PLAN: SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - IDPC
PROCESO: GESTIÓN DE SISTEMAS DE INFORMACIÓN Y TECNOLOGÍA
Versión: 8 del 29 de Diciembre de 2023

Contenido

1. Objetivo

Fortalecer el Modelo de Seguridad y Privacidad de la Información en el Instituto Distrital de Patrimonio Cultural.

2. Alcance

El alcance se encuentra definido para todo el personal del Instituto Distrital de Patrimonio Cultural, tanto contratistas de apoyo a la gestión como personal de planta y terceros que tengan acceso a la información de la Entidad; en todos los niveles jerárquicos, desde los directivos hasta los asistenciales.

Se debe tener especial atención, con las empresas de vigilancia, servicios generales y las que prestan el servicio de mensajería.

El presente plan de seguridad de la información está proyectado para la vigencia 2023.

3. Definiciones

Activo de Información: Es cualquier elemento que procese información, la almacena o ayude a protegerla, pero, además, que genere valor para la Entidad.

Backup: Es la copia de los datos importantes de un dispositivo primario en uno ó varios dispositivos secundarios, ello para que en caso de que el primer dispositivo sufra una avería electromecánica o un error en su estructura lógica, sea posible contar con la mayor parte de la información necesaria

Bring Your Own Device (BYOD): Tendencia que se está presentando en las empresas y entidades, que consiste en que los empleados, servidores públicos o contratistas de prestación de servicios utilizan para el trabajo su propio computador o dispositivo móvil, celular o tableta.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Continuidad de Negocio: describe los procesos y procedimientos que una organización pone en marcha para garantizar que las funciones esenciales puedan continuar durante y después de un desastre.

Contraseña: Código secreto que se introduce en una máquina, para poder accionar un mecanismo o para acceder a ciertas funciones informáticas.

Control: Acciones o mecanismos definidos, para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

Continuidad del Negocio: Describe los procesos y procedimientos que una organización pone en marcha, para garantizar que las funciones esenciales, puedan continuar durante y después de un desastre.

Disponibilidad: Propiedad de la información, de estar accesible y utilizable, cuando lo requiera una entidad autorizada.

Información: Datos organizados de tal forma que tienen un significado. Consecuencias que genera un riesgo una vez se materialice.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

4. Normatividad

Ley 23 de 1982. Ley sobre derechos de autor

Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de
certificación y se dictan otras disposiciones.

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1450 de 2011. Por la cual se expide el Plan Nacional de Desarrollo, 2010-2014.

Ley Estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales.

Ley 1712 de 2014, Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.

Decreto 1078 de 2015, Por medio del cual se expide el Decreto Único. Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

Resolución Distrital 305 de 2008, Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, caridad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.

Resolución 004 de 2017, Por la cual se modifica la Resolución 305 de 2008 de la CDS.

MINTIC Resolución 500 de marzo 10 de 2021, “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” modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”

Documento CONPES 3701 de 2011 - Lineamientos de Políticas sobre ciberseguridad y ciberdefensa.

Documento CONPES 3854 de 2016 - Política Nacional de Seguridad Digital.
Documento CONPES 3995 de 2020 - Política Nacional De Confianza y Seguridad Digital

NTC/ISO 27001:2013. Sistemas de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información.

5. Responsabilidades

Subdirección de Gestión Corporativa: Garantizar los recursos y definir las actividades necesarias para la implementación del plan asegurando su cumplimiento.

Gestión de Sistemas de Información y Tecnología: Ejecutar las actividades definidas para salvaguardar la información y planear campañas de sensibilización con temas de seguridad.

Direccionamiento Estratégico: Definir contexto estratégico de la Entidad con enfoque de Seguridad de la Información.

Oficina de Comunicación Estratégica: Diseñar y divulgar campañas de sensibilización en temas de seguridad.

Administración de Bienes e Infraestructura: Definir protocolos de seguridad física.

Gestión Documental: Definir las actividades para la clasificación y etiquetado de información física.

Seguimiento y Evaluación (Control Interno): Realizar auditoría al Sistema de Gestión de Seguridad de la Información.

6. Actividades Plan

El plan detallado se anexa en el formato de seguimiento de plan de seguridad de la información, a continuación, se describen las actividades, responsable y producto.

