Fecha última actualización: 30/01/2024

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2022 - 2026

UNIDAD ADMINISTRATIVA ESPECIAL
DIRECCIÓN NACIONAL DE DERECHO DE AUTOR
GRUPO INTERNO DE TRABAJO UNIDAD DE COMUNICACIONES, SERVICIO AL CIUDADANO Y TECNOLOGIAS DE LA INFORMACION

REVISIÓN
2024

www.derechodeautor.gov.co Teléfono 601786 82 20 / Línea gratuita: 01 8000 127878
info@derechodeautor.gov.co Calle 28N° 13a - 15 Piso 17. Bogotá D.C, Colombia.

Tabla de contenido

1. INTRODUCCIÓN

La seguridad de la información es una prioridad para la Dirección Nacional de Derechos de Autor, en este documento se implementan reglas y lineamientos técnicos para el uso controlado de activos de información que minimice el riesgo de pérdida de datos, accesos no autorizados, divulgación no controlada, duplicación e interrupción intencional de la información y demás amenazas que afecten la integridad de la información. Por lo tanto, es deber de los funcionarios, contratistas y/o terceros acatar y proteger las políticas que este documento expresa y en concordancia a los lineamientos vigentes de la Norma NTC – ISO - IEC 27001:2013 [**Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos],** con el fin de asegurar la continuidad de los procesos, actividades y servicios de igual manera maximizando la eficiencia y la mejora continua de los procesos administrativos para con la comunidad.

2. DEFINICIONES

Para una mejor comprensión del presente documento se toman como referencia los presentes términos y definiciones establecidos en la Norma ISO 27000:2013 Aceptación del riesgo: Decisión informada de asumir un riesgo concreto.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento Hardware y de Software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos relacionado con el tratamiento de datos. El activo representa los datos de la DNDA que tienen valor para los procesos de la entidad, pueden ser un documento físico, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información calificada o reservada de la DNDA.

Acceso a la Información: Conjunto de técnicas para buscar, categorizar, modificar y acceder a la información que se encuentra en un sistema de bases de datos, bibliotecas, archivos e Internet.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema.

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Análisis de riesgos cualitativo: Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la criticidad del impacto y la probabilidad de ocurrencia.

Análisis de riesgos cuantitativo: Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

Autenticación: Provisión de una garantía de que una característica afirmada por una entidad es correcta.

Autenticidad: Propiedad de que una entidad es lo que afirma ser.

CID: Acrónimo español de confidencialidad, integridad y disponibilidad, las dimensiones básicas de la seguridad de la información.

Confidencialidad: propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
La información debe ser accedida sólo por aquellas personas que lo requieran como una necesidad legítima para la realización de sus funciones. La revelación no autorizada de la información calificada de acuerdo con un nivel de confidencialidad alta implica un grave impacto en la Dirección Nacional de Derecho de Autor, en términos económicos, de su imagen y ante sus clientes.

Controles Preventivos: actúan sobre la causa de los riesgos, con el fin de disminuir su probabilidad de ocurrencia y constituyen la primera línea de defensa contra ellos; también actúan para disminuir la acción de los agentes generadores de los riesgos.

Controles Detectivos: se diseñan para descubrir un evento, regularidad o un resultado no previsto; alertan sobre la presencia de los riesgos y permiten tomar medidas inmediatas; pueden ser manuales o computarizados. Generalmente sirven para supervisar la ejecución del proceso y se usan para verificar la eficacia de los controles preventivos. Ofrecen la segunda barrera de seguridad frente a los riesgos, pueden informar y registrar la ocurrencia de los hechos no deseados, accionar alarmas, bloquear la operación de un sistema, monitorear, o alertar a los servidores públicos.

3. NORMATIVIDAD RELACIONADA

Para la Actualización de este Plan se tiene como base, la norma ISO – IEC 27001:2013 Sistema de Gestión de la Seguridad de la Información, el Modelo de Seguridad y Privacidad de la información (Políticas, Manuales, Guías y Formatos), el cumplimiento de:

