Deporte

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

2025

GIT Tecnología de la Información y las Comunicaciones -TIC´S

Contenido

1. OBJETIVO

Establecer las directrices a los funcionarios, contratistas y terceros que cumplan funciones en el Ministerio del Deporte para el estricto cumplimiento de las políticas de seguridad de la información, que aplican en la gestión de sus labores al interior de la entidad, asimismo se determina las responsabilidades de los mismos y se formaliza el compromiso de la alta dirección frente a la seguridad de la información.

2. ALCANCE

Las políticas de seguridad de la información abarcan la plataforma informática que soporta las operaciones, las instalaciones físicas dónde se procesa la información y todos los activos de información identificados para cada uno de los procesos definidos en el Mapa de Procesos del Ministerio del Deporte. Constituyen la posición oficial de la Entidad en relación con la seguridad de la infraestructura física y virtual y las medidas adecuadas de protección en relación con sus funciones legales.

Las políticas de seguridad de la información son de carácter obligatorio y deben ser conocidas y aplicadas por todos los funcionarios, contratistas y terceros que ejecuten funciones y cumplan responsabilidades en la Entidad. El desconocimiento de las políticas no exonera de cumplirlas, de las responsabilidades asignadas, ni de las consecuencias disciplinarias y/o jurídicas que se generen de su incumplimiento.

Con el fin de garantizar el buen funcionamiento de la Entidad se dispondrá de las herramientas tecnológicas que el Ministerio del Deporte considere son las adecuadas para la ejecución de las actividades de funcionarios, contratistas y terceros; el uso adecuado de las mismas es de carácter obligatorio y la utilización de otras herramientas diferentes a las dispuestas por la entidad no está permitido y podrá generar consecuencias disciplinarias y/o legales de acuerdo a su incumplimiento.

Para dar cumplimiento a la Política de Administración del Riesgo de la entidad, se identificarán los riesgos relacionados con seguridad de la información, los cuales serán administrados y gestionados por cada uno de los procesos como primera línea de defensa, estos procesos serán los responsables de mantener controles efectivos y acciones de tratamiento sobre los riesgos de manera permanente. Como segunda línea de defensa operará el GIT TICS acompañando procedimental y técnicamente la implementación de los controles requeridos y finalmente la tercera línea de defensa estará a cargo de la Oficina de Control Interno, la cual proporcionará una evaluación y un aseguramiento objetivo e independiente sobre la gestión de estos riesgos.

Las políticas de seguridad de la información están articuladas con el Plan Estratégico de Tecnología de la Información (PETI).

3. DEFINICION DE TERMINOS Y CONSIDERACIONES GENERALES

3.1 Definición de Términos

■ **Seguridad de la información**

Se entiende como la preservación, aseguramiento y cumplimiento de las siguientes características de la información:

■ **Confidencialidad:**
Los activos de información solo pueden ser accedidos y custodiados por aquellos que tengan el permiso adecuado.

■ **Integridad:**
El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su trazabilidad.

■ **Disponibilidad:**
Los activos de información sólo pueden ser obtenidos a corto plazo por aquellos que tengan los permisos adecuados.

■ **Ciberseguridad**

Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio.

■ **Dispositivos móviles:**

Son aquellos dispositivos de tamaño pequeño, con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, con memoria limitada y que ha sido diseñado específicamente para una función, pero que puede llevar a cabo otras funciones más generales (como portátiles, teléfonos inteligentes, tabletas, relojes inteligentes, agendas digitales, videoconsolas portátiles, reproductores digitales, cámaras fotográficas digitales, cámaras de video digitales, entre otros) que nos facilitan trabajar fuera de las instalaciones del Ministerio del Deporte.

■ **Información:**

Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

■ **Grupo de Soporte o servicio:**

Centro de atención al usuario mediante el cual el GIT - TIC´s presta servicios para gestionar y atender de requerimientos relacionados con los servicios TIC en Mindeporte.

■ **OneDrive:**

Plataforma en la nube de Microsoft 365 que permite guardar los archivos o documentos (Ejemplo: información pública de las áreas de Mindeporte) en línea y acceder a ellos desde cualquier lugar o equipo con conexión a Internet.

■ **Riesgo:**

Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

■ **Software base:**

Cada equipo de cómputo está configurado con el Hardware y Software básico necesario para su funcionamiento: Sistema operativo: Windows, IOS o Linux, Ofimática: Office 365 (Access, Excel, OneNote, OneDrive, Outlook, PowerPoint, Publisher, Word.), Software para descomprimir Archivos: 7-Zip, Antivirus, Chat y conferencias: Microsoft Teams.

■ **Dirección MAC (Media Access Control - Control de Acceso al Medio):**
Una dirección MAC, también conocida como dirección física, es un valor de 48 bits único e irrepetible que identifica todo dispositivo conectado a una red. Cada dispositivo tiene su propia dirección MAC determinada que es única a nivel mundial ya que es escrita directamente, en forma binaria, en el hardware del interfaz de red en el momento de su fabricación. Sinónimo: dirección física, dirección hardware.

■ **Teletrabajo:** Es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios, utilizando como soporte las tecnologías de la información y las comunicaciones - TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo.

■ **Trabajo remoto en casa:**

Es la directriz del Gobierno Nacional dentro del marco de la emergencia sanitaria, con el fin de que las personas desarrollen sus actividades laborales desde su casa y se mitigue la propagación del Covid-19.

3.2 Consideraciones generales de las políticas de seguridad de la información

En años recientes el tema de la seguridad de la información ha cobrado mayor relevancia, dadas las cambiantes condiciones y nuevas plataformas de cómputo disponibles. La posibilidad de interconectarse a través de redes ha abierto nuevos horizontes, situación que ha llevado a la aparición de nuevas amenazas en los sistemas computarizados. La información es considerada actualmente como el activo más importante de las

organizaciones y es por ello que se debe tener muy presente cómo protegerla ante cualquier tipo de ataque o amenaza, bien sea físico o lógico, y contar con políticas bien definidas que permitan brindar protección adecuada a los activos de información.

Con el ánimo de establecer el Sistema de Gestión de Seguridad de la Información del Ministerio del Deporte, este documento define los lineamientos para gestionar la seguridad de la información buscando minimizar la probabilidad e impacto de la materialización de los riesgos a los cuales está expuesta la entidad.

En Colombia, la Comisión Intersectorial de Políticas y Gestión de la Información para la Administración Pública recomienda la implementación de políticas de seguridad de la información a través de los estándares internacionales, apoyándose principalmente en las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022

El Ministerio del Deporte establece que estas políticas de seguridad de la información deben ser revisadas al menos una vez al año con el fin de actualizarlas, si así se requiere, para evitar su obsolescencia y pérdida de vigencia, así como para adaptarse a los cambios tecnológicos y nuevas modalidades de amenazas.

4. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La Política General de Seguridad de la Información del Ministerio del Deporte aplica para los funcionarios, contratistas y terceros que laboran en las instalaciones de la entidad y/o manejan información responsabilidad de la entidad desde otros lugares. Su cumplimiento es responsabilidad directa de cada uno de ellos y su divulgación se realiza por medio de la intranet, en el sistema de información documental y el portal web de la entidad.

En el contexto de este documento los usuarios, de acuerdo con su rol asignado por un coordinador o supervisor, son personas que agregan, modifican, eliminan o consultan información almacenada en los sistemas de información de la entidad.

