ALCALDÍA MAYOR
DE BOGOTÁ D.C.
CULTURA, RECREACIÓN Y DEPORTE
Instituto Distrital de Recreación y Deporte

SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA
ÁREA DE SISTEMAS

MANUAL DE POLÍTICAS DE SEGURIDAD DIGITAL Y DE LA INFORMACIÓN

2019

TABLA DE CONTENIDO

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 (en adelante 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 (en adelante 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.

- 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 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 27001:2013.

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.

3. DEFINICIONES

Tomadas de las normas NTC ISO/IEC 27001:2013, 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 de sobreescritura 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 aplicándole 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 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 27001:2013)
- **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 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.

- **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 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.

- **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 Ingles Virtual Private 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.

4. POLÍTICAS DE SEGURIDAD DIGITAL Y DE LA INFORMACIÓN

4.1. REVISIÓN DEL MANUAL DE POLÍTICAS DE SEGURIDAD DIGITAL Y DE LA INFORMACIÓN

Las políticas de seguridad digital y de la información deben ser revisados y actualizados (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.

4.2. ORGANIZACIÓN DE LA SEGURIDAD

4.2.1. 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 SGSI, los cuales son: Isolucion, 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.

4.2.2. Separación de deberes

- 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.

4.2.3. 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.

- 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.

4.2.4. 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.

4.3. DISPOSITIVOS MÓVILES Y TELETRABAJO

4.3.1. Dispositivos móviles

- El Área de Sistemas restringe la conexión de dispositivos móviles tales como smartphones y tablets a las redes principales del IDRD, a excepción de los dispositivos que sean propiedad de la entidad o cuenten con autorización del jefe de cada área de la entidad. Se dispone de una red de invitados para la conexión de estos equipos, que permitirá la salida hacia Internet, pero no permitirá la conexión con equipos de cómputo o servidores del IDRD.

- Las estaciones de trabajo y equipos portátiles que son propiedad del IDRD cuentan con software licenciado y protección contra código malicioso.

- El contratista que utilice equipos de cómputo de su propiedad para el desarrollo del objeto del contrato debe:

  ✓ Garantizar que el software instalado en su equipo sea legal y cuente con las licencias requeridas para su conexión a la red del IDRD.

  ✓ Contar con software antivirus instalado y licenciado para su conexión a la red del IDRD.

  ✓ El IDRD se reserva el derecho de monitorear y revisar cuando se requiera, el software instalado y utilizado en equipos de cómputo y servidores conectados a la red de la entidad.

4.3.2. Teletrabajo

- 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.

- 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.

4.4. SEGURIDAD DE LOS RECURSOS HUMANOS

4.4.1. Vinculación, desvinculación y cambio de empleo

- En atención a los requisitos de la norma NTC-ISO/IEC 27001:2013 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 laboral y el retiro laboral se encuentran en los contratos de prestación de servicios.

4.4.2. Capacitación y entrenamiento en seguridad digital y de la información

- El IDRD debe asegurar que todos los funcionarios, contratistas y todos aquellos con acceso a la información y que tengan definidas responsabilidades de seguridad digital y de la información sean competentes (en cuanto a capacitación formal y no formal) para desempeñar sus funciones u obligaciones. Para ello, el proceso de Gestión de Talento Humano elabora anualmente el Plan Institucional de Capacitación (PIC), siguiendo las indicaciones del procedimiento de capacitación.

4.4.3. Procesos disciplinarios

4.4.3.1. Los procesos disciplinarios en el IDRD se llevan a cabo de acuerdo con la Ley 1952 de 2019 "Por el cual se expide el Código General Disciplinario", por parte de la Oficina de Control Disciplinario Interno.

4.4.4. Intercambio de información

- El IDRD emite acto administrativo para los servidores públicos e incluye una cláusula de confidencialidad en los contratos con terceros que tengan acceso a la información y que por alguna razón requieran conocer o intercambiar información pública clasificada o publica reservada. En estos quedan especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se firman antes de permitir el acceso o uso de dicha información.

- El intercambio de información con organismos de control y autoridades de supervisión se rige por el procedimiento de atención a entes externos de control y las directrices que impartan para el intercambio de información, tales como, tokens y firmas digitales.

4.5. GESTIÓN DE ACTIVOS

4.5.1. Inventario de activos

- El Oficial de Seguridad de la Información elabora y mantiene actualizado el inventario de activos de seguridad de la información, de acuerdo con las directrices del procedimiento gestión de activos.

4.5.2. Asignación de activos

- La asignación de equipo de cómputo se realiza de acuerdo al procedimiento Salidas, Traslado y Reintegro de Bienes.

4.5.3. Uso aceptable de los activos

- 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.

- 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.

4.5.3.1. Uso de equipos de cómputo

- Está prohibido que personal ajeno al Área de Sistemas, destape o retire partes de los equipos de cómputo que pertenecen al inventario del IDRD.

- La instalación de cualquier tipo de software o hardware en los equipos de cómputo es responsabilidad del Área de Sistemas y, por tanto, se debe realizar una solicitud de soporte para la realización de estas labores.

