PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Objetivo: Establecer, implementar y mantener el Modelo de Seguridad y Privacidad de la información, alineado con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad de la Operación, del Instituto Distrital de las Artes – Idartes.		
Alcance: Inicia desde el establecer, implementar y mantener el Modelo de Seguridad y Privacidad de la Información en el Idartes, tomando como piloto el proceso de Gestión de Tecnologías de la Información y las Comunicaciones - TIC y que este sea replicado a los demás procesos y sedes del Instituto.		
Fecha de aprobación	**Responsable del documento**	**Ubicación**
18-01-2022	Oficina Asesora de Planeación y Tecnologías de la Información	Intranet Comunicarte

Histórico de cambios		
Versión	**Fecha de emisión**	**Cambios realizados**
01	25/07/2018	Emisión inicial
02	30/01/2019	Actualización de riesgos de seguridad y privacidad de la información
03	31/01/2020	Actualización normativa
04	31/01/2021	Actualización de riesgos de seguridad y privacidad de la información
05	16/01/2022	Actualización de riesgos de seguridad y privacidad de la información

Elaboró	**Revisó**	**Aprobó**	**Avaló**
14/01/2022 **Andrés Briceño Díaz** Contratista Oficial de Seguridad de la Información	**17/01/2022** **Aurora Camila Crespo Murillo** Contratista de la Oficina Asesora de Planeación y Tecnologías de la Información	**14/01/2022** **Edgar Alfonso Cipagauta Pedraza** Profesional Especializado OAP-TI **18/01/2022** **Carlos Alfonso Gaitán Sánchez** Jefe de la Oficina Asesora de Planeación y Tecnologías de la Información	**18/01/2022** **Carlos Alfonso Gaitán Sánchez** Jefe de la Oficina Asesora de Planeación y Tecnologías de la Información

Contenido

INTRODUCCIÓN

La información en las empresas es considerada hoy en día uno de sus activos más importantes y valiosos, es de vital importancia para la toma de decisiones, para que las organizaciones sean más competitivas, innovadoras, presten mejores bienes, servicios y ofrezcan información confiable, ágil y acertada a sus clientes y usuarios. Sin dejar de mencionar que hoy por hoy los Activos De Información, son atacados constantemente, generando un aumento en el número de incidentes de seguridad de la información a nivel mundial que generan a las empresas pérdida de su buena imagen, problemas con sus clientes, pérdidas económicas y problemas legales, todo aunado a la presencia de la pandemia por Covid-19 que nos ha generado la necesidad imperativa de avanzar en la implementación y apropiación de nuevas tecnologías para el trabajo remoto, lo que impulsó la implementación de las estrategias TI enfocadas a la masificación del gobierno digital.

Es por la importancia de la información, que el Instituto Distrital de las Artes – Idartes, a través del presente documento establece la planificación, implementación, evaluación y mejora del Modelo de Seguridad y Privacidad de la Información, determinado por las necesidades, objetivos, estructura organizacional, los procesos misionales y tamaño de la Entidad, así como requisitos legales y exigencias de seguridad de la información dadas por MINTIC establecido en el Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018 en el artículo 2.2.9.1.1.3 Principios, que define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 que define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital; así como la Resolución 00500 de 2021 y sus anexos que incorporan lineamientos en materia de Seguridad Digital en las entidades del estado.

La política de gobierno digital tiene como objetivo promover lineamientos, planes, programas y proyectos en el uso y apropiación de las TIC para generar confianza en el uso del entorno digital, propendiendo por el máximo aprovechamiento de las tecnologías de la información y las comunicaciones. Además establece como habilitador transversal la seguridad y privacidad de la información, mediante el cual se definen de manera detallada la implementación de controles de seguridad físicos y lógicos con el fin de asegurar de manera eficiente los trámites, servicios, sistemas de información, plataforma tecnológica e infraestructura física y del entorno de las Entidades públicas de orden nacional y territorial, gestionando de manera eficaz, eficiente y efectiva los activos de información, infraestructura critica, los riesgos e incidentes de seguridad y privacidad de la información y así evitar la interrupción en la prestación de los servicios de la Entidad enmarcados en su modelo de operación por procesos.

