**PLAN: SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - IDPC**

PROCESO: GESTIÓN DE SISTEMAS DE INFORMACIÓN Y TECNOLOGÍA

Versión: 10 del 30 de diciembre de 2024

# Contenido

1. [**Objetivo** 1](#_heading=h.gjdgxs)
2. [**Alcance** 1](#_heading=h.30j0zll)
3. [**Definiciones** 2](#_heading=h.1fob9te)
4. [**Normatividad** 3](#_heading=h.3znysh7)
5. [**Responsabilidades** 4](#_heading=h.2et92p0)
6. [**Actividades Plan 5**](#_heading=h.tyjcwt)
7. [**Control de Cambios 7**](#_heading=h.1t3h5sf)
8. [**Créditos 8**](#_heading=h.4d34og8)

# Objetivo

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

# 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 2025.

# Definiciones

**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 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.

# 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.

# 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.

# 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 la  infraestructura informática  Perimetral del Instituto Distrital de Patrimonio Cultural IDPC. | Gestión de sistemas de  información y tecnología  (Oficial de seguridad de la  información) | Tres (3) Informes de las  pruebas de vulnerabilidad |
| 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 | Establecer el BCP del proceso de gestión de sistemas de información y tecnología Y presentar ante el comité institucional de gestión y desempeño la necesidad de crear el BCP institucional | Gestión de sistemas de  información y tecnología  (Oficial de seguridad de la  información) | Un (1) Documento de BCP del Proceso de Gestión de Sistemas de Información y Tecnología. |
| 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) | dos (2)  capacitaciones realizadas a funcionarios y  contratistas (Listas de  asistencia y  presentación)  Formulario de evaluación al  Contenido |
| 9 | Realizar la actualización del manual de seguridad y privacidad de la información. | Gestión de Sistemas de  Información y Tecnología  (Oficial de Seguridad de la  Información) | Un (1) Documento actualizado. |
| 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 |
| 11 | Elaborar una guía para gestionar los eventos del sistema de seguridad perimetral. | Gestión de Sistemas de  Información y Tecnología  (Oficial de Seguridad de la  Información) | Una (1) guía de eventos de seguridad. |
| 12 | Elaborar el instructivo de gestión de los ambientes de desarrollo, pruebas y producción. | Gestión de Sistemas de  Información y Tecnología  (Oficial de Seguridad de la  Información y equipo de desarrollo) | Un (1) Documento de gestión de los ambientes de desarrollo, pruebas y producción. |
| 13 | Realizar una prueba de Ingeniería Social. | Gestión de Sistemas de  Información y Tecnología  (Oficial de Seguridad de la  Información) | Un (1) informe del resultado de la prueba de ingeniería social y plan de mejora si corresponde. |
| 14 | Realizar una evaluación de seguridad a los centros de cableado en aplicación de los controles del MSPI. | Gestión de Sistemas de  Información y Tecnología  (Oficial de Seguridad de la  Información) | Un (1) informe del resultado de la evaluación. |
| 15 | Actualizar la Política de Seguridad y Privacidad de la Información (Partes interesadas). | Gestión de Sistemas de  Información y Tecnología  (Oficial de Seguridad de la  Información) | Una (1) Política de Seguridad y Privacidad de la Información actualizada. |
| 16 | Realizar la calificación de riesgos de seguridad de la información y la valoración de sus controles.  ISO27001 2022 | Gestión de Sistemas de  Información y Tecnología  (Oficial de Seguridad de la  Información) | Una (1) matriz de riesgos con registro de las calificaciones. |

## 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 |
| 31/01/2024 | 09 | Ajuste de las actividades a ejecutar. | Mejora | Resultado de revisión y autocontrol |
| 30/12/2024 | 10 | Ajuste de las actividades a ejecutar. | Mejora | Resultado de revisión y autocontrol |

# Créditos

| **Elaboró** | **Revisó** | **Aprobó** |
| --- | --- | --- |
| Ángel Antonio Díaz Vega | Mary Rojas |  |
| 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 | Comité Institucional de Gestión y Desempeño |
| Aprobado | Acta del 30-12-2024 Comité Institucional de Gestión y Desempeño | |