan de riesgos y las actividades dentro del Plan para el tratamiento de riesgos 2022.

Por lo anterior, se contempla como fase cero el atender los riesgos identificados en la valoración de riesgos e implementar el plan de tratamiento de riesgos 2022 como se muestra a continuación:

	ACTIVIDAD	FECHA
1.	Revisión de estado de tratamiento y controles de línea base de seguridad	1 TRIMESTRE 2020
2.	Identificación y evaluación de riesgos de seguridad y privacidad de la información	2 TRIMESTRE 2020
3.	Tratamiento y control de riesgos de seguridad y privacidad de la información	3 TRIMESTRE 2020
4.	Monitoreo, planes de mejoramiento	TRIMESTRAL 2020

En paralelo la estrategia contempla el trabajo continuo en Capacitación Concientización en seguridad y privacidad de la información. Lo anterior buscando controlar las acciones que afectan la seguridad de la información y que ponen en riesgo la disponibilidad, confidencialidad e integridad en el Instituto Distrital de Protección y Bienestar Animal, como son:

- Dejar los computadores encendidos en horas no laborables.
- Enviar información clasificada del instituto por correo físico, copia impresa, o electrónica sin la debida autorización y/o sin la utilización de los protocolos establecidos para la divulgación.
- Guardar información clasificada en cualquier dispositivo de almacenamiento que no pertenezca al Instituto.
- Conectar computadores portátiles u otros dispositivos electrónicos personales a la red de datos del Instituto sin la debida autorización.
- Ingresar a la red de datos por cualquier servicio de acceso remoto sin la autorización de la Subdirección de Gestión Corporativa – Grupo de sistemas, y sin la autorización de los propietarios de los activos de información, quienes determinan quienes acceden a la información y con que privilegios.
- Usar servicios de internet en los equipos del instituto, diferente al provisto por la oficina de sistemas.
- Promoción y mantenimiento de actividades personales, o utilización de los recursos tecnológicos del instituto para beneficio personal.
- Permitir que personas ajenas al Instituto ingresen sin previa autorización a las áreas restringidas o donde se procese información digital.

- No clasificar y/o etiquetar la información.
- No guardar bajo llave documentos impresos que contengan información clasificada al terminar la jornada laboral.
- No retirar de forma inmediata todos los documentos con información sensible que envíen las impresoras y dispositivos de copiado.
- Reutilizar papel que contenga información sensible, no borrar la información estricta de tableros o pizarras al finalizar las reuniones de trabajo y no garantizar que no queden documentos o notas escritas sobre las mesas.
- Hacer uso de la red de datos del Instituto, para obtener, mantener o difundir material publicitario o comercial (no institucional), así como distribución de cadenas de correos.
- Instalar software en la plataforma tecnológica del Instituto cuyo uso no esté autorizado por la Subdirección de Gestión Corporativa – Grupo de sistemas, y que pueda atentar contra las leyes de derechos de autor o propiedad intelectual.
- Uso de la identidad institucional digital (cuenta de usuario y contraseña) de otro usuario o facilitar, prestar o permitir el uso de su cuenta personal a otro funcionario o contratista.
- Dejar al alcance de personas no autorizadas los dispositivos portátiles, móviles y de almacenamiento removibles, entregados para actividades propias del cumplimiento de sus funciones.
- Retirar de las instalaciones del Instituto computadores de escritorio, portátiles e información física o digital clasificada previamente como confidencial o restringida, sin autorización o abandonarla en lugares públicos o de fácil acceso.
- Entregar, enseñar o divulgar información clasificada del Instituto a personas o entidades no autorizadas.
- Llevar a cabo actividades ilegales, o intentar acceso no autorizado a la plataforma tecnológica del instituto o de terceras partes.
- Ejecutar cualquier acción que difame, afecte la reputación o imagen del Instituto o alguno de sus funcionarios, utilizando para ello la plataforma tecnológica.
- Realizar cambios no autorizados en la plataforma tecnológica del Instituto.
- Otorgar privilegios de acceso a los activos de información a funcionarios o terceros no autorizados.
- Ejecutar acciones para eludir y/o modificar los controles establecidos en los lineamientos de la política de seguridad de la información.

