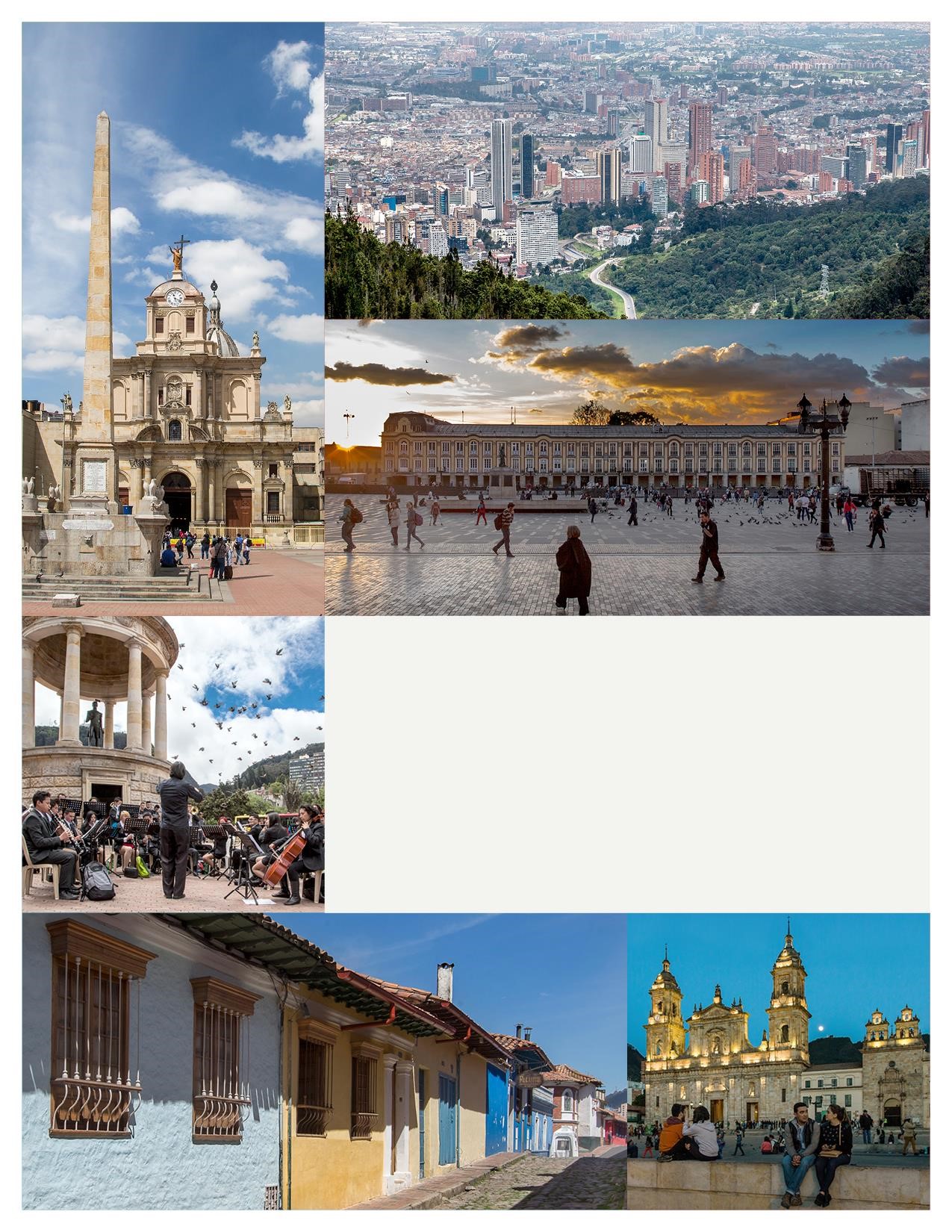
Vigencia: 28 Diciembre 2020

Versión: 03



INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL



**Plan**

Seguridad y privacidad de la información - IDPC

**Proceso**

Gestión de Sistemas de Información y Tecnología

# **OBJETIVO**

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

# **ALCANCE**

Abarca a 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 esta proyectado para cuarto trimestre del 2020 y la vigencia 2021