- Los equipos de cómputo no podrán ser trasladados del sitio asignado inicialmente, ni cambiar el funcionario o contratista al que le fue asignado, sin previo aviso al Área de Sistemas.

- Debe respetarse y no modificarse la configuración de hardware y software establecido por el Área de Sistemas.

- Se restringe el acceso de medios extraíbles (USB, celulares, discos externos, CD, DVD, entre otros) para almacenamiento de información institucional en algunas estaciones de trabajo de la entidad, de acuerdo con las políticas de restricción del anexo 7 del modelo de seguridad y privacidad de la información de áreas financieras en entidades públicas.

- Toda actividad informática (escaneos de seguridad, ataques de autenticación o de denegación de servicio, etc.) no autorizada que afecte tanto las redes corporativas como los sistemas de información del IDRD, está prohibida y dará lugar a los procesos disciplinarios y/o legales correspondientes.

- Durante la permanencia en las instalaciones del IDRD, los equipos de cómputo externos, deben estar conectados únicamente a la red de datos corporativos configurada por el Área de Sistemas.

- Los equipos de cómputo (CPU y monitor), servidores, teléfonos IP y equipos de comunicaciones, deben conectarse a los puntos de corriente eléctrica identificados como regulados.

- La conexión eléctrica de equipos personales debe hacerse a través de los puntos eléctricos no regulados. El IDRD no se responsabiliza por daños que puedan sufrir estos dispositivos.

- La seguridad física e integridad de los equipos de cómputo que ingresen a las instalaciones del IDRD y que no son propiedad de la entidad, son responsabilidad única y exclusiva de sus propietarios. El IDRD, no es responsable por estos equipos en ningún caso.

4.5.3.2. Uso de internet

- Está prohibido conectar módems o celulares (en modo Access Point) para acceder a Internet, dentro de la red WAN de la entidad.

- Queda prohibido a todos los funcionarios y contratistas acceder a cualquier página o dirección que contenga material pornográfico en cualquiera de sus variantes, o bien páginas que promuevan cualquier tipo de ideas que puedan ser consideradas ofensivas para las normas del IDRD tales como violencia, terrorismo, grupos al margen de la ley, discriminación, entre otras.

- Se prohíbe el envío, descarga o visualización de información con contenido que atente contra la integridad moral personal, institucional o que conlleven a la comisión de algún delito.

- Con el propósito de minimizar la probabilidad de saturación, interrupción, alteraciones no autorizadas y errores en la red del IDRD, no se permite el envío o descarga de información masiva como música, videos y software no autorizado.

- Todo funcionario o contratista es responsable del contenido de toda comunicación e información que se envíe o descargue desde su cuenta (correo, directorio activo y demás aplicaciones) institucional.

- Todas las actividades realizadas en los sistemas de información del IDRD, podrán ser monitoreadas con el fin de preservar la seguridad informática de la entidad.

- Los funcionarios o contratistas no deben intentar burlar o evadir los sistemas de seguridad y de control de acceso; acciones de esta naturaleza se consideran violatorias de las políticas de la entidad y de la ley y serán sancionadas de acuerdo con la Ley 1952 de 2019 "Por el cual se expide el Código General Disciplinario" .

4.5.3.3. Uso del correo institucional

- La entidad proveerá a todos los funcionarios y contratistas un correo electrónico institucional en el dominio idrd.gov.co, de acuerdo con las funciones u obligaciones realizadas y a la capacidad de cuentas disponibles del IDRD.

- La cuenta de correo electrónico institucional es personal e intransferible, los usuarios son completamente responsables de todas las actividades realizadas con sus credenciales de acceso y el buzón asociado al correo de la entidad.

- El correo electrónico institucional se debe utilizar estrictamente como herramienta de comunicación del IDRD, es decir, que debe ser usado para transmitir información relacionada única y exclusivamente con el desarrollo de las funciones misionales y de apoyo asignadas.

- Teniendo en cuenta que el correo electrónico institucional es una herramienta para el intercambio de información necesaria que permita el cumplimiento de las funciones u obligaciones propias de cada cargo y no una herramienta de difusión masiva de información, no debe ser utilizada como servicio personal de mensajes o

cadenas a familiares o amigos, esquemas piramidales, terrorismo, pornografía, programas piratas, proselitismo político, religioso o racial, amenazas, estafas, virus o código malicioso, acciones de esta naturaleza se consideran violatorias de las políticas de la entidad y de la ley y serán sancionadas de acuerdo con la Ley 1952 de 2019 "Por el cual se expide el Código General Disciplinario"

- El servidor de correo bloquea archivos adjuntos o información nociva como archivos .exe o de ejecución de comandos.

- Bajo ningún motivo se debe abrir o ejecutar un correo de origen desconocido, debido a que podría tener código malicioso (virus, troyanos, keyloggers, gusanos, etc.), lo cual podría atentar contra los sistemas, programas y datos del IDRD.

- No está permitido abrir, usar o revisar indebidamente la cuenta de correo electrónico de otro usuario como si fuera propia.

- El funcionario o contratista debe notificar correos sospechosos a través de la mesa de ayuda GLPI, administrada por el Área de Sistemas mediante el correo a soporte@idrd.gov.co. Estos correos no deben ser reenviados a ningún usuario.