- Consumir alimentos y bebida, cerca de cuartos o plataformas tecnológicas.
- Realizar cualquier otra acción que contravenga disposiciones constitucionales, legales o institucionales.

Cada una de las prácticas anteriormente mencionadas u otras que afecten la seguridad de la información, acarrearán medidas administrativas, acciones disciplinarias y/o penales a que haya lugar, de acuerdo con los procedimientos establecidos para cada caso.

En una segunda fase se deben desarrollar y establecer la implementación de políticas específicas de seguridad de la información con cada una de las áreas del IDPYBA, se van a adoptar 5 políticas específicas de acuerdo con la guía impartida por MinTic para la seguridad y privacidad de la información, a continuación, se mencionan las políticas específicas a adoptar:

- Política Controles Criptográficos
- Políticas de Firewall
- Políticas Base de Datos
- Políticas de Áreas Seguras
- Política de Desarrollo de Software

Se entiende Política de seguridad como una declaración de alto nivel que describe la posición de la entidad sobre un tema específico entorno a la Seguridad y privacidad de la información.

9. ACTIVIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la vigencia 2022 se deben establecer las siguientes las actividades en materia de Seguridad y Privacidad de Información.

ETAPA	ACTIVIDADES	ENTREGABLE	RESPONSABLE DE LA TAREA	Trimestre 1			Trimestre 2			Trimestre 3			Trimestre 4		
				1	2	3	1	2	3	1	2	3	1	2	3
PLANEAR	a) Diagnóstico con herramienta MSPI del MINTIC	Herramienta de diagnóstico diligenciada	Profesional Subdirección de gestión Corporativa - Tecnología	X	X	X									
	b) Autodiagnóstico con herramienta MINTIC de Gobierno Digital	Informe técnico diagnóstico del MSPI	Profesional Subdirección de gestión Corporativa - Tecnología	X	X	X									

	c) Establecer un plan de acción de acuerdo con los resultados de la auditoría interna realizada por la oficina de control interno al sistema de gestión de seguridad de la información	Plan de acción para resolver inconformidades en la auditoria de seguridad	Profesional Subdirección de gestión Corporativa - Tecnología	X	X	X										
	d) Formalizar el Plan de Sensibilización y Comunicación de Seguridad de la Información. *. Hacer encuesta de seguridad de la información *. Fortalecer los contenidos orientados a grupos.	Plan de sensibilización en seguridad de la información para el Instituto	Profesional Subdirección de gestión Corporativa - Tecnología	X	X											
	e) Solicitud auditorías internas	Formalización de solicitud de auditoría de seguridad de la información	Profesional Subdirección de gestión Corporativa - Tecnología				X									
	f) Actualización de valoración y clasificación de activos de la información	Matriz de clasificación de Activos de información actualizad	Profesional Subdirección de gestión Corporativa - Tecnología				X	X	X							
	g) Planeación y solicitud de permisos para desarrollar pruebas de intrusión, pruebas phising, revisión seguridad de la información de la red y/o Ethical Hacking	Formalización de autorización de pruebas de seguridad al interior del Instituto	Profesional Subdirección de gestión Corporativa - Tecnología		X	X										
	h) Generar indicadores de medición interna	Documento con indicadores de gestión	Profesional Subdirección de gestión Corporativa - Tecnología	X	X											
	i) Revisar y actualizar el plan de continuidad de negocio de TI.	Documento continuidad de negocio	Profesional Subdirección de gestión Corporativa - Tecnología				X									
HACER	a) Implementación estrategia de uso y apropiación seguridad y privacidad de la información	Evidencia de capacitación impartida en seguridad de la información	Toda la Entidad		X	X	X	X	X	X	X	X	X	X		

