PLAN DE CAPACITACIÓN; SENSIBILIZACIÓN Y COMUNICACIÓN DE SEGURIDAD DE LA INFORMACIÓN -IDPC

PROCESO: GESTIÓN DE SISTEMAS DE INFORMACIÓN Y TECNOLOGÍA

Versión: 2 del 29 diciembre de 2023

Contenido

1. Introducción

El Ministerio de las Tecnologías de las Información y las Comunicaciones - MINTIC, a través del Modelo de Seguridad y Privacidad de la Información (MSPI), ha establecido pautas para la implementación de lineamientos y directrices que permiten robustecer la seguridad y privacidad de la información, más sin embargo esto no es suficiente, razón por la cual es fundamental involucrar el factor humano debido a que en la mayoría de los casos los incidentes de seguridad son originados por este factor, por razones de desconocimiento en seguridad del información y el rol que desempeñan en la entidad, afectando la preservación de disponibilidad, integridad y confidencialidad de la información.

De acuerdo a lo anterior surge la necesidad de capacitar, sensibilizar y comunicar a los funcionarios, contratistas, colaboradores y partes interesadas externas del Instituto Distrital de Patrimonio Cultural - IDPC, en temas de Seguridad de la Información permitiendo concientizar sobre la importancia de la preservación de disponibilidad, integridad y confidencialidad de la información, mitigando de esta manera los incidentes de seguridad de la información.

2. Objetivo

Establecer las estrategias para capacitar, sensibilizar y comunicar a los funcionarios, contratistas, colaboradores y partes interesadas externas del Instituto Distrital de Patrimonio Cultural - IDPC las directrices, políticas, controles y buenas prácticas establecidas en el Sistema de Gestión de Seguridad de la Información (SGSI), las cuales conducen a la preservación de la confidencialidad, integridad y disponibilidad de la información.

3. Alcance

El presente documento aplica para todos los funcionarios, contratistas, colaboradores y partes interesadas externas del Instituto Distrital de Patrimonio Cultural – IDPC.

4.Definiciones

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

Amenaza: Ente o escenario interno o externo, que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

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

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.

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

Impacto: Consecuencias que genera un riesgo una vez se materialice.

Información: Datos organizados de tal forma que tienen un significado.

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

Incidente de Seguridad de la Información: Se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información de la entidad.

Ingeniería Social: Conjunto de técnicas maliciosas que se aprovechan de la debilidad humana para robar información.

Partes interesadas: Son todos aquellos individuos, grupos u organizaciones que tengan algún beneficio o perjuicio, relacionado con los intereses y actividades de la entidad.

Riesgo: Escenario de incertidumbre, bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitándose cumplir con sus objetivos.

Sensibilización: Proceso de comunicación activo que promueve transformación, cambio de actitudes y comportamientos en las personas de la entidad.

Vulnerabilidad: Falencia o debilidad que es inherente a los activos de información o a los controles.

5. Roles y Necesidades

Tabla 1 Roles y Necesidades

ROL	OBJETIVO DE CONOCIMIENTO
Directivos y jefes de dependencias	Deben conocer las leyes, directivas, lineamientos, políticas y procedimientos relacionados con el Sistema de Gestión de Seguridad de la Información, también deben comprender el liderazgo que su rol tiene y que su ejemplo permitirá orientar las actuaciones del personal bajo su cargo
Funcionarios y Contratistas	Deben conocer todos los lineamientos del Sistema de Gestión de Seguridad de la Información y las reglas de comportamientos adecuados para proteger los sistemas e información institucional que tienen a su cargo. A su vez deben ser conscientes de la importancia de reportar cualquier incidente, vulnerabilidad o riesgo potencial que afecte la seguridad de la información.
Administradores de Sistemas	Deben conocer las políticas de Seguridad de la Información, en especial los controles de seguridad relacionados con los sistemas de información a su cargo.
Administradores de infraestructura tecnológica y personal de soporte	Deben conocer las leyes, directivas, lineamientos, políticas y procedimientos relacionados con el Sistema de Gestión de Seguridad de la Información, para soportar las operaciones críticas del IDPC de manera apropiada, adicionalmente deberán estar en capacidad de orientar y hacer cumplir los lineamientos del Sistema de Gestión de Seguridad de la Información en el IDPC.
Partes interesadas externas	Deben conocer las directrices y lineamientos que el IDPC establece para acceder a la información y correspondiente protección que en el cumplimiento de sus funciones u obligaciones requieran conocer.

Estrategias de Comunicación y Divulgación

5.1 Socialización de Documentación

El Instituto Distrital de Patrimonio Cultural Cuando se realice la creación o actualización correspondiente a la documentación del Sistema de Gestión de Seguridad de la Información, se deberá realizar la gestión correspondiente para dar a conocer al personal del Instituto Distrital de Patrimonio Cultural - IDPC, los lineamientos contenidos en el mismo.

Las actividades a tener en cuenta son las siguientes:

- Con el apoyo de la dependencia responsable diseñar piezas gráficas en relación al documento a socializar y/o difundir por medio de los canales internos (correo electrónico, intranet, fondo de escritorio) establecidos por el Instituto Distrital de Patrimonio Cultural -IDPC.
- Realizar reuniones virtuales o presenciales en los casos que se requiera brindar aclaración en el documento divulgado.

Periodicidad: De acuerdo a la creación o actualización y publicación relacionada con la documentación del SGSI.

- así como el retiro de permisos, privilegios y configuraciones realizadas sobre dicho dispositivo.

5.2 Noticias o Boletines Informativos de Seguridad de la Información

Es fundamental que todas las partes interesadas del Instituto Distrital de Patrimonio Cultural – IDPC, sean sensibilizadas y concientizadas en temas de Seguridad de la Información, adoptando e implementando medidas y controles estrictos para salvaguardar la confidencialidad, integridad y disponibilidad de los sistemas e información del IDPC, es por ello que la responsable del Sistema de Gestión de Seguridad de la Información socializará noticias o boletines informativos de Seguridad.

Las actividades a tener en cuenta son las siguientes:

- Diseñar piezas gráficas que contengan noticias o boletines de Seguridad de la Información.

- Realizar la publicación por medio de los canales internos (correo electrónico, intranet, fondo de escritorio) establecidos por el Instituto Distrital de Patrimonio Cultural -IDPC
- En caso de presentarse alguna duda se brindará la respuesta correspondiente.

Periodicidad: De acuerdo a lo establecido en el cronograma de Capacitación, Sensibilización y Comunicación de Seguridad de la Información.

6. Implementación

A continuación, se evidencia el cronograma de Capacitación, Sensibilización y Comunicación de Seguridad de la Información el cual será implementado para la vigencia 2021.

Tabla 2Cronograma de trabajo

No	Temática	Canal de Comunicación	Medio de comunicación	Herramienta	Primer Trimestre	Segundo Trimestre	Tercer Trimestre	Cuarto Trimestre
1	**Manual de políticas de seguridad y privacidad de la información, tips Seguridad de la Información, Boletín informativo Seguridad de la Información, divulgación,campañas ataques informáticos o socialización documentación del SGSI.**	**Comunicación al interior de la entidad**	**Correo electrónico, intranet, boletín IDPC, reuniones.**	**Piezas gráficas**	**x**	**x**	**x**	**x**

7. Evaluación

Con la finalidad de realizar la evaluación al Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información, se elaborará una encuesta sobre el estado de sensibilización de Seguridad de la Información por medio de Formulario Google para que los usuarios realicen el diligenciamiento correspondiente.

- Impacto en la organización, dependiendo del rol y cargo.
- Conocimiento sobre el Manual de Políticas de Seguridad de la Información.

• Identificación de necesidades de capacitación y/o reinducción.
• Identificación de nuevas habilidades de entrenamiento.

8. Evaluación Mejoramiento del Plan de Capacitaciones

El Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información, debe mantenerse actualizado, razón por la cual es necesario realizar la correspondiente revisión y actualización del contenido, teniendo en cuenta los resultados obtenidos de la evaluación de las actividades realizadas, permitiendo de esta manera definir los ajustes y mejoras correspondientes.

De igual manera es fundamental tener en cuenta factores relacionados con avances tecnológicos, adquisición de nuevas aplicaciones e infraestructura, nuevas amenazas y vulnerabilidades, modalidades de ingeniería social, nuevas leyes o normatividad que impliquen adoptar nuevas medidas de seguridad que permitan mejorar el Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información.

9. Control de cambios

Fecha	Versión	Cambios Introducidos	Simplificación o mejora	Origen
28/08/2021	01	Creación del documento.	Mejora	MSPI.
29/12/2023	02	Cambio de formato	Mejora	Resultados de revisión y autocontrol

10. Créditos

Elaboró	**Revisó**	**Aprobó**
Nombre(s): Ángel Diaz vega	Nombre(s): Mary Elizabeth Rojas Muñoz	Nombre: Aura López
Cargo – Rol: Contratista – Oficial de Seguridad de la Información - Subdirección	Cargo – Rol: Profesional especializado Subdirección de Gestión Corporativa	Cargo: Jefa Subdirección de Gestión Corporativa
Documento de aprobación	Memorando interno con N° radicado 20235600183403 del 29-12-2023	