4.5.4. Devolución de activos

- La devolución de activos se controla mediante el formato de acta de entrega del cargo en el caso de funcionarios, y se emite un certificado de Almacén General para el caso de los contratistas.

- La devolución de equipos de cómputo se realiza de acuerdo al procedimiento Salidas, Traslado y Reintegro de Bienes.

4.5.5. Clasificación de la información

- En atención a los requisitos de la norma NTC-ISO/IEC 27001:2013, 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 con el procedimiento etiquetar y manejar la información del IDRD.

4.5.6. Gestión de medios removibles (unidades de almacenamiento)

- El IDRD promueve el uso de carpetas compartidas en lugar de medios removibles (USB, discos externos, CD/DVD, entre otros) para el intercambio de información al interior de la entidad.

- Las unidades de medios removibles de las estaciones de trabajo, equipos portátiles y servidores se administran mediante directorio activo y quien requiera hacer uso de estas unidades debe solicitar al correo soporte@idrd.gov.co. la activación al Área de Sistemas, previa autorización del Jefe del área y/o dependencia, indicando el tiempo por el cual se requiere la activación. Las personas que requieran los medios removibles habilitados de forma permanente, deben tener una autorización firmada por el Jefe de dependencia y/o área, y el Responsable del Área de Sistemas.

- Los jefes de área y/o dependencia controlan el ingreso y salida de las instalaciones del IDRD los equipos de cómputo de la entidad y medios extraíbles de almacenamiento de información, mediante el formato de orden de salida.

- Los medios removibles en los que se almacene información catalogada como información pública clasificada e información pública reservada deben estar cifrados, de acuerdo con las directrices del procedimiento gestión de activos.

4.5.7. Disposición de los medios

- Los medios que contienen información confidencial pública clasificada o pública reservada se deben disponer en forma segura, mediante incineración, destrucción o el borrado de datos antes de ser reutilizados o dados de baja, por el Área de Sistemas.

- Los discos de backups que contienen información pública clasificada o información pública reservada se deben cifrar antes de ser entregados por el área de Sistemas a la empresa transportadora.

- La información almacenada en medios removibles debe ser transferida a medios nuevos antes de que se vuelvan ilegibles, de acuerdo con el tiempo de vida útil de los mismos.

4.5.8. Transferencia de medios físicos

- Para la transferencia de medios físicos se deben seguir las directrices del procedimiento etiquetar y manejar la información del IDRD, y sus documentos relacionados.

4.6. CONTROL DE ACCESO

4.6.1. Control de acceso

4.6.1.1. El Área de Sistemas controla el acceso mediante el enfoque basado en roles, 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.

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

4.6.3. 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.

4.6.4. 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 puede guardar o escribir las contraseñas en papeles físicos o documentos de texto como bloc de notas, word o las notas de windows. Sin embargo, las contraseñas podrán ser almacenadas en claveros de la aplicación KeePass.

- 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.

  - ✓ 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. 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 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.

4.6.5. 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.

  - 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, exfuncionario, 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.

- 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.

4.7. CONTROL CRIPTOGRÁFICO

- El Área de Sistemas debe determinar los algoritmos criptográficos y protocolos autorizados para su uso en la entidad y configurar los sistemas para permitir únicamente aquellos algoritmos autorizados, teniendo en cuenta la información de los grupos de interés con el fin de descartar algoritmos de cifrados débiles tales como DES, RC3, RC4 y protocolos débiles tales como SSLv2 y SSLv3. Se debe considerar en su lugar el uso de algoritmos tales como AES (cifrado simétrico), RSA (cifrado asimétrico) y los protocolos SSL/TLS 1.2 o 1.3 y tamaños de cifrado de 168 o 256 bits (cifrado simétrico) y 2048 bits (cifrado asimétrico) preferiblemente.

- Las llaves criptográficas deben ser cambiadas anualmente o cada vez que se sospeche que han perdido su confidencialidad.

- La administración de llaves criptográficas y certificados digitales está a cargo del Área de Sistemas. Sin embargo, la administración de tokens bancarios, tokens para acceso a sistemas de información de Entes de Control y firmas digitales, estarán a cargo de cada uno de los funcionarios o contratistas a quienes les fueron asignados para el desempeño de sus funciones y/u obligaciones.

- Los funcionarios o contratistas a quienes les fueron asignados tokens bancarios y tokens de acceso sistemas de información de Entes de Control, deben almacenarlos bajo llave cuando no los están utilizando o cuando se van a retirar de sus puestos de trabajo.

4.8. SEGURIDAD FÍSICA Y DEL ENTORNO

4.8.1. Áreas seguras

- El IDRD cuenta con los siguientes controles para prevenir el acceso no autorizado a las instalaciones de la entidad.