El propietario de un determinado sistema de información será el área que tenga la incidencia directa o administración de este, y deberá actuar de acuerdo con los diferentes procedimientos que se definan respecto a la gestión de la seguridad de la información. Desde el GIT TIC´s se presta el apoyo técnico y administración de los servidores donde se encuentre alojado el sistema, y el soporte puntual se realiza con los desarrolladores del mismo. Para adquirir un perfil es necesario solicitar al administrador del sistema a través del Grupo de Soporte la asignación de usuario y contraseña.

4.1 Asignación de responsabilidades para la seguridad de la información

Las responsabilidades de la seguridad de la información competen al personal del Ministerio del Deporte entre funcionarios, contratistas y proveedores que manejan, administran y procesan información por medios físicos o tecnológicos en la entidad para el cumplimiento

de sus responsabilidades funcionales en el marco del proceso al que pertenece dentro del mapa de procesos de la entidad.

La responsabilidad frente a la gestión, administración y custodia de los medios de Tecnología de la Información y las Comunicaciones del Ministerio del Deporte, está a cargo de GIT TIC´s y las responsabilidades en relación al liderazgo, gestión y administración de seguridad de la información, serán asignadas a un profesional del GIT TIC's por el Coordinador del área, quien de acuerdo a las necesidades y casos presentados escala los temas de acuerdo a las competencias profesionales presentes en el grupo.

4.2 Segregación de tareas

Al presentarse un determinado requerimiento se realiza el respectivo análisis y escalamiento de actividades; de acuerdo a las directrices que determine el coordinador del área estas tareas serán asumidas por un profesional idóneo presente en el GIT TIC´s.

4.3 Contacto con las autoridades

El rol de punto de contacto con las autoridades competentes en materia de seguridad de la información recae en el Coordinador del GIT TIC´s

4.4 Contacto Con Grupos De Interés Especial

Al presentarse un determinado requerimiento se realiza el respectivo análisis y escalamiento de actividades; de acuerdo a las directrices que determine el coordinador del área este contacto hacia los grupos de interés será asumido por un profesional idóneo presente en el GIT TIC´s.

4.5 Seguridad de la información en la gestión de proyectos

La seguridad de la información en la gestión de proyectos será asignada a un profesional idóneo del GIT TIC´s; dicha designación la realiza el Coordinador del área, quien de acuerdo a las necesidades y casos presentados escala los temas de acuerdo a las competencias profesionales presentes en el grupo.

5. POLITICAS ESPECIFICAS DE SEGURIDAD DE LA INFORMACIÓN

5.1. POLITICA PARA EQUIPOS DE CÓMPUTO

5. 1. 1 Instalación de equipos de cómputo

- Todo equipo de cómputo (computadores, equipos portátiles, dispositivos móviles y otros periféricos), que esté o sea conectado a la Red de datos del Ministerio del Deporte, ya sea físicamente o por red inalámbrica, o aquel que en forma autónoma se tenga y que sea propiedad de la entidad deberá sujetarse a las normas y procedimientos de instalación que establezca el GIT TIC´s.

- El GIT TIC´s, en articulación con Almacén, deberá mantener el registro detallado de inventario y características técnicas de todos los equipos de cómputo propiedad del Ministerio del Deporte.

- Los equipos de cómputo de uso en el Ministerio que sean de propósito específico y tengan una misión crítica asignada, deberán ubicarse dentro de un área que cumpla con los requerimientos que el GIT TIC´s tenga establecidos en sus lineamientos como son: seguridad física, condiciones ambientales y alimentación eléctrica controladas, protección con control de acceso, entre otros.

- Los responsables de las distintas áreas de Mindeporte conjuntamente con el GIT TIC´s deberán dar cabal cumplimiento a las normas de instalación, y notificaciones correspondientes de actualización, reubicación, reasignación, y todo aquello que implique movimientos en la ubicación o adjudicación de equipos de cómputo.

- La responsabilidad de la protección física de los equipos fijos recae en principio, en quien sean asignados por inventario; igualmente, corresponde al asignatario notificar al GIT TIC´s cualquier movimiento físico de los equipos asignados que sea requerido.

- La salida de equipos móviles (portátiles, tablets, celulares corporativos) por fuera de las instalaciones de Mindeporte, debe estar respaldada con un seguro especial que ampare las posibles eventualidades sucedidas durante dichos movimientos, y antes de su salida, se debe notificar al GIT TIC´s y a Almacén para acompañar el respectivo procedimiento.

5.1.2 Asignación de equipos de cómputo

- Todo usuario del Ministerio del Deporte al que se le asigne un equipo de cómputo (computadores, equipos portátiles, dispositivos móviles y otros periféricos) propiedad de Mindeporte, será responsable de su buen uso y seguridad física.

- El asignatario deberá verificar que el equipo de cómputo entregado cuente con todas las herramientas de software necesarias para realizar sus labores, como sistema(s) de información, antivirus, procesador de texto, entre otros. En caso de detectar la falta de algún software que requiera para su trabajo, deberá notificarlo al Grupo de Soporte por los medios de contacto disponibles para que el GIT TIC's realice la respectiva instalación.

5.1.3 Responsabilidades y cuidados de los equipos de cómputo

- Los usuarios no deben abrir los computadores, impresoras, reguladores de voltaje u otros equipos asignados, con el fin de inspeccionarlos, verificar su funcionamiento o mucho menos retirar o instalar componentes internos.

- Los equipos de cómputo que así lo permitan deberán estar protegidos con un dispositivo de seguridad (precinto o guaya), que se coloca en el computador para evitar que personas no autorizadas abran el equipo o lo desplacen de la zona asignada para las labores. Una vez colocado, el dispositivo no podrá ser retirado sin su respectivo registro en el formato de control del GIT TIC´s.

- Se prohíbe el consumo de alimentos y bebidas en zonas cercanas al equipo de cómputo.

- Las CPU no deben ser utilizadas como soporte de ningún elemento que atente contra su normal funcionamiento y ventilación (como carpetas, legajadores, resmas o cualquier otro objeto). Tampoco les deben ser colocados o adheridos elementos como plantas, ornamentos, fotografías, bebidas, alimentos, libros o manuales, ni bloquear de cualquier forma las rejillas de ventilación.

- Cada usuario es responsable de apagar el equipo y el monitor que están a su cargo al finalizar su jornada de trabajo.

- El usuario es el encargado de asegurarse de que sus archivos cuenten con las protecciones necesarias de escritura, lectura y ejecución para los casos en que estos estén compartidos con otros usuarios.

- Es responsabilidad del usuario realizar el respaldo (Backup) de su información incluido correo electrónico; los contratistas deben entregar al supervisor en medio magnético la documentación producto de la labor contratada al finalizar el contrato.

- El GIT TIC´s deberá habilitar el bloqueo de pantalla automático de los equipos luego de un período de inactividad de 7 minutos.

- En caso de notar un mal funcionamiento en el sistema, presencia de virus, código malicioso, SPAM o algún otro problema con su equipo asignado, el usuario deberá notificar a Soporte TIC´s de acuerdo con lo definido en el procedimiento de Reporte de Incidentes.

- Es responsabilidad del usuario realizar chequeos con software antivirus de los archivos ubicados en medios extraíbles (disquetes, memorias externas USB, CD, DVD, discos duros externos). Los usuarios deberán explorar los discos antes de copiar o abrir archivos o antes de utilizarlos para iniciar el sistema.

- Todos los equipos de cómputo deben contar con software antivirus instalado y actualizado.

- Los usuarios deberán reportar al GIT TIC´s, sobre daños o pérdida del equipo que tengan a su cuidado y sea propiedad de Mindeporte.

