INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
CULTURA, RECREACIÓN Y DEPORTE
Instituto Distrital del Patrimonio Cultural

Plan

Seguridad y privacidad de la información - IDPC

Proceso

Gestión de Sistemas de Información y Tecnología

Vigencia: 31 enero de 2022

Versión: 06

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 2022

3. DEFINICIONES

TÉRMINO	DEFINICIÓN
Activo de Información	Es cualquier elemento que procese información, la almacene 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 ó 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 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
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.

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. Requisitos.

5. RESPONSABILIDADES

Subdirección de Gestión Corporativa: Definir las actividades necesarias para la implementación del plan y asegurar 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 auditoria 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.

ID	Actividades	RESPONSABLE	Productos
1	Actualizar el autodiagnóstico de Seguridad y Privacidad de la Información de acuerdo con las normas internacionales ISO 27001 y el MSPI de MinTIC. (Realizar de manera semestral)	Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información)	2 Autodiagnóstico de la evaluación de MSPI
2	Mantener actualizado el documento de las políticas de MSPI de acuerdo con las normas internacionales ISO 27001 y la estrategia de Gobierno en Digital.	Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información)	1 actualización del Manual de políticas de seguridad y privacidad de la información (Mejora Continua)
3	Actualizar la política de protección de datos personales	Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información)	1 Documento de política de datos personales
4	Realizar 1 prueba de auditoría técnica de seguridad sobre la infraestructura informática del IDPC.	Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información)	1 Informe de Auditoría Técnica
5	Gestionar una revisión interna del estado del SGSI en la entidad (De ser posible se debería realizar por algún experto externo a la entidad)	Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información)	Documento de la Gestión realizada para la revisión interna del SGSI.

6	Realizar el BIA (análisis de impacto del negocio) para definir el plan de recuperación de desastres de los procesos de tecnología y seguridad de la información.	Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información)	1 Informe BIA (análisis de impacto del negocio)
7	Elaborar el procedimiento de gestión de incidentes de seguridad de la información.	Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información)	1 procedimiento de adoptado en el SIG
8	Elaborar el plan de recuperación de desastres basado en la norma ISO 22301 vigente (Se limita a la definición del DRP)	Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información)	Plan de recuperación de desastres
9	Actualizar la metodología de riesgos de seguridad digital.	Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información)	1 Manual de Gestión de riesgos actualizado 1 Matriz de identificación y valoración de riesgos de seguridad de la información
10	Capacitar a funcionarios y contratistas sobre los riesgos de seguridad digital.	Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información)	1 Capacitación realizada
11	Actualizar, clasificar y valorar los Activos de Información	Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información)	Matriz de activos de información actualizada
12	Realizar monitoreo a los riesgos de seguridad de la información	Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información)	2 matrices de monitoreo

7. CONTROL DE CAMBIOS

Fecha	Versión	Cambios Introducidos	Simplificación o mejora	Origen
28/01/2019	1	Creación del Documentos		
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	
28/01/2022	06	Ajuste de Objetivo, alcance y las actividades a ejecutar en el año 2022	Mejora	Revisión de actualización

8. CRÉDITOS

Elaboró	Revisó	Aprobó
Ángel Antonio Díaz Vega Contratista – Oficial de Seguridad de la Información - Subdirección de Gestión Corporativa	Mary Rojas Contratista – Líder TI - Subdirección de Gestión Corporativa	Juan Fernando Acosta Mirkow Subdirector de Gestión Corporativa
Aprobado	Acta Comité Institucional de Gestión y Desempeño, de 31 de enero 2022	