- ✓ Vigilancia privada para el ingreso y salida de las instalaciones. Al ingreso se valida si el visitante lleva equipo(s) de cómputo y se informa a la recepción para que se realice el registro correspondiente.
- ✓ Torniquetes con sistema de acceso biométrico en la entrada, para funcionarios y contratistas.
- ✓ Las personas de recepción son las encargadas de validar el ingreso de visitantes con el área correspondiente, registrar al visitante (si es su primera visita), imprimir la identificación del visitante y registrar equipo(s) de cómputo (en caso de que el visitante deba ingresar equipo(s) de cómputo).
- ✓ Cámaras de seguridad en los pasillos del IDRD, monitoreadas todo el tiempo desde un centro de monitoreo.
- ✓ El datacenter del IDRD cuenta con sistema de detección y extinción de incendios, aire acondicionado redundante, sistema de alimentación ininterrumpida (UPS) y corriente regulada.
- Las áreas del IDRD están delimitadas por una barrera física y el ingreso debe hacerse a través de una puerta de acceso controlada por cerraduras.

- Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

- El datacenter debe contar con mecanismos que permitan garantizar que se cumplen los requisitos ambientales (temperatura, humedad, voltaje, entre otros) especificados por los fabricantes de los servidores y equipos de comunicaciones que alberga.

- Todo acceso al datacenter del IDRD será registrado en una bitácora o por medio de control de acceso biométrico con el fin de dejar rastros de auditoría.

- El IDRD cuenta con un plan de emergencias con el fin de brindar protección contra amenazas externas.

- El IDRD cuenta con una zona de despacho y carga. Para acceder a dicha área el vehículo debe pasar por dos controles físicos de acceso y es acompañado por un vigilante y/o por el supervisor del contrato durante la carga o descarga.

4.8.2. Ubicación y protección de los equipos

- El datacenter está ubicado en el Área de Sistemas, de forma tal que personas no autorizadas no puedan ver la información durante su uso y el acceso físico es controlado por el responsable del Área de Sistemas o quien este delegue.

- Se debe hacer seguimiento a las condiciones (temperatura, humedad, voltaje, apertura y cierre de puertas) que pueden llegar a afectar los equipos almacenados en el Datacenter.

4.8.3. Servicios de suministro

- El IDRD cuenta con aire acondicionado de contingencia, un sistema de alimentación no interrumpida (UPS) que asegura el tiempo necesario para apagar adecuadamente los servidores donde se alojan los sistemas de información ante una falla en el suministro de energía y un enlace de red redundante con el mismo proveedor de servicios de internet (con un anillo de fibra óptica cada uno).

4.8.4. Seguridad del cableado

- El Datacenter de la entidad debe cumplir con la normatividad de cableado estructurado y está debidamente certificado.

4.8.5. Mantenimiento de equipos

- El Área de Sistemas establece, ejecuta (mantenimiento correctivo), subcontrata (mantenimiento preventivo) y hace seguimiento a los planes anuales de mantenimiento de la infraestructura tecnológica de la entidad.

4.8.6. Seguridad de equipos y activos fuera de las instalaciones

- La salida de equipos propiedad del IDRD es controlada mediante el formato de orden de salida, firmada por el Jefe del área y/o dependencia y el responsable del Área de Servicios Generales. Esta política aplica para todos los funcionarios y contratistas, excepto para el Director y los Subdirectores.

- Los medios removibles propiedad del IDRD que son retirados de las instalaciones de la entidad con Backup deben ser debidamente cifrados por el Área de Sistemas.

- Los funcionarios y contratistas que retiren equipos o medios removibles propiedad del IDRD fuera de las instalaciones de la entidad deben seguir las siguientes directrices:

  - ✓ Bajo ninguna circunstancia los equipos de cómputo pueden ser dejados desatendidos en lugares públicos o a la vista, en el caso que esté siendo transportado en un vehículo.
  - ✓ Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.
  - ✓ En caso de pérdida o robo de un equipo de la entidad, se debe poner la denuncia ante la autoridad competente e informar inmediatamente al Jefe del área y/o dependencia, al responsable del Almacén General y al responsable del Área de Sistemas para que se inicie el trámite interno correspondiente.

4.8.7. Disposición segura o reutilización de equipos

- Cuando una estación de trabajo, equipo portátil o medio removible vaya a ser reasignado o dado de baja, se debe realizar una copia de respaldo de la información de la entidad que allí se encuentre almacenada (en caso de ser necesario). Posteriormente, el equipo debe ser sometido a un proceso de eliminación segura de la información almacenada (destrucción física, eliminación o sobreescritura de los medios que contienen información) con el fin de evitar pérdida de la información y/o recuperación no autorizada de la misma.

4.8.8. Equipo desatendido, escritorio limpio y pantalla limpia

- Los funcionarios y contratistas del IDRD deben conservar su escritorio físico libre de información propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o personal que no tenga autorización para su uso o conocimiento, cada vez que se vayan a retirar de sus puestos de trabajo.

- Al imprimir documentos de carácter confidencial (información pública clasificada e información pública reservada), éstos deben ser retirados de la impresora inmediatamente.

- Los computadores muestran por defecto el fondo y protector de pantalla del IDRD; este no podrá ser modificado y debe permanecer activo.

- Los funcionarios y contratistas del IDRD deben bloquear la pantalla de su computador cuando por cualquier motivo se ausenten del puesto de trabajo.

- Se prohíbe el almacenamiento de información personal en los computadores y servidores del IDRD.

- El escritorio lógico debe estar libre de información pública clasificada e información pública reservada.