Tabla 1 Actividades Plan

ID	ACTIVIDADES	RESPONSABLE	PRODUCTOS
1	Actualizar el diagnóstico de seguridad y privacidad de la información de acuerdo con las normas ISO 27001 y el MSPI y de Mintic.	Gestión de sistemas de información y tecnología (Oficial de seguridad de la información)	Dos (2) autodiagnósticos de MSPI
2	Mantener actualizado el manual de las políticas de seguridad de la privacidad de la información de acuerdo con las normas ISO 27001 y la estrategia de gobierno digital	Gestión de sistemas de información y tecnología (Oficial de seguridad de la información)	Un (1) actualización del manual de políticas de seguridad y privacidad de la información (mejora continua)
3	Realizar una auditoría técnica de seguridad sobre la infraestructura informática del Instituto Distrital de Patrimonio Cultural IDPC.	Gestión de sistemas de información y tecnología (Oficial de seguridad de la información)	Un (1) informe de auditoría técnica
4	Realizar dos (2) pruebas de vulnerabilidades sobre la infraestructura informática perimetral del Instituto Distrital de Patrimonio Cultural IDPC.	Gestión de sistemas de información y tecnología (Oficial de seguridad de la información)	Dos (2) Informes de las pruebas de vulnerabilidad
5	Mantener actualizado el inventario de activos de información junto con los líderes de cada uno de los	Gestión de sistemas de información y tecnología (Oficial de seguridad de la información)	Una (1ª) actualización

ID	ACTIVIDADES	RESPONSABLE	PRODUCTOS
	procesos del Instituto Distrital de Patrimonio Cultural IDPC		del inventario de activos de información
6	Gestionar la matriz de riesgos de seguridad de la información (Identificar, valorar y apoyar la gestión del tratamiento)	Gestión de sistemas de información y tecnología (Oficial de seguridad de la información)	Dos (2) seguimientos de la matriz de riesgos de seguridad de la información
7	Gestionar las pruebas al plan de recuperación de desastres DRP.	Gestión de sistemas de información y tecnología (Oficial de seguridad de la información)	Un (1) informe con los resultados de las pruebas del plan DRP
8	Capacitar a funcionarios y contratistas sobre los riesgos de seguridad digital. - Formulario de evaluación al contenido	Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información)	Un (1) informe de capacitación realizada a funcionarios y contratistas (Listas de asistencia y presentación)
9	Incorporar en la Metodología de desarrollo de software, el ciclo de vida de desarrollo de software seguro.	Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información)	Un (1) Documento con Metodología de desarrollo de software y el ciclo de vida de desarrollo de software seguro para IDPC
10	Actualizar la declaración de aplicabilidad	Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información)	Un (1) Documento de declaración de aplicabilidad actualizada

7. Control de Cambios

Fecha	Versión	Cambios Introducidos	Simplificación o mejora	Origen
28/01/2019	01	Creación del documento.		
28/01/2020	02	Ajuste de formato y contenido.		
14/12/2020	03	Ajuste de objetivo, alcance y las actividades a ejecutar.	Mejora	Requerimiento FURAG
27/08/2021	04	Ajuste fecha de vigencia, actividades a ejecutar y modificación nombre actividad - producto No. 29, se incluye la actividad No. 30.	Mejora	FURAG.
11/11/2021	05	Se ajusta el producto a entregar en la actividad No. 18. Se ajusta el producto a entregar en la actividad No. 23	Mejora	
20/12/2021	06	Ajuste de Objetivo, alcance y las actividades a ejecutar	Mejora	Revisión de actualización
30/01/2023	07	Ajuste de responsabilidades, alcance y las actividades a ejecutar.	Mejora	Revisión de actualización
29/12/2023	08	Cambio de formato	Mejora	Resultado de revisión y autocontrol

8. Créditos

Elaboró	Revisó	Aprobó
Ángel Antonio Diaz Vega	Mary Rojas	Aura Herminda López Salazar
Cargo – Rol: Contratista – Oficial de Seguridad de la Información Subdirección de Gestión Corporativa	Cargo – Rol: Contratista Líder TI- Subdirección de Gestión Corporativa	Cargo – Rol: subdirectora de la Subdirección de Gestión Corporativa Comité Institucional de Gestión y Desempeño
Aprobado	Memorando interno con N° radicado 20235600183403 del 29-12-2023	