Requisito legal	Directriz de cumplimiento
Ley 44 de 1993	Por el cual de modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944.
Ley 565 de 2000	Por medio de la cual se aprueba el “Tratado de OMPI-Organización Mundial de la Propiedad Intelectual – sobre Derechos de Autor (WTC)”, adoptado en Ginebra, el 20 de diciembre de 1996.
Ley 603 de 2000	Esta ley se refiere la protección de los derechos de autor en Colombia.
Ley 719 de 2001	Por cual se modifican las Leyes 23 de 1982 y 44 de 1993 y se dictan otras disposiciones.
Decreto 1377 de 2013	Decreto por el cual se reglamenta parcialmente la Ley 1581de 2012.
Decreto 460 de 1995	Por el cual se reglamente el Registro Nacional del Derecho de Autor y se regula el Depósito Legal.
Decreto 162 de 1996	Por el cual se reglamenta la Decisión Andina 351 de 1993 y la Ley 44 de 1993, en relación con las Sociedades de Gestión Colectiva de Derecho de Autor o de Derechos Conexos.
Decreto 1360 de 1989	Por el cual se reglamente la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor.
Ley 463 de 1998	Por medio de la cual se aprueba el “Tratado de Cooperación en materia de patentes (PCT)”, elaborado en Washington el 19 de junio de 1970, enmendado el 28 de septiembre de 1979 y modificado el 3 de febrero de 1984, y el reglamento del tratado de cooperación en materia de Patentes.

Decreto 2591 de 2000	Por el cual se reglamenta parcialmente la Decisión 486 de la Comisión de la Comunidad Andina.
Ley 1341 de 2009	Por la cual se definen los 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 del Espectro y se dictan otras disposiciones.
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.
Decreto 1747 de 2000	Por el cual se reglamenta parcialmente la Ley 527 de 199, en los relacionados con las entidades de certificación, los certificados y las firmas digitales.
Resolución 26930 de 2000	Por la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores.
Ley 1266 de 2008	Por la cual se dictan las disposiciones generales del Habeas 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 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 posiciones.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

www.derechodeautor.gov.co Teléfono 601786 82 20 / Línea gratuita: 01 8000 127878
info@derechodeautor.gov.co Calle 28N° 13a - 15 Piso 17. Bogotá D.C, Colombia.

NTC / ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos.
NTC/ISO 27002:2013	Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información.

4. OBJETIVO GENERAL

Generar un documento de lineamientos, buenas prácticas y los elementos que conforman la política de seguridad que deben cumplir los funcionarios, contratistas y terceros que presten sus servicios o tengan al algún tipo de relación con La Dirección Nacional de Derechos de Autor.

4.1.Objetivos Específicos

- Crear, implementar y concientizar a los funcionarios, contratistas y proveedores de la DNDA sobre la seguridad de la información y su importancia.
- Actualizar los procesos informáticos de la -Dirección Nacional de derechos de autor con el fin de mejorar el desarrollo de las actividades institucionales y sus servicios.
- Mediante la utilización del Modelo de Seguridad y Privacidad de la Información (MSPI), se busca contribuir al incremento de la transparencia en la gestión pública.
- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en las entidades.
- Contribuir a mejorar los procesos de intercambio de información pública.
- Optimizar la gestión de la seguridad de la información al interior de las entidades.
- Revisar los roles relacionados con la privacidad y seguridad de la información al interior de la entidad para optimizar su articulación.

5. CONOCIMIENTO DE LA ENTIDAD

5.1. Visión

La Dirección Nacional de Derecho de Autor será a 2026 una entidad innovadora y optimizada digitalmente en la prestación de sus servicios, posicionada y reconocida en el ámbito nacional e internacional, por la promoción y preservación del derecho de autor y los derechos conexos.

5.2. Misión

Contribuir a la permanente protección de los titulares del derecho de autor y de los derechos conexos, fomentando la creatividad e incrementando el desarrollo de la riqueza cultural del país, facilitando el acceso a la justicia especializada para el respeto y solución de conflictos; generando apropiación y difusión para el reconocimiento, protección y aprovechamiento sostenible en la temática autoral, mediante alianzas estratégicas, que permitan fortalecer tecnológicamente los servicios de registro, protección, observancia y aprovechamiento del derecho de autor y los derechos conexos.

6. POLÍTICAS DE SEGURIDAD

6.1. Acceso a la información

De acuerdo con las actividades del contratista o personal de planta y el manual de funciones de cada dependencia, únicamente tendrán acceso a la información necesaria para el desarrollo de sus actividades.

Los usuarios de los sistemas de información que la Dirección Nacional de Derechos de Autor posee o adquiera tendrán un único usuario y contraseña para consulta y edición de la información, dependiendo del área o dependencia; los funcionarios tendrán acceso a la información, quien a su vez será responsable del hurto, sustracción, daño parcial o total de la información que se genere, ingrese y se edite en el área que tiene a cargo.