Teniendo en cuenta la creciente participación de ciudadanos en el entorno digital, la alta dependencia de la infraestructura digital y el aumento en el uso y adopción de nuevas Tecnologías de la Información y las Comunicaciones (TIC) traen consigo una serie de riesgos e incertidumbres relacionados con la seguridad digital, lo cual exige que el país cuente con suficientes capacidades para su gestión adecuada y oportuna, las amenazas, los ataques e incidentes de seguridad digital cada día son más sofisticados y complejos e implican graves consecuencias de tipo económico o social, esto conlleva al deterioro de la confianza digital y la desaceleración del desarrollo de los países en el futuro digital y debido a lo anterior, los gobiernos alrededor del mundo han venido atendiendo los nuevos

retos para la detección y manejo de amenazas, ataques e incidentes cibernéticos mediante la formulación y actualización de estrategias o políticas relacionadas con la seguridad digital en el marco de la pandemia y la apropiación de estrategias TI..

En atención a esto el Idartes tiene el firme propósito de avanzar en su transformación digital incluyó en su Plan Estratégico Institucional 2020-2024 los lineamientos de la Política de Gobierno Digital, a través de diversas iniciativas estratégicas de fortalecimiento institucional, participación y empoderamiento de ciudadano, arquitectura empresarial y seguridad de la información.

ALCANCE Y ENTREGABLES

Establecer, implementar y mantener el Modelo de Seguridad y Privacidad de la Información en el IDARTES, tomando como piloto el proceso de Gestión de Tecnologías de la Información y las Comunicaciones - TIC y que este sea replicado en las unidades de gestión y a los demás procesos y sedes del Instituto, con este documento y su alineación con el Plan Estratégico de Tecnologías de la Información PETI se referencia la estrategia TI y aporta línea de acción apoyando la ejecución de los proyectos, contemplando actualizaciones, para lograr los objetivos estratégicos engranados al Plan Estratégico Institucional y el marco de Referencia de arquitectura Empresarial del comprender, analizar, construir y presentar, con el enfoque de la estructuración del modelo de gestión Estrategia, Gobierno, Información, Sistemas de Información, Infraestructura de TI, Uso y Apropiación y Seguridad..

RESUMEN EJECUTIVO

El resumen ejecutivo constituye una parte fundamental del Plan, para el diseño y planificación del Modelo de Seguridad y Privacidad de la Información el cual debe ser conocido por todo el Instituto, así como tener en cuenta los compromisos y normatividad establecida por el Ministerio de las Tecnologías de la Información y Comunicaciones MINTIC y la Alta Consejería Distrital de TIC - ACDTIC para las entidades gubernamentales; como lineamientos, políticas y directrices establecidas, según la De acuerdo con el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015 (DUR-TIC), "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones", la Política de Gobierno Digital será definida por MinTIC y se desarrollará a través de componentes y habilitadores transversales que, acompañados de lineamientos y estándares, permitirán el logro de propósitos que generarán valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC.

Por otra parte, el resumen ejecutivo Técnico y Administrativo del Instituto, los instrumentos y guías diseñados por MINTIC, se tomaron como base para establecer la implementación del Modelo de Seguridad de la Información - MSPI, mediante la formulación de iniciativas, estrategias que garanticen el apoyo y cumplimiento de sus objetivos y funciones, que soporte adecuadamente los procesos misionales, estratégicos, transversales, de evaluación y mejora;

entendiendo que a través de la Oficina asesora de planeación y tecnologías de la información es quien liderar la política de MIPG Seguridad Digital y Gobierno Digital alineado con el Plan estratégico institucional IDARTES 2020-2024.

Es importante mencionar en esta instancia, que la Oficina asesora de planeación y tecnologías de la información tiene como función formular y liderar el diseño, planeación, implementación y control de las actividades y productos asociados a la seguridad y privacidad de la Información, garantizando la integridad y debida custodia de la información, en línea con la normatividad y legislación vigente y la Política de Gobierno Digital, abordando los siguientes aspectos

Formulación, actualización y divulgación de líneas específicas referentes a Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación.
Implementar un Modelo de Seguridad y Privacidad de la Información del Idartes.
Salvaguarda de la información institucional
Administrar controlar y gestionar los incidentes de la seguridad de la información.
Apoyar a las unidades de gestión en diligenciar los formularios y autodiagnósticos que emitan las entidades cabeza de sector para verificar la correcta implementación de las políticas y lineamientos establecidos (MINTIC, ACDTIC y DAFP), entre otras.
Optimización de sistemas de apoyo a la infraestructura tecnológica Idartes

DIAGNÓSTICO Y AUTODIAGNÓSTICO

El IDARTES, por ser una Entidad del orden Distrital que debe dar cumplimiento a las metas establecidas por MINTIC, en Seguridad de la Información, elemento habilitador de la Política de Gobierno Digital (antes conocido como el componente de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea – GEL), para la estructuración del contexto, análisis, e implementación se utilizaron herramientas de diagnóstico definidas por los entes rectores en lineamientos para dar complimiento a la estrategia de apropiación de Gobierno Digital y Seguridad Digital.

