BOGOTÁ
Instituto Distrital
de Recreación y Deporte

INSTITUTO DISTRITAL DE RECREACIÓN Y DEPORTE - IDRD

COPIA IMPRESA NO CONTROLADA

SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA

ÁREA DE SISTEMAS

MANUAL DE POLÍTICAS DE SEGURIDAD DIGITAL Y DE LA INFORMACIÓN

2025

BOGOTÁ
Instituto Distrital
de Recreación y Deporte

TABLA DE CONTENIDO

Contenido

COPIA IMPRESA NO CONTROLADA

COPIA IMPRESA NO CONTROLADA

1. OBJETIVO GENERAL

El presente documento tiene como objetivo fundamental, establecer las políticas en seguridad digital y de la información que debe seguir todo el personal (funcionarios, contratistas, proveedores y visitantes) del Instituto Distrital de Recreación y Deporte (IDRD), con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información y de sus activos relacionados.

2. OBJETIVOS ESPECÍFICOS

- Establecer un esquema de seguridad digital y de la información claro, transparente y aplicable bajo la responsabilidad del IDRD en cuanto a la administración del riesgo se refiere.
- Comprometer a todo el personal del IDRD con el Sistema de Gestión de Seguridad de la Información (SGSI), con el fin de que este sea eficaz a la hora de preservar la seguridad digital y de la información y sus activos asociados.
- Proteger la información y recursos tecnológicos utilizados por el IDRD frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información de la entidad.
- Proteger los activos de información, de tal manera que se garantice su confidencialidad, integridad y disponibilidad de acuerdo con el nivel de criticidad establecido en la clasificación y valoración de dichos activos realizada en el Instituto.
- Definir directrices para el uso de los componentes de hardware, software, información física e información digital del IDRD, con el fin de contribuir a la reducción del riesgo de ocurrencia de incidentes de seguridad de la información en el marco del Modelos de seguridad y Privacidad de la Información (MSPI).

- Este documento describe las políticas de seguridad digital y de la información definidas por el IDRD, teniendo en cuenta la estrategia de Gobierno Digital de

COPIA IMPRESA NO CONTROLADA

MINTIC, la ley estatutaria de protección de datos personales (Ley 1581 de 2012) y sus decretos reglamentarios, y demás legislación aplicable, además de la norma NTC - ISO/IEC 27001:2022.

Estas políticas se aplican en todo el ámbito del IDRD, a sus recursos, a la totalidad de los procesos, directivos, funcionarios, contratistas, terceros que laboren o tengan relación con la entidad y visitantes.

Tanto el Director, Subdirectores, Jefes de Dependencias, Personal de Planta y Contratistas sea cual fuere su nivel jerárquico son responsables de la implementación de estas políticas digitales y de seguridad de la información.
La vigencia de las políticas aquí señaladas se establecerá desde la aprobación de este documento hasta la expedición de la siguiente versión.

COPIA IMPRESA NO CONTROLADA

3. DEFINICIONES

Tomadas de las normas NTC ISO/IEC 27001:2022, NTC ISO 31000:2011 y NTC ISO/IEC 27005:2009.

- **Activos de seguridad de la información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (hardware, software, información física o digital, personas), que tenga valor para la entidad.

- **Antivirus:** Programa especializado en la detección y, si es posible, en el bloqueo y/o eliminación de virus informáticos.

- **Autenticación:** Servicio que permite verificar la identidad de un ciudadano para acceder a trámites y servicios que requieran, a través de medios electrónicos.

- **Backup:** Copia de seguridad de los datos, de tal forma que se pueda restaurar un sistema después de una pérdida de información. Se puede realizar en medios magnéticos, servidores externos y almacenar en un lugar seguro.

- **Borrado seguro:** Proceso sobre escritura de información en un disco duro u otro medio de almacenamiento informático, que hace que la recuperación de los datos residuales sea una tarea prácticamente imposible.

- **Cifrar:** Es el proceso para volver ilegible información considerada importante. Se trata de una medida de seguridad usada para almacenar o transferir información delicada que no debería ser accesible a terceros. La información una vez cifrada sólo puede leerse aplicando una clave.

- **Confidencialidad:** La información debe ser accesible sólo a aquellas personas autorizadas.

- **Criptografía:** La criptografía es una técnica o conjunto de métodos cuya función es transformar un determinado mensaje o información en otro totalmente distinto ilegible para aquellas personas que no estén autorizadas a leerlo.

- **Disponibilidad:** La información y los servicios deben estar disponible cuando se le requiera.

- **Firmware:** Es un programa informático que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo. Está fuertemente integrado con la electrónica del dispositivo, es el software que tiene directa interacción con el hardware, siendo así el encargado de controlarlo para

COPIA IMPRESA NO CONTROLADA

ejecutar correctamente las instrucciones externas. De hecho, el firmware es uno de los tres principales pilares del diseño electrónico.

- **Hardware:** Es un término genérico para todos los componentes físicos.

- **IDRD:** Instituto Distrital de Recreación y Deporte.

- **Incidente:** Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Integridad:** La información y sus métodos de procesamiento deben ser completos y exactos.

- **Información:** Datos relacionados que tienen valor para la entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada (ISO/IEC 27001:2022).

- **Información pública:** Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad (Guía No. 5. Guía para la Gestión y Clasificación de Activos - MINTIC).

- ***Información pública clasificada:*** Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida

COPIA IMPRESA NO CONTROLADA

por terceros sin autorización del propietario (Guía No. 5. Guía para la Gestión y Clasificación de Activos - MINTIC).

- **Información pública reservada:** Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica (Guía No. 5. Guía para la Gestión y Clasificación de Activos - MINTIC).

- **Keepass:** Es un gestor de contraseñas con una infinidad de opciones que contribuyen a ofrecer una fiabilidad en seguridad mediante el cifrado de contraseñas.

- **Keylogger (Registrador de teclas):** Es una herramienta maliciosa que se encarga de registrar las pulsaciones que se hacen sobre el teclado con el fin de capturar lo digitado.

