Objetivo:

El presente documento pretende diseñar un plan de seguridad y privacidad de la información con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, en el Instituto Distrital de la Artes.

Alcance:

El plan de seguridad y privacidad de la información está dirigido a los funcionarios, contratistas, proveedores de servicios de TIC, proveedores de servicios y terceros que utilicen de manera itinerante los recursos tecnológicos del Instituto Distrital de las Artes – Idartes.

Fecha de Aprobación	Responsable del Documento	Ubicación
30 de Julio de 2018	Área de Tecnología	Página Intranet: http://comunicarte.idartes.gov.co/idartes

HISTÓRICO DE CAMBIOS		
Versión	**Fecha de Emisión**	**Cambios realizados**
1	30 de Julio 2018	Emisión Inicial
Oficinas Participantes		
Subdirección Administrativa y Financiera Área de TIC		

Elaboró:	Aprobó:	Validó	Aprobó
ORIGINAL FIRMADO **Luis Albeiro Cortés** Contratista Área de Tecnología	ORIGINAL FIRMADO **Juan Carlos Cubillos** Profesional Universitario Área de Tecnología ORIGINAL FIRMADO **Liliana Valencia Mejía** Subdirectora Administrativa y Financiera	ORIGINAL FIRMADO **Camila Crespo Murillo** Contratista Oficina Asesora de Planeación	ORIGINAL FIRMADO **Luis Fernando Mejía Castro** Jefe Oficina Asesora de Planeación

TABLA DE CONTENIDO

LISTA DE FIGURAS

INTRODUCCIÓN

La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Entidad.

1. OBJETIVO DEL DOCUMENTO

El objetivo es diseñar un plan de seguridad y privacidad de la información con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, en el Instituto Distrital de la Artes.

2. ALCANCE

El plan de seguridad y privacidad de la información está dirigido a los funcionarios, contratistas, proveedores de servicios de TIC, proveedores de servicios y terceros que utilicen de manera itinerante los recursos tecnológicos del Instituto Distrital de las Artes – IDARTES.

3. FASE PLANIFICACION

Para desarrollar el plan de seguridad y privacidad de la información en el Instituto Distrital de las Artes – IDARTES es necesario utilizar los resultados obtenidos en el autodiagnóstico donde se contempla el estado actual de la entidad, identificación del nivel de madurez y el levantamiento de información.

Para desarrollar el plan de seguridad de seguridad y privacidad de la información se debe tener en cuenta: los procesos que impactan directamente la consecución de objetivos misionales, servicios, sistemas de información, ubicaciones físicas e interrelaciones del Modelo con otros procesos.

Figura 1. - Fase de planificación para MSPI

Fuente: Guía Modelo de Seguridad y Privacidad de la Información– MINTIC

4. ESTADO ACTUAL

A continuación, se presenta el resultado del análisis de brecha del nivel de madurez frente a los controles del Anexo A, del estándar ISO 27001:2013, y la guía de controles del Modelo de Seguridad de Privacidad. Se puede evidenciar la calificación de cada dominio frente a la escala de evaluación definida y también en comparación con la calificación objetivo en el IDARTES.

Figura 2. – Evaluación de efectividad de controles 27001 -2013

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	51	100	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	71	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	42	100	EFECTIVO
A.9	CONTROL DE ACCESO	71	100	GESTIONADO
A.10	CRIPTOGRAFÍA	20	100	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	48	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	54	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	59	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	37	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	50	100	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	46	100	EFECTIVO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	50	100	EFECTIVO
A.18	CUMPLIMIENTO	53,5	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		**51**	**100**	EFECTIVO

Fuente: Herramienta autoevaluación - Seguridad y Privacidad de la Información– MINTIC

Figura 3. – Brecha Anexo A 27001:2013

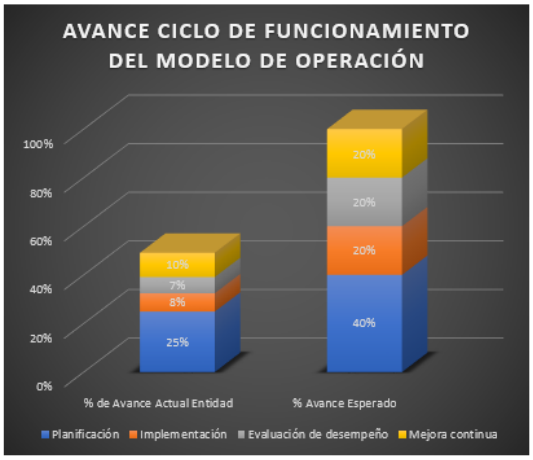
Fuente: Herramienta autoevaluación - Seguridad y Privacidad de la Información– MINTIC

El avance PHVA (Planear, Hacer, Verificar y Actuar) permite evidenciar el avance en el ciclo del modelo de seguridad

definido en el documento MSPI, el cual está alineado con los plazos para la implementación de las actividades que se establecieron para el Manual de Gobierno en Línea.