5.1.4 Cambios al hardware y software

- Los equipos de cómputo no deben ser alterados ni mejorados (cambios de procesador, adición de memoria o tarjetas) sin el consentimiento, evaluación técnica y autorización del GIT TIC´s.

- La actualización o cambios de hardware en los equipos de cómputo serán llevados a cabo únicamente por personal del GIT TIC´s o por proveedores a quien éste autorice. Cualquier tarea de cambio o actualización realizada en los equipos deberá relacionarse en el formato de Mantenimiento Preventivo/Correctivo dispuesto en el sistema Isolución.

- Todos los equipos de cómputo de Mindeporte se encuentran relacionados en un inventario donde se reflejan sus características, configuración y ubicación. Cualquier alteración de estos aspectos queda estrictamente prohibida. El GIT TIC´s es la única dependencia encargada de controlar y ejecutar cualquier cambio.

- Queda estrictamente prohibido instalar, remover o deshabilitar software en computadores o servidores de la entidad sin las debidas autorizaciones. El único autorizado para realizar tareas de instalación o desinstalación de programas, así como cambios en la configuración del sistema operativo, es el personal del GIT TIC´s.

- Los equipos de cómputo no deben tener instalado ningún otro software que no sea el licenciado y requerido para que el usuario desarrolle sus actividades de trabajo.

Nota: La intervención directa del usuario para reparar cualquier equipo está expresamente prohibida; El GIT TIC´s gestionará la correspondiente intervención por personal interno o externo para dar solución a los casos de soporte que le sean reportados.

5.1.5 Mantenimiento de los equipos de cómputo

- Al GIT TIC´s, corresponde la realización del mantenimiento preventivo y correctivo de los equipos de cómputo de propiedad del Ministerio del Deporte.
- En el caso de los equipos de cómputo atendidos por terceros el GIT TIC´s deberá supervisar y documentar el proceso de mantenimiento.
- Queda estrictamente prohibido por parte del GIT TIC's dar soporte y mantenimiento a equipos de cómputo que no sean propiedad de Mindeporte.

5.1.6 Actualización de software de los equipos de cómputo

- Al GIT TIC´s, corresponde realizar la actualización a los equipos de cómputo de propiedad del Ministerio del Deporte, correspondiente al software base (sistema operativo), software antivirus, software ofimático entre otras aplicaciones autorizadas requeridas por el usuario para el cumplimiento de sus responsabilidades funcionales.

- Para el caso de los equipos de cómputo de propiedad de contratistas o de terceros (proveedores) conectados a la red interna de la entidad, deberán tener actualizado el software base (sistema operativo) y antivirus. GIT TIC´s deberá verificar el estado de la actualización de dichos equipos antes de conectarlos a la red interna para preservar la seguridad de la información.

- El soporte por parte de GIT TIC'S para equipos de cómputo de propiedad de terceros, se limitará a la configuración de aplicaciones propias de la entidad para que el usuario pueda cumplir sus responsabilidades contractuales, siempre y cuando el sistema operativo sea compatible con la aplicación y cumpla con los requisitos exigidos en el punto anterior.

5.1.7 Reubicación de los equipos de cómputo

- Las reubicaciones físicas de equipos de cómputo las realizará únicamente el GIT TIC´s. con previa autorización del responsable del área y notificando del movimiento a Almacén.

- El equipo de cómputo a reubicar sea de Mindeporte o bien externo, debe contar con la autorización del responsable del área y del GIT TIC´s, informando el lugar a donde se hará la reubicación con los medios necesarios para la instalación del equipo.

- Si el área donde se va a reubicar el equipo de cómputo no cuenta con las condiciones mínimas para su funcionamiento y seguridad (punto de red, corriente regulada, seguridad física) se deberá informar al GIT TIC´s mínimo 15 días antes de la reubicación para verificar las condiciones y posibles adecuaciones a que haya lugar.

5.1.8 Eliminación segura de la información de equipos y medios

Los documentos físicos o digitales con información confidencial que requieran ser destruidos o eliminados, deberán someterse a un borrado seguro de su información antes de su entrega o dada de baja; dicha eliminación será responsabilidad del área que custodia dicha información.

5.1.9 Equipo de usuario desatendido

- Todo equipo de cómputo desatendido por un periodo mayor a 7 minutos deberá ser bloqueado automáticamente por política de Directorio Activo para evitar robo de información o cambios sobre la información almacenada.
- Todo usuario que deba dejar su equipo desatendido deberá realizar el bloqueo manual del equipo.

5.1.10 Equipos de terceros conectados a la red LAN

Todo equipo de cómputo de contratistas o proveedores que ingrese a la entidad debe contar con software licenciado o en su defecto con licenciamiento Open Source. Mindeporte no se hace responsable del licenciamiento o información allí almacenada.

Para aquellos equipos que requieran estar en las instalaciones de la entidad permanentemente, se debe exigir al tercero contar con software licenciado o licenciamiento Open Source, en caso de requerir acceso a Internet deben contar con software Antivirus instalado. Se debe realizar una verificación técnica previa de estos equipos por el área de soporte TIC's de Mindeporte a fin de proteger la red interna de la entidad contra cualquier software malicioso que pudiesen contener.

No se permite la conexión a las redes internas de la entidad (alámbrica o Wi-Fi Mindeporte) de equipos de terceros para realizar labores temporales en la entidad.

5.2 POLITICA DE CONTROL DE ACCESO

5.2.1 Usuario y contraseña del dominio Mindeporte

- El GIT TIC´s le asignará a cada usuario de la plataforma tecnológica de Mindeporte un nombre de usuario para el acceso al equipo de cómputo y a la Red, el cual estará conformado por las dos primeras letras del nombre seguidas por el primer apellido. En caso de ya existir se le buscará una combinación factible.

- El GIT TIC's asignará a los usuarios contraseñas provisionales para que puedan acceder por primera vez a los sistemas o equipos que les sean asignados al momento de vincularse a la entidad.

- El usuario deberá cambiar la contraseña provisional suministrada por una nueva contraseña, luego de ingresar por primera vez a los sistemas o a un equipo de cómputo asignado por la entidad. La nueva contraseña que debe crear el usuario, debe ser acorde a las buenas prácticas de seguridad. Dicha contraseña es confidencial y no debe ser transferirla por ningún motivo a otra persona.

- Como buena práctica de creación de contraseña, no deben ser nombres propios y debe ser una mezcla de números, letras y caracteres especiales para fortalecer su confidencialidad.

- La cuenta del dominio Mindeporte (usuario y contraseña) son responsabilidad exclusiva de cada uno de los usuarios y no deben ser divulgados a ninguna persona, a menos que exista un requerimiento legal. De acuerdo con lo anterior, los usuarios no deben obtener palabras claves u otros mecanismos de acceso de otros usuarios que pueda permitirles un acceso indebido, ni guardar la contraseña en scripts, macros, teclas de función de terminal, archivos de texto, en computadores o en otras ubicaciones en donde personas no autorizadas puedan verlas y usarlas.

- El GIT TIC's debe suministrar y garantizar el cambio de contraseña a los usuarios para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, según su perfil y rol, las credenciales de acceso son de uso personal e intransferible.
- La conexión remota a la red de área local del Mindeporte debe establecerse a través de una conexión VPN, la cual debe ser aprobada, registrada y monitoreada por el GIT TIC's.
- El GIT TIC's debe asegurar que las redes inalámbricas de la Entidad cuenten con métodos de autenticación que evite accesos no autorizados.
- El GIT TIC's debe realizar el cambio de contraseñas de las redes inalámbricas de la Entidad mínimo tres (3) veces al año.