4.9. SEGURIDAD DE LAS OPERACIONES

4.9.1. Documentación de procedimientos operativos

- Se debe contar con procedimientos documentados para las actividades operativas asociadas con las instalaciones de procesamiento de información.

4.9.2. Control de cambios

- Los cambios en los procesos de negocio serán gestionados por el Comité Institucional de Gestión y Desempeño.

- Los cambios en la documentación de los procesos se deben realizar siguiendo las directrices del procedimiento para la elaboración y control de documentos.

- Los cambios en los sistemas de procesamiento de información se realizan de acuerdo con las directrices del procedimiento gestionar cambios de seguridad de la información.

- El procedimiento gestionar el desarrollo y/o actualización de software contiene los lineamientos para gestionar cambios relacionados con actualización o desarrollo de nuevos módulos del Sistema de Información Misional (SIM).

4.9.3. Gestión de capacidad

- El IDRD gestiona la capacidad de su plataforma tecnológica (hardware y software) de acuerdo con las indicaciones del procedimiento gestionar la capacidad de infraestructura tecnológica.

4.9.4. Separación de los ambientes

- El IDRD cuenta con ambientes de desarrollo y producción separados por máquinas físicas y máquinas virtuales.

- El IDRD controla el acceso al ambiente de desarrollo de la misma forma que controla el acceso al ambiente de producción, siguiendo las directrices de la política de control de acceso.

4.10. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

- Se deben proteger las estaciones de trabajo, equipos portátiles y servidores del IDRD contra códigos maliciosos.

- Los contratistas que hagan uso de sus equipos portátiles personales deben contar con un software antivirus licenciado.

- El servicio de antivirus no requiere de solicitud o autorización para su uso, todos los equipos conectados a la red deben tener el antivirus instalado y activo.

- El único servicio de antivirus autorizado para las estaciones de trabajo y los equipos portátiles de los funcionarios del IDRD es el asignado directamente por el Área de Sistemas, el cual cumple con todos los requisitos técnicos y de seguridad requeridos.

- El usuario no debe propiciar el intercambio de archivos que hayan sido identificados como infectados por virus o códigos maliciosos o sean sospechosos de estar infectados.

- El usuario no debe instalar o emplear programas no autorizados para manejo de antivirus.

- Los usuarios no deben desactivar o eliminar los archivos que forman parte del programa antivirus.

- El programa antivirus debe ser instalado única y exclusivamente por el Área de Sistemas, en los servidores, estaciones de trabajo y equipos de cómputo de los funcionarios y contratistas del IDRD.

4.11. COPIAS DE RESPALDO

- La entidad debe realizar copias de respaldo de la información y pruebas periódicas a las mismas. Para ello el Área de Sistemas cuenta con el procedimiento gestión de backup de la sede administrativa.

- El Área de Sistemas establece las políticas y estándares de copias de seguridad para los sistemas de información y bases de datos.

- Las copias de respaldo se guardan únicamente con el objetivo de restaurar información cuando por situaciones como borrado de datos, incidente de seguridad de la información, defectos en los discos de almacenamiento, problemas de los servidores o equipos de cómputo, o por requerimientos legales, sea necesario recuperarla.

- Las copias de respaldo o backup son verificadas periódicamente por el Área de Sistemas con el fin de certificar su funcionalidad validez y correcto proceso de restauración, de acuerdo con los lineamientos del procedimiento gestión de backup de la sede administrativa.

- Los funcionarios y contratistas son responsables de almacenar la información que requiera copias de respaldo, en las carpetas compartidas asignadas por el Área de Sistemas a cada una de las áreas del IDRD, dado que la información que se encuentre almacenada en ubicaciones diferentes no será respaldada.

4.12. REGISTRO Y SUPERVISIÓN

4.12.1. Registro de eventos

- Los sistemas operativos, servicios y sistemas de información que hacen parte de la infraestructura para el procesamiento de información y comunicaciones de la entidad, deben generar archivos de registro de eventos (logs) definidos en conjunto por los responsables de su administración.

4.12.2. Protección de la información de registro

- El Área de Sistemas con el fin de proteger la información de registro de modificación por parte de usuarios no autorizados, administradores u operadores de los sistemas

de información, implementa mecanismos de copiado de logs en "tiempo real" a un sistema por fuera del control de administradores y operadores de los sistemas.

4.12.3. Sincronización de relojes

- Con el fin de obtener un control apropiado para la relación adecuada de eventos no deseados en la infraestructura o para la investigación efectiva de incidentes, los relojes de los diferentes equipos de cómputo, servidores y sistemas de información utilizados por el IDRD, deben estar sincronizados.

4.13. CONTROL DE SOFTWARE OPERACIONAL

4.13.1. 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.

4.14. GESTIÓN DE LA VULNERABILIDAD TÉCNICA

4.14.1. Gestión de las vulnerabilidades técnicas

- El Área de Sistemas, es responsable de verificar de manera periódica (al menos bimestralmente) 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.