Figura 4. – Brecha Anexo A 27001:2013

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actu	% Avance Esperado
2015	Planificación	25%	40%
2016	Implementación	8%	20%
2017	Evaluación de desempeño	7%	20%
2018	Mejora continua	10%	20%
TOTAL		49%	100%



Fuente: Herramienta autoevaluación - Seguridad y Privacidad de la Información– MINTIC

5. PLAN DE ACCIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Busca generar un plan de seguridad y privacidad alineado con el propósito misional, para la vigencia 2018 se tiene contemplado realizar las siguientes actividades en cada una de las gestiones que compone la estrategia de Gobierno Digital y el modelo nacional de gestión de riesgos de seguridad digital y según el estándar NTC-ISO-IEC 27001:2013.

A continuación, se presenta el plan de seguridad y privacidad de la información contemplando:

Fase: comprende cada ciclo de operación (Diagnostico, planificación, implementación, evaluación de desempeño y mejora continua), las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

Actividades: Acciones a desarrollar en cumplimiento de cada fase.

Descripción: Explicación de lo que se espera realizar de acuerdo con las actividades establecidas y metas a cumplir, la descripción está alineada a las directrices distritales y nacionales.

Metas: producto o indicador a entregar.

Responsable: Responsable, área o dependencia que deberá facilitar el acceso a la información y evidencias sobre la definición e implementación del control o requisito a evaluar.

FASE	ACTIVIDADES	DESCRIPCIÓN	METAS	RESPONSABLE
Diagnóstico	Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad.	En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información a través del diligenciamiento de la herramienta de diagnóstico MINTIC.	Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad. Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	Gestión TIC Control interno Disciplinario. Gestión Documental Gestión de bienes servicios y planta física Oficina asesora de Planeación
	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.	Proceso de descubrir falencias en los sistemas y aplicaciones que pueden llegar a ser aprovechados por un atacante. Dichas falencias pueden ser descubiertas a nivel del host o en la administración o configuración o diseño del mismo.	Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Gestión TIC

FASE	ACTIVIDADES	DESCRIPCIÓN	METAS	RESPONSABLE
Planificación	Actualizar la política de seguridad y privacidad de la información	Política de Seguridad de la Información de la Entidad: A) Se definen los Objetivos, Alcance de la Política. B) Debe estar alineada con la estrategia y objetivos de la entidad. C) Política aprobada y socializada al interior de la entidad por la alta dirección. Guía No 2 – Política General MSPI	Política de Seguridad y Privacidad de la Información actualiza	Gestión TIC
	Actualizar Manual con las políticas de seguridad y privacidad de la información.	Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y a la parte externa pertinente. Guía No 2 – Política General MSPI	Manual de políticas de seguridad y privacidad de la información actualizadas	Gestión TIC
	Elaborar y aprobar los procedimientos de seguridad y privacidad de la información debidamente documentados, socializados y aprobados.	Procedimientos de seguridad y privacidad de la información de acuerdo con los requerimientos exigidos en la NTC 27001. Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información.	Procedimientos de seguridad de la información.	Gestión TIC