El área de Control Interno estará delimitando las políticas de acceso a la información mediante el cumplimiento del presente documento, de igual manera notificará al encargado del subgrupo de TI los cambios de funcionarios o usuarios en los

sistemas de información para la respectiva creación de cuentas, bloqueo o la eliminación de estas, según se dé el caso.

6.2. Seguridad de la información

Los funcionarios, contratistas y proveedores de la Dirección Nacional de Derecho de Autor son responsables de la información que por medio electrónico, digital, escrito o verbal le sea entregado y cumplirán de igual manera con los principios de confidencialidad, protegiendo la integridad de la información y la buena imagen de la Entidad.

Llegado el caso en que un funcionario, contratista o proveedor tenga acceso a información, la cual no es de su área o dependencia, deberá informar en el menor tiempo posible a la Oficina de Control Interno o al funcionario encargado del subgrupo de TI.

6.3. Seguridad para servicios informáticos

Se entiende por servicios informáticos todas aquellas plataformas de escritorio o vía web que facilitan el desarrollo de las actividades de los funcionarios, contratistas y proveedores de la Dirección Nacional de Derecho de Autor.

- **Correo electrónico:**

Las cuentas de correo institucionales son creadas por el subgrupo de TI de la entidad, por lo tanto, serán las únicas cuentas de correo utilizadas para el desarrollo de las actividades y no se deberá reproducir, copiar y enviar información por distintas cuentas de correo, se hará excepciones en las cuales el Director General o quien haga sus veces autorice y será responsable por la información.

El correo institucional cuenta con un servicio de chat el cual deberá ser usado de manera responsable.

6.4. Seguridad en estaciones de trabajo

Una vez el funcionario se le asigne un equipo de cómputo o dispositivo será responsable por la información e integridad de los equipos y mantendrá las configuraciones que se le asignen.

- **Administrador de usuarios:**

A cada funcionario se le creará un usuario con una contraseña estándar, la cual deberá cambiar por una contraseña de mínimo 8 caracteres incluyendo números, letras mayúsculas, letras minúsculas y símbolos, esta contraseña deberá cambiarse con una periodicidad.

- **Roles y privilegios de acceso a la información.**

El funcionario y/o contratista solo podrá acceder a la información para el buen desarrollo de sus actividades, el cual lo especificará el manual de funciones o contrato.

6.5. Seguridad de Comunicaciones de Datos

Las bases de datos, información contable, claves de acceso, aplicaciones web o de escritorio, información personal y sistemas de información que no sea autorizada para la publicación por el Director General, deberá ser tratada como información reservada y será prohibida su reproducción, edición, impresión o divulgación.

6.6. Software de la Entidad

Todo software que ingrese a la entidad deberá ser adquirido bajo el marco legal vigente, de igual manera deberá tener un manual de usuario, manual de seguridad, proveedor, tipo de licenciamiento, fecha de caducidad de la licencia y soporte técnico ofrecido.

6.7. Actualización de hardware

La adquisición de nuevos equipos se deberá realizar bajo la norma técnica de estandarización, registros de soporte técnico y control de insumos para la toma de decisiones de adquisición de equipos y dispositivos.

6.8. Disposición de la Información

En los escritorios de los funcionarios de la Dirección Nacional de Derecho de Autor no deberán reposar USB, Discos Duros Externos, o cualquier dispositivo de almacenamiento, todo esto con el fin de reducir los riesgos de acceso no autorizado a la información, deberán estar en un gabinete bajo llave según lo considere el Director General o quien haga sus veces.

6.9. Prácticas de uso de Internet

Los funcionarios de la Dirección Nacional de Derecho de Autor deberán tener en cuenta las siguientes normas para el acceso a Internet:

- No tendrán acceso a las redes sociales, chats, blogs u otras plataformas que no sean para el buen desarrollo de sus actividades, se realizarán excepciones previa autorización y supervisión del Director General o quien haga sus veces.
- No se permitirán descargas Multimedia, aplicaciones, etc., que no sean autorizadas por el Director General y funcionario encargado del área sistemas de la Dirección Nacional de Derecho de Autor.
- No abrir correos, archivos adjuntos o aplicaciones desconocidas, ya que pueden estar infectados con software malicioso (virus), en caso de ser abiertos o iniciados, informar al funcionario encargado del subgrupo de TI en el menor tiempo posible.
- Se establecerán políticas internas de las dependencias para salvaguardar la integridad y confidencialidad de la información y los dispositivos, ya sea mediante el software antivirus u otro aplicativo, previamente autorizado por el funcionario encargado del subgrupo de TI.
- Los funcionarios de la Dirección Nacional de Derecho de Autor no podrán utilizar la cuenta de correo institucional con fines personales.
- Todos los funcionarios, contratistas y proveedores tienen prohibido descargar, consultar o reproducir contenido sexual o material pornográfico, tanto de internet como en los equipos de cómputo.

7. SEGURIDAD LÓGICA

7.1. Inventario tecnológico

Se realizará un inventario tecnológico donde se tenga un registro verídico de la cantidad de equipos de cómputo con que cuenta la entidad.

Se creará un registro de custodia por parte de almacén de los equipos, impresoras u otros dispositivos asignados a cada funcionario y/o contratista.

7.2. Usuarios, contraseñas y privilegios

Con base en el registro de custodia responsabilidad de los equipos de cómputo pertenecientes de la Dirección Nacional de Derecho de Autor se crearán usuarios

y contraseñas para el inicio de sesión en cada una de las estaciones de trabajo. Estas claves serán administradas por encargado del subgrupo de TI.

Los privilegios que sean asignados a cada funcionario o contratista dependerán de las actividades que le sean asignadas según el manual de funciones de la Dirección Nacional de Derecho de Autor o en su contrato, dichos privilegios no excederán ni limitaran el buen desarrollo de las actividades.

El usuario administrador de todos los equipos de cómputo de la Dirección Nacional de Derecho de Autor será definido por el encargado del subgrupo de TI, los demás privilegios serán asignados de acuerdo con el manual de funciones y/o actividades del contratista.

Se realizarán revisiones mensuales de las claves de acceso, realizando comprobaciones de cantidad de usuarios, El área de talento humano y el área de contratación, notificarán cambios en el personal por medio escrito, o vía correo electrónico a la oficina de control interno quien reportará al encargado del subgrupo de TI.

Se realizará una base de datos con los usuarios y contraseñas mensuales de los funcionarios y contratistas que tengan bajo su custodia un equipo de cómputo o dispositivo, el cambio de contraseñas estará sujeto al usuario responsable.

Cada funcionario deberá limpiar de manera cuidadosa los equipos que tiene a cargo de tal manera que se alargue la vida útil de los dispositivos.

No se permitirá el uso de equipos de propiedad de la Dirección Nacional de Derechos de Autor a terceros sin previa autorización del Gerente y al contratista encargado del área de sistemas.
Las contraseñas de aplicativos, correos electrónicos, equipos de cómputo o cualquier otro sistema de información deberán cumplir las siguientes especificaciones por seguridad:

- Mínimo 8 caracteres que contenga letras mayúsculas, minúsculas, símbolos y números.
- No deberán contener nombres de los funcionarios, nombre o lema de la Dirección Nacional de Derechos de Autor nombre de usuario o documento de identidad del contratista.
- El procedimiento para reinicio de contraseñas y/o creación de usuarios de accesos se realizará la solicitud mediante comunicación escrita al encargado del subgrupo de TI de la Dirección Nacional de Derechos de Autor.

8. SEGURIDAD DE COMUNICACIONES

8.1. Topología de Red

- Deberá existir documentación electrónica e impresa sobre la tipología de red y diagramas topológicos de la ubicación de los puntos de red.
- Se creará una base de datos con los distintos usuarios y contraseñas de los dispositivos de red (Router, Switch, servidores, etc.).

8.2. Conexiones

- La conexión a internet será suministrada únicamente para temas relacionados con el buen desarrollo de las actividades de los funcionarios y/o contratistas según el manual de funciones o contrato.
- Las claves de acceso a internet inalámbrico de la entidad se realizará la solicitud mediante un formato que será firmado por el Director o quien haga sus veces dirigido a control interno, una vez control interno haga la solicitud al encargado del subgrupo de TI se procederá a facilitar las claves de acceso.
- Por ningún motivo se permitirán conexiones a internet inalámbrico a terceros a menos que este en el marco de una actividad institucional o sea autorizado por el Director.
- Los funcionarios de La Dirección Nacional de Derechos de Autor no podrán acceder a configuraciones del equipo de cómputo impresoras u otros dispositivos.
- Las redes Wi-Fi que estén a nombre de La Dirección Nacional de Derechos de Autor, se realizarán las conexiones mediante el filtro de Seguridad por número MAC del dispositivo, para ello se deberá solicitar por escrito al administrador de Sistemas por escrito.

8.3. Antivirus

- Se deberá adquirir un software antivirus que se ajuste a las necesidades de seguridad de la Dirección Nacional de Derechos de Autor bajo los lineamientos legales.
- Se realizarán análisis periódicos con el software antivirus instalado en los

equipos de cómputo de propiedad.

- Se informará a control interno acerca de la incidencia de virus en los equipos asignados a los funcionarios de la Dirección Nacional de Derechos de Autor, con el fin de implementar medidas que eviten la incidencia de esta falla.

9. SEGURIDAD EN APLICACIONES

9.1. Sistemas Operativos

- Se instalará el Sistema Operativo del cual se tiene licencias adquiridas.
- Se instalará la versión de office actualizada bajo licenciamiento.
- En los equipos de cómputo se instalará libre office para evitar licenciamiento.
- Para los equipos que no cuenten con licenciamiento se instalaran sistemas operativos alternos y una versión libre de gestión de documentos, hasta que no sean adquiridas e instaladas nuevas licencias por parte de La Dirección Nacional de Derechos de Autor.

9.2. Control de Aplicaciones

- Si por algún caso un funcionario o contratista solicita la instalación de aplicativos en los equipos de cómputo para el desarrollo de sus actividades se deberá informar por medio escrito a la oficina de control interno con copia al funcionario del subgrupo de TI.
- Las actualizaciones de aplicativos se realizarán únicamente si presentan fallas e incompatibilidades.
- En caso de reinstalación de un equipo de cómputo el funcionario está obligado a realizar una copia de seguridad de la información.
- El funcionario, contratista o proveedor no está autorizado para instalar o iniciar ningún tipo de software o aplicativo que no esté en el marco del manual de funciones o contrato, en caso de ser necesario enviará la solicitud a Control interno con copia al funcionario encargado del subgrupo de TI.
- Se establecerán fechas en común acuerdo con las dependencias de La

Dirección Nacional de Derechos de Autor para la realización de mantenimientos físicos y lógicos preventivos en los equipos de propiedad de La Dirección Nacional de Derechos de Autor. El área de sistemas y/o contratista encargado del área de sistemas no está en la obligación de reparar, diagnosticar e instalar software en equipos personales.

- Los equipos de cómputo personales de los funcionarios, contratistas o terceros no podrán tener instalado software con licencia de propiedad de La Dirección Nacional de Derechos de Autor, en caso contrario será autorizado por el Gerente quien a la vez notificará a Control Interno y al subgrupo de TI, además, el funcionario o quien haga sus veces, será el responsable de la información que en dicho equipo de cómputo personal tenga acceso.

9.3. Control de Cambios

- Se implementarán formatos o planillas para documentar los cambios de software, hardware o aplicativos que se realicen en los equipos de propiedad de La Dirección Nacional de Derecho de Autor.
- La solicitud de cambio de configuraciones, aplicativos, sistemas operativos o hardware deberán ser solicitadas por escrito especificando la siguiente información:
  a. Sistema, Aplicación o hardware afectado.
  b. Funcionario que solicita el cambio.
  c. Descripción general de la solicitud.
  d. Firma del supervisor o encargado de la dependencia.
  e. Se emitirán mensualmente recomendaciones de seguridad informática basados en los hallazgos que se tengan durante la revisión de los equipos, aplicativos o navegación web.
- Los procedimientos para la adquisición de hardware y software por parte de La Dirección Nacional de Derecho de Autor, se deberá tener en cuenta:
  a. Análisis Costo – Beneficio.
  b. Comprobación de adaptabilidad y compatibilidad con los sistemas operativos y/o aplicaciones actualmente instaladas.

c. Evaluación de las medidas de seguridad, respaldo y soporte.

d. Solicitud de manuales de uso de cada aplicación y/o herramienta de hardware.

e. Evaluación y diagnóstico por parte del funcionario del área de La Dirección Nacional de Derechos de Autor.

10. SEGURIDAD FÍSICA

10.1. Equipamiento

Deberá existir una adecuada protección física por parte de los funcionarios hacia los equipos y dispositivos de propiedad la Dirección Nacional de Derechos de Autor, por otra parte, el funcionario del subgrupo de TI velará por:

- Mantenimiento de los equipos de cómputo cada 4 meses.
- Mantenimiento correctivo de los equipos de cómputo una vez sea detectado una falla.