4.15. CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN

4.15.1. Controles sobre auditorías de sistemas de información

- Para la ejecución de auditorías a los sistemas de información se deben tener en cuenta las siguientes consideraciones:

  - ✓ Los requisitos de auditoría para acceso a sistemas y a datos se deben acordar con el Jefe de área y/o dependencia involucrada.
  - ✓ El alcance de las pruebas técnicas de auditoría se debe acordar y controlar.
  - ✓ Las pruebas de auditoría (incluidas las pruebas de análisis de vulnerabilidades y/o hacking ético) que puedan afectar la disponibilidad del sistema se deben realizar fuera de horas laborales.
  - ✓ Se debe hacer seguimiento de todos los accesos y logs para producir un rastro de referencia.

4.16. SEGURIDAD EN LAS COMUNICACIONES

4.16.1. Gestión de la seguridad en las redes

- 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.

- 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).

- 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.

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

4.16.2. Transferencia de información

- Los funcionarios y contratistas deben seguir las indicaciones del Área de Archivo y Correspondencia documental para la transferencia de información siguiendo los parámetros de la clasificación de la información de acuerdo con las tablas de retención documental del IDRD.

4.17. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

4.17.1. Requisitos de seguridad de los sistemas de información

- El Área de Sistemas debe definir los requisitos de seguridad de la información para sistemas de información nuevos o mejoras a los sistemas de información existentes, contratados externamente o desarrollados en la entidad. Para ello, deben tener en cuenta:

- ✓ El nivel de confianza requerido con relación a la identificación declarada de los usuarios, para obtener los requisitos de autenticación de usuario. Por ejemplo, la implementación de segundos factores de autenticación y un sistema de gestión de contraseñas que exija el uso de contraseñas fuertes, el cambio periódico de contraseñas y que guarde un historial de contraseñas para evitar de nuevo su uso.
- ✓ Los procesos de suministro de acceso y de autorización para usuarios, al igual que para usuarios privilegiados o técnicos. Por ejemplo, el suministro de datos de acceso por correo electrónico.
- ✓ Las necesidades de protección de activos involucrados, en particular acerca de disponibilidad, confidencialidad e integridad. Por ejemplo, cifrado de información almacenada, el envío de información por canales cifrados.
- ✓ Los requisitos obtenidos de los procesos del negocio, tales como los requisitos de ingreso, seguimiento, y no repudio, formularios de autenticación mediante HTTPS, cifrado de contraseñas almacenadas y uso de firmas digitales.
- ✓ Los requisitos de trazabilidad (registro de eventos) de las actividades de los usuarios.
- ✓ La necesidad de exigir la implementación de metodologías de desarrollo seguro.

- Las dependencias del IDRD que contraten el desarrollo de software o adquieran software de terceros, deben apoyarse en el Área de Sistemas para definir los requisitos de seguridad de la información de los mismos.

4.17.2. Seguridad en los procesos de desarrollo y soporte

4.17.2.1. Desarrollo seguro

- La entidad vela porque el desarrollo interno o externo de los sistemas de información cumpla con los requisitos de seguridad esperados, así como con pruebas de aceptación y seguridad al software desarrollado. Además, la entidad asegura que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la entidad.

4.17.2.2. Cambios en sistemas, plataforma tecnológica o paquetes de software

- Los cambios en sistemas deben llevarse a cabo de acuerdo con el procedimiento gestionar cambios de seguridad de la información.

4.17.2.3. Principios de desarrollo seguro

- El Área de Sistemas debe definir e implementar principios de desarrollo seguro en actividades de construcción de sistemas de información internos.

- Los principios de desarrollo establecidos se deben revisar con regularidad (al menos anualmente) para asegurar que están contribuyendo a mejorar los estándares de seguridad dentro del proceso de desarrollo y asegurar que permanezcan actualizados en términos de combatir nuevas amenazas potenciales y seguir siendo aplicables a los avances en las tecnologías y soluciones que se aplican.

4.17.2.4. Ambiente de desarrollo seguro

- El Área de Sistemas aplica los mismos controles aplicados al ambiente de producción en el ambiente de desarrollo, tales como, control de acceso, copias de respaldo, registro de eventos y separación de ambientes (desarrollo y producción).

- El Área de Sistemas debe implementar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo y producción han sido aprobadas, de acuerdo con el procedimiento de gestionar cambios de seguridad de la información.

- El Área de Sistemas debe contar con sistemas de control de versiones para administrar los cambios en los sistemas de información desarrollados al interior de la entidad.

4.17.2.5. Desarrollo contratado externamente

- Las áreas y/o dependencias deben asegurase que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento en el cual se especifiquen las condiciones de uso del software y los derechos de propiedad intelectual.

- Las áreas y/o dependencias deben exigir el suministro de evidencia que se realizaron pruebas de seguridad al software desarrollado por terceros.

- Los principios de desarrollo seguro se deben aplicar, en donde sea pertinente, a desarrollos contratados externamente.

- Las áreas y/o dependencias que contraten desarrollos externos deben asegurar que se realicen pruebas de aceptación del software, con el fin de verificar el cumplimiento de los requisitos de seguridad acordados.

- Las áreas y/o dependencias deben tener en cuenta e incluir en los acuerdos contractuales la necesidad de que el software cumpla con las leyes y regulaciones aplicables.

- Las áreas y/o dependencias deben incluir en acuerdos contractuales, en donde sea posible, el derecho de la entidad a realizar auditorías durante el desarrollo del contrato.