5.2.2 Control de la información

- Los recursos disponibles a través de la Red de Mindeporte serán de uso exclusivo para asuntos relacionados con las actividades laborales del Ministerio.

- Los usuarios deben informar inmediatamente a Soporte TIC´s toda vulnerabilidad encontrada en los sistemas de Red, aparición de virus o programas sospechosos e intentos de intromisión y no deben distribuir este tipo de información interna o externamente.

- Los usuarios no deben intentar sobrepasar los controles de los sistemas, examinar los computadores y redes de la entidad en busca de archivos de otros sin su autorización o introducir intencionalmente software diseñado para acceder, causar daño o impedir el normal funcionamiento de los sistemas.

- Los usuarios no deben suministrar información de Mindeporte calificada como pública clasificada o pública reservada a ningún ente externo sin antes obtener las autorizaciones respectivas.

- Los usuarios que administren información sobre datos personales (semiprivado, privados y sensibles) deber mantener total reserva sobre la información y no pueden cederla ni entregarla a ningún tercero por ningún motivo a no ser que medie un requerimiento legal. Así mismo, el usuario deberá usar medidas de seguridad interna para proteger dicha información, dado que es su responsabilidad el cuidado y protección de la información que maneja y administra.

- Para casos de transferencia de información, calificada como pública clasificada, pública reservada y de datos personales solicitado por otras entidades públicas y privadas, deberá ser escalada al líder funcional o coordinador del área y éste, deberá a su vez, solicitar a GIT TIC'S las medidas técnicas requeridas para proteger la información a compartir o transferir a otra entidad y realizar todas las medidas administrativas necesarias para aclarar las responsabilidades que tiene la entidad solicitante, sobre la información suministrada, dado que la entrega de información como el caso de los datos personales a otras entidades no exime al Ministerio del Deporte de la responsabilidad sobre su tratamiento.

- Para el caso de interoperabilidad entre entidades del Estado, el Ministerio del Deporte debe adoptar el Marco de Interoperabilidad de Seguridad Digital definido por el Ministerio de Tecnología de la Información y las Comunicaciones - Mintic y establecer los lineamientos administrativos, las responsabilidades internas funcionales (procesos de Mindeporte involucrados) y las responsabilidades tecnológicas (GIT TIC's).

- Los usuarios no deben consultar, modificar, destruir, copiar o distribuir los archivos de la entidad sin los permisos respectivos.

- Todo usuario que utilice los recursos de los sistemas y de Red, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad, confiabilidad y auditabilidad de la información que maneje, especialmente si dicha información ha sido clasificada como crítica.

- Los computadores, sistemas y otros equipos conectados a la red deben usarse solamente para actividades laborales propias de Mindeporte, por lo tanto, los usuarios no deben usar sus equipos para asuntos personales a menos que exista una autorización previa que evalúe el riesgo informático de tal actividad.

- Las carpetas compartidas en la Red de Mindeporte a las cuales todos los usuarios tengan permiso de lectura o escritura no deben contener información sensible del Ministerio; en caso de ser así la carpeta compartida debe estar configurada para que accedan a ella solo los usuarios autorizados.

5.2.3 Control de acceso local a la red cableada e inalámbrica

- El acceso a la red cableada de la entidad sólo será proporcionado por GIT TIC´s a los usuarios a través de la conectividad de los equipos de cómputo de propiedad de la entidad asignados a los funcionarios.

- Los funcionarios y/o servidores públicos de la entidad no deben conectar sus equipos de cómputo personales llevados a la entidad en la red cableada, aunque sí podrán tener acceso a la red inalámbrica. Así mismo, deberán permitir que Soporte TIC´s, identifique la dirección MAC (Media Access Control) del equipo de cómputo como mecanismo de control de seguridad de la información y digital en la entidad.

- Los usuarios en calidad de contratistas y/o proveedores, no podrán conectar sus equipos de cómputos personales a la red cableada de la entidad. Sólo podrán tener acceso a través alguna de las categorías de red inalámbrica (Wifi) de la entidad, la cual será asignada por Soporte TIC´s de acuerdo con las responsabilidades contractuales. La anterior asignación, se realizará con previa solicitud y autorización del responsable de la supervisión del contratista o del proveedor con la fecha de inicio definida en el acta de inicio del contrato a través del Grupo de Soporte del GIT TIC´s. En este orden, para que el contratista o proveedor pueda conectarse a la red inalámbrica de la entidad (Wifi), deberá permitir que el Grupo de Soporte TIC´s, identifique la dirección MAC (Media Access Control) del equipo de cómputo por controles de seguridad de la información y digital en la entidad.

- Dado el carácter unipersonal del acceso a la Red de Mindeporte, el GIT TIC´s verificará el uso responsable, acorde a las políticas de seguridad de la información.

- El acceso lógico a equipos especializados de cómputo (servidores, enrutadores, bases de datos, Access Point, Switches, etc.) conectados a la red es únicamente permitido y administrado por el GIT TIC´s.

- Todo equipo de cómputo que esté o sea conectado a la Red, tanto cableada como inalámbrica de Mindeporte, o aquellas que en forma autónoma se tengan y que sean propiedad del Ministerio, deberá sujetarse a los procedimientos de acceso que emite el GIT TIC´s.

- Los equipos de visitantes solo podrán conectarse a la Red de Visitantes de Mindeporte utilizando la conexión Wi-Fi, puesto que ésta se encuentra en una VLAN o red lógica independiente con el fin de garantizar la seguridad de la red interna y una vez cumplidos todos los requisitos mencionados en la política de seguridad de la información.

- Las redes públicas provistas por la entidad deben estar separadas de sus redes privadas y deben tener una definición de políticas de seguridad y controles específicos que impidan su acceso a las demás redes internas.

5.2.4 política de control de acceso remoto/teletrabajo

- El GIT TIC´s es el responsable de proporcionar el servicio de acceso remoto y establecer las políticas de acceso a los recursos informáticos disponibles.
- Para el caso especial de acceso a los recursos de los servidores de Mindeporte por terceros, dicho acceso deberá ser autorizado y monitoreado por el GIT TIC´s.
- El usuario de estos servicios deberá sujetarse al Reglamento de uso de la Red de Mindeporte y en concordancia con los lineamientos generales de uso de Internet.
- El acceso remoto que realicen funcionarios, contratistas de prestación de servicios o proveedores de servicios deberá contar con la supervisión del área de Soporte Técnico del GIT TIC´s. Una vez finalice la labor se debe cerrar el aplicativo utilizado para evitar accesos no autorizados.

5.3 POLITICA PARA COMPUTACIÓN MÓVIL Y COMUNICACIONES

- Para los dispositivos móviles de propiedad de la entidad a cargo y/o custodia de un funcionario de Mindeporte, se deberá solicitar su conexión a la red interna de la entidad a través del Grupo de Soporte del GIT TIC´S para que ésta previamente identifique y relacione la dirección MAC del dispositivo y poder tener el debido control de ciberseguridad.

- No está permitida la conexión de dispositivos móviles que no sean propiedad de la entidad a la red interna de Mindeporte (WI-FI Mindeporte) salvo excepciones autorizadas por los lideres y/o jefes funcionales del área con la debida solicitud a GIT TIC's justificando los fines laborales, proporcionando la dirección MAC del dispositivo y especificando la fecha solicitada de conexión a la red interna de la entidad. Los dispositivos móviles que se conecten a la red sin la debida autorización podrán ser automáticamente desconectados.

