

Contenido

Contenido	1
1. Objetivo	2
2. Alcance	2
3. Definiciones.....	2
4. Responsabilidades.....	3
5. Actividades Plan.....	4
6. Control de Cambios	6
7. Créditos	7

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 2024.

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. 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.

5. 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 27001:2022, el MSPI y actualizar el diagnóstico del GAP de protección de datos personales.	Gestión de sistemas de información y tecnología (Oficial de seguridad de la información)	Dos (2) Autodiagnósticos con el Instrumento de diagnóstico MSPI y el GAP de protección de datos personales. (Instrumentos de diagnóstico vigentes)
2	Evaluar y actualizar la documentación del MSPI que requiera ser ajustada de acuerdo con los lineamientos institucionales y normativos aplicables.	Gestión de sistemas de información y tecnología (Oficial de seguridad de la información)	Una (1) la matriz de riesgos de seguridad actualizada de acuerdo a las definiciones de la norma NTC ISO IEC 27001:2022 - NTC ISO IEC 27002:2022
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 tres (3) pruebas de vulnerabilidades sobre	Gestión de sistemas de información y tecnología	Tres (3) Informes de las pruebas de

PLAN: SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - IDPC
PROCESO: GESTIÓN DE SISTEMAS DE INFORMACIÓN Y TECNOLOGÍA
 Versión: 9 del 31 de enero de 2024

ID	ACTIVIDADES	RESPONSABLE	PRODUCTOS
	la infraestructura informática perimetral del Instituto Distrital de Patrimonio Cultural IDPC.	(Oficial de seguridad de la información)	vulnerabilidad abril – agosto -
5	Mantener actualizado el inventario de activos de información junto con los líderes de cada uno de los procesos del Instituto Distrital de Patrimonio Cultural IDPC	Gestión de sistemas de información y tecnología (Oficial de seguridad de la información)	Una (1) actualización del inventario de activos de información
6	Gestionar la matriz de riesgos de seguridad de la información y reportar los riesgos de acuerdo con las definiciones institucionales. (Identificar, valorar y apoyar la gestión del tratamiento)	Gestión de sistemas de información y tecnología (Oficial de seguridad de la información)	Tres (3) informes de seguimiento de la matriz de riesgos de seguridad de la Información y la matriz de riesgos de seguridad actualizada (cuatrimestral)
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 de evaluación a los servicios de seguridad en el plan de DRP (funcionalidad de los controles de seguridad)
8	Capacitar a funcionarios y contratistas sobre la seguridad de la información fortaleciendo la cultura y apropiación en el IDPC.	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) Formulario de evaluación al Contenido

PLAN: SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - IDPC
PROCESO: GESTIÓN DE SISTEMAS DE INFORMACIÓN Y TECNOLOGÍA
 Versión: 9 del 31 de enero de 2024

ID	ACTIVIDADES	RESPONSABLE	PRODUCTOS
9	Capacitar a funcionarios y contratistas sobre la Protección de datos personales fortaleciendo la cultura y apropiación en el IDPC.	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) Formulario de evaluación al Contenido
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

6. 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	

PLAN: SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - IDPC
PROCESO: GESTIÓN DE SISTEMAS DE INFORMACIÓN Y TECNOLOGÍA
 Versión: 9 del 31 de enero de 2024

Fecha	Versión	Cambios Introducidos	Simplificación o mejora	Origen
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
30/01/2024	09	Ajuste de las actividades a ejecutar.	Mejora	Resultado de revisión y autocontrol

7. Créditos

Elaboró	Revisó	Aprobó
Ángel Antonio Díaz Vega	Mary Rojas	Comité Institucional de Gestión y Desempeño
Cargo – Rol: Contratista – Oficial de Seguridad de la Información Subdirección de Gestión Corporativa	Cargo – Rol: Profesional Especializado Código 222 grado 03 Subdirección de Gestión Corporativa	Acta No. 01 de 30 de enero de 2024
Aprobado	Acta No. 01 de 30 de enero de 2024 Comité Institucional de Gestión y Desempeño	