- Cuando se contrata un desarrollo externo se debe acordar el cumplimiento de los niveles de soporte requeridos por la entidad. Adicionalmente, se debe acordar la entrega de manual(es) técnico(s), que describa(n) la estructura interna del sistema, así como el diccionario de datos, librerías y archivos que lo conforman; y manual(es) funcional(es), que describa(n) las funcionalidades de cada una de las opciones del menú de la aplicación.

4.17.2.6. Pruebas de seguridad de sistemas

- Se debe exigir tanto para desarrollos internos como externos la ejecución de pruebas funcionales que incluyan la evaluación de los requisitos de seguridad de la información y la protección contra vulnerabilidades conocidas.

4.17.2.7. Pruebas de aceptación de sistemas

- Se deben realizar pruebas de aceptación del software, independientemente de que sea un desarrollo interno o un desarrollo contratado externamente, con el fin de validar los requisitos de seguridad de la información y la adherencia a prácticas de desarrollo de sistemas seguros (en donde sea aplicable). En estas pruebas se puede hacer uso de herramientas automatizadas, tales como herramientas de análisis de códigos o escáneres de vulnerabilidad, y se debe verificar que se han corregido los defectos relacionados con la seguridad.

- De ser posible, las pruebas de aceptación se deben llevar a cabo en un ambiente de pruebas realista, para asegurar que el sistema no introducirá vulnerabilidades al ambiente de la entidad, y que las pruebas son confiables.

- En donde la funcionalidad de la seguridad no satisface el requisito especificado, antes de comprar el software se debe reconsiderar el riesgo introducido y los controles asociados.

4.17.2.8. Datos de prueba

- El Área de Sistemas debe certificar que la información a ser entregada a los desarrolladores (tanto internos como externos) para sus pruebas es enmascarada o que los datos sensibles son eliminados con el fin de no revelar información confidencial de los ambientes de producción y, por ende, dar cumplimiento a la Ley 1581 de 2012 (Ley de Protección de Datos Personales) y la Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información pública).

4.18. RELACIÓN CON LOS PROVEEDORES

4.18.1. Seguridad digital y de la información en las relaciones con los proveedores

4.18.1.1. Seguridad digital y de la información para las relaciones con proveedores

- El IDRD establece mecanismos de control en sus relaciones con proveedores y/o contratistas, con el objetivo de asegurar la información a la que tengan acceso o servicios que sean provistos por los mismos, y que se cumpla con las políticas de la entidad.

4.18.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores

- Los supervisores de contratos se asegurarán de comunicar las políticas y procedimientos a los proveedores y/o contratistas.

- Se deben incluir en los acuerdos con proveedores y/o contratistas, como mínimo, los siguientes requisitos de seguridad de la información:

  - ✓ Cláusula de confidencialidad.
  - ✓ Cláusula de protección de datos personales.
  - ✓ Cláusula que defina las responsabilidades que continúan después de terminado el contrato (por ejemplo, confidencialidad durante 5 años después de terminado el contrato).
  - ✓ Cumplimiento de las políticas de seguridad de la información del IDRD.

- ✓ Acciones a tomar en caso de incumplimiento de las políticas de seguridad de la información.
- ✓ Reporte de eventos de seguridad de la información a través de los canales definidos en el procedimiento gestionar incidentes de seguridad de la información.
- ✓ Etiquetado y manejo de la información de acuerdo con las directrices del procedimiento etiquetar y manejar la información del IDRD.
- ✓ Cláusula de seguimiento y revisión de los servicios prestados por los proveedores y/o contratistas para asegurar que los términos y condiciones de seguridad de la información de los acuerdos se cumplan.
- ✓ Responsabilidades de los proveedores incluidos en la cadena de suministro, tales como, soporte técnico y garantía.

- En caso de que el contratista haga uso de un equipo de cómputo de su propiedad:
  - ✓ Cifrar el disco o la partición donde se almacena información del IDRD.
  - ✓ Eliminar la información del IDRD al terminar el contrato.
  - ✓ Aceptar con o sin previo aviso seguimiento al cumplimiento de las obligaciones anteriores.
- Los supervisores de contratos, deben administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad de la información establecidos con ellos, y monitoreando la aparición de nuevos riesgos.
- Los accesos a los sistemas de información y equipos de cómputo requeridos por los proveedores, deben ser solicitados de manera formal al Área de Sistemas a través del correo soporte.idrd.gov.co.

4.19. GESTIÓN DE INCIDENTES DE SEGURIDAD DIGITAL Y DE LA INFORMACIÓN

- El IDRD realiza el seguimiento a los incidentes de seguridad de la información de acuerdo con las directrices del procedimiento gestionar incidentes de seguridad de la información.

4.20. ASPECTOS DE SEGURIDAD DIGITAL Y DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

4.20.1. Continuidad de la seguridad de la información

- El IDRD planifica e implementa la continuidad del negocio (PCN) teniendo en cuenta no sólo los recursos tecnológicos, sino también los demás activos de información y los procesos críticos de la entidad, además de la continuidad de la seguridad de la información.