	c) Implementación pruebas de seguridad, según los permisos concedidos	Evidencia de pruebas realizadas de seguridad al interno de Instituto	Toda la Entidad			X		X			X					
	d) Evaluación y tratamiento del riesgo activos de información	Plan de tratamiento y control de riesgo	Profesional Subdirección de gestión Corporativa - Tecnología						X	X						
	e) Implementar Plan de Continuidad del Negocio	Reportes de avance del Plan de Continuidad de Negocio	Profesional Subdirección de gestión Corporativa - Tecnología						X	X	X	X	X			
VERIFICAR	a) Verificación vigencia y reestructuración de plan de seguridad	Documento con la verificación de cumplimiento de las acciones realizadas y ajustes requeridos	Profesional Subdirección de gestión Corporativa - Tecnología			X		X			X			X	X	
	b) Revisión Política de seguridad y plan de manejo de su implementación	Documento actualizado del estado de políticas de seguridad y evidencia de implementación de políticas de seguridad	Profesional Subdirección de gestión Corporativa - Tecnología				X		X			X			X	
	c) Verificación compromiso de la Alta Dirección	Presentación a la dirección con las actividades realizadas y el plan trimestral de seguridad de la información	Alta dirección y Profesional Subdirección de gestión Corporativa - Tecnología	X			X		X			X				
	d) Revisión de indicadores de seguridad	Documento con reporte de indicadores de gestión	Profesional Subdirección de gestión Corporativa - Tecnología				X		X			X			X	
	e) Recibir auditorias solicitadas	Evidencia de participación en auditoria	Profesional Subdirección de gestión Corporativa - Tecnología						X	X	X					
ACTUAR	a) Plan de mejoramiento	Documento con el plan actualizado de seguridad de la información, indicando los planes de mejora	Profesional Subdirección de gestión Corporativa - Tecnología				X		X			X	X	X		

A continuación, se indican las métricas del plan de Seguridad y privacidad de la información para la vigencia del 2022.

PRODUCTO (ENTREGABLE) DE LA VIGENCIA	UNIDAD DE MEDIDA	META ESPERADA	RESPONSABLE ACTIVIDAD	FECHA INICIO	FECHA TERMINACIÓN	DESCRIPCIÓN TAREAS	% PONDERACIÓN TAREA
Documento de creación de Políticas y/o Procedimiento	Unidad	5	Profesional Subdirección de gestión Corporativa - Tecnología	Febrero	Octubre	Revisión y creación de Políticas de Seguridad de la información y procedimiento para su implementación.	20,0%
Documento de Autodiagnóstico con herramienta MINTIC de Gobierno Digital	Unidad	1		Enero	Noviembre	Actualizar y hacer seguimiento al Autodiagnóstico de Seguridad y privacidad de la Información con la herramienta MINTIC de Gobierno Digital	10,0%
Documento con el Plan de Continuidad del Negocio	Unidad	1		Marzo	Noviembre	Creación del Plan de Continuidad del Negocio	25,0%
Documento de Activos de Información Actualizado	Unidad	1		Junio	Diciembre	Actualización y Clasificación de los Activos de Información	10,0%
Informe de Auditoria	Unidad	1		Octubre	Diciembre	Recibir auditorias solicitadas	20,0%
Informe de Valoración y tratamiento de Riesgos	Unidad	1		Julio	Diciembre	Valoración de Riesgos, tratamiento y controles de Seguridad de la Información	15,0%

10. GRUPO OPERATIVO DE SEGUIMIENTO A LA SEGURIDAD Y DE LA INFORMACIÓN

El grupo de operativo de seguridad de la información continuara con sus funciones de impulsar, hacer seguimiento y/o verificación de las actividades en materia de seguridad y privacidad de la información, que en conjunto con el Comité Institucional de Gestión y Desempeño harán seguimiento al cumplimiento de este plan, junto con los demás planes que sean implementados en pro de proteger la privacidad de la información.