Conforme a lo enunciado a continuación se plasman los resultados obtenidos de la valoración con el Instrumento Evaluación MSPI realizado en el cuarto trimestre de 2021 con el fin de reflejar el panorama actual de la entidad en el marco de la apropiación del gobierno digital en lo referente a la seguridad y privacidad de la información.

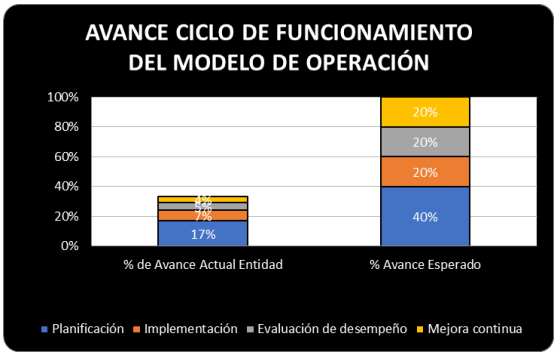
EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

Resultados Instrumento de Identificación de la Línea Base de Seguridad

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	60	100	EFECTIVO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	48	100	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	32	100	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	46	100	EFECTIVO
A.9	CONTROL DE ACCESO	53	100	EFECTIVO
A.10	CRIPTOGRAFÍA	40	100	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	47	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	45	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	35	100	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	38	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	30	100	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	34	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	30	100	REPETIBLE
A.18	CUMPLIMIENTO	40	100	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		**41**	**100**	EFECTIVO

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA		
	COMPONENTE	% de Avance	% Avance
2021	Planificación	17%	40%
	Implementación	7%	20%
	Evaluación de desempeño	5%	20%
	Mejora continua	4%	20%
TOTAL		**33%**	**100%**

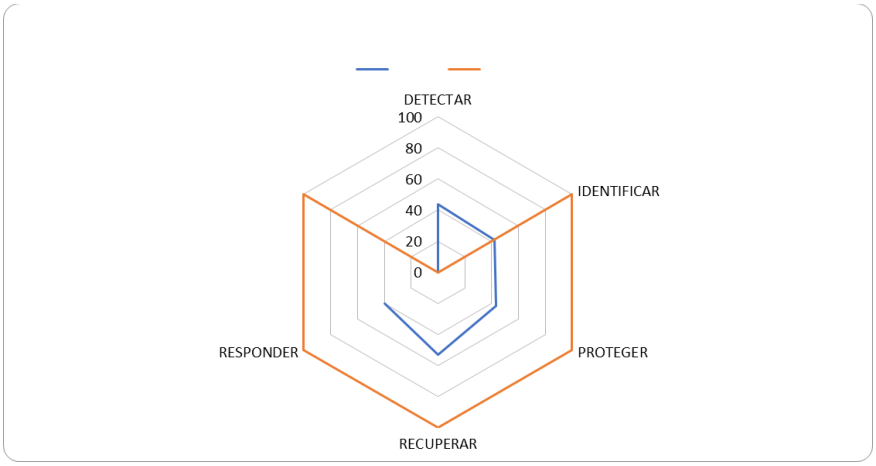


En el documento se puede apreciar la calificación obtenida en cada uno de los controles y la calificación objetivo versus la meta establecida, que debió cumplir el Instituto el 31 de diciembre de 2021.

Ahora bien, frente al poco avance del Instituto en el año 2020, en el último trimestre de 2021 la Oficina asesora de planeación y tecnologías de la información realizo nuevamente el autodiagnóstico el cual dio como resultado un porcentaje de efectividad de los controles ISO 27001:2013 Anexo A del 30% y de un 35% en el ciclo PHVA

A nivel de ciber seguridad se avanzó en la ejecución de controles en el marco de los lineamientos de la resolución 00500 de 2021 y abordando las actividades del plan de tratamiento de riesgos de la seguridad de la información 2021 y el plan de seguridad y privacidad de la información 2021 los cuales al cuarto trimestre obtuvieron los siguientes resultados

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
FUNCION CSF	CALIFICACIÓN ENTIDA	NIVEL IDEAL CSF
DETECTAR	43,75	100
IDENTIFICAR	42	100
PROTEGER	43,44262295	100
RECUPERAR	53,33333333	100
RESPONDER	40	100



NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Así mismo, con la actualización de la herramienta de autodiagnóstico teniendo en cuenta el dominio de seguridad de la información que hace parte integral de la arquitectura de la estrategia TI se presenta un contexto de la implementación y avances en la aplicación de los controles de seguridad y privacidad de la información.