10.2. Controles de acceso

Las siguientes medidas, protocolos y controles serán adoptados para garantizar la seguridad e integridad de los servidores, rack y cuarto de centro de datos que alojan la infraestructura de red, configuración y acceso a la información de La Dirección Nacional de Derecho de Autor.

- Solo podrá ingresar el funcionario encargado del subgrupo de TI y será el único funcionario que tendrá la disposición de autorizar junto con el Director General quien puede ingresar a esta área.
- El cuarto de centro de datos permanecerá cerrado y bajo llave y sistema lector de huellas las cuales estarán a cargo del funcionario del subgrupo de TI.
- El personal externo de La Dirección Nacional de Derecho de Autor que necesite ingresar al área de sistemas deberá solicitar de manera escrita el ingreso justificando el cambio y el procedimiento a seguir de manera escrita, será supervisado el ingreso por el funcionario encargado del subgrupo de TI y el funcionario de control interno.

Los siguientes son los procedimientos para seguir para el correcto funcionamiento de las dependencias en cuanto al tema de seguridad informática:

- Según sea el caso, se deshabilitarán los parlantes de los equipos de cómputo.
- Se bloquearán los puertos USB para la conexión de memorias USB, discos duros externos etc., esto con el fin de evitar propagación de virus en los equipos de cómputo.
- Los funcionarios, contratistas y proveedores no están autorizados para trasladar equipos de cómputo sin previa autorización por parte del funcionario de Almacén y el funcionario del subgrupo de TI, dicho cambio se registrará en la planilla de control de cambios del área de Almacén.
- No se permitirán el traslado de impresoras, escáner u otros dispositivos entre los funcionarios o dependencias, sin previa autorización del Director e informar a la oficina de control interno con copia al funcionario encargado del subgrupo de TI.
- Los equipos portátiles, Tablets, u otros dispositivos portables deberán permanecer dentro de las instalaciones de La Dirección Nacional de Derechos de Autor, si fuese necesario su traslado deberá ser autorizado por el Director con copia al funcionario de Almacén y al funcionario del subgrupo de TI.
- Los computadores o dispositivos que sean usados para las salidas a campo las dependencias encargadas de la salida tendrán control exclusivo y serán responsables de dichos dispositivos, el subgrupo de TI no dispondrá ni tendrá responsabilidad sobre ellos.
- Los funcionarios, contratistas y proveedores de La Dirección Nacional de Derechos de Autor únicamente podrán imprimir documentos que estén en el marco del desarrollo de sus actividades que el manual de funciones o contrato especifique.

10.3. Riesgos que afrontan los sistemas de información e infraestructura tecnológica

TIPO DE PROCEDIMIENTO	FACTOR DE RIESGO	PREVENCION Y MITIGACION

Fuego o Incendio: Destrucción o pérdida parcial o total de la infraestructura tecnológica	**MEDIO**	Extintores ubicados estratégicamente según normativa legal vigente.
Robo: Perdida de los equipos	**MEDIO**	Alarmas, Cámaras de Seguridad.
Vandalismo: Daño a los equipos e infraestructura de datos	**MEDIO**	Seguridad Privada, Policial, Alarmas y Copias de Seguridad.
Fallas en equipos de Cómputo: Eliminación de información y Configuración.	**MEDIO**	Garantías de Equipos de Cómputo y dispositivos, Copias de Seguridad, Backup´s de Configuración, Mantenimientos lógicos y físicos preventivos.
Errores Humanos: Eliminación de Información, Configuración o Sabotaje	**ALTO**	Capacitación de funcionarios, Copias de Seguridad, Revisiones de Acceso a los sistemas de información
Virus Informáticos: Pérdida total o parcial de información y/o configuración	**ALTO**	Actualizaciones de Sistemas Operativos, Actualización de Software Antivirus, Copias de Seguridad, Controles periódicos.
Desastres Naturales: Destrucción de Equipos	**MEDIO**	Copias de Seguridad
Accesos no Autorizados: Filtración no autorizada de información, ataques cibernéticos.	**BAJO**	Cambios de contraseñas periódicamente, implementación y seguimiento de las políticas de seguridad de la información, copias de seguridad.
Robo de Información: Difusión, publicación o reproducción de la información sin autorización	**ALTO**	Cambio de contraseñas, seguimiento de políticas de seguridad informática, supervisión y control de acceso a la información.
Fraude –Suplantación de Usuarios: Modificación o desvíos de información.	**BAJO**	Cambio de contraseñas, seguimiento de políticas de seguridad informática, supervisión y control de acceso a la información.