- Sólo se podrán conectar dispositivos móviles que no sean propiedad de la entidad a la red WI-FI Mindeporte-Invitados o Wi-Fi Gratis para la Gente que requieran hacer uso de Internet temporalmente no mayor a dos horas, evitando la congestión del canal de Internet de la entidad. El usuario deberá aceptar las políticas de conexión establecidas por la entidad para poder conectarse a la red.

5. 4 POLITICA PARA TELETRABAJO Y TRABAJO REMOTO EN CASA

A continuación, se definen las directrices que se establecen para el uso de dispositivos móviles, trabajo remoto en casa y teletrabajo para los servidores públicos y contratistas del Ministerio del Deporte, con el fin de preservar la disponibilidad, integridad y confidencialidad de la información de la entidad.

5.4.1 Directrices dispositivos móviles

- Autorizar la salida de equipos de dispositivos móviles para la ejecución de actividades fuera de las instalaciones de Mindeporte.
- No permitir la salida de equipos de escritorio para la ejecución de cualquier actividad fuera de las instalaciones de Mindeporte. Cuando por alguna excepción se requiera la salida de un equipo de escritorio deberá tener la autorización previa del coordinador del GIT-TIC´s y de Almacén, con el fin de verificar qué tipo de información se encuentra almacenada en éste y aplicar controles necesarios antes de su salida.

- Hacer buen uso de los dispositivos móviles (portátiles, tabletas y teléfonos móviles entre otros) que son asignados para el desempeño de sus funciones laborales u obligaciones contractuales.

- Contar con un sistema de autenticación, como un patrón, código de desbloqueo o una clave, para todos los dispositivos móviles que almacenen información de Mindeporte.

- Utilizar en los dispositivos móviles únicamente redes seguras y con la protección adecuada para evitar acceso o divulgación no autorizada de la información almacenada y procesada en ellos, evitando su conexión a redes inseguras como las de aeropuertos, restaurantes o cafés Internet a menos que se haga a través de VPN.

- Mantener apagado el bluetooth o cualquier otra tecnología inalámbrica que exista o llegara a existir.

- Utilizar los equipos móviles asignados por Mindeporte exclusivamente para desempeñar las funciones asignadas al cargo o las obligaciones contractuales pactadas.

- El uso de los equipos asignados debe ser exclusivo del servidor público o contratista, por lo tanto, no debe realizar préstamos de estos.

- No instalar ni configurar en los servicios ni en la infraestructura tecnológica de Mindeporte (computadores de escritorio, equipos móviles, servidores de cómputo físicos y virtuales, etc.) software para conexiones remotas gratis o de pago como: . Gotomypc, TeamViewer, LogMeIn, AnyDesk, etc.

- Asegurar que los dispositivos móviles provistos por Mindeporte cuenten con los siguientes controles:

    1. Uso de usuario y contraseña para acceso al mismo.
    2. Uso de software antivirus provisto por Mindeporte.
    3. Restricción de privilegios administrativos para los usuarios.
    4. Uso de software licenciado y provisto por Mindeporte (Software base).
    5. Adquisición de pólizas que cubran el hardware y la información de los dispositivos, contra perdida o hurto.

5.4.2 Directrices teletrabajo

El Ministerio del Deporte como entidad del estado, se acoge a la ley 1221 de 2008, la cual establece las normas para promover y regular el Teletrabajo. En este orden, los funcionarios con modalidad de teletrabajo deberán acogerse a la resolución 000934 del 13 de septiembre del 2023 *"Por la cual se implementan las modalidades del Teletrabajo en el Ministerio del Deporte y se dictan otras disposiciones".* Así mismo, deberán cumplir con las siguientes directrices:

- Hacer buen uso de los dispositivos de los equipos de cómputo que son asignados para el desempeño de las funciones laborales u obligaciones contractuales.
- Contar con un sistema de autenticación, como un patrón, código de desbloqueo o una clave, para el equipo de cómputo donde se almacena información de Mindeporte.

- Utilizar en los equipos de cómputo únicamente redes seguras y con la protección adecuada para evitar acceso o divulgación no autorizada de la información almacenada y procesada en ellos.
- El uso de los equipos de cómputo asignados debe ser exclusivo del servidor público, por lo tanto, no debe realizar préstamos de estos ni realizar actividades o almacenamiento de información personal.
- No instalar ni configurar en los servicios ni en la infraestructura tecnológica de Mindeporte (computadores de escritorio, equipos móviles, servidores de cómputo físicos y virtuales, etc.) software para conexiones remotas gratis o de pago como: Gotomypc, TeamViewer, LogMeIn, AnyDesk, etc.
- Acatar el procedimiento de Teletrabajo establecido en la normatividad correspondiente vigente tanto externa como interna.
- Derecho de revisar la utilización de los equipos de cómputo ante cualquier indicio de un uso inapropiado del mismo o inspeccionarlo o disponer de el de cualquier forma, dado que tanto el dispositivo como la información almacenada es propiedad de Mindeporte
- Cumplir el procedimiento de Teletrabajo establecido en la normatividad correspondiente vigente tanto externa como interna.
- Asistir a las capacitaciones necesarias sobre las políticas y controles de seguridad de la información publicados y vigentes de Mindeporte
- El servidor púbico que aplica al teletrabajo debe firmar ante la Oficina de Talento Humano el compromiso de cumplimiento de controles de seguridad de la información para preservar la confidencialidad, integridad y disponibilidad de la información**.**

- Si al teletrabajador Mindeporte le asigna uno o varios dispositivos móviles, éstos deben garantizar el cumplimiento de los siguientes controles:

    - ✓ Uso de usuario y contraseña para acceso al mismo.
    - ✓ Uso de software antivirus provisto por Mindeporte.
    - ✓ Restricción de privilegios administrativos para los usuarios.
    - ✓ Uso de software licenciado y provisto por Mindeporte (Software base).
    - ✓ Adquisición de pólizas que cubran el hardware y la información de los dispositivos, contra perdida o hurto.

En el caso en que el teletrabajador, de común acuerdo con Talento Humano, establezca que el equipo de cómputo a utilizar para el cumplimiento de sus funciones laborales sea su equipo personal, éste deberá tener como mínimo un antivirus licenciado y actualizado para ejercer dicha labor. En este sentido, GIT TIC’s a través de conexión remota, validará el cumplimiento de este requerimiento.

5.4.3 Directrices trabajo remoto en casa

La ley 2121 de 2021, crea el régimen de trabajo remoto y establece las normas para esta modalidad por lo cual Mindeporte, en calidad de entidad del estado, se acoge a esta ley para la aplicación de esta modalidad para los servidores públicos, la cual deberá ser aprobada por Talento Humano, quién deberá solicitar a GIT TIC's le asignación de los equipos de cómputo para que pueda realizar el cumplimiento de sus funciones en esta modalidad de trabajo, la cual tiene una connotación parecida a la modalidad de Teletrabajo, por lo tanto, deberá acogerse según corresponda, a las directrices de teletrabajo establecidas en el numeral anterior 5.2.5.2 de esta política y atender a las siguientes directrices adicionales:

- No instalar ni configurar en los servicios ni en la infraestructura tecnológica de Mindeporte (computadores de escritorio, equipos móviles, servidores de cómputo físicos y virtuales, etc.) software para conexiones remotas gratis o de pago como: Gotomypc, TeamViewer, LogMeIn, AnyDesk, etc.
- Contar con las aprobaciones requeridas para establecer conexión remota (VPN) a los dispositivos de la plataforma tecnológica de Mindeporte y acatar las instrucciones de acceso establecidas para las conexiones remotas.
- Establecer conexiones remotas únicamente a través de las VPN seguras y utilizar computadores en sitios confiables (Ej. Casa) y, en ninguna circunstancia, en computadores públicos, de hoteles o cafés internet, entre otros.
- Realizar la solicitud de conexión VPN por medio del Grupo de Soporte del GIT TIC´s.
- El servidor público o contratista que solicite acceso por medio de una VPN es responsable del uso adecuado del acceso remoto.
- Configurar las conexiones remotas a los servicios tecnológicos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores asignadas dentro de Mindeporte.

