INSTITUTO DISTRITAL DE
PATRIMONIO CULTURAL

MANUAL DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

En las siguientes secciones de este documento, se establecen el alcance del Subsistema de Gestión de Seguridad de la Información para el Instituto Distrital del Patrimonio Cultural - IDPC, así como los parámetros que orientan el plan de seguridad de la información y las acciones a seguir para prevenir la aparición o repetición de no conformidades.

1 Tabla de contenido

2 INTRODUCCIÓN.

Para el Instituto Distrital del Patrimonio Cultural - IDPC la seguridad de la información es un reto que se ha construido a través de un cuidadoso proceso que articula su misión, objetivos y valores corporativos.

En el desarrollo de este manual, se ha revisado el enfoque basado en procesos de la institución y se definirán procedimientos documentados del sistema de gestión de la seguridad de la información.

3 ALCANCE DEL MANUAL.

El Manual del Subsistema de Gestión de Seguridad de la información del Instituto Distrital del Patrimonio Cultural – IDPC está basado en la norma internacional ISO 27001:2013 donde en esta norma se encuentran plasmadas las especificaciones para la creación de un sistema de gestión de la seguridad de la información (SGSI).

Este manual tiene por esencia recoger, analizar y definir los diferentes lineamientos que rigen al Subsistema de Gestión de Seguridad de la Información del Instituto Distrital del Patrimonio Cultural – IDPC.

4 OBJETIVO MANUAL.

Presentar en forma clara y coherente los elementos que conforman las políticas de seguridad de la información que deben conocer y cumplir todos los directivos, funcionarios contratistas y terceros que presten sus servicios o tengan algún tipo de relación con el Instituto distrital del patrimonio cultural IDPC.

5 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN.

5.1 Objetivo General

Preservar la confidencialidad, integridad y disponibilidad de los activos de información relevantes para el Instituto Distrital de Patrimonio Cultural.

5.2 Objetivos específicos

- Prevenir la divulgación no autorizada de los activos de información del Instituto Distrital de Patrimonio Cultural.
- Prevenir modificaciones no autorizadas de los activos de la información del Instituto Distrital de Patrimonio Cultural.

- Controlar los activos de información de tal manera que permanezcan accesibles a los integrantes del Instituto Distrital de Patrimonio Cultural que se encuentren autorizados.
- Asegurar que los funcionarios, contratistas y demás colaboradores del IDPC, entiendan sus responsabilidades en relación con la seguridad de la información del IDPC y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de la información.

6 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN.

El Instituto Distrital del Patrimonio Cultural - IDPC, se compromete a preservar la confidencialidad, disponibilidad e integridad, de sus activos de información, protegiéndolos contra amenazas internas y externas, mediante una identificación, valoración, implementación de controles, monitoreo y seguimiento de los niveles de riesgo de acuerdo a la metodología de gestión de riesgos en seguridad a niveles aceptables, manteniendo la mejora continua; apoyando el logro de sus objetivos y el cumplimiento de los compromisos institucionales con la lucha anticorrupción, lucha antipiratería, con la confidencialidad, la circulación y divulgación adecuada de la información, y con el gobierno en línea.

7 COMPROMISO DE LA DIRECCIÓN.

La Alta Dirección aprueba DE-GF-01 Política General de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la entidad, adicionalmente realiza la conformación del Comité de informática y de Seguridad de la Información del Instituto Distrital de Patrimonio Cultural mediante Resolución No 037 del 01 de febrero de 2016, como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la entidad.

La Alta Dirección de la Entidad demostrará su compromiso a través de:

- La promoción activa de una cultura de seguridad.
- Facilitar la divulgación de este documento a todos los Subdirectores, funcionarios, contratistas de la Entidad.
- El aseguramiento de los recursos adecuados para implementar y mantener la Política General de Seguridad de la Información

8 COMITÉ DE INFORMÁTICA Y DE SEGURIDAD DE LA INFORMACIÓN.

El comité de informática y de seguridad de la información se encarga de definir el alcance, planificar, controlar y verificar los procesos del SGSI. El comité es primordial en la implementación del SGSI ya que es el ente que regula cualquier cambio dentro del sistema de gestión, siempre apuntando a una mejora constante.

8.1 RESPONSABILIDADES DEL COMITÉ.

Las responsabilidades del comité son las siguientes:

- Formular y evaluar propuestas para la adecuación y modernización tecnológica en Consonancia con las necesidades de los proyectos de la Entidad.
- Elaborar Propuestas para dotar a la Entidad gradualmente de una plataforma tecnológica acorde con las necesidades de la contemporaneidad.
- Acompañar la formulación y la proyección presupuestal para la asignación de Recursos hacia la adecuación y modernización conforme a las necesidades existentes de la Entidad.
- Aprobación de las políticas de la seguridad de la información, como su alcance.
- Aprobar los roles y las responsabilidades de los funcionarios públicos dueños de la información.
- Aprobar el uso de metodologías/estándares y los informes para revisión por parte de la Alta Dirección, así mismo aprobar el plan de trabajo y los cambios al mismo
- Impulsar la implementación.
- Establecer estrategias para sensibilización y concienciación del SGSI.
- Realizar el seguimiento y/o verificación de la implementación de requisitos, controles e indicadores del SGSI.
- Supervisar la integración del SGSI con el Sistema integrado de gestión.
- Recopilar las necesidades de recursos por parte de los diferentes procesos en torno a la seguridad de la información y demás responsabilidades inherentes al Comité para el establecimiento, implementación, mantenimiento y mejora continua del Subsistema de Gestión de Seguridad de la Información.

9 NORMATIVIDAD.

El diseño e implementación del Subsistema de Gestión de Seguridad de la Información del Instituto Distrital del Patrimonio Cultural - IDPC es basado en la normatividad exigida por el Ministerio de las Tecnologías de la Información y Comunicaciones en el “Manual 3.1 para la Implementación de la Estrategia de Gobierno en línea para entidades del Orden Nacional”. Ley 1273 de 2009 denominada “Protección de la información y los datos”, normas ISO 2700 Sistema de Gestión de Seguridad de la Información, ISO 27002 Guía de buenas prácticas de seguridad de la información, ISO 27005, Guía para la Gestión de los riesgos de la seguridad de la información.

10 TERMINOS Y DEFINICIONES.

Acción correctiva: Medida de tipo reactivo orientada a eliminar la causa de una no conformidad asociada a la implementación y operación del SGSI con el fin de prevenir su repetición.

Acción preventiva: Medida de tipo pro-activo orientada a prevenir potenciales no conformidades asociadas a la implementación y operación del SGSI.

Aceptación del Riesgo: Decisión de aceptar un riesgo.

Activo: Según [ISO/IEC 13335-12004]: Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos del IDPC. Se pueden clasificar de la siguiente manera:

- **Datos:** Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en el IDPC.
- **Aplicaciones:** Es todo el software que se utiliza para la gestión de la información.
- **Personal:** Es todo el personal del IDPC, el personal subcontratado, los clientes, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información del IDPC.
- **Servicios:** Son tanto los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a clientes y usuarios.
- **Tecnología:** Son todos los equipos utilizados para gestionar la información y las comunicaciones
- **Instalaciones:** Son todos los lugares en los que se alojan los sistemas de información.
- **Equipamiento auxiliar:** Son todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos.

Administración de riesgos: Gestión de riesgos, es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales.

Conocimiento del riesgo: Es el proceso de la gestión del riesgo compuesto por la identificación de escenarios de riesgo, el análisis y evaluación del riesgo, el monitoreo y seguimiento del riesgo y sus componentes y la comunicación para promover una mayor conciencia del mismo que alimenta los procesos de reducción del riesgo y de manejo de desastre.

Administración de incidentes de seguridad: Un sistema de seguimiento de incidentes (denominado en inglés como issue tracking system, trouble ticket system o incident ticket system) es un paquete de software que administra y mantiene listas de incidentes, conforme son requeridos por una institución. Un sistema de reportes de incidencias es similar a un Sistema de seguimiento de errores (bugtracker) y, en algunas ocasiones, una entidad de software puede tener ambos.

Alerta: Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

Amenaza: Según [ISO/lEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: Según [ISO/lEC Guía 73:2002): Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Auditabilidad: Los activos de información deben tener controles que permitan su revisión. Permitir la reconstrucción, revisión y análisis de la secuencia de eventos.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Autenticidad: Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, Propiedad que garantiza que la identidad de un sujeto o recurso es la que declara, Se aplica a entidades tales como usuarios, procesos, sistemas de información.

Base de datos de gestión de configuraciones (CMDB, Configuration Management Database): Es una base de datos que contiene toda la información pertinente acerca de los componentes del sistema de información utilizado en una organización de servicios de TI y las relaciones entre esos componentes. Una CMDB ofrece una vista organizada de los datos y una forma de examinar los datos desde cualquier perspectiva que desee. En este contexto, los componentes de un sistema de información se conocen como elementos de configuración (CI). Un CI puede ser cualquier elemento imaginable de TI, incluyendo software, hardware, documentación y personal, así como cualquier combinación de ellos. Los procesos de gestión de la configuración tratan de especificar, controlar y realizar seguimiento de elementos de configuración y los cambios introducidos en ellos de manera integral y sistemática.

B57799: Estándar británico de seguridad de la información, publicado por primera vez en 1995. En 1998, fue publicada la segunda parte. La parte primera es un conjunto de buenas prácticas para la gestión de la seguridad de la información –no es certificable- y la parte segunda especifica el sistema de gestión de seguridad de la información –es certificable.

La parte primera es el origen de ISO 17799 e ISO 27002 y la parte segunda de ISO 27001. Como tal el estándar, ha sido derogado ya, por la aparición de estos últimos.

Características de la Información: las principales características son la confidencialidad, la disponibilidad y la integridad.

CobiT - Control Objectives for Information and related Technology: Publicados y mantenidos por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de Tecnología de Información rectores, actualizados, internacionales y generalmente aceptados para ser empleados por gerentes de empresas y auditores.

Compromiso de la Dirección: Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.

Computo forense: También llamado informática forense, computación forense, análisis forense digital o exanimación forense digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Confiabilidad: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, de otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda).

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización - tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma.

Denegación de servicios: Acción iniciada por una persona u otra causa que incapacite el hardware o el software, o ambos y después niegue el servicio.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Disponibilidad: Según [ISO/IEC 13335-1: 2004): característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Gestión de claves: Controles referidos a la gestión de claves criptográficas.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

Gusanos: Es un programa de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Siempre dañan la red (aunque sea simplemente consumiendo ancho de banda).

Impacto: Resultado de un incidente de seguridad de la información.

Incidente: Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: La información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras. Puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

Ingeniería Social: En el campo de la seguridad informática, es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos ganando su confianza muchas veces. Es una técnica que pueden utilizar investigadores privados, criminales, delincuentes computacionales (conocidos como cracker) para obtener información, acceso o privilegios en sistemas de información que les permiten realizar algún acto que perjudique o exponga a la persona o entidad a riesgos o abusos.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISOIIEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

PDCA Plan-Do-Check-Act: Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

Phishing: Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

Plan de continuidad del negocio (Bussines Continuity Plan): Plan orientado a permitir la continuación de las principales funciones del Instituto en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos (Risk treatment plan): Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:20005): intención y dirección general expresada formalmente por la Dirección.

SGSI Sistema de Gestión de la Seguridad de la Información: Según [ISO/IEC 27001: 20005]: la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Servicios de tratamiento de información: Según [ISO/IEC 27002:20005]: cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizados para su alojamiento.

Spamming: Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La vía más usada es el correo electrónico.

Sniffers: Programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente o de control, aunque también puede ser utilizado con fines maliciosos.

Spoofing: Falsificación de la identidad origen en una sesión: la identidad es por una dirección IP o Mac Address.

Tratamiento de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.

Trazabilidad: Propiedad que garantiza que las acciones de una entidad se pueden rastrear únicamente hasta dicha entidad.

Troyano: Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.

Usuario: en el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores del IDPC, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red del IDPC y a quienes se les otorga un nombre de usuario y una clave de acceso.

Valoración de riesgos: Según [ISO/lEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

Virus: tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o conocimiento del usuario.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISOIIEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

11 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

11.1 Políticas generales de seguridad de la información.

Las Políticas de Seguridad de la Información, surgen como una herramienta institucional para concienciar a cada uno de los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con el IDPC sobre la importancia y sensibilidad de la información y servicios críticos, de tal forma que le permitan desarrollar adecuadamente sus labores y cumplir con su propósito misional.

11.1.1 Objetivos.

Definir las pautas de propósito general para asegurar una adecuada protección de la información del IDPC.

Definir las responsabilidades y los principios generales necesarios para asegurar que la información que proveen nuestros sistemas de procesamiento computarizados y la infraestructura tecnológica de hardware y software que los soporta, sean confiables y siempre estén seguras y a la vanguardia tecnológica.

Implantar los mecanismos para que dicha información y la infraestructura que la soporta estén protegidas contra la destrucción, la alteración, el acceso no autorizado, la distribución y divulgación accidental o deliberada.

Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.

11.1.2 Aplicabilidad.

Estas son políticas que aplican al Director, Subdirectores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales del IDPC.

11.1.3 Lineamientos.

Se debe verificar que se definan, implementen, revisen y actualicen las políticas de seguridad de la información.

El líder SIG y el líder del área TI deberán diseñar, programar y realizar los programas de auditoría del Subssistema de gestión de seguridad de la información, las cuales estarán bajo la coordinación de control interno.

Todo aplicativo informático o software debe ser comprado, revisado y aprobado por el Área TI en concordancia con los procedimientos de Adquisición de Bienes y Servicios.

El IDPC debe contar con un firewall o dispositivo de seguridad perimetral para la conexión a Internet o cuando sea inevitable para la conexión a otras redes en outsourcing o de terceros.

Los Subdirectores deben asegurarse que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad, se realizan correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información del IDPC.

El comité de informática y de seguridad de la información y el área TI del IDPC definirá de acuerdo a la clasificación de la información, que datos deben ser cifrados y dará las directrices necesarias para la implementación de los respectivos controles (dispositivos a

emplear, mecanismos de administración de claves, políticas de uso de sistemas de cifrado de datos).

11.2 Políticas para Usuarios del IDPC.

11.2.1 Objetivo.

Definir las pautas generales para asegurar una adecuada protección de la información del IDPC por parte de los usuarios del Instituto.

11.2.2 Aplicabilidad.

Esta política se aplica al Director, Subdirectores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales del IDPC.

11.2.3 Lineamientos.

El IDPC instalará los programas que han sido adquiridos legalmente en los equipos asignados en las cantidades requeridas para suplir las necesidades. El uso de programas sin su respectiva licencia y autorización del IDPC (imágenes, vídeos, software o música), obtenidos a partir de otras fuentes (internet, dispositivos de almacenamiento externo), puede implicar amenazas legales y de seguridad de la información para el Instituto, por lo que ésta práctica no está autorizada.

Todo el software usado en la plataforma tecnológica del IDPC debe tener su respectiva licencia y acorde con los derechos de autor.

El IDPC no se hace responsable por las copias no autorizadas de programas instalados o ejecutados en los equipos asignados a sus funcionarios o contratistas.

Los programas instalados en los equipos, son de propiedad del IDPC, la copia no autorizada de programas o de su documentación, implica una violación a la política general del IDPC. Aquellos funcionarios, contratistas o demás colaboradores que utilicen copias no autorizadas de programas o su respectiva documentación, quedarán sujetos a las acciones disciplinarias establecidas por el IDPC o las sanciones que especifique la ley.

El IDPC se reserva el derecho de proteger su buen nombre y sus inversiones en hardware y software, fomentando controles internos para prevenir el uso o la realización de copias no autorizadas de los programas de propiedad del Instituto. Estos controles pueden incluir valoraciones periódicas del uso de los programas, auditorías anunciadas y no anunciadas.

Los recursos tecnológicos y de software asignados a los funcionarios del IDPC son responsabilidad de cada funcionario y/o Contratista.

Los usuarios son los responsables de la información que administran en sus equipos personales y deben abstenerse de almacenar en ellos información no institucional, la información debe estar organizada de acuerdo con las Tablas de Retención Documental.

Los usuarios solo tendrán acceso a los datos y recursos autorizados por el IDPC, y serán responsables disciplinaria y legalmente de la divulgación no autorizada de esta información.

Es responsabilidad de cada usuario proteger la información que está contenida en documentos, formatos, listados, etc., los cuales son el resultado de los procesos informáticos; adicionalmente se deben proteger los datos de entrada de estos procesos.

Los dispositivos electrónicos (computadores, impresoras, fotocopiadoras, escáner, etc.) solo deben utilizarse para los fines autorizados por el Instituto.

Cualquier evento o posible incidente que afecte la seguridad de la información, debe ser reportado inmediatamente al Área de TI del IDPC.

Mediante el Programa de Gestión Documental se definirán las instrucciones para el desarrollo de actividades de los datos de los sistemas de información y aplicaciones.

11.3 Política de uso de discos de red o carpetas virtuales.

11.3.1 Objetivo.

Asegurar la operación correcta y segura de los discos de red o carpetas virtuales.

11.3.2 Aplicabilidad.

Esta política se aplica al Director, Subdirectores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales del IDPC.

11.3.3 Lineamientos.

Para que los usuarios tengan acceso a la información ubicada en los discos de red, el Subdirector o Asesor deberá enviar un correo autorizando el acceso y permisos, correspondientes al rol y funciones a desempeñar al Área de TI del IDPC. Los usuarios tendrán permisos de escritura, lectura o modificación de información en los discos de red, dependiendo de sus funciones y su rol.

La información almacenada en cualquiera de los discos de red debe ser de carácter institucional.

Está prohibido almacenar archivos con contenido que atente contra la moral y las buenas costumbres del Instituto o las personas, como pornografía, propaganda racista, terrorista o cualquier software ilegal o malicioso, ya sea en medios de almacenamiento de computadores de escritorio o portátiles, tabletas, celulares inteligentes, etc. o en los discos de red.

Se prohíbe extraer, divulgar o publicar información de cualquiera de los discos de red sin expresa autorización del Subdirector de la dependencia correspondiente.
Se prohíbe el uso de la información de los discos de red con fines publicitarios, de imagen negativa, lucrativa o comercial.

La responsabilidad de generar las copias de respaldo de la información de los discos de red, está a cargo del Área de TI.

11.4 Política de respaldo y restauración de información.

11.4.1 Objetivo.

Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla.

11.4.2 Aplicabilidad.

Esta política será aplicada por el área TI y/o responsables de los activos de información que decidan sobre la disponibilidad en integridad de los datos.

11.4.3 Lineamientos.

La información de cada sistema debe ser respaldada regularmente sobre un medio de almacenamiento como Disco duros, CD, DVD, etc.

El administrador de los servidores, los sistemas de información o los equipos de comunicaciones, es el responsable de definir la frecuencia de respaldo y los requerimientos de seguridad de la información y el asignado por el subdirector de gestión corporativa es el responsable de realizar los respaldos periódicos.

Todas las copias de información crítica deben ser almacenadas en un área adecuada y con control de acceso.

Las copias de respaldo se guardarán únicamente con el objetivo de restaurar el sistema luego de un virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, materialización de amenazas, catástrofes y por requerimiento legal.

Es obligación de los usuarios finales verificar la realización de las copias en las carpetas destinadas para este fin.

Deben existir al menos una copia de la información de los discos de red, la cual deberá permanecer fuera de las instalaciones del IDPC.

La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información.

La dependencia de gestión corporativa debe mantener un inventario actualizado de las copias de respaldo de la información y los aplicativos o sistemas del IDPC.

Los medios que vayan a ser eliminados deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.

Es responsabilidad de cada dependencia mantener depurada la información de las carpetas virtuales para la optimización del uso de los recursos de almacenamiento que entrega el IDPC a los usuarios.

11.5 Política de control de acceso.

11.5.1 Objetivo.

Definir las pautas generales para asegurar un acceso controlado, físico o lógico, a la información de la plataforma informática del IDPC.

11.5.2 Aplicabilidad.

Esta política se aplica al Director, Subdirectores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales del IDPC.

11.5.3 Lineamientos.

El IDPC proporcionará a los funcionarios y contratistas (personas naturales) todos los recursos tecnológicos necesarios para que puedan desempeñar las funciones para las cuales fueron contratados, por tal motivo no se permite conectar a la red o instalar dispositivos fijos o móviles, tales como: computadores portátiles, tabletas, enrutadores, agendas electrónicas, celulares inteligentes, access point, que no sean autorizados por la dependencia de subdirección de gestión Corporativa.

El IDPC suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.

Es responsabilidad del usuario el manejo que se les dé a las claves asignadas.

Solo usuarios designados por la dependencia de la Subdirección de Gestión Corporativa estarán autorizados para instalar software o hardware en los equipos, servidores e infraestructura de telecomunicaciones del IDPC.

Todo trabajo que utilice los servidores del IDPC con información del Instituto, sus funcionarios o contratistas, se debe realizar en sus instalaciones, no se podrá realizar ninguna actividad de tipo remoto sin la debida aprobación del IDPC.

La conexión remota a la red de área local del IDPC debe ser hecha a través de una conexión VPN segura suministrada por el Instituto, la cual debe ser aprobada, registrada y auditada. El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado.

11.6 Política de transferencia de información.

11.6.1 Objetivo.

Asegurar la seguridad de la información y el software cuando son intercambiados dentro o fuera del IDPC.

11.6.2 Aplicabilidad.

Esta política se aplica al Director, Subdirectores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales del IDPC.

11.6.3 Lineamientos.

Toda transferencia de información perteneciente al IDPC a la cual tengamos acceso por razones técnicas o comerciales debe ser susceptible de trazabilidad.

El IDPC en caso de tener un servicio de transferencia de archivos deberá realizarlo empleando protocolos seguros. Cuando el origen sea el IDPC hacia entidades externas, el IDPC establecerá los controles necesarios para preservar la seguridad de la información; cuando el origen de la transferencia sea una entidad externa, se acordarán las políticas y controles de seguridad de la información con esa entidad; en todo caso se deben revisar y proponer controles en concordancia con las políticas de seguridad de la información del IDPC; los resultados de la revisión de requerimientos de seguridad se documentarán y preservarán para futuras referencias o para demostrar el cumplimiento con las políticas y con los controles de seguridad del IDPC.

Los usuarios de las subdirecciones del IDPC no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red del Instituto, sin la autorización de la dependencia de la Subdirección de Gestión Corporativa.

La asesoría jurídica del IDPC debe establecer en los contratos que se creen con los funcionarios y contratistas, los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas por la divulgación no autorizada de información de beneficiarios del instituto que les ha sido entregada en razón del cumplimiento de los objetivos misionales del IDPC.

Los usuarios no deben utilizar el correo electrónico como medio para enviar o recibir información sensible del instituto o de sus beneficiarios.

No está permitido el intercambio de información sensible del instituto por vía telefónica.

Los propietarios de los activos de información deben asegurar la validación y garantizar que el Intercambio de información solamente se realice si se encuentra autorizada y dando cumplimiento a las Políticas de Seguridad.

Los propietarios de los activos de información deben velar porque la información del IDPC sea protegida de divulgación no autorizada por parte de los terceros a quienes se entrega esta información, verificando el cumplimiento de las clausulas relacionadas en los contratos, Acuerdos de confidencialidad o Acuerdos de intercambio establecidos.

11.7 Política de seguridad para las relaciones con proveedores.

11.7.1 Objetivo.
Mantener los niveles acordados de seguridad de la información y de prestación de los servicios de los proveedores, en concordancia con los acuerdos establecidos con estos.

11.7.2 Aplicabilidad.
Esta política se aplica al Director, Subdirectores, funcionarios, contratistas, proveedores y en general a todos los usuarios de la información que cumplan con los propósitos generales del IDPC.

11.7.3 Lineamientos.
La asesoría jurídica del IDPC debe definir los modelos de Acuerdos de Confidencialidad y/o de Intercambio de Información entre el instituto y proveedores incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos.

Los Supervisores de contratos con terceros deben monitorear periódicamente, el cumplimiento de los Acuerdos de Niveles de Servicio, Acuerdos de Confidencialidad, Acuerdos de Intercambio de información y los requisitos de Seguridad de la Información de parte de los terceros proveedores de servicios.

11.8 Política de Tercerización u Outsourcing.

11.8.1 Objetivo.
Mantener la seguridad de la información y los servicios de procesamiento de información, a los cuales tienen acceso terceras partes, entidades externas o que son procesados, comunicados o dirigidos por estas.

11.8.2 Aplicabilidad.
Estas son políticas que aplican a contratistas, proveedores de outsourcing, consultores y contratistas externos, personal temporal y en general a todos los usuarios de la información que realicen estas tareas en el IDPC.

11.8.3 Lineamientos.

La asesoría jurídica debe establecer criterios de selección que contemplen la historia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por el Instituto.

Se deben identificar los riesgos para la información y los servicios de procesamiento de información que involucren partes externas al IDPC. El resultado del análisis de riesgos será la base para el establecimiento de los controles y debe ser presentado al comité de informática y de seguridad de la información y al área de TI antes de firmar el contrato de outsourcing.

Con el fin de proteger la información de ambas partes, se debe formalizar un acuerdo de confidencialidad. El acuerdo deberá definir claramente el tipo de información que intercambiarán las partes, los medios, la frecuencia y los procedimientos a seguir.

Si la información intercambiada lo amerita teniendo en cuenta la clasificación de la información de acuerdo a los niveles de seguridad, se debe preparar y legalizar un acuerdo de confidencialidad entre el Instituto y el outsourcing de acuerdo al objetivo y al alcance del contrato; el cual debe quedar firmado por ambas partes. En todos los casos deben firmarse acuerdos de niveles de servicio que permitan cumplir con las políticas de seguridad de la información y con los objetivos del IDPC.

11.9 Políticas para funcionarios y contratistas del Área de TI.

11.9.1 Objetivo.

Definir las pautas generales para asegurar una adecuada protección de la información del IDPC por parte de los funcionarios y contratistas de TI del el Instituto.

11.9.2 Aplicabilidad.

Estas políticas aplican a los funcionarios, contratistas, colaboradores del IDPC actuales o por ingresar y a terceros que estén encargados de cualquier sistema de información.

11.9.3 Lineamientos.

El personal TI no debe dar a conocer su clave de usuario a terceros sin previa autorización del Subdirector de Gestión Corporativa.

Los documentos y en general la información de procedimientos, seriales, software etc. deben mantenerse custodiados en todo momento para evitar el acceso a personas no autorizadas.

Para el cambio o retiro de equipos de funcionarios y/o Contratistas, se debe llevar a cabo mejores prácticas para la eliminación de la información de acuerdo al software disponible en el Instituto mediante el formateo seguro.

Los funcionarios y/o Contratistas encargados de realizar la instalación o distribución de software, sólo instalarán productos con licencia y software autorizado.

Los funcionarios y/o Contratistas del Área de TI no deben otorgar privilegios especiales a los usuarios sobre las estaciones de trabajo, sin la autorización correspondiente de los Subdirectores o asesores de las distintas dependencias.

Los funcionarios y/o Contratistas del Área de TI se obligan a no revelar a terceras personas, la información a la que tengan acceso. En consecuencia, se obligan a mantenerla de manera confidencial y privada y a protegerla para evitar su divulgación.

Los funcionarios y/o Contratistas del Área de TI no utilizarán la información para fines comerciales o diferentes al ejercicio de sus funciones.

Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar de tal forma que asegure su protección y disposición en un futuro.

Las copias licenciadas y registradas del software adquirido, deben ser únicamente instaladas en los equipos y servidores del Instituto.

La copia de programas o documentación, requiere tener la aprobación escrita del IDPC y del proveedor si éste lo exige.

El personal del Área de TI debe velar por que se cumpla con el registro en la bitácora de acceso a los servidores físicamente, de las personas que ingresen y que hayan sido autorizadas previamente por área o por quien esta delegue.

Por defecto deben ser bloqueados, todos los protocolos y servicios que no se requieran en los servidores; no se debe permitir ninguno de ellos, a menos que sea solicitado y aprobado oficialmente por el Instituto a través del comité de informática y de seguridad de la información o el Subdirector de Gestión Corporativa.

Todos los servidores deben ser configurados con el mínimo de servicios necesarios y obligatorios para desarrollar las funciones designadas.

Las pruebas de laboratorio o piloto deben ser autorizadas por el líder del Área de TI, para sistemas de información, de software tipo freeware o shareware o de sistemas que necesiten conexión a internet; estas deben ser realizadas sin conexión a la red LAN del

Instituto y con una conexión separada de internet o en su defecto con una dirección IP diferente a las direcciones públicas de producción.

11.10 Política de uso de Internet.

11.10.1 Objetivo.

Establecer los lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.

11.10.2 Aplicabilidad.

Estas son políticas que aplican a la Dirección, Subdirectores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales del IDPC.

11.10.3 Lineamientos.

La navegación en Internet debe realizarse de forma razonable y con propósitos laborales.

No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas del IDPC o que representen peligro para el Instituto como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas por el IDPC.

El acceso a este tipo de contenidos con propósitos de estudio de seguridad o de investigación, debe contar con la autorización expresa del comité de informática y de seguridad de la información del IDPC.

La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio de Internet/Intranet, en forma específica el usuario debe cumplir los requerimientos de la política de uso de internet descrita en este manual.

11.11 Política de Uso de Correo Electrónico.

11.11.1 Objetivo.

Definir las pautas generales para asegurar una adecuada protección de la información del IDPC, en el uso del servicio de correo electrónico por parte de los usuarios autorizados.

11.11.2 Aplicabilidad.

Estas son políticas que aplican a la Dirección, Subdirectores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales del IDPC.

11.11.3 Lineamientos.

Los usuarios del correo electrónico corporativo son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información.

Los servicios de correo electrónico corporativo se emplean para servir a una finalidad operativa y administrativa en relación con el instituto.

Todos los correos electrónicos procesados por los sistemas, redes y demás infraestructura TIC del IDPC se consideran bajo el control del Instituto.

Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en el IDPC y no debe utilizarse para ningún otro fin.

Cada subdirector del área deberá solicitar la creación de las cuentas electrónicas diligenciando el formato GS-F07, sin embargo, el área de Talento Humano para funcionarios de planta y temporales y el respectivo Subdirector para los contratistas del IDPC son los responsables de solicitar la modificación o cancelación de las cuentas electrónicas al área de TI del IDPC.

El envío de cadenas de correo, envío de correos masivos con archivos adjuntos de gran tamaño que puedan congestionar la red, no está autorizado.

No está autorizado, el envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre del Instituto.

Cuando un funcionario, contratista o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico y se retire del IDPC, su cuenta de correo será desactivada.

Las cuentas de correo electrónico son propiedad del IDPC, las cuales son asignadas a personas que tengan algún tipo de vinculación laboral con el instituto, ya sea como personal de planta, contratistas, consultores o personal temporal, quienes deben utilizar este servicio única y exclusivamente para las tareas propias de la función desarrollada en el Instituto y no debe utilizarse para ningún otro fin.

Cada usuario es responsable del contenido del mensaje enviado y de cualquier otra información adjunta al mismo.

Todos los mensajes pueden ser sujetos a análisis y conservación permanente por parte del Instituto.

Cuando los correos electrónicos superan 10 MB se debe utilizar las herramientas colaborativas en la nube para el envío de los archivos adjuntos.

La dependencia de subdivulgación diseñara la plantilla general de las firmas de correos corporativos.

Todo usuario es responsable por la destrucción de los mensajes cuyo origen sea desconocido y por lo tanto asumirá la responsabilidad y las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En estos casos no se debe contestar dichos mensajes, ni abrir los archivos adjuntos y se debe reenviar el correo a la cuenta sistemas@idpc.gov.co con la frase “correo sospechoso” en el asunto.

12 CUADRO DE CAMBIOS.

Versión	Fecha de Aprobación	Cambios Realizados
1	**Fecha:** 24 de noviembre de 2016	Documento Original

ELABORÓ		REVISÓ		APROBÓ	
NOMBRE:	Bladmin Dario Barreto	NOMBRE:	Juan Fernando Acosta	NOMBRE:	Mediante Acta de Comité de Seguridad de la información
CARGO/DEPENDENCIA:	Contratista Profesional / Subdirección de Gestión Corporativa	CARGO/DEPENDENCIA:	Subdirector de Gestión Corporativa	DEPENDENCIA:	N/A
FECHA:	08/09/2016	FECHA:	24/11/2016	FECHA:	24/11/2016