

INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL



Plan

Seguridad y Privacidad de la Información-IDPC

Proceso

Gestión de Sistemas de Información y Tecnología

Vigencia: 28/01/2020

Versión: 02

1. **OBJETIVO**

Presentar el plan de seguridad y privacidad de la información del IDPC y los elementos que lo conforman, como marco de referencia para el establecimiento y regulación de lineamientos y medidas que permitan el aseguramiento de la protección y uso adecuado de la información y activos de información que la soportan al interior de la Entidad.

1. **ALCANCE**

El presente documento identifica e incluye las orientaciones para la gestión del ciclo de operación del modelo de seguridad y privacidad de la información - MSPI, el cual debe ser aplicado sobre todos los procesos del Instituto y de cumplimiento por parte de todos los servidores públicos con relación contractual. Se amplía información en la sección del PETI que referencia el Modelo de seguridad y privacidad la información y las políticas de seguridad.

1. **DEFINICIONES**

|  |  |
| --- | --- |
| **TÉRMINO** | **DEFINICIÓN** |
| Seguridad Informática | Entendemos por seguridad informática el conjunto de medidas adicionales a las usadas en el procesamiento computarizado normal, tales como: políticas, estándares, procedimientos, mecanismos, dispositivos y recursos, asignados expresamente para proteger la información contra su destrucción accidental o deliberada y su modificación o divulgación no autorizada. |
| Privacidad de Información | La protección de datos, también llamada **privacidad** de información, es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema **informático** pueden ser compartidos con terceros. |
| Activos de Información | Información importante que desea proteger frente a cualquier situación que suponga un riesgo o amenaza. Esta información que resulta fundamental para la organización es lo que se denomina activo. |
| Correo Electrónico | [Servicio de red](https://es.wikipedia.org/wiki/Servicio_de_red) que permite a los usuarios enviar y recibir mensajes mediante [redes de comunicación electrónica](https://es.wikipedia.org/wiki/Red_de_telecomunicaci%C3%B3n). |
| 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 |
| 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. |
| Internet | Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación. |

1. **NORMATIVIDAD**

**Ley 527 de 2099**. Por 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 1266 de 2008.** Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países 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 1341 de 2009**. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - TIC- Se crea la agencia Nacional de espectro y se dictan otras disposiciones.

**Ley 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.

**Decreto 1008 del 2018**. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

**Resolución 2999 del 2008**. Por el cual se adoptan las políticas de seguridad para el manejo de la información y se dictan otras normas para el uso y administración de los bienes y servicios informáticos del Ministerio TIC.

**Resolución 2007 de 2018**. Por la cual se actualiza la política de tratamiento de datos personales del Ministerio/Fondo TIC.

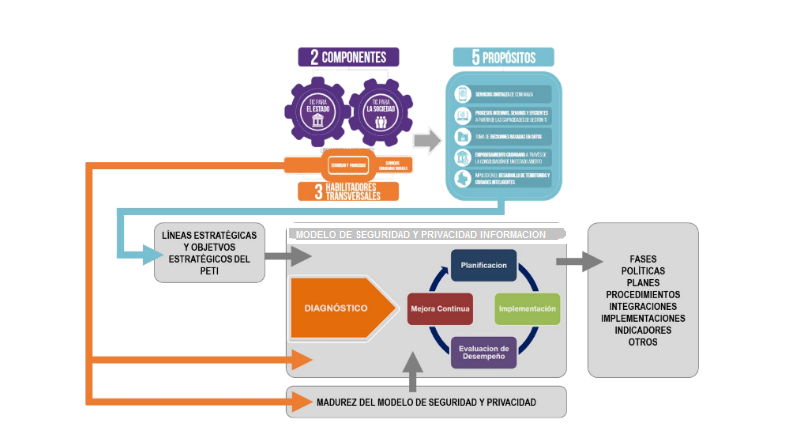
**Resolución 2133 de 2018**. Por la cual se establecen las condiciones especiales del Teletrabajo en el Ministerio de Tecnologías de la Información y las Comunicaciones, y se deroga las resoluciones No 3559 y 4950 de 2013, 2313 y 494 de 2014 y 2787 de 2016.