Descripción del problema

El IDARTES es un Establecimiento público del orden distrital, con personería jurídica, autonomía administrativa, financiera y patrimonio propio, encargado de garantizar el ejercicio de los derechos culturales, mediante la promoción de las artes en el Distrito Capital, contribuyendo al desarrollo de sujetos creativos, sensibles, respetuosos de la diferencia, aportando a la construcción de una ciudad incluyente y solidaria.

La mayoría de la información generada en las diferentes Subdirecciones requiere de controles efectivos, de procedimientos internos para que permita brindar las condiciones para custodiar sus datos, sistemas de información, plan de tratamientos de riesgos de seguridad y privacidad de la información y acción para el uso y salvaguarda de la información. Por lo anterior es pertinente y necesario planear e implementar el Modelo de Seguridad y Privacidad de la Información - MSPI en IDARTES de manera gradual y transversal, en sus procesos, tomando como piloto el proceso de Gestión de Tecnologías de la Información y las Comunicaciones TIC, por ser este el que tiene en su hacer, la seguridad de la información del Instituto.

El Modelo de Seguridad y Privacidad de la Información permitirá aplicar los controles pertinentes que garanticen la protección de los activos de información, que eviten y prevengan problemas legales, perdida económicas y daño reputacional, así como garantizar el cumplimiento de planes, programas, proyectos, metas y objetivos. Adicional, permitirá al IDARTES cumplir con las exigencias normativas y legales establecidas por MinTIC en el elemento habilitador de Seguridad Digital, según el Decreto 1008 del 14 de junio de 2018, por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones y dictó otras disposiciones.

Justificación

La Oficina asesora de planeación y tecnologías de la información, luego de revisar el informe de Valoración del autodiagnóstico 2020, el cual arrojó como resultado un avance frente al compromiso con MinTIC de cumplir al 100%; ha evidenciado que la mayoría de la información requiere mejoras de clasificación, controles administrativos, físicos y lógicos.

Es responsabilidad del Idartes implementar líneas de acción que permitan el tratamiento de los riesgos de seguridad y privacidad de la información. El recurso humano del Idartes, en cumplimiento de los objetivos misionales y

administrativos del instituto, por lo tanto, es necesario establecer los controles necesarios para identificar las causas y consecuencias de la materialización de los riesgos. Por lo anterior este plan pretende trazar la ruta a seguir para orientar y facilitar la gestión de la seguridad y privacidad de la información, de forma eficiente y efectiva, desde la identificación hasta la definición de controles para su gestión.

Razón por la cual es pertinente y necesario realizar la actualización e implementación del Modelo de Seguridad y Privacidad de la Información, no solo para dar cumplimiento a las metas establecidas por el MinTIC, si no para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información, así como crear una cultura organizacional que permita realizar y mantener un MSPI en el tiempo.

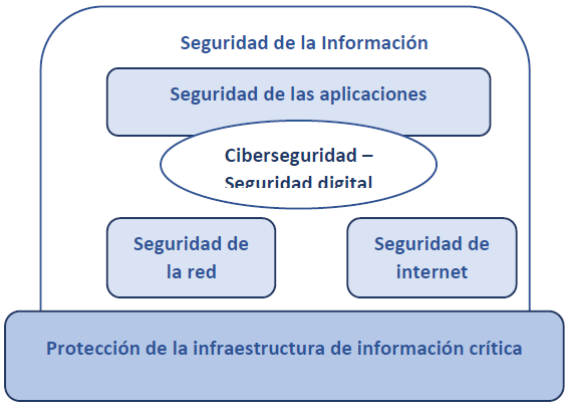


Ilustración 1. Relación entre la ciberseguridad y otros ámbitos de la seguridad (Fuente: ISO/IEC 27032)

OBJETIVOS

Objetivo General

Establecer, implementar y mantener el Modelo de Seguridad y Privacidad de la información, alineado con las normas ISO 27001 y 27032, y también, los lineamientos incorporados con la Resolución 00500 de 2021 fortaleciendo la gestión de la Política de Seguridad Digital y Continuidad de la Operación, para implementar dentro del Instituto Distrital de las Artes – IDARTES.

Objetivos Específicos

- Formular e implementar controles con una política de seguridad de la información
- Conocer, asumir, gestionar y tratar los riesgos de seguridad de la información de una manera sistemática, documentada y eficiente.

- Aplicar los controles pertinentes, lineamientos, normatividad y directrices nacionales y distritales de obligatorio cumplimiento para las entidades públicas.
- Planificar e implementar seguridad y privacidad de la información
- Evaluar la eficacia de los controles implementados
- Actuar frente a los incidentes de seguridad y privacidad de la información que generen afectación sobre la operación de la entidad.
- Aportar en el desarrollo e implementación de la estrategia de seguridad digital del Idartes.
- •Establecer procedimientos de seguridad que permitan a la Entidad apropiar el habilitador de seguridad en la política de Gobierno Digital.
- Institucionalizar la seguridad y privacidad de la información en los procesos y procedimientos de las Entidades.
- Mediante la implementación eficiente, eficaz y efectiva del MSPI, se busca contribuir al incremento de la transparencia en la gestión pública.
- Contribuir en el desarrollo y ejecución del plan estratégico institucional, través del plan de seguridad y privacidad de la información.

Implementar controles

Idartes en la vigencia 2021 gestiono la incorporación de una Política de Seguridad de la Información a los instrumentos de gestión de tecnología, para buscar la articulación con el Modelo Integrado de gestión y Planeación – MIPG como herramienta dinamizadora, dado que el elemento habilitador de Seguridad de la Información, ; el modelo consta de cinco (5) fases las cuales permiten que las Entidades puedan gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información. Por ello, los sujetos obligados deben abordar las siguientes fases:

1. Diagnóstico: Realizar un diagnóstico, cuyo objetivo es identificar el estado actual de la Entidad respecto a la adopción del MSPI.
2. Planificación: Determinar las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta el contexto de interno y externo del Idartes.
3. Operación: Implementar los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.
4. Evaluación de desempeño: Determinar el sistema y forma de evaluación de la adopción del modelo.
5. Mejoramiento Continuo: Establecer procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición.

En la fase de implementación del MPSI, según las necesidades y requerimientos del IDARTES la actividad correspondiente a la documentación de políticas, procedimientos, guías y demás mecanismos solicitados en los controles se dividen en dos sub-fases ya que para realizar las actividades de la fase de planeación se requiere elaborar el inventario de activos de información y otras actividades iniciales pertenecientes al proceso de Gestión TIC.

Ilustración 2. Ciclo del Modelo de Seguridad y Privacidad de la Información

Conforme a la Política de Seguridad de la Información y el Autodiagnóstico de evaluación del MSPI 2021, se plantean los siguientes controles para abordar la implementación de seguridad Digital en la vigencia 2022 para el Idartes.

Controles de seguridad y privacidad de la información				
Categoría	**Control**	**Actividades**	**Responsable**	**Fecha máxima de implementar**
Administrativos				
Organización de la seguridad de la información	Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización	Definir y asignar las responsabilidades de la seguridad de la información	OAP-TI	31/12/2022
		Definir lineamientos que especifiquen cuándo y a través de que autoridades se debe contactar a las autoridades	OAP-TI	31/12/2022
		La seguridad de la información se debe integrar al(los) método(s) de gestión de proyectos de la organización, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte de un proyecto.	OAP-TI	31/12/2022

Controles de seguridad y privacidad de la información				
Categoría	**Control**	**Actividades**	**Responsable**	**Fecha máxima de implementar**
Seguridad de los recursos humanos	Asegurar que el personal y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que son considerados.	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	OAP-TI	31/12/2022
		Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	OAP-TI	31/12/2022
	Asegurar que los funcionarios y contratistas tomen consciencia de sus responsabilidades sobre la seguridad de la información y las cumplan.	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	OAP-TI	31/12/2022
		Todos los empleados de la Entidad, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	OAP-TI	31/12/2022
Gestión de Activos	Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.	Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	OAP-TI	31/12/2022
		Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	OAP-TI	31/12/2022

Controles de seguridad y privacidad de la información				
Categoría	**Control**	**Actividades**	**Responsable**	**Fecha máxima de implementar**
	Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la Entidad.	La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	OAP-TI	31/12/2022
Aspectos de seguridad de la información de la gestión de la continuidad del negocio	La continuidad de la seguridad de la información debe incluir en los sistemas de gestión de la continuidad del negocio de la Entidad.	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa	OAP-TI	31/12/2022
Relaciones con los proveedores	Seguridad de la información en las relaciones con los proveedores	Asegurar la protección de los activos de la entidad que sean accesibles para los proveedores	OAP-TI	31/12/2022
Técnicos				
Requisitos del negocio para control de acceso	Se debe limitar el acceso a información y a instalaciones de procesamiento de información.	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	OAP-TI	31/12/2022
Gestión de acceso de usuarios	Se debe asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	OAP-TI	31/12/2022
Control de acceso a sistemas y aplicaciones	Se debe evitar el acceso no autorizado a sistemas y aplicaciones.	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.	OAP-TI	31/12/2022
Controles criptográficos	Asegurar el uso apropiado y eficaz de la criptografía para	Se debe desarrollar e implementar un lineamiento sobre el uso de controles	OAP-TI	31/12/2022

Controles de seguridad y privacidad de la información				
Categoría	**Control**	**Actividades**	**Responsable**	**Fecha máxima de implementar**
	proteger la confidencialidad, la autenticidad y/o la integridad de la información.	criptográficos para la protección de la información.		
Seguridad física y del entorno	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	Se debe definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.	OAP-TI	31/12/2022
		Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	OAP-TI	31/12/2022
	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	OAP-TI	31/12/2022
		El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información deben estar protegido contra interceptación, interferencia o daño.	OAP-TI	31/12/2022
		Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	OAP-TI	31/12/2022
Seguridad de las operaciones	Asegurar las operaciones correctas y seguras de las instalaciones de	Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	OAP-TI	31/12/2022

Controles de seguridad y privacidad de la información				
Categoría	**Control**	**Actividades**	**Responsable**	**Fecha máxima de implementar**
	procesamiento de información.	Se debe separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	OAP-TI	31/12/2022
	Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.	Se debe implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	OAP-TI	31/12/2022
	Proteger contra la pérdida de datos.	Se debe hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	OAP-TI	31/12/2022
	Asegurar la integridad de los sistemas operacionales.	Se debe implementar procedimientos para controlar la instalación de software en sistemas operativos.	OAP-TI	31/12/2022
	Prevenir el aprovechamiento de las vulnerabilidades técnicas.	Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	OAP-TI	31/12/2022
Seguridad de las comunicaciones	Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.	Se debe identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	OAP-TI	31/12/2022
	Mantener la seguridad de la información transferida dentro de	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	OAP-TI	31/12/2022

Controles de seguridad y privacidad de la información				
Categoría	**Control**	**Actividades**	**Responsable**	**Fecha máxima de implementar**
	una organización y con cualquier entidad externa.	Se debe identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	OAP-TI	31/12/2022
Seguridad de los sistemas de información	Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	OAP-TI	31/12/2022
	Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	OAP-TI	31/12/2022
		establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	OAP-TI	31/12/2022
Gestión de incidentes y mejoras en la seguridad de la información	Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.	Se debe establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	OAP-TI	31/12/2022
		Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	OAP-TI	31/12/2022
		Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la	OAP-TI	31/12/2022

Controles de seguridad y privacidad de la información				
Categoría	**Control**	**Actividades**	**Responsable**	**Fecha máxima de implementar**
		información observada o sospechada en los sistemas o servicios.		
		Generar comunicación adecuada dentro de la gestión de incidentes de seguridad de la Información	OAP-TI	31/12/2022

APLICABILIDAD

La Declaración de Aplicabilidad (Statement of Applicability - SOA) referenciado en el numeral 6.1.3d de la norma ISO-27001, es un documento que lista los objetivos y controles que se van a implementar en la Entidad, en este entendido y conforme al análisis realizado para establecer los controles del presente plan, este tipo de análisis se hace evaluando el cumplimiento de la norma ISO-27001, para cada uno de los controles establecidos en los 14 dominios o temas relacionados con la gestión de la seguridad de la información que este estándar.

CONTROL Y SEGUIMIENTO

Es importante conocer de manera permanente los avances en la gestión, los logros de los resultados y metas propuestas, para la implementación del modelo habilitador de la Política de Gobierno Digital. Para tal fin es importante establecer los tiempos, recursos previstos para el monitoreo, desempeño, resultados y aceptación de estos en el comité de gestión institucional y desempeño, como lo establece el MIPG. La Oficina Asesora de Planeación y Tecnologías de la Información debe realizar el seguimiento y control a la implementación y/o mantenimiento de la Seguridad de la Información.

Se debe revisar periódicamente por cada responsable de los procesos al interior de las entidades, junto con su equipo los siguientes aspectos:

Ajustes y modificaciones:
Después de su publicación y durante el respectivo año de vigencia, se podrán realizar los ajustes y las modificaciones necesarias orientadas a mejorar el plan de seguridad y privacidad de la información, en este caso, deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.

Monitoreo:
En concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de seguridad y privacidad de la información.

Seguimiento:
El jefe de control interno, o quien haga sus veces, debe adelantar seguimiento a la gestión de seguridad y privacidad de la información, en este sentido, es necesario que en sus procesos de seguimiento interno analicen las causas, los riesgos y la efectividad de los controles incorporados en el documento.

Es importante que las Entidades conozcan de manera permanente los avances en su gestión, los logros de los resultados y metas propuestas, para la implementación del modelo habilitador de la Política de Gobierno Digital. Para tal fin es importante establecer los tiempos, recursos previstos para el monitoreo, desempeño, resultados y aceptación de estos en el comité de gestión institucional y desempeño, como lo establece el MIPG.

Los temas de seguridad y privacidad de la información, seguridad digital y en especial la Política y el Plan de Seguridad y Privacidad de la Información deben ser tratados y aprobados en el comité institucional de gestión y desempeño de ser necesario para su optimo cumplimiento.

NORMATIVIDAD

Tipo de norma	Entidad que expide	Descripción normativa
Decreto 1360 de 1989	Presidencia de Colombia	Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor.
Decreto 2150 de 1995	MINISTERIO DE JUSTICIA Y DEL DERECHO	Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
Ley 572 de 1999	Congreso de la República	Comercio Electrónico, Firmas Digitales, Intercambio electrónico de datos.
Documento Conpes 3072 de 2000	Conpes	Agenda de Conectividad
Decreto 3816 de 2003	Presidencia de Colombia	Por el cual se crea la Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública

Tipo de norma	Entidad que expide	Descripción normativa
Conpes 3292 de 2004	Conpes	Señala la necesidad de eliminar, racionalizar y estandarizar trámites a partir de asociaciones comunes sectoriales e intersectoriales (cadenas de trámites), enfatizando en el flujo de información entre los eslabones que componen la cadena de procesos administrativos y soportados en desarrollos tecnológicos que permitan mayor eficiencia y transparencia en la prestación de servicios a los ciudadanos.
Directriz 5 de 2005	Alcaldía Mayor de Bogotá	Por la cual la Alcaldía Mayor de Bogotá define Políticas Generales y directrices que orienten el desarrollo tecnológico.
Decreto 619 de 2007	Alcaldía Mayor de Bogotá	Por el cual se establece la Estrategia de Gobierno Electrónico en el Distrito.
Decreto 316 de 2008	Alcaldía Mayor de Bogotá	Por medio del cual se modifica parcialmente el artículo 3 del Decreto Distrital 619 de 2007 que adoptó las acciones para el desarrollo de la Estrategia Distrital de Gobierno Electrónico.
Ley 1273 de 2009	Congreso de la República	Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"· y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1341 de 2009	Congreso de la República	Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones
Decreto 235 de 2010	Ministerio del Interior y Justicia	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.
Conpes 3701 de 2011	Conpes	Lineamientos de política para la Ciberseguridad y Ciberdefensa
Ley 1581 de 2012	Congreso de la República	Por el cual se dictan disposiciones generales para la protección de datos personales
Decreto 884 de 2012	Presidencia de Colombia	Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones

Tipo de norma	Entidad que expide	Descripción normativa
Decreto 2364 de 2012	Ministerio del Interior y Justicia	Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones
Decreto 19 de 2012	Presidencia de Colombia	Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública
Resolución 396 de 2012	Idartes	Por medio de la cual se crea el Comité Técnico de Seguridad de la Información - CTSI- del Instituto Distrital de las Artes - IDARTES.
Ley 1618 de 2013	Presidencia de Colombia	Por medio de la cual se establecen las disposiciones para garantizar el pleno ejercicio de los derechos de las personas con discapacidad. Art 16. Derecho a la información y comunicaciones
Decreto 1377 de 2013	Presidencia de Colombia	Por el cual se reglamenta parcialmente la Ley 1581 de 2012
Decreto 596 de 2013	Alcaldía Mayor de Bogotá	Por el cual se dictan medidas para la aplicación del Teletrabajo en organismos y entidades del Distrito Capital
ley 1712 de 2014	Congreso de la República	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones
Resolución 383 de 2014	Idartes	Por la cual se modifica la Resolución No 396 de 2012, "por medio de la cual se crea el Comité Técnico de Seguridad de la Información - CTSI- del Instituto Distrital de las Artes - IDARTES".
Ley 1753 de 2015	Congreso de la República	Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "TODOS POR UN NUEVO PAÍS" "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 103 de 2015	Presidencia de Colombia	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1081 de 2015	Presidencia de Colombia	Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República
Decreto 1078 de 2015	Presidencia de Colombia	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías

Tipo de norma	Entidad que expide	Descripción normativa
		de la Información y las Comunicaciones
Conpes 3854 de 2016	Conpes	Política Nacional de Seguridad Digital. Lo que a su vez se traduce en una economía digital con cada vez más participantes en el país. Desafortunadamente, el incremento en la participación digital de los ciudadanos trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado. Situación que debe ser atendida, tanto brindando protección en el ciberespacio para atender estas amenazas, como reduciendo la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo
Decreto 415 de 2016	Departamento Administrativo de la Función Pública	Se modifica el decreto 1083 de 2015 y se definen los lineamientos del modelo integral de planeación y gestión para el desarrollo administrativo y la gestión de la calidad para la gestión pública.
Resolución 4 de 2017	Secretaría General Alcaldía Mayor de Bogotá D.C. - Comisión Distrital de Sistemas - CDS	Por la cual se modifica la Resolución 305 de 2008 de la CDS
Decreto 728 de 2017	Ministerio de las Tecnologías de la Información y las Comunicaciones	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto. Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de las zonas de acceso público a internet inalámbrico
Decreto 1413 de 2017	Ministerio de las Tecnologías de la Información y las Comunicaciones	En el Capítulo 2 Características de los Servicios Ciudadanos Digitales, Sección 1 Generalidades de los Servicios Ciudadanos Digitales
Resolución 2710 de 2017	Ministerio de las Tecnologías de la Información y las Comunicaciones	Por la cual se establecen lineamientos para la adopción del protocolo IPv6

Tipo de norma	Entidad que expide	Descripción normativa
Decreto 728 de 2017	Ministerio de las Tecnologías de la Información y las Comunicaciones	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto. Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno
Circular 30 de 2017	Alta Consejería de TICs	Implementación CSIRT de Gobierno
Circular 36 de 2017	Alta Consejería de TICs	Lineamientos de avance del modelo de seguridad y privacidad de la información
Resolución 3436 de 2018	Ministerio de las Tecnologías de la Información y las Comunicaciones	Por la cual se reglamentan los requisitos técnicos, operativos y de seguridad que deberán cumplir las zonas de acceso a Internet inalámbrico de que trata el Capítulo 2, Título 9, Parte 2, Libro 2 del Decreto 1078 de 2015.
Decreto 612 de 2018	Departamento Administrativo de la Función Pública	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
Decreto 1008 de 2018	Ministerio de las Tecnologías de la Información y las Comunicaciones	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
Circular 2 de 2018	Ministerio de las Tecnologías de la Información y las Comunicaciones	Cumplimiento legal y normativo respecto a seguridad de la información
Conpes 3920 de 2018	Conpes	Big Data, la política tiene por objetivo aumentar el aprovechamiento de datos, mediante el desarrollo de las condiciones para que sean gestionados como activos para generar valor social y económico. En lo que se refiere a las actividades de las entidades públicas, esta generación de valor es entendida como la provisión de bienes públicos para brindar respuestas efectivas y útiles frente a las necesidades sociales.
Guia 6 de 2019	Ministerio de las Tecnologías de la	Guía para la construcción del Plan Estratégico de Tecnologías de Información PETI

Tipo de norma	Entidad que expide	Descripción normativa
	Información y las Comunicaciones	
Ley 1955 del 2019	Presidencia de Colombia	Establece que las entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)
Decreto 2106 de 2019	Departamento Administrativo De La Función Pública	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública Cap. II Transformación Digital Para Una Gestión Pública Efectiva
Conpes 3975 de 2019	Conpes	Define la Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital con el fin de que puedan enfocar sus esfuerzos en este tema.
Decreto 620 de 2020	Departamento Administrativo De La Función Pública	Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales
Resolución 00500 de 2021	Ministerio de las Tecnologías de la Información y las Comunicaciones	“Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”
Resolución 00500 de 2021 Anexo 1	Ministerio de las Tecnologías de la Información y las Comunicaciones	Documento Maestro del Modelo de Seguridad y Privacidad de la Información Dirigida a las Entidades del Estado
Directiva 09 de 2021	Secretaría Jurídica Distrital	Buenas prácticas en el uso de fotografías y videos para la protección de derechos de autor

RECURSOS DOCUMENTALES

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Documento Maestro del Modelo de Seguridad y Privacidad de la Información. Versión 4
Resolución 00500 de 2021 - Anexo 01
Bogotá. 2021

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Instrumento de Autodiagnóstico de gobierno digital Bogotá. 2021

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Instrumento de Evaluación del Modelo de Seguridad y Privacidad de la Información Bogotá. 2021

ORGANIZACIÓN INTERNACIONAL DE ESTANDARIZACIÓN – ISO
Norma Internacional ISO 27001. Ginebra, Suiza 2018