5.5 POLITICA DE CONTENIDO PÁGINA WEB E INTRANET DE MINDEPORTE

El material que aparezca en la página de Internet de Mindeporte deberá ser aprobado por el GIT Comunicaciones según lo establecido en la Política Editorial publicada en Isolución, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).

El material que se requiera publicar en la Intranet de Mindeporte deberá ser aprobado por el jefe del área del material a publicar y debe de estar de acuerdo con las normas y procedimientos establecidos en la Política Editorial de la entidad.

5.6 POLITICA DE ACCESO A LOS SISTEMAS DE INFORMACIÓN

- Tendrá acceso a los sistemas de información solo el personal de Mindeporte que sea titular de una cuenta del dominio Mindeporte o bien tenga la autorización del GIT TIC´s.
- El manejo de información que se considere de uso restringido deberá ser cifrada con el objeto de garantizar su seguridad.
- La instalación y uso de los sistemas de información se rigen por el reglamento de uso de la Red de Mindeporte y por las normas y procedimientos establecidos por el GIT TIC´s.
- Los servidores de bases de datos son dedicados, por lo que se su acceso estará permitido únicamente al personal expresamente autorizado por el GIT TIC´s.
- El control de acceso a cada sistema de información será determinado de acuerdo con la unidad responsable de generar y procesar los datos involucrados.

5.7 POLITICA DE CONTROL DE ACCESO FÍSICO

- Los funcionarios deben portar el carné de la entidad en lugar visible durante su permanencia en las instalaciones.
- Los empleados deben reportar a la mayor brevedad, cualquier sospecha de pérdida o robo de sus carnés de identificación y tarjetas de acceso físico a las instalaciones.
- El ingreso al Centro de Computo por parte de terceros debe realizarse acompañado de un funcionario del GIT TIC´s, previo registro en el libro de control.
- Los funcionarios no deben permitir que personal desconocido o no autorizado ingrese a zonas de acceso controlado.
- El ingreso a las áreas con información sensible debe estar protegido con controles de acceso efectivos.
- Los funcionarios solo deben ingresar a zonas a las cuales han sido autorizados.
- No podrán salir de las instalaciones equipos de cómputo de propiedad de Mindeporte sin la respectiva autorización del GIT de Gestión Administrativa.
- Todo visitante debe presentar en la recepción su identificación para ser registrado cumpliendo con el procedimiento diseñado para tal fin.
- Todo equipo de cómputo o periférico personal que ingrese a las instalaciones deberá ser registrado por minuta al momento de su ingreso y descargarse a su salida por el personal de seguridad.
- Toda persona debe permitir la revisión de su maletín o bolso por el personal de seguridad al ingresar o salir de las instalaciones.
- Al finalizar su relación laboral o contrato de servicios con la entidad, todos los privilegios de acceso a las instalaciones de Mindeporte que fueron otorgados al empleado deberán ser revocados.

5.8 POLITICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SOFTWARE

5.8.1 Adquisición de software o contratación de nuevos desarrollos

- En concordancia con la política del Ministerio, el GIT TIC´s es la dependencia responsable de establecer los mecanismos de adquisición de bienes y servicios informáticos para todas las áreas de la entidad.
- El GIT TIC´s propiciará la adquisición de licencias de sitio, licencias flotantes, licencias por empleado y licencias por volumen, para obtener economías de escala.
- Corresponderá al GIT TIC´s generar los lineamientos para el tipo de licenciamiento, cobertura, transferibilidad, certificación y vigencia.
- Todo nuevo servicio de procesamiento de información que requiera la entidad debe ser previamente aprobado por la Coordinación del GIT TIC´s, el cual verificará que éste cumpla con la política de seguridad de la información tal y con los requerimientos técnicos establecidos por Mindeporte.
- Todo nuevo desarrollo de software que el Ministerio contrate deberá contar con la aprobación, acompañamiento y seguimiento del GIT TIC's durante todo su ciclo de vida, para asegurar que dicho desarrollo cumpla con todos los requerimientos técnicos, de compatibilidad y seguridad de la información establecidos por Mindeporte.
- En todo proceso de adquisición de software para la entidad se deben incluir los requerimientos de seguridad de la información, como capacidad de integración con el Directorio Activo, generación de registros de eventos, manejo de perfiles de usuario y niveles de acceso, entre otros.

5.8.2 Instalación de software

- Corresponde al GIT TIC´s establecer las normas y procedimientos para la instalación y supervisión del software básico para cualquier tipo de equipo.
- En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permitirá la instalación de software con licenciamiento apropiado y en observancia de la propiedad intelectual.
- El GIT TIC´s es el área responsable de brindar asesoría y acompañamiento al Ministerio para la instalación de software informático y de telecomunicaciones.
- La instalación de software no licenciado, o que pertenezca a una licencia de un tercero ajeno a la entidad, queda totalmente prohibido para equipos y dispositivos que se encuentren asociados al controlador de dominio de Mindeporte.
- Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos que se conecten a las redes de la entidad dispongan de software de seguridad (antivirus, firewalls, privilegios de acceso, y otros que se apliquen).

- Está prohibida la instalación de software de la entidad en equipos personales o que no sean propios de la entidad a menos que sea autorizado para llevar a cabo alguna de las modalidades de Teletrabajo.

5.8.3 Desarrollo, cambios y/o actualizaciones de software y sistemas

- Adquisición y actualizaciones. La adquisición y actualización de software para equipos de cómputo y de telecomunicaciones se llevará a cabo de acuerdo con la vigencia de su licenciamiento, el cual es controlado por el GIT TIC´s.
- Separación de ambientes de producción y desarrollo. Todo nuevo desarrollo de software debe contar con ambientes de desarrollo y de producción separados, lo cual debe ser un requerimiento en los estudios previos que elabore el área; el supervisor designado deberá verificar el adecuado funcionamiento del sistema en el ambiente de desarrollo para poder aprobar su paso a producción.
- Cambios y/o actualizaciones. Los cambios y/o actualizaciones a los sistemas de información que se encuentren en producción, serán efectuados y verificados en un entorno de pruebas para corroborar su adecuado funcionamiento antes de su paso al ambiente productivo, dejando evidencia de las pruebas efectuadas.
- Documentación de cambios y/o actualizaciones. Todo cambio y/o actualización en los sistemas de información que se encuentren en producción, deberá documentarse de acuerdo con el procedimiento de Gestión de Cambios.

5.8.4 Verificación de software instalado

El GIT TIC´s realizará revisiones periódicas para asegurar que sólo el software autorizado y con licencia esté instalado en los equipos de cómputo de Mindeporte.

Corresponderá al GIT TIC´s dictar las normas, procedimientos y calendarios de verificación del software instalado de acuerdo con los procedimientos y lineamientos de la norma NTC-ISO/IEC 27001.