- **Logs de auditoría o registros de eventos:** Registro de eventos almacenados en un archivo, que contiene información relevante de las actividades realizadas sobre sistemas y aplicaciones informáticas. Los logs de auditoría son el principal instrumento para detectar, diagnosticar, auditar y analizar problemas de todo tipo, especialmente aquellos que tienen que ver con la seguridad de los datos, de la red, el uso del servicio de navegación en Internet, los errores de las máquinas centrales (Servidores), periféricos, etc.
- **MINTIC:** Ministerio de Tecnologías de la Información y las Comunicaciones.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información
- **Pendrive usb:** Es un tipo de dispositivo de almacenamiento de datos que utiliza memoria flash para guardar información.
- **Plan de contingencia:** Es un conjunto de procedimientos alternativos a la operatividad normal de cada entidad. Su finalidad es la de permitir el funcionamiento

COPIA IMPRESA NO CONTROLADA

de ésta, aun cuando alguna de sus funciones deje de hacerlo a causa de algún incidente tanto interno como externo a la organización

- **Programas utilitarios:** Hacen referencia a software diseñado para realizar una función determinada. El término utilitario se refiere normalmente al software que resuelve problemas relacionados con la administración del sistema. Algunos ejemplos de software utilitario son: aplicaciones para cifrado y descifrado de archivos, aplicaciones para compresión de archivos, software antivirus, navegadores (Google Chrome, Mozilla Firefox, entre otros) editores de texto, administradores de tareas, aplicaciones para realizar copias de respaldo, entre otros.
- **Programas utilitarios privilegiados:** Los programas utilitarios privilegiados son aquellos que tienen la capacidad de anular el sistema y los controles de las aplicaciones. Algunos ejemplos son: Interfaz de línea de comandos (cmd en Windows o terminal en linux), administrador de tareas, sniffers de red (wireshark, bettercap, entre otros), herramientas de administración de red.
- **Proyecto:** Planes de trabajo con acciones sistemáticas, planteados por las diferentes áreas del IDRD en busca de alcanzar los objetivos de la entidad, que requieren una asignación presupuestal, se rigen por el manual de contratación establecido en la entidad, manteniendo el adecuado manejo de la información.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.

COPIA IMPRESA NO CONTROLADA

No Repudio: Se refiere a la capacidad de garantizar que, cuando se realiza un intercambio de información, el receptor de la información no puede negar haberla recibido, y el emisor de la información no puede negar haberla enviado.

Malware: Se replica así mismo al adjuntarse a otro programa o archivo

PHISHING, VISHING: Es una forma de ingeniería social en la cual un atacante intenta de forma fraudulenta adquirir información confidencial, haciéndose pasar por un "tercero de confianza

Ransomware: Este malware está diseñado para mantener captivo un sistema de computación o los datos que contiene hasta que se realice un pago

- **Seguridad digital:** Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la gestión del riesgo de seguridad digital y la implementación efectiva de medidas de ciberseguridad y Ciberdefensa.
- **Teamviewer:** Es la principal solución de software para soporte remoto, acceso remoto y colaboración en línea.
- **TIC:** Tecnologías de la Información y las Comunicaciones.
- **Troyano:** Es un programa malicioso capaz de alojarse en un computador y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de apoderarse de la información o controlar remotamente a la máquina.
- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
- **UPS:** Uninterruptible Power Supply- Sistemas de Energía Ininterrumpible.
- **VPN:** En informática, acrónimo del Inglés Virtual Prívate Networks, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- **WIFI:** Wireless Fidelity - Fidelidad inalámbrica.

COPIA IMPRESA NO CONTROLADA

4. ALCANCE

Este manual, está enmarcado en la Política de Seguridad Digital, del Modelo de seguridad y privacidad de la información - MSPI y el Modelo Integrado de Planeación y Gestión – MIPG, los cuales proporcionan lineamientos que comprenden todas las actividades que involucran los activos de información, atendidos por parte de los servidores públicos y colaboradores de la Entidad.

5. POLÍTICAS DE SEGURIDAD DIGITAL Y DE LA INFORMACIÓN

El Ministerio de las TIC expidió el Decreto 767 del 2022 para la actualización de la Política Colombiana de Gobierno Digital, donde el habilitador de Seguridad Digital estructura lineamientos para fortalecer la transformación digital y para brindar servicios ciudadanos digitales seguros por medio del fortalecimiento de la seguridad de la información en las Entidades del estado, al aplicar un enfoque de gestión de seguridad y privacidad a los activos de información. El presente documento busca el fortalecimiento de la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en el IDRD, con el fin de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

COPIA IMPRESA NO CONTROLADA

5.1. Revisión del manual de políticas de seguridad digital y de la información

Las políticas de seguridad digital y de la información deben ser revisadas y actualizadas (en caso de ser necesario) al menos una vez al año o cuando haya cambios relevantes en el contexto estratégico del IDRD, con el fin de asegurar que sigan siendo adecuados a la estrategia y necesidades de la organización. Esta actividad es responsabilidad del Oficial de Seguridad de la Información.

5.2. Roles y responsabilidades

- Todo aquel que tenga acceso a la información del IDRD, será responsable de velar por la seguridad digital y de la información a la que tiene acceso y de cumplir las políticas descritas en este documento; entre ellos están: funcionarios, contratistas, proveedores y visitantes.

- Es responsabilidad de los funcionarios y contratistas consultar permanentemente los medios establecidos por el IDRD para comunicación de

la documentación del MSPI, los cuales son: Isolución, correo electrónico y Orfeo, con el fin de estar al tanto de los cambios a políticas y procedimientos de seguridad digital y de la información. El incumplimiento de procedimientos o políticas de seguridad digital y de la información por no atención de los comunicados oficiales no exime al funcionario o contratista de las medidas que pueda tomar el IDRD, como se menciona en la sección 7 de este documento.