# **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. |

# **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.

# **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.

# **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 | Diagnosticar la Seguridad y Privacidad de la Información de acuerdo a las normas internacionales ISO 27001 y el MSPI de MinTIC. | Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información) | - Plan de Seguridad y privacidad de la información para la vigencia 2020 - Autodiagnóstico de la evaluación de MSPI |
| 2 | Definir las políticas de MSPI de acuerdo a 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) | - Documento con la Política general del modelo de seguridad de la información - Documento con el manual de políticas de seguridad de la información |
| 3 | Elaborar documento que contenga el marco normativo y estándares de tecnología. | Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información) | Normograma actualizado de SGSI |
| 4 | Definir metodología para la gestión de activos de información. | Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información) | - Documento con la metodología para la gestión de activos de información - Instrumento/herramienta para la gestión de activos de información |
| 5 | Realizar acciones para fortalecer la toma de conciencia sobre la seguridad de la información. | Gestión de Sistemas de Información y Tecnología Gestión Talento Humano | Campañas de divulgación de seguridad de la información |
| 6 | Estructurar e implementar la metodología de riesgos de seguridad y privacidad de la información. | Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información) | Documento con la metodología de gestión de Riesgos de Privacidad y Seguridad de la Información |
| 7 | Elaborar modelo de matriz de riesgos para la seguridad y privacidad de la información. | Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información) | Instrumento/herramienta para la gestión de riesgos de seguridad de la información |
| 8 | Definir los roles y responsabilidades que se debe tener para el gobierno de seguridad de la información del IDPC. | Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información) | Documento con los roles y responsabilidades de SGSI |
| 9 | Realizar pruebas de auditoría técnica de seguridad sobre la infraestructura informática del IDPC. | Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información) | Informe de vulnerabilidades |
| 10 | Elaborar contexto estratégico de la organización | Direccionamiento Estratégico | Matriz DOFA con enfoque de Seguridad de la información |
| 11 | Identificar partes interesadas pertinentes al SGSI | Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información) | Listado de partes interesadas |
| 12 | Identificar los requisitos de las partes interesadas en relación con seguridad de la información | Gestión de Sistemas de Información y Tecnología | Informe de las necesidades de las partes interesadas |
| 13 | Definir el alcance del SGSI | Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información) | Acto administrativo en el que se define el alcance en términos de los procesos que están incluidos en el SGSI (Se recomienda que se incluya los procesos misionales, Gestión Documental y Sistemas y tecnología) |
| 14 | Definir indicadores de eficacia para el SGSI | Direccionamiento Estratégico Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información) | Tablero de indicadores de SGSI (mínimo tres indicadores 1. Cumplimiento de actividades del plan de acción, 2. Implementación de controles, 3. Nivel de apropiación del SGSI ) |
| 15 | Identificar activos de información | Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información) | Inventario de activos de información (Sugiere contar con un inventario de toda la entidad y uno por proceso) |
| 16 | Gestionar riesgos de seguridad de la información (Identificar, valorar y tratar) | Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información) | Matriz de riesgos de seguridad de la información |
| 17 | Elaborar una Declaración de Aplicabilidad que tenga los controles necesarios y la justificación de las exclusiones | Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información) | Declaración de Aplicabilidad |
| 18 | Elaborar documento donde se definan las competencias mínimas de las personas que vayan a manejar información sensible (Asegurar que las personas sean competentes, basándose en: educación, formación o experiencia adecuadas.) | Gestión de Sistemas de Información y Tecnología Gestión Talento Humano Gestión Contractual | Documento de competencias mínimas |
| 19 | Definir y elaborar un plan de comunicación y divulgación del SGSI (Divulgar política, alcance, roles y responsabilidades de seguridad de la información y algunos controles) | Comunicación Estratégica | Plan de comunicación y divulgación del SGSI |
| 20 | Ejecución del plan de comunicación y divulgación del SGSI | Comunicación Estratégica | Piezas de divulgación |
| 21 | Elaborar guía, instructivo o lista de contacto para las autoridades y grupos de interés (autoridades reguladoras u otras autoridades y organismos que podrían necesitar ser contactados en caso de consultas, incidentes y emergencias. Y grupos de interés, como proveedores de TI, páginas, foros y blogs de Seguridad de la información) | Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información) | Guía, instructivo o lista de contactos |
| 22 | Oficializar mesa de trabajo con el personal o encargado de Gestión de Proyectos de la entidad, con el fin de integrar la seguridad de la información en el ciclo de vida de los proyectos. | Direccionamiento Estratégico Gestión de Sistemas de Información y Tecnología (Oficial de Seguridad de la Información) | Documento metodológico de gestión de proyectos con seguridad de la información |
| 23 | Fortalecer las políticas de autenticación de usuario en el Directorio Activo | Gestión de Sistemas de Información y Tecnología (Ingeniero Servidores) | Política implementada en el Directorio Activo |
| 24 | Elaborar procedimiento, instructivo o manual para la gestión de usuarios | Gestión de Sistemas de Información y Tecnología (Ingeniero Servidores) | Procedimiento, instructivo o manual |
| 25 | Elaborar protocolo o manual interno de seguridad física, definiendo los perímetros de seguridad y las áreas seguras. (Se recomienda incluir como área segura la dependencia de sistemas y los centros de datos y cableado) | Administración de Bienes e Infraestructura | Protocolo o manual interno |
| 26 | Aplicar política de pantalla limpia desde directorio activo | Gestión de Sistemas de Información y Tecnología (Ingeniero Servidores) | Política implementada en el Directorio Activo |
| 27 | Implementar sistema de monitoreo (Nagios, Zabbix) para medir la capacidad tecnológica | Gestión de Sistemas de Información y Tecnología (Ingeniero Redes) | Sistema de monitoreo y gestión de capacidad |
| 28 | Segmentar la red acuerdo a la clasificación, los niveles de confianza, dominios (público, escritorios, servidor, funciones, etc.). Separar las redes cableada e inalámbrica (Incluyendo invitados) | Gestión de Sistemas de Información y Tecnología (Ingeniero Redes) | Red segmentada |
| 29 | Establecer convenios con grupos especializados para respuesta a incidentes de seguridad de la información (ColCERT o CSIRT Gobierno) | Gestión de Sistemas de Información y Tecnología (Jefe TIC - Oficial de Seguridad de la Información) | Convenio establecido |
| 30 | Alinear metodología de activos de información con las tablas de retención documental TRD y la metodología de clasificación y etiquetado de la información | Gestión Documental Gestión de Sistemas de Información y Tecnología | Nuevas metodologías alineadas entre si |

# **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 |

# **CRÉDITOS**

|  |  |  |
| --- | --- | --- |
| Elaboró | Revisó | Aprobó |
| Luis Cortes Castiblanco  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 | Mediante Acta Comité Institucional de Gestión y Desempeño 14 de diciembre 2020 | |