- El IDRD realiza pruebas periódicas (al menos anualmente) al plan de continuidad del negocio y de continuidad de la seguridad de la información implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

4.20.2. Redundancias

- El IDRD establece e implementa un Plan de Recuperación de Desastres (DRP) como parte del Plan de Continuidad de Negocio (PCN) con el fin de asegurar la redundancia y continuidad de las instalaciones de procesamiento de información.

- El IDRD realiza pruebas periódicas (al menos anualmente) al DRP, con el fin de asegurar que los controles tecnológicos implementados son válidos y eficaces durante situaciones adversas.

4.21. CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

4.21.1. Identificación de la legislación aplicable y de los requisitos contractuales

- La Oficina Asesora Jurídica y el Oficial de Seguridad deben identificar, documentar y mantener actualizados los requisitos legales y contractuales aplicables al IDRD que están relacionados con seguridad de la información. Para ello, se pueden apoyar en los Jefes de áreas y/o dependencias.

4.21.2. Derechos de propiedad intelectual

- El Área de Sistemas realiza revisiones periódicas (al menos semestralmente), con el fin de asegurar que todo el software que se ejecute en la entidad esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.

- Los funcionarios o contratistas no deben instalar software o sistemas de información en sus estaciones de trabajo o equipos portátiles suministrados para el desarrollo de sus funciones.

- Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de ley; no obstante, el Área de Sistemas puede distribuir un número de copias de software bajo una licencia otorgada.

- Los supervisores de contratos deben asegurarse de incluir cláusulas de propiedad intelectual y derechos de autor en contratos con terceros.

4.21.3. Protección de registros

- El IDRD se obliga a proteger todos los registros que muestren evidencia del cumplimiento de los requisitos normativos, legales o regulatorios contra la pérdida de confidencialidad, disponibilidad e integridad, siguiendo las directrices del procedimiento etiquetar y manejar la Información del IDRD.

- El IDRD protege el listado maestro de documentos a través del aplicativo ISOLUCION.

4.21.4. Privacidad y protección de información de datos personales

- El IDRD, es responsable del tratamiento de los Datos Personales, tal y como este término se define en la Ley 1581 de 2012, respeta la privacidad de cada uno de los terceros que le suministren sus datos personales a través de los diferentes puntos de recolección y captura de dicha información. Por lo tanto, la entidad implementa los controles necesarios para su protección y en ningún momento divulga esta información a terceras partes a menos que cuente con la autorización formal de los mismos o en los casos en que la ley lo permita.

4.21.5. Reglamentación de controles criptográficos

- El IDRD, se rige por la Ley 527 de 1999 (acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y otras disposiciones) y sus decretos reglamentarios, según se requiera.

4.22. REVISIONES DE SEGURIDAD DIGITAL Y DE LA INFORMACIÓN

4.22.1. Revisión independiente de la seguridad digital y de la información

- La Oficina de Control Interno realiza auditorías internas de revisión al menos una vez al año, siguiendo las directrices del procedimiento de auditorías internas de control interno. Esta revisión independiente es necesaria para asegurar la conveniencia, la adecuación y la eficacia continuas del enfoque de la entidad para gestionar la seguridad digital y de la información.

4.22.2. Cumplimiento con las políticas y normas de seguridad

- Los Jefes de área y/o dependencia deben revisar con regularidad (al menos una vez por año) el cumplimiento de las políticas y procedimientos de seguridad de la información dentro de su área de responsabilidad.

4.22.3. Revisión del cumplimiento técnico

- El Área de Sistemas debe coordinar la revisión periódica (al menos semestralmente) de los sistemas de información utilizados en el IDRD, para determinar el cumplimiento con las políticas y procedimientos de seguridad de la información. Para ello, se debe determinar a qué sistemas de información se hará revisión cada vez.

4.22.4. Medidas a adoptar en caso de incumplimiento

- El incumplimiento de una o más políticas descritas en este documento, está sujeto a las sanciones disciplinarias, fiscales y penales que se deriven de la conducta del implicado, incluso cuando se encuentre en situaciones administrativas como permisos, licencias, vacaciones, suspensiones en ejercicio del empleo o en comisión, de acuerdo con la Ley 734 de 2002, la Ley 906 de 2004 y la Ley 1273 de 2009.

5. NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD DIGITAL Y DE LA INFORMACIÓN

Toda violación de estas políticas se debe notificar al Área de Sistemas a través de alguno de los canales disponibles y al correo electrónico soporte@idrd.gov.co.

Asimismo, se deben notificar situaciones tales como: personas ajenas al IDRD sin identificación y sin acompañamiento en las oficinas, correos maliciosos o sospechosos, reinicio de los equipos de cómputo o enrutadores, uso de software ilegal, divulgación, alteración y robo de información.

VALIDÓ	REVISÓ	APROBÓ
JAVIER RIOS MOLINA **Profesional Especializado Área de Sistemas**	LILIANA DÍAZ POVEDA **Subdirectora Administrativa y Financiera** MARTHA RODRIGUEZ MARTÍNEZ **Jefe Oficina Asesora de Planeación**	PEDRO ORLANDO MOLANO PÉREZ **Director General** Fecha de Aprobación: 31 DIC 2019