- El Oficial de Seguridad de la Información (OSI), asume la responsabilidad por el desarrollo e implementación de la seguridad digital y de la información, comprueba el cumplimiento de las políticas, en caso de requerirse presta asesoría a todo aquel que maneje información de la entidad, coordina las actividades de la gestión de riesgos de la seguridad digital y de la información, apoya la identificación de controles y reportará al Comité Institucional de Gestión y Desempeño del Instituto Distrital de Recreación y Deporte.

5.3. Segregación de funciones

- Todo aquel que tenga acceso a la información del IDRD, debe tener claramente definidas sus funciones u obligaciones, con el fin de reducir el uso no autorizado, indebido o accidental de los activos de información.
- Todos los sistemas de información de la entidad, deben implementar reglas de acceso, de tal forma que existan roles entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

5.4. Responsabilidades de la dirección

La Dirección General debe demostrar su compromiso con la formulación, implementación, operación, seguimiento, revisión, mantenimiento y mejora de los

COPIA IMPRESA NO CONTROLADA

mecanismos destinados a garantizar la seguridad de la información en el Instituto, mediante las siguientes acciones:

- **A través de un Comité Institucional de Gestión y Desempeño:** El Instituto Distrital de Recreación y Deporte - IDRD es responsable de la aprobación y seguimiento de la estrategia para la implementación de la Política Digital, así como de la Seguridad y Privacidad de la Información.
- **Comunicación interna:** La Dirección General debe garantizar que la entidad esté informada sobre la importancia de cumplir con los objetivos de seguridad de la información, las responsabilidades legales asociadas y la necesidad de una mejora continua, en alineación con los objetivos estratégicos del Instituto.

Además, el director, subdirectores, gerentes y jefes de oficinas asesoras tienen la responsabilidad de asegurar el cumplimiento de las normas y políticas de seguridad de la información establecidas por la Dirección General del Instituto Distrital de Recreación y Deporte – IDRD.

COPIA IMPRESA NO CONTROLADA

5.5. Contacto con autoridades y grupos de interés

- El IDRD mantiene contacto con las autoridades competentes para el cumplimiento de la ley, organismos de control y autoridades de supervisión correspondientes. Para mantener contacto con organismos de control y autoridades de supervisión se siguen las directrices del procedimiento de atención a entes externos de control. Adicionalmente, el Área de Sistemas cuenta con un directorio actualizado de autoridades y grupos de interés como: CSIRT- Distrito, CSIRT GOBIERNO, CAI virtual, MINTIC entre otros.

5.6. Contacto con grupos de interés especial

- El Área de Sistemas junto con el Oficial de Seguridad mantendrá contacto con grupos especializados, foros y asociaciones profesionales en el campo de la seguridad de la información. Lo anterior, con el fin de estar al día con la información relacionada con la seguridad digital y de la información y recibir advertencias de actualizaciones, ataques, y vulnerabilidades del software y firmware utilizado en el IDRD.

5.7. Inteligencia de amenazas

- Permite a las entidades identificar y defenderse contra ataques informáticos, malware, intrusiones o cualquier actividad que pueda comprometer sus activos digitales.

5.8. Seguridad digital y de la información en la gestión de proyectos

La seguridad digital y de la información debe ser parte integral en la entidad y se debe asegurar que los riesgos de seguridad digital y de la información se identifiquen y traten como parte de los proyectos. Esto aplica a cualquier proyecto, independientemente de su naturaleza. Por lo tanto, es responsabilidad de los Jefes de dependencia y/o área asegurar que se sigan las siguientes directrices:

- Incluir objetivos de seguridad digital y de la información en los objetivos del proyecto.
- Realizar valoración de los riesgos de seguridad digital y de la información en la fase de estudios previos del proyecto, para identificar los controles necesarios.
- Hacer seguimiento a los riesgos y controles aplicados para tratar los riesgos, durante todas las fases del proyecto.

5.9. Inventario de información y otros activos asociados

COPIA IMPRESA NO CONTROLADA

Recopilación y registro detallado de todos los recursos, datos y activos críticos dentro de una entidad que son esenciales para sus operaciones y seguridad. Este inventario es una parte clave en la gestión de riesgos y en la protección de la información, ya que permite identificar, clasificar y priorizar los activos según su importancia y vulnerabilidad. Los activos que suelen incluirse en este inventario pueden ser:

- Información: Datos confidenciales, registros, bases de datos, documentos digitales, correos electrónicos y otros tipos de información relevante para el negocio.
- Hardware: Servidores, computadoras, dispositivos móviles, redes y otros equipos físicos utilizados para almacenar, procesar o transmitir información.
- Software: Aplicaciones, sistemas operativos, herramientas de seguridad, plataformas de gestión y cualquier otro programa utilizado para la operación de la infraestructura.
- Recursos humanos: El personal clave o colaboradores que gestionan, procesan o tienen acceso a información crítica.
- Redes y comunicaciones: Infraestructura de telecomunicaciones y redes que permiten el intercambio de datos e información.
- Servicios de terceros: Contratos, proveedores o socios que gestionan o tienen acceso a activos críticos de la organización.

COPIA IMPRESA NO CONTROLADA

5.10. Uso aceptable de la información y otros activos asociados

La información, archivos físicos, sistemas, servicios, y los equipos (ej. estaciones de trabajo, portátiles, impresoras, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos, entre otros) propiedad de la entidad, son activos de la entidad y se proporcionan a los funcionarios, contratistas y terceros autorizados, para cumplir con los propósitos de la entidad.

5.11. Devolución de bienes

- La devolución de bienes se controla mediante el formato de acta de entrega del cargo en el caso de funcionarios, para los contratistas se emite un certificado de paz y salvo del Almacén General.
- La devolución de equipos de cómputo se realiza de acuerdo al procedimiento Salidas, Traslado y Reintegro de Bienes.
- Para la entrega del puesto de trabajo por traslado o entrega definitiva de algún funcionario, es responsabilidad de los jefes de área solicitar la entrega de la información a la cual se tenía acceso, así mismo solicitar al área de sistemas la desactivación de los usuarios de los sistemas de información.
- En el caso de los contratistas antes de finalizar la vigencia del contrato, el supervisor del contrato deberá solicitar la entrega de la información física y electrónica relacionado con el objeto del contrato.

5.12. Clasificación de la información

- En atención a los requisitos de la norma NTC-ISO/IEC 27001:2022, la Ley 1712 de 2014 y el Decreto 103 de 2015, el IDRD clasifica, etiqueta y maneja la información y sus activos asociados de acuerdo índice de información reservada y/o clasificada del IDRD publicada en la página web de la entidad idrd.gov.co

COPIA IMPRESA NO CONTROLADA

5.13. Etiquetado de la información

- De acuerdo con la clasificación de la información establecida por el IDRD y en el cumplimiento de los requisitos exigidos por el Archivo General de la Nación y el Archivo Distrital es el área de archivo y correspondencia quienes dictan las políticas relacionadas con metadatos, marcas de agua, etiquetas físicas conservando la confidencialidad de la información.

5.14. Transferencia de la información

- Se deberán seguir las indicaciones establecidas en el decreto 575 del 29 de nov de 2023, garantizando las condiciones de integridad y confidencialidad de la información, además de la privacidad y protección de datos personales.

5.15. Control de acceso

El área de sistemas controla el acceso mediante el enfoque basado en roles y aplicando los siguientes principios:

- **Lo que necesita conocer:** Solamente se concede acceso a la información que la persona necesita para la realización de sus tareas (diferentes tareas/roles significan diferentes cosas que se necesita saber y, en consecuencia, diferentes perfiles de acceso).
- **Lo que necesita usar:** Solamente se concede acceso a las instalaciones de procesamiento de información (equipos de TI, aplicaciones, procedimientos, recintos) que la persona necesita para la realización de su tarea/trabajo/rol.

COPIA IMPRESA NO CONTROLADA

5.15.1. Acceso a redes y a servicios en red

- Ningún funcionario o contratista podrá compartir archivos o carpetas de un equipo de cómputo a otro sin la respectiva autorización del Área de Sistemas.
- El acceso a redes Wi-Fi se controla con autenticación por contraseña utilizando el protocolo WPA2-PSK.
- El Área de Sistemas proporciona un servicio de conectividad a todos los funcionarios y contratistas de la entidad para la navegación en internet, la cual es controlada mediante perfiles de navegación.
- La conexión remota a la red de área local del IDRD, debe ser realizada a través de una conexión VPN segura o mediante conexión por teamviewer, suministrada por el Área de Sistemas, previa autorización del responsable del

área y/o dependencia, quien es el encargado de realizar la solicitud formal al Área de Sistemas.

5.15.2. Gestión de acceso de usuarios

- El registro y cancelación de usuarios, el suministro de acceso a usuarios, la gestión de derechos de acceso privilegiado, la gestión de información de autenticación secreta, y la revisión, retiro o ajuste de los derechos de acceso se realizan de acuerdo con el procedimiento para gestionar acceso a los medios de procesamiento de información.

5.15.3. Uso de información de autenticación secreta (Responsabilidades de los usuarios)

- Cada usuario es responsable de mantener a salvo la contraseña de ingreso al equipo. Adicionalmente, los usuarios autorizados a acceder a los sistemas de información del IDRD, son responsables de la seguridad de las contraseñas y cuentas de usuario. Cabe resaltar que las contraseñas son únicas e intransferibles.
- No se debe guardar o escribir las contraseñas en papeles físicos o documentos de texto como bloc de notas, documentos de word o las notas de windows. Sin embargo, las contraseñas podrán ser almacenadas en llaveros de la aplicación como KeePass u otros similares.
- La contraseña escogida para el acceso a cada uno de los sistemas de información del IDRD debe:
  - ✓ Ser diferente para cada aplicación o sistema de información con excepción de aquellos sistemas que se autentiquen contra el directorio activo.
  - ✓ No debe contener características personales o de los parientes tales como nombres, apellidos, fechas de cumpleaños o alguna otra fecha importante.

COPIA IMPRESA NO CONTROLADA

- ✓ No debe contener palabras de diccionario. Las palabras en idioma inglés y español son las primeras utilizadas por los atacantes.
- ✓ Las contraseñas se deben establecer teniendo en cuenta los siguientes parámetros: Deben contener mayúsculas, minúsculas, números, caracteres especiales y mínimo ocho (08) caracteres.

- Las contraseñas deben ser cambiadas cada seis (6) meses como máximo, para ello, las aplicaciones controladas mediante el directorio activo al igual que el correo electrónico, exigirán el cambio automático de las contraseñas con la periodicidad mencionada.
- Está prohibido facilitar o proporcionar acceso a las aplicaciones e información a usuarios del IDRD o a terceros no autorizados.
- Para desbloquear la clave de acceso a los diferentes sistemas de información, el usuario debe realizar la solicitud ante la mesa de ayuda a través del correo **soporte@idrd.gov.co** En caso tal, que la aplicación bloqueada sea el correo electrónico, la solicitud podrá ser realizada por el Jefe inmediato.

COPIA IMPRESA NO CONTROLADA

5.15.4. Control de acceso a sistemas y aplicaciones

- El control de acceso a sistemas y aplicaciones se rige por la política de control de acceso y el procedimiento para gestionar acceso a los medios de procesamiento de información.
  - Las aplicaciones críticas del IDRD deben contar con certificado de seguridad HTTPS.
  - Las aplicaciones críticas del IDRD deben implementar mecanismos de protección contra intentos de ingreso mediante fuerza bruta, tales como recaptcha y/o bloqueo de cuentas por un tiempo determinado después de múltiples intentos o doble factor de autenticación.

- Con el fin de controlar el acceso no autorizado a sistemas y aplicaciones, las contraseñas de cuentas de administración genéricas (root, SYS, SYSADMIN, cuenta de administrador de Windows, entre otras) deben ser cambiadas anualmente o cada vez que cada vez que expire el tiempo de acceso concedido a un funcionario, ex funcionario, contratista y/o proveedor.
- El Área de Sistemas debe cambiar las contraseñas por defecto (y donde sea posible, los usuarios por defecto) de las aplicaciones y servicios utilizados por el IDRD.
- El uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones, no está permitido para fines diferentes a las actividades propias del Área de Sistemas.
- El IDRD controla el uso de programas utilitarios privilegiados mediante directorio activo y sistema de antivirus endpoint.
- Para acceder a los códigos fuente de programas y elementos asociados (tales como diseños, especificaciones, planes de verificación y planes de validación) se debe contar con autorización del Área de Sistemas. Lo anterior, con el fin de evitar la introducción de funcionalidades no autorizadas, evitar cambios involuntarios y mantener la confidencialidad de propiedad intelectual valiosa.

COPIA IMPRESA NO CONTROLADA

5.16. Gestión de identidad

Para la gestión de identidad dentro del IDRD se debe seguir el procedimiento de gestión de Identidad del proceso de gestión de TI contenido en la documentación dentro de isolución.

5.17. Información de autenticación

El área de sistemas deberá crear una contraseña inicial para los usuarios nuevos creados de acuerdo con el procedimiento de gestión de identidad, esta deberá ser de complejidad alta y deberá contener caracteres alfanuméricos, mayúsculas y carácter especiales y su longitud deberá ser mayor de 10 caracteres, será de un solo uso y deberá ser cambiada inmediatamente por los usuarios una vez se acceda por primera vez.

Es responsabilidad del usuario el manejo de los usuarios asignados para acceder a los sistemas de información del IDRD, no deberá anotar el usuario en posit o papeles pegados a las pantallas o sobre el escritorio.

El área de sistemas activará los log de registro de eventos de inicio de sesión en los sistemas de información y los almacenará por mínimo 6 meses, a su vez controlará el número de intentos para iniciar sesión en los sistemas de información y una vez superado este número de intentos errados bloqueará el usuario de manera preventiva para evitar ataques de fuerza bruta.

La contraseña asignada para validarse en los sistemas de información es personal, secreta e intransferible no debe ser compartida a ninguna persona, solo podrá ser cambiada por solicitud del usuario o en caso que la persona ya no tenga vínculo con el IDRD el jefe del área podrá realizar la solicitud en la mesa de servicios tecnológicos.

COPIA IMPRESA NO CONTROLADA

5.18. Derechos de acceso

Para la creación de los usuarios se deberá seguir con el procedimiento de gestión de identidad del proceso de gestión de TI, además se deberá definir los roles en cada uno de los sistemas de información para asignar los accesos a la información necesaria de acuerdo con el desarrollo de las funciones y/o obligaciones de los usuarios.

El administrador técnico de cada sistema de información deberá realizar actualización de los roles asignados a cada usuario con cada jefe de área por lo menos una vez

por año, para verificar que sean los que debe tener de acuerdo con sus funciones, a su vez deberá desactivar los usuarios que ya no se encuentren en el área o por solicitud del jefe del área.

Los usuarios que se encuentren vinculados al directorio activo se deberán desactivar una vez se termine el contrato, por novedades informadas por el área de talento humano, o cuando se detecte algún evento de seguridad relacionado con el usuario.

Para la creación de usuarios de entidades externas o ajenos al IDRD estos deberán ser solicitados por el jefe del área y deberán ser autorizados por el subdirector administrativo quien tiene el rol de oficial de seguridad de la información de la entidad.

Cada sistema de información deberá tener dentro de su documentación la matriz de roles y perfiles con la descripción de los permisos de acceso a cada sistema de información.

COPIA IMPRESA NO CONTROLADA

5.19. Seguridad de la información de las relaciones con los proveedores

Dentro de los contratos con proveedores deberá quedar estipulado el cumplimiento del manual de políticas de seguridad de la información y se deberá diligenciar un acuerdo de confidencialidad para el acceso a la información que pueda tener dentro del desarrollo de las obligaciones contractuales, En el mismo sentido y a través del seguimiento a la ejecución, se garantizará que los supervisores de los contratos, convenios o acuerdos sean los responsables de aplicar las políticas y procedimientos de seguridad de la información durante la ejecución de los mismos. Estos lineamientos deberán ser comunicados a los proveedores y terceros a través de los canales dispuestos por el IDRD.

5.20. Requisitos de seguridad de la información en contratos con terceros

Mantener la seguridad y privacidad de los activos de información y los servicios de procesamiento de información a los cuales se les ha autorizado acceso a las partes externas denominados proveedores; o que son procesados, comunicados o dirigidos por estos.

Asegurar que las partes involucradas cumplan con normativas de privacidad y protección.

5.21. Gestión de la seguridad de la información en la cadena de suministro de tic

Garantizar la integridad, confidencialidad y disponibilidad de los datos en todas las etapas del ciclo de vida de los productos y servicios tecnológicos.

5.22. Seguimiento, revisión y monitoreo de los servicios del proveedor

Es la evaluación continua del desempeño del proveedor, especialmente en lo que respecta a la seguridad de la información, cumplimiento de SLA (Acuerdos de Nivel de Servicio), y la gestión de riesgos. Un seguimiento eficaz debe centrarse en varios elementos clave:

- **Evaluación periódica del rendimiento**: Verificar que el proveedor esté cumpliendo con los términos acordados en el contrato, como tiempos de respuesta, disponibilidad del servicio, y la calidad de la entrega.
- **Evaluación de la seguridad**: Asegurarse de que el proveedor mantenga y actualice adecuadamente sus controles de seguridad. Esto incluye la revisión de políticas, procedimientos y medidas de protección de datos (como el cifrado y control de accesos).
- **Indicadores clave de rendimiento (KPIs)**: Establecer y monitorear KPIs relacionados con la seguridad, como la cantidad de incidentes de seguridad reportados, el tiempo de respuesta ante incidentes, la efectividad de las

COPIA IMPRESA NO CONTROLADA

medidas correctivas y la satisfacción del cliente respecto a los servicios proporcionados.

5.23. Seguridad de la información para el uso de servicios en la nube

Son los datos que están almacenados y procesados en servidores externos. Para proteger la información, tanto los usuarios como los proveedores de servicios en la nube deben seguir buenas prácticas y aplicar medidas de seguridad adecuadas.

5.24. Planificación y preparación de la gestión de incidentes de seguridad

El IDRD a través del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, promoverá entre los empleados públicos y contratistas, el reporte y seguimiento de incidentes relacionados con la seguridad y privacidad de la información y sus medios. Así mismo, asignará responsables para el tratamiento de los mismos, quienes investigarán y solucionarán los incidentes reportados, de acuerdo a su sana crítica.

El Director del IDRD o su delegado son los únicos autorizados para reportar incidentes de seguridad y privacidad ante las autoridades de defensa nacional, policía, fiscalía y de control. En esta medida, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas, medios de comunicación o la ciudadanía.

COPIA IMPRESA NO CONTROLADA

5.25. Evaluación y decisión en los eventos de seguridad de la información

Un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las actividades del negocio y amenazar la seguridad de la información.

5.26. Aprendizaje de los incidentes de seguridad de la información

La política de gestión de incidentes de seguridad de la información de la entidad y sus procedimientos de apoyo definen los métodos estándar para identificar, realizar seguimiento y responder a los incidentes de seguridad de la información de la entidad.

5.27. Seguridad de información durante interrupciones

Dentro de la activación del plan de recuperación de desastres DRP, se debe mantener las medidas de seguridad de la información con el fin de evitar que se aumente el riesgo de pérdida de confidencialidad integridad o disponibilidad de la información, de acuerdo con los activos de información afectados dentro del posible incidente.

COPIA IMPRESA NO CONTROLADA

5.28. Preparación de las tic para la continuidad del negocio

El IDRD dispondrá los planes necesarios para la continuidad de la operación de los servicios, los cuales serán operados por los líderes de los procesos. El Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, la Oficina Asesora de Planeación, la Subdirección Administrativa y la Oficina Sistemas liderarán conjuntamente la elaboración del Análisis de Impacto del Negocio (BIA) y del Plan de Continuidad de la Operación de los Servicios (BCP).

El Plan de Continuidad de los Servicios del IDRD de la Información y las Comunicaciones contendrá el Plan de Continuidad de Tecnologías y los Planes de Emergencia y Contingencia, así como cualquier estrategia orientada a la continuidad de la prestación del servicio del IDRD.

La subdirección administrativa y financiera y el área de sistemas liderarán, implementarán y actualizarán el Plan de Continuidad de las TIC (Plan de Recuperación ante Desastres Tecnológicos) alineado a su vez con el BIA y el BCP. Este plan incluirá escenarios de falla, estrategias de recuperación, roles y responsabilidades, plan de comunicación, pruebas y demás atributos que la entidad defina, lo cual permite propender por la disponibilidad y el acceso a los sistemas, datos y aplicaciones de información críticos en caso de interrupciones o eventos disruptivos.

5.29. Requisitos legales, estatutarios, reglamentarios y contractuales

El área de planeación, mediante la estrategia de Seguridad de la Información, deberá identificar, registrar y actualizar todos los requisitos contractuales, legales y reglamentarios, con el propósito de proteger la información de la entidad y asegurar el cumplimiento de la legislación vigente, utilizando la herramienta para verificar los requisitos legales.

- La Oficina de Jurídica deberá ofrecer orientación al MSPI de Seguridad de la Información en la elaboración de la documentación técnica y administrativa, con el objetivo de integrar un marco normativo en la gestión de las Tecnologías de la Información.

COPIA IMPRESA NO CONTROLADA

5.30. Derechos de propiedad intelectual

Los funcionarios, contratistas y colaboradores que ejecuten actividades de adquisición o licenciamiento de software tienen el deber de seguir los lineamientos de compra pública e incluir dentro de los estudios previos y pliegos de condiciones, los términos mediante los cuales se acreditará que la forma del licenciamiento, la forma en la que se ejercerán derechos morales y patrimoniales de autor, el número

máximo de usuarios o recursos, la forma de instalación y los procedimientos para mantener las condiciones de licencia adecuadas, desechar o transferir software a otros.

5.31. Protección de registros

La oficina de planeación, en colaboración con la Oficina de Gestión Documental, deberá definir y establecer lo siguiente:

- Lineamientos para la retención, almacenamiento, manejo y eliminación de registros e información tanto física como digital.
- Implementación de controles para salvaguardar la confidencialidad, integridad y disponibilidad de los registros.
- Procedimientos para el almacenamiento a largo plazo y manejo adecuado de los registros, tanto físicos como digitales.

Asimismo, la OAPTI será responsable de identificar, gestionar y documentar los controles criptográficos requeridos para la infraestructura tecnológica del Idartes

5.32. Privacidad y protección de datos personales

EL IDRD a través del Oficial de Seguridad y Privacidad de la Información, o quien haga sus veces, velará por la identificación, documentación y cumplimiento de los requisitos legales enmarcados en la seguridad y privacidad de la información, de acuerdo con lo establecido por el gobierno nacional, entre ellos los referentes a derechos de autor y propiedad intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública, para lo cual dispondrá una Matriz de Requisitos Legales para su control y seguimiento.

EL IDRD deberá disponer, a través del Oficial de protección de datos o quien haga sus veces, de los controles necesarios para la protección de la información personal

COPIA IMPRESA NO CONTROLADA

de los empleados públicos, contratistas y partes interesadas externas, en los términos del artículo 15 de la Constitución política, regulado por la Ley 1581 de 2012 y sus decretos reglamentarios, además deberá atender al cumplimiento del principio de responsabilidad demostrada y las obligaciones derivadas del rol de Responsable y/o encargado del tratamiento de datos personales, en los términos establecidos por la **Ley 1581 de 2012 y el Decreto 1377 de 2014**.

EL IDRD a través de la Oficial de protección de datos personales y la oficina jurídica del IDRD, se establecerá y comunicará la política específica sobre privacidad y protección de la IIP, que, a efectos de la legislación local, corresponde a la Política de Tratamiento de Datos Personales.

COPIA IMPRESA NO CONTROLADA

5.33. Proceso disciplinario

De acuerdo con el debido proceso

5.34. Responsabilidades después de la terminación o cambio de empleo

En atención a los requisitos de la norma NTC-ISO/IEC 27001:2022 y la legislación aplicable con relación a la contratación pública, la vinculación laboral, retiro laboral y el cambio de cargo se llevarán a cabo siguiendo las indicaciones del procedimiento de provisión del talento humano y el procedimiento de desvinculación de personal.
En el caso de los contratistas, los lineamientos para la vinculación y terminación contractual se encuentran las obligaciones generales y específicas de los contratos de prestación de servicios.

5.35. Política de Seguridad de Transferencia de información

Los funcionarios y funcionarias, contratistas o terceros que requieran transferir externamente información sensible (pública clasificada o pública reservada), deben

firmar el **"Acuerdo de confidencialidad"** donde se describan las responsabilidades de las partes y se garantice la reserva de la información; de igual forma, deben contar con la autorización previa de su jefe o jefa inmediata.

Los funcionarios y funcionarias, contratistas o terceros que requieran transferir información para el cumplimiento de sus funciones, deben utilizar los medios, herramientas de cifrado y demás recursos aprobados y dispuestos por el Proceso de Gestión de las tecnologías de la información para tal fin.

La transferencia o intercambio de información con entes de control y autoridades de supervisión, se rige por las directrices y mecanismos que dispongan dichos entes de control y la normatividad vigente.

Se deben implementar herramientas de cifrado de información cuando se trate de información pública reservada y pública clasificada, de acuerdo a lo definido por el Comité de Sistemas y Seguridad de la Información o su delegado, en todo caso, se debe garantizar el uso de los controles establecidos por el IDRD.

COPIA IMPRESA NO CONTROLADA

Sin excepción, los intercambios de información con otras entidades o partes externas interesadas, diferentes a los entes de control, deben estar soportados por medio de contratos, convenios o acuerdos formalizados, en donde se determinarán los medios y controles para el tratamiento de la información. De igual forma, se deben firmar acuerdos de confidencialidad que garanticen la protección de la información durante y después del tiempo de ejecución de los compromisos, cumpliendo la normatividad vigente en materia de protección de datos, especialmente la relativa a la Ley de Habeas Data (Ley 1266 de 2008 y sus decretos reglamentarios), la Ley de Protección de Datos Personales (Ley 1581 de 2012 y decretos reglamentarios) y Ley de Transparencia (Ley 1712 de 2014 y sus decretos reglamentarios).

Para la transferencia de información se deben analizar y tratar los riesgos relativos al uso de la información y la utilización de los diferentes canales de comunicación, de forma que se mantengan en los niveles de seguridad aceptables del Instituto de Recreación y Deporte IDRD. En cualquier medio que se lleve a cabo la transferencia de información (física o electrónica), se debe dar el cumplimiento a las políticas y procedimientos de seguridad de la información, de tal forma que se preserven los niveles de confidencialidad e integridad de los datos contenidos o transferidos.

5.36. Trabajo remoto

Cuando se requiera realizar labores de teletrabajo el jefe del área y/o dependencia a la cual pertenece el funcionario o contratista, debe solicitar al Área de Sistemas la creación de una VPN, indicando el tiempo por el cual estará vigente la conexión, los servicios, ambientes y aplicativos a los cuales se requiere acceder. Previo a la entrega de las credenciales de acceso, el funcionario o contratista se debe comprometer a hacer un uso adecuado de la VPN.

COPIA IMPRESA NO CONTROLADA

En los casos en los cuales el acceso y procesamiento de la información del IDRD, sea mediante la modalidad de teletrabajo, los responsables de estas actividades deben dar cumplimiento a las condiciones y restricciones definidas entorno a la seguridad de la información, tales como:

- Seguridad física y de comunicaciones.
- Amenazas de accesos no autorizados a información o recursos.
- Uso de equipos con software licenciado.

5.37. Reporte de eventos de seguridad de la información

Los funcionarios y contratistas de la entidad deben reportar los eventos de seguridad de la información identificados, de acuerdo con el procedimiento gestionar incidentes

de seguridad de la información, los canales de comunicación con el área de sistemas son el correo electrónico soporte@idrd.gov.co, de manera física en el área de sistemas.

5.38. Escritorio y pantallas limpias

Con el fin de establecer controles para el aseguramiento de la información del Instituto Distrital de Recreación y Deporte IDRD, los funcionarios y funcionarias y/o contratistas deben adoptar buenas prácticas para el manejo y administración de la información física y electrónica que se encuentra a su cargo, a fin de evitar que personas no autorizadas accedan a la misma. Para ello, los funcionarios y funcionarias, contratistas o terceros deben cumplir los siguientes lineamientos:

Los funcionarios y funcionarias y/o contratistas deben guardar en forma segura documentos y elementos de almacenamiento externos como (CD, DVD, USB, equipos portátiles, entre otros) en especial cuando no se encuentren en sus sitios de trabajo; para evitar accesos no autorizados, pérdida o daño de la información.

Es responsabilidad de los usuarios y usuarias bloquear la sesión de usuario en el computador donde realice su autenticación, con el protector de pantalla designado por la entidad, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su sitio de trabajo.

Los equipos de cómputo deberán quedar apagados al finalizar la jornada laboral o cuando una ausencia temporal supere las cuatro horas.

No imprimir trabajos o documentos que no sean del Instituto Distrital de Recreación y Deporte IDRD.

COPIA IMPRESA NO CONTROLADA

No está autorizado modificar el fondo del escritorio o protector de pantalla, ya que estos son de uso institucional.

5.39. Gestión de vulnerabilidades técnicas

El Área de Sistemas, es responsable de verificar de manera periódica (al menos semestralmente) la información publicada por parte de los fabricantes y foros de seguridad en relación con nuevas vulnerabilidades identificadas que puedan afectar los sistemas de información de la entidad.

Se debe generar y ejecutar por lo menos una vez al año un plan de análisis de vulnerabilidades y/o hacking ético para las plataformas críticas del IDRD, cuya viabilidad técnica y de administración lo permita.

Los correctivos que requieran ser aplicados en las plataformas tecnológicas, derivados de la identificación de vulnerabilidades técnicas, son responsabilidad del Área de Sistemas, siguiendo las directrices del procedimiento gestionar cambios de seguridad de la información.

COPIA IMPRESA NO CONTROLADA

5.40. Instalación de software en sistemas operativos

El proceso de instalación y desinstalación de software está autorizado exclusivamente al personal de soporte del Área de Sistemas. Por lo tanto, a cualquier otro servidor público o contratista no le es permitido realizar esta labor.

Para la instalación de software se deben seguir las siguientes directrices:

- El software propietario debe contar con su respectiva licencia y en el caso del software libre debe estar permitido el uso comercial.
- El instalador debe ser descargado de la página oficial del fabricante.

- Debe verificarse la integridad del archivo por medio de la comprobación de códigos hash (siempre que el fabricante proporcione esta información).
- Debe dejarse evidencia documentada de que las directrices anteriores fueron seguidas a cabalidad.

Se debe proporcionar capacitación adecuada a los usuarios y al personal técnico en los aspectos de operación y funcionalidad de los nuevos sistemas de información o mejoras a sistemas de información existentes, antes de su puesta en marcha.

Todos los sistemas nuevos y mejorados deben estar completamente soportados por una documentación suficientemente amplia y actualizada, y no deben ser puestos en el ambiente de producción sin contar con la documentación disponible.

COPIA IMPRESA NO CONTROLADA

5.40.1. Mecanismos de control

El Área de Sistemas debe definir e implementar los mecanismos de control que considere apropiados para proteger la confidencialidad, integridad y disponibilidad de las redes, los servicios en red y la información por allí transmitida.

5.40.2. Mecanismos de separación de redes

El Área de Sistemas define e implementa los mecanismos de separación de las redes del IDRD con base en los niveles de confianza (por ejemplo, dominio de acceso público, dominio de equipos de escritorio, dominio de servidores), por áreas y/o dependencias (por ejemplo, Área de Talento Humano, Área de Servicios Generales, Área de Gestión Financiera, Área de Sistemas) o alguna combinación (por ejemplo, un dominio de servidores que se conecta a múltiples dependencias).

5.40.3. Red de datos y red de voz

El Área de Sistemas debe mantener separadas la red de datos y la red de voz, con el fin de minimizar el impacto de interceptación de información en alguna de las dos redes, cuando la capacidad de puntos de red lo permitan.

5.40.4. Acceso remoto

El acceso remoto a las redes de la entidad se controla mediante conexiones VPN y teamviewer.

COPIA IMPRESA NO CONTROLADA

5.41. Filtrado web

El área de sistemas definirá los perfiles en el firewall y sus respectivas restricciones de navegación de cada uno

5.42. Uso de criptografía

Ofrecer mecanismos criptográficos apropiados para salvaguardar la confidencialidad, autenticidad e integridad de la información, según sea necesario.

De acuerdo con los roles y responsabilidades en el manejo de la información, se autorizará el uso de herramientas de cifrado para los funcionarios, contratistas y, en general, para todas las personas que trabajen en el IDRD.

Los funcionarios o contratistas autorizados para el uso de sistemas de cifrado de datos deberán asegurar la disponibilidad, integridad y confidencialidad de las llaves, herramientas y algoritmos de cifrado, así como de la información a la que se haya aplicado este proceso. Para la eliminación de la información cifrada o descifrada, se implementarán técnicas de borrado seguro.

5.43. Gestión de cambios

Para la planeación y estructuración de las ventanas de mantenimiento por actualización, implementación de nuevos servicios que puedan generar indisponibilidad de algún servicio en el ambiente de producción es necesario diligenciar el formato de control de cambios de seguridad con el fin de ser aprobado por el comité de seguridad de la información del área de sistemas compuesto por un representante del grupo de infraestructura, un representante del grupo de sistemas de información, el responsable del área de sistemas y el responsable de seguridad de la información, quienes aprobaran la ejecución del control de cambios de acuerdo a la programación

5.44. Gestión de la Continuidad

Es responsabilidad de la Subdirección Administrativa y Financiera, a través del Proceso de Gestión de Tecnologías de la información en el establecimiento, operación, seguimiento y mejora del plan de contingencia informático.

El Comité de Gestión Institucional de Gestión y Desempeño, es responsable de gestionar los recursos necesarios para definir, implementar, mantener y mejorar un plan de continuidad de la operación informática, que garantice la protección de los activos de información críticos para el instituto Distrital de Recreación y Deporte - IDRD.

COPIA IMPRESA NO CONTROLADA

El equipo de tecnología es responsable de la validación de la existencia del Plan de Contingencia Informático o Plan de Continuidad del Negocio, que garantice la recuperación de la operación informática frente a la posible materialización de riesgos de seguridad de la información.

El equipo de sistemas debe realizar una revisión, y de ser necesario, actualizar anualmente el mapa de riesgos del proceso de gestión de seguridad de la

información y recursos tecnológicos de acuerdo con el resultado de los simulacros o el análisis de los eventos presentados.

ELABORÓ	REVISÓ	APROBÓ
MARTHA P. MATEUS **Contratista Área de Sistemas**	JUAN CARLOS RODRIGUEZ WALTERO **Subdirector Administrativo y Financiero**	JUAN CARLOS RODRIGUEZ WALTERO **Subdirector Administrativo y Financiero** Fecha de Aprobación: 13022025
	Nancy Elizabeth Moreno **Jefe Oficina Asesora de Planeación (E)**	

COPIA IMPRESA NO CONTROLADA