5.8.5 Software propiedad de Mindeporte

- Todo el software adquirido por Mindeporte sea por compra, donación o cesión es propiedad del Ministerio y mantendrá los derechos que la ley de propiedad intelectual le confiera.
- El GIT TIC´s en coordinación con Almacén deberá mantener un registro de todo el software propiedad de Mindeporte.

- Todos los sistemas de software (programas, bases de datos, sistemas operativos, interfaces) desarrollados con o a través de los recursos de Mindeporte se mantendrán como propiedad del Ministerio respetando la propiedad intelectual del mismo.
- Es obligación de todos los usuarios que manejen información masiva, mantener el respaldo correspondiente de la misma ya que esta se considera como un activo de la entidad que debe preservarse.
- Los datos, las bases de datos y los recursos informáticos del Ministerio deben estar resguardados.
- Corresponderá al GIT TIC´s promover y difundir los mecanismos de respaldo y salvaguarda de los datos y de software.
- El GIT TIC´s gestionará la solicitud de patentes y derechos de creación de software propiedad del Ministerio en los casos que aplique.
- El GIT TIC´s administrará los diferentes tipos de licencias de software y vigilará su vigencia en concordancia con la política de seguridad de la información de Mindeporte.

5.8.6 Uso de software

Cualquier software que requiera ser instalado para trabajar sobre la Red de Mindeporte deberá ser evaluado por el GIT TIC´s previo a su instalación.

Todo el software propiedad de Mindeporte deberá ser usado exclusivamente para asuntos relacionados con temas laborales de la entidad.

5.8.7 Propiedad intelectual

Corresponde al GIT TIC´s procurar que todo el software instalado en Mindeporte esté de acuerdo con la normatividad vigente sobre propiedad intelectual.

5.8.8 Aislamiento de sistemas sensibles

Los sistemas que se consideren sensibles deben estar en ambientes separados, esto con el fin de evitar accesos no autorizados, robo de información u otros que pudiesen configurar incidentes de seguridad de la información.

5.8.9 Seguridad en entornos de desarrollo y prueba

Para ambientes de desarrollo y pruebas se debe realizar ofuscamiento de los datos sensibles para evitar robo o acceso no autorizados de información, para lo cual el

funcionario asignado del GIT TIC´s debe evaluar cuales datos debe ofuscar de acuerdo con la calificación de la información.

5.8.9 Control de acceso al código fuente de los programas

La custodia del código fuente de los sistemas de información de Mindeporte estará en cabeza del Coordinador del GIT TIC´s, quien lo almacenará bajo llave en un medio externo y en caso de modificaciones deberá actualizarlo con los cambios y la documentación respectiva de acuerdo con el procedimiento de gestión de cambios.

5.8.10 Construcción de sistemas seguros

- Todos los accesos que se hagan a los sistemas deben ser validados.
- Si se utiliza un lenguaje que no sea compilado, asegurarse de limpiar el código que se pone en producción, para que no contenga rutinas de pruebas, comentarios o cualquier tipo de mecanismo que pueda dar lugar a un acceso indebido.
- Si se utiliza un lenguaje compilado, se debe garantizar que la compilación se realiza utilizando las mejores optimizaciones disponibles y que no se incluya información para depuración.
- Desde el GIT TIC´S, se deben establecer los procedimientos necesarios para implementar medidas y/o controles de seguridad sobre los desarrollos de aplicaciones internas, considerándolo en las etapas del ciclo de vida de desarrollo de software (SDLC)
- El equipo de desarrollo o cualquier funcionario o contratista que ejerza esta labor de desarrollar aplicaciones para Mindeporte, deberá utilizar software de versionamiento de código para controlar los cambios y/o actualizaciones en el código fuente.
- Se deben ejecutar escaneos de vulnerabilidades estáticos al código fuente de las aplicaciones desde la primera versión y realizar las remediaciones necesarias en caso en que se identifiquen vulnerabilidades en el código. Así mismo, generar las nuevas versiones de código fuente limpio de la aplicación o sistema de información.
- El código fuente y su versionamiento deberán ser almacenados en medios de almacenamiento dispuestos por GIT TIC'S, quién deberá tener implementados controles de seguridad para la protección de los respectivos códigos fuente.
- Deben incluirse pruebas de cubrimiento del código para garantizar que todo el código es probado.
- Nunca confiar en los datos que ingresan a la aplicación, todo dato debe ser verificado para garantizar que lo que está ingresando a los sistemas es lo esperado y además evitar ataques por inyección de código.
- Cualquier funcionalidad, campo, botón o menú nuevo debe agregarse de acuerdo con los requerimientos de diseño. De esta forma se evita tener porciones de código que resultan siendo innecesarias.

- Cualquier cambio que se haga debe quedar documentado, esto facilitará modificaciones futuras.

5.8.11 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación

- Garantizar que cuando se cambian las plataformas de operación (sistemas operativos, bases de datos, plataformas y aplicaciones), se revisan las aplicaciones críticas del negocio, y se prueban para asegurar que no haya impacto adverso en las operaciones o seguridad de Mindeporte.
- Revisar los procedimientos de integridad y control de aplicaciones para asegurar que no estén comprometidos debido a los cambios en las plataformas de operaciones.
- Garantizar que la notificación de los cambios en la plataforma operativa se hace a tiempo para permitir las pruebas y revisiones apropiadas antes de la implementación.
- Garantizar que los cambios realizados en los sistemas de información se revisan escaneando vulnerabilidades y mitigándolas.

5.8.12 Protección de transacciones de los servicios de las aplicaciones

- La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
- Exigir al operador de TI que incluya consideraciones de seguridad de la información para las transacciones de los servicios de las aplicaciones.
- Asegurar que la información de autenticación secreta de usuario, de todas las partes, se valide y verifique.
- Los protocolos usados para comunicarse entre todas las partes involucradas sean seguros.
- El almacenamiento de los detalles de la transacción se realice en un entorno que no sea accesible públicamente.
- Que en donde se use una autoridad confiable (por ejemplo, para los propósitos de emitir y mantener firmas o certificados digitales), la seguridad esté integrada e incluida en todo el proceso de gestión de certificados/firmas de un extremo a otro. relacionados con las actividades del Ministerio.

5.9 POLITICAS PARA EL CORREO ELECTRÓNICO INSTITUCIONAL DEL MINISTERIO

5.9.1 Asignación de cuenta de correo

- Las cuentas de correo electrónico del dominio de Mindeporte deberán solicitarse mediante un ticket de soporte por el área de Talento Humano para nuevos funcionarios o por el jefe del área a la que se asignará el contratista, adjuntando el formato de solicitud de cuentas de usuario donde se detallen los datos del usuario o usuarios a quien(es) se le(s) asignará la cuenta.
- El usuario y contraseña para autenticarse en el correo serán iguales a los utilizados para el usuario del dominio Mindeporte; la dirección de correo tendrá el siguiente formato: <usuarioDeRed>@mindeporte.gov.co
- Aquellas áreas o proyectos que requieran un correo electrónico para su uso genérico deberán solicitarlo mediante ticket de soporte al área del GIT TIC´s adjuntando el formato respectivo con la aprobación del jefe de área.
- Los mensajes y la información contenida en los buzones de correo son propiedad de Mindeporte y cada usuario, como responsable de su buzón, deberá conservar solamente los mensajes relacionados con el desarrollo de sus funciones.
- Todos los usuarios que dispongan de cuenta de correo electrónico institucional están en la obligación de revisar sus mensajes entrantes al menos dos veces al día. Así mismo, es su responsabilidad depurar el buzón de entrada para mantener espacio libre.