**Resolución 512 de 2019**. Por la cual se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información

**CONPES 3701 de 2011**. Lineamientos de Política para Ciberseguridad y Ciberdefensa.

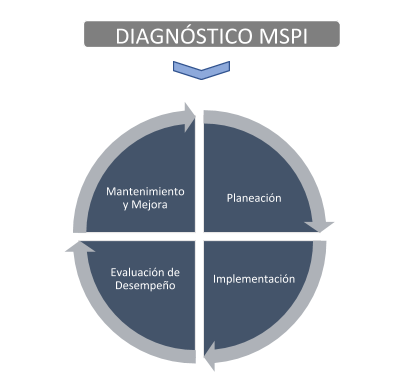
**CONPES 3854 de 2016.** Política Nacional de Seguridad digital.

1. **CONTENIDO**

Este Plan acoge el objetivo general de la Política de Gobierno Digital al igual que el PETI, definido así: “Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital”.

## CICLO DE OPERACIÓN DEL MSPI

Para la etapa inicial de los propósitos de diseño del Modelo de gestión de seguridad de la información (MSPI), se identificó la necesidad de definir las 5 fases que orientarán el ejercicio para los propósitos de protección de la información de la Entidad bajo un modelo sostenible; las fases del ciclo de operación se definen de la siguiente manera basadas en una fase inicial de diagnóstico:



## DIAGNÓSTICO DEL MSPI

En esta fase y mediante el uso de herramientas de diagnóstico, se deben desarrollar actividades de reconocimiento y valoración del estado de gestión, cumplimento de requisitos y lineamientos de seguridad de la información basado con el Modelo de Seguridad y Privacidad de Información de la estrategia de Gobierno Digital y de la implementación de controles de seguridad de la información con visión de mitigar todo tipo de escenario de riesgo asociado que pudiese generar un impacto indeseado a la Entidad.

El resultado de la evaluación de diagnóstico permitirá establecer el nivel de madurez del ciclo de operación del modelo de seguridad y privacidad de la información en el IDPC, y el mapa de ruta para las actividades claves de las fases de diseño y establecimiento del mismo modelo.

## PLANEACIÓN DEL MSPI

Partiendo de las [Políticas de Seguridad de la Información.](http://idpc.gov.co/archivos-pdf/2016/Normatividad/DE-GF-01_Politica_Seguridad_Informatica_IDPC.pdf) del IDPC se definirá una estructura de roles y asignación formal de responsabilidades orientados a la seguridad y privacidad de la información en diferentes niveles de la Entidad para permitir la adecuada y oportuna toma de decisiones enfocados al cumplimiento de los objetivos de seguridad y privacidad de la información (MSPI).

**Impacto**

Equipo de Sistemas, Incluyendo los funcionarios quienes laboran en el área de tecnología, tales como, profesionales y personal de apoyo.

Líderes de áreas y de procesos, entendiendo los propósitos de la Entidad y a los cuales deberán prestar su apoyo y responsabilidad para su aplicación.

Grupos Internos de Trabajo, tales como Control Interno, Gestión Humana, Jurídico, Planeación y demás áreas operativas del Instituto, para promover y aplicar las políticas, estándares y demás lineamientos del manual de seguridad de la información.

Terceras partes, tales como socios comerciales o de negocio, auditores externos y entidades de regulación, quienes requieren de su consulta para la comprensión de la estructura y conformación de la seguridad de la información, en beneficio del cumplimiento de las obligaciones legales, contractuales y demás aplicables.

Todos los funcionarios, contratistas, pasantes o partes interesadas, que presten sus servicios o tengan algún tipo de relación con la Entidad, quienes deben ser informados de las responsabilidades de seguridad a través de los términos y condiciones o contratos laborales, procedimientos de seguridad y guías, entrenamiento y sensibilización.

### Plan de Comunicaciones

El Instituto identificará y aplicará un plan de comunicaciones, de sensibilización y de capacitación que promueva estrategias para crear, incentivar y mantener una cultura organizacional mediante la generación de competencias y hábitos de protección de la información en todos los niveles de la Entidad.

El plan de comunicaciones de seguridad y privacidad de la información, y especialmente con respecto a actividades de socialización y sensibilización dirigida a los servidores públicos será ejecutado en conjunto con el apoyo del área de comunicaciones del IDPC.

## FASE DE IMPLEMENTACIÓN

El IDPC establecerá y liderará la gestión de seguridad de la información a través de la identificación de una estructura de roles y responsabilidades, que involucran las actividades de direccionamiento, implementación y control operacional en beneficio del cumplimiento de los propósitos de protección de la información y su mantenimiento eficaz a través del tiempo, así como de la conformación y asignación de responsabilidades pertinentes al sistema de gestión de seguridad de la información de la Entidad.

### Gestión de Activos de Información

Todos aquellos activos de información del Instituto Distrital de Patrimonio Cultural incluida la información que sea sensible o crítica para la operación o cumplimiento de la misión de la Entidad, deberán contar con la asignación de protección de su confidencialidad, integridad y disponibilidad en concordancia con los resultados de una evaluación de riesgos y el nivel de exposición identificado.

Los Activos de información de los procesos del IDPC deberán ser identificados y administrados dentro de un inventario, al igual que valorados con respecto a su sensibilidad o criticidad frente a impactos de afectación sobre la confidencialidad, integridad y disponibilidad de estos.

Se deberá integrar el Plan de preservación digital a largo plazo y también lo establecido en el Plan Anti-corrupción y de Atención al Ciudadano, con el fin de armonizar e identificar los riesgos y activos de información generados por el Instituto.

### Acceso y Uso de información

Todo servidor público o persona entenderá y asumirá su responsabilidad de protección de la información a través de su acceso y uso apropiados.

El IDPC será el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los servidores públicos o terceros, derivados del objeto y en cumplimiento de las funciones o tareas asignadas bajo acuerdo contractual.

Todos los servidores públicos o terceros deberán firmar el acuerdo de confidencialidad y transparencia, en el cual se establece la responsabilidad de confidencialidad de la información de la Entidad bajo su responsabilidad.

La información que será preservada por Sistemas, al momento de realizar BackUp, será la que se encuentra en la carpeta “Mis Documentos” de cada computador, allí debe reposar la información de carácter institucional, la gestión de esta copia de seguridad se realizará mediante el agente Datto y estará relacionada con el usuario de dominio del equipo de cómputo.

### Clasificación de la Información

Toda información al interior del IDPC deberá recibir el nivel de clasificación apropiado de acuerdo con las necesidades de protección del mismo, y a los riesgos potenciales asociados. Toda Información clasificada deberá recibir el sistema de etiquetado con la identificación del nivel de clasificación asignado.

### Uso y protección de equipo de cómputo

En los equipos de cómputo del Instituto de Patrimonio Cultural, tanto de arriendo como propios, se restringe la instalación de software o programas, sistemas de información, herramientas de software que no sean licenciados y autorizados. Por esta razón se solicita clave de administrador para realizar estas acciones, dicha clave es únicamente conocida por el equipo de Sistemas.

El equipo de cómputo no podrá ser utilizado para actividades de divulgación, propagación o almacenamiento de contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso, o cualquier otro uso que no esté autorizado.

A su vez en las Políticas establecidas en el firewall se bloquearán todos los contenidos que no son pertinentes y de riesgo para los usuarios.

### Uso de Correo Electrónico

El IDPC tendrá el derecho a realizar monitoreo o seguimiento del uso del correo electrónico a todos funcionarios y/o contratistas a quienes se les conceda una cuenta dentro del dominio del idpc.gov.co.

Los usuarios no deberán participar en correo electrónico que incite o incentive el envío de cadenas o publicidad que no sean de interés o estén relacionados con el IDPC. No se deberá realizar el envío o distribución de información catalogada como confidencial, interna o privada dentro o fuera de la del IDPC (sin la autorización correspondiente).

No se podrá hacer uso de lenguaje ofensivo, inapropiado o con declaraciones de blasfemia, obscenidad, ilegales, incitadores a infringir la ley, hostigamiento basado en sexo, raza, nacionalidad, contenido despectivo o difamatorio en cualquier mensaje electrónico para con sus compañeros, clientes, proveedores u otros; por lo tanto, los daños y perjuicios que pueda llegar a causar, serán de completa responsabilidad de la propietario de la cuenta de correo electrónico que la haya generado.

Se prohíbe el envío de correos masivos al interior de la organización; sólo los usuarios autorizados por el área de comunicaciones podrán enviar dichos correos.

Está prohibido utilizar el correo electrónico para el intercambio de información o de software que violen las leyes de derechos de autor.

Es responsabilidad de los usuarios de correo electrónico hacer mantenimiento a su buzón de correo: eliminar mensajes de la bandeja de entrada, archivar mensajes, Eliminar definitivamente los mensajes.

### Uso de Impresora y servicio de impresión

Los documentos que se impriman en las impresoras del IDPC deberán ser de carácter institucional, labores. La reparación o mantenimiento de las impresoras es exclusivo de ejecución por parte del Equipo de Sistemas o la empresa Proveedora del Servicio y ningún funcionario o persona podrá realizar dicha actividad.

También se tiene establecido la creación de usuario para impresión y copias, con el fin de generar un indicador de consumo y conocer el estado de gasto de papel, para visualizar la disminución de este impacto con las campañas de cero papeles, Orfeo y lo contemplado en el PIGA.

### Fondos de Pantalla y Bloqueo

Las pantallas de equipos de usuarios deberán ser bloqueadas para aquellos momentos en que no esté utilizando el equipo o ante la ausencia del funcionario de su puesto de trabajo, en concordancia con el programa de uso eficiente de energía.

El Fondo de Pantalla será actualizado por el área de Sistemas de manera centralizada con el fin de divulgar información institucional que se requiera.

### Uso de Internet

El Instituto se reserva el derecho de realizar monitoreo o seguimiento de los accesos a sitios en internet realizados por parte de los funcionarios públicos. El Instituto permitirá el acceso a servicios de internet, con lineamientos que garanticen la navegación y uso controlados de componentes del servicio. Se restringirá toda posibilidad de descarga de software no autorizado o código malicioso en los equipos de cómputo del Instituto a través de internet, así mismo el acceso y uso del servicio de internet se concederá sólo para propósitos laborales o fines particulares definidos y aprobados por el Instituto. Para los propósitos de almacenamiento de archivos e información, el Instituto dispone del servicio en la nube OneDrive.

Se restringirá el acceso a sitios web dedicados a compartir material audiovisual fotos, videos, streaming tales como Facebook, Youtube, Flickr, etc. Con las excepciones establecidas en los Roles por temas de naturaleza objetivo misional como sucede en el área de Comunicaciones. Estos Roles se identifican en las Políticas establecidas en el Firewall.

No se permitirá el acceso a sitios WEB con contenidos que están en contra de la ley, principios de ética moral del IDPC tales como, pornografía, terrorismo, contenidos obscenos, discriminación racial o similar.

Todos los dispositivos de la infraestructura de conectividad inalámbrica del IDPC, al conectarse a la red institucional estarán bajo las políticas establecidas en el Firewall del Instituto.

## ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Se deberán estructurar pautas y lineamientos de control de seguridad de la información para las actividades de adquisición, desarrollo y mantenimiento de los sistemas de información del IDPC, para las cuales se promulgue la confidencialidad, integridad y disponibilidad como parte integral de los mismos.

El proceso de adquisición y desarrollo de las aplicaciones debe ser estructurado y ordenado, considerando las diferentes etapas del ciclo de vida de las soluciones. La documentación de cada uno de los sistemas implantados en el Instituto debe contener la guía para brindar soporte, la cual incluye copia del contrato con el proveedor que lo brinda, en caso de que aplique esta modalidad, especificando los Acuerdos de Nivel de Servicio establecidos, los interlocutores y los procedimientos para obtener el servicio.

Dentro del PETI se contempla el Plan de Adquisiciones, el área de Sistemas realiza un acompañamiento desde el estudio de Conveniencia y oportunidad, hasta la entrega e implementación de los componentes de Tecnologías de Información adquiridas por el IDPC.

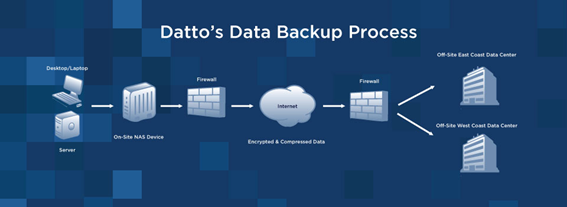
## GESTIÓN DE PROVEEDORES

El IDPC identificará pautas para establecer y mantener relaciones claras y fortalecidas con aquellos terceros con quien se establezca una relación contractual bien sea de servicios o de productos, que aseguren el adecuado cumplimiento de los acuerdos establecidos, donde se garantice la aplicación de medidas de seguridad de la información en cumplimiento de los objetivos de la Entidad.

## GESTIÓN DE SEGURIDAD EN LA CONTINUIDAD DEL NEGOCIO

La Entidad identificará las necesidades y requisitos de seguridad de la información para su vinculación en el plan de continuidad de negocio, de modo que se asegure que, ante situaciones de crisis o desastres, no se descuide los niveles de seguridad y se incurra en impactos indeseados.

Para esta finalidad el IDPC cuenta con la Solución de BackUp Datto, 4 en 1 que en caso de desastre nos permite recuperar un servidor en 5 minutos en el Cloud: Recuperación Virtual de Servidores Onsite y Offsite. Externalización de datos, manteniendo los parámetros establecidos en temas de seguridad y privacidad de la información, derechos de autor y control sobre la información.



### 

## EVALUACIÓN MSPI

Con el propósito de conocer los estados de cumplimiento de los objetivos de seguridad de la información, se mantendrán esquemas de seguimiento y medición al cumplimiento de aspectos del modelo de seguridad y privacidad de información que permitan contextualizar una toma de decisiones de manera oportuna.

Para este fin, el IDPC definirá procedimientos que permitan:

* Definir y orientar actividades para la identificación de situaciones de eventos o incidentes de seguridad y privacidad de la información.
* Definir los esquemas de atención a los eventos e incidentes de seguridad de la información, en beneficio de prevenir y mitigar escenarios de impacto a la Entidad.
* Emprender revisiones regulares de la eficacia del MSPI (que incluyen el cumplir la política de seguridad de la información, los objetivos, los controles) teniendo en cuenta los resultados de las auditorías de seguridad, incidentes, medición de la eficacia sugeridas y la retroalimentación de las partes interesadas. Apoyo en Control Interno y Herramientas de Autodiagnóstico entregadas por Planeación generando un indicador del MSPI.
* Revisar las valoraciones de riesgos de manera regular, asegurando que los niveles de riesgos residuales son comprendidos y aceptados.
* Realizar ejercicios de auditoría interna del MSPI.

## MEJORA DEL MSPI

La Entidad con la visión de mantenimiento y mejora de los aspectos de seguridad de la información, tomará en cuenta los resultados de la fase de Evaluación y los indicadores y se:

* Identificarán e implementarán acciones correctivas y preventivas que mitiguen situaciones de impacto.
* Implementarán acciones de mejora basadas en las lecciones aprendidas de las experiencias de seguridad internas o de otras compañías.
* Asegurará que las mejoras cumplen con los objetivos y propósitos definidos por el Instituto.

1. **CONTROL DE CAMBIOS**

| **Fecha** | **Versión** | **Naturaleza del cambio** |
| --- | --- | --- |
| 28-01-2019 | 1 | Creación del Documentos |
| 28/01/2020 | 2 | Ajuste de formato y contenido |

1. **CRÉDITOS**

|  |  |  |
| --- | --- | --- |
| Elaboró | Revisó | Aprobó |
| Mary Rojas  Contratista – Subdirección de Gestión Corporativa  Cristian Velásquez - Profesional  contratista Equipo SIG,  Oficina Asesora de Planeación | Mary Rojas  Contratista – Subdirección de Gestión Corporativa | Juan Fernando Acosta Mirkow  Subdirector de Gestión Corporativa |
| Aprobado | Comité Institucional de Gestión y Desempeño 28 de enero de 2020 | |