FASE	ACTIVIDADES	DESCRIPCIÓN	METAS	RESPONSABLE
Planificación	Actualizar roles y responsabilidades seguridad y privacidad de información.	Se debe definir roles y responsabilidades de seguridad de la información (Anexo 27001:2013, A6.1.1) Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información.	Roles y responsabilidades seguridad y privacidad de información.	Gestión TIC
	Actualizar documento con la metodología para identificación, clasificación y valoración de activos de información. Matriz con la identificación, valoración y clasificación de activos de información.	Inventario de activos de Información, revisado y aprobado por la alta Dirección a. Determinar el criterio la importancia del activo. b. Determinar el propietario del activo. c. Según la clasificación Ley 1712 de 2014 medio de la cual se crea la Ley de Transparencia Guía No 5 - Gestión De Activos	Documento de Metodología de Gestión de activos de información. Matriz Inventario de activos de información.	Gestión TIC
	Actualizar la normativa referente a la seguridad y privacidad de la información	Contribuir al cumplimiento normativo, incluida la adopción de normas corporativas vinculantes: Ley 1581 y Registro Nacional de Bases de Datos (RNBD) de la Superintendencia de Industria y Comercio.	Matriz Legal de SGSI Política de privacidad de datos actualizada Registro Nacional de Bases de Datos (RNBD)	Gestión TIC Oficina asesora de Planeación Oficina Asesora Jurídica

FASE	ACTIVIDADES	DESCRIPCIÓN	METAS	RESPONSABLE
Planificación	Actualizar y/o elaborar los siguientes documentos: metodología de gestión de riesgos, plan de tratamiento de riesgos y declaración de aplicabilidad.	**Metodología y criterios de riesgo de seguridad,** aprobado por la alta Dirección que incluya: 1. Criterios de Aceptación de Riesgos o tolerancia al riesgo que han sido informados por la alta Dirección. 2. Criterios para realizar evaluaciones de riesgos. **Evaluaciones de riesgos**: a. Identificar los riesgos asociados con la pérdida de la confidencialidad, de integridad y de disponibilidad de la información dentro del alcance. b. Identificar los dueños y/o responsables de los riesgos. c. Evaluar las consecuencias (impacto) d. Evaluar la probabilidad que ocurran los riesgos identificados e. Determinar los niveles de riesgo. f. Evaluar los riesgos g. Priorizarlos riesgos analizados para el tratamiento de riesgos. **Plan de tratamiento de riesgo**s y la **declaración de aplicabilidad**: a. Tratar los riesgos, teniendo en cuenta los resultados de la evaluación de riesgos. b. Determinar los controles tratamiento de riesgos. c. Comparar los controles con los del Anexo A de la norma 27001 de 2013 d. La declaración de aplicabilidad debe indicar si los objetivos de control y los controles se encuentran implementados y en operación. Guía No 7 - Gestión de Riesgos	Documento con la metodología de gestión de riesgos. Identificación, Valoración y tratamiento de riesgo. Declaración de Aplicabilidad	Gestión TIC

FASE	ACTIVIDADES	DESCRIPCIÓN	METAS	RESPONSABLE
Planificación	Documento con el Plan de diagnóstico para la Transición IPv4 a IPv6 transición de IPv4 a IPv6.	Plan de diagnóstico que debe contener los siguientes componentes: Inventario de TI (Hardware y software) , Informe de la Infraestructura de red de comunicaciones, recomendaciones para adquisición de elementos de comunicaciones , de cómputo y almacenamiento con el cumplimiento de IPv6. Guía No 20 - Transición IPv4 a IPv6	Plan de diagnóstico de IPv4 a IPv6. Inventario de activos de IPv6.	Gestión TIC
Implementación	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.	Indicadores de gestión está orientada principalmente en la medición de efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información. Guía No 9 - Indicadores de Gestión SI.	Indicadores De Gestión.	Gestión TIC
Evaluación del Desempeño	Documento con auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.	Documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías, verificando como se asegura que los hallazgos, brechas, debilidades y oportunidades de mejora se subsanen, para asegurar la mejora continua. Guía No 15 – Guía de Auditoría.	Plan de Ejecución de Auditorias	Gestión TIC Control Interno
Mejora Continua	Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados.	Resultados de la ejecución plan de seguimiento, evaluación y análisis para el MSPI. Guía No 17 – Mejora Continua	Plan de mejora continua	Gestión TIC Oficina asesora de Planeación

6. NORMATIVA

Decreto 612 de 2018

Decreto único reglamentario 1078 de 2015

Guía - Modelo de Seguridad y Privacidad de la Información - MINTIC

NTC-ISO-IEC27001:2013: Sistemas de Gestión de la Seguridad de la información.

NTC-ISO-IEC27002:2013: Código de Buenas Prácticas en Gestión de la Seguridad de la Información

7. DEFINICIONES

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

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.

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la
justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

MSPI: Modelo de Seguridad y privacidad de la información.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

(Fuente ISO 27000)