5.9.2 Uso permitido

- La cuenta de correo asignada a un usuario es personal e intransferible.
- Los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de acceso y su buzón asociado al Ministerio. El tener una cuenta de correo electrónico institucional compromete y obliga a cada usuario a aceptar las normas establecidas para su buen uso y a someterse a ellas.
- El correo es un servicio de la entidad para sus funcionarios y contratistas por lo que su uso es exclusivamente para actividades laborales.
- Queda estrictamente prohibido el uso del correo electrónico para propagar mensajes de tipo cadena. Si la entidad recibe quejas, denuncias o reclamaciones por estas prácticas, se tomarán las medidas disciplinarias pertinentes. El número máximo de destinatarios permitidos para envío de correo es de 500 por mensaje.
- Queda estrictamente prohibido el uso del correo electrónico para divulgar información calificada como pública, clasificada o reservada del Ministerio del Deporte sin la respectiva autorización de la entidad, en cumplimiento de lo establecido en la Ley 1712 de 2014.
- Queda estrictamente prohibido el uso del correo electrónico para difundir mensajes de tipo comercial, financiero, político, religioso o temas similares no relacionados con las actividades de la entidad.

- Queda estrictamente prohibido utilizar la cuenta de correo asignada por la entidad, para actividades personales.
- Queda estrictamente prohibido utilizar la cuenta de correo asignada por la entidad, para reenviarse información propiedad del Ministerio del Deporte a una cuenta de dominio personal.
- Queda estrictamente prohibido utilizar la cuenta de correo asignada por la entidad, para generar cambios dentro de ésta para reenvíos automáticos a cuentas de correo con dominios externos diferentes a @mindeporte.gov.co.
- Queda estrictamente prohibido utilizar la cuenta de correo asignada por la entidad, para generar cambios dentro de ésta (cambiar configuración o generar reglas) para reenvíos automáticos a cuentas de correo con dominios de @mindeporte.gov.co. de colaboradores diferentes a su superior inmediato.
- Queda estrictamente prohibido generar y compartir cuentas de correo con dominios externos diferentes a @mindeporte.gov.co para el envío, solicitud o transmisión de información propiedad del Ministerio del Deporte y hacer uso de estas cuentas como si fueran de la entidad.
- Queda estrictamente prohibido intentar o apoderarse de claves de acceso de otros usuarios y/o acceder y/o modificar mensajes de otro usuario.
- No está permitido el envío de correos con archivos adjuntos de más de 50 MB (megabytes); los correos entrantes con archivos adjuntos de más de 50 MB no serán aceptados por el servidor de correo. En casos especiales el GIT TIC's podrá autorizar una ampliación de esta capacidad previa solicitud mediante ticket de soporte justificado por el jefe del área respectiva.
- El manejo de las direcciones de correo electrónico genéricas asignadas a un área o proyecto son responsabilidad de los jefes de área, quienes podrán delegar la atención de dicha cuenta de correo sin eximirse de la responsabilidad por el cumplimiento de las presentes normas e independientemente del accionar del personal en el cual delegue tales funciones.

5.9.3 Buenas prácticas de seguridad de la información

- Las comunicaciones realizadas a través del correo electrónico institucional se consideran una comunicación de tipo oficial y se debe hacer uso preferente de este medio en las comunicaciones al interior de la entidad de acuerdo con lo indicado en la Directiva Presidencial 04 de 2012, "Eficiencia administrativa y lineamientos de la política Cero Papel en la administración pública".
- Es aconsejable no utilizar la dirección de correo institucional en suscripciones, boletines, listas de distribución de empresas comerciales u otras no relacionadas con temas laborales a fin de evitar la saturación del correo con mensajes tipo Spam y prevenir el ingreso a la entidad de correos con contenidos dañinos o maliciosos.

- Es recomendable que los mensajes de correo considerados no importantes sean eliminados de la bandeja de entrada, evitando así consumir espacio innecesario de la cuota de correo.
- Se recomienda que los archivos grandes que se requiera adjuntar a mensajes de correo electrónico sean en lo posible comprimidos mediante software de compresión de archivos para así evitar la degradación del servicio de correo, el consumo excesivo de ancho de banda y la saturación involuntaria de los buzones de los destinatarios.

5.9.4 Seguridad del correo

- Para asegurar la estabilidad y seguridad, el GIT TIC´s tendrá la potestad de aplicar controles y monitoreo al tráfico de mensajes de correo con el fin de evitar riesgos tanto para los usuarios como para la entidad.
- Si se retira momentáneamente de su puesto de trabajo, deberá bloquear su sesión de usuario (mediante los comandos Windows+L o Ctrl-Alt-Supr y Bloquear) y al retirarse de su puesto al final de su jornada de trabajo, deberá cerrar las aplicaciones (navegadores, correo o aplicativos) que esté usando y apagar el equipo y monitor.
- Los archivos adjuntos con extensiones que puedan representar potenciales amenazas a la seguridad de la información no serán aceptados por el correo tanto entrante como saliente.
- Si sospecha que su clave de acceso a la red o al correo ha sido vulnerada, cambie de inmediato las contraseñas o informe mediante un ticket de soporte al GIT TIC´s por los medios de contacto disponibles a la mayor brevedad para realizarle el cambio.
- La información enviada a través del correo electrónico será responsabilidad exclusiva del emisor, por lo tanto, revise cuidadosamente tanto el contenido como los destinatarios de todos sus correos antes de oprimir el botón de envío.

5.9.5 Eliminación de cuenta de correo

Toda cuenta de correo electrónico será eliminada 3 días después de la notificación de retiro del funcionario y será responsabilidad de éste realizar la copia y entrega de la información existente en el buzón a quien deba recibir el cargo.

5.10 POLITICAS DE INTERNET

5.10.1 Asignación de permiso de acceso a internet

El acceso a Internet es uno de los servicios ofrecidos a través de la Red de Mindeporte. Este servicio es inherente a cada usuario del dominio autenticado en un computador.

La autenticación para el servicio de Internet (usuario y contraseña) será igual a la utilizada para el usuario del dominio Mindeporte.

El canal de acceso a Internet de Mindeporte es de uso compartido entre todos los usuarios de la entidad, por lo tanto, el nivel de uso individual influye en el grado de calidad del servicio para la totalidad de los usuarios.

La asignación de permisos de Internet estará basada en los protocolos de red de la IEEE y dichos permisos serán configurados por el personal a cargo de la administración de infraestructura de red y seguridad de Mindeporte.

5.10.2 Uso permitido

- El servicio de acceso a Internet es exclusivamente para las actividades institucionales.
- El uso de internet para asuntos personales se permite siempre y cuando su utilización sea por tiempo limitado dentro de los horarios establecidos para ello y esté de acuerdo con las políticas de buen uso del Internet y no influya de manera negativa en el desempeño de las tareas y responsabilidades para con la entidad. Los horarios establecidos para acceder a correos personales y redes sociales son los siguientes: entre las 12:00 pm y 2:00 pm y a partir de las 5:00 pm hasta las 8:00 am del día siguiente; en un horario diferente estos accesos estarán bloqueados (estas restricciones no aplicarán para funcionarios o contratistas del Grupo Interno de Trabajo GIT Comunicaciones). El uso personal podría ser denegado en los casos en que se detecte que el usuario hace uso excesivo o indebido de los recursos del canal de Internet.
- Los usuarios de Internet utilizarán únicamente los servicios para los cuales están autorizados y no deberán usar este servicio para acceder o modificar archivos que no sean de su propiedad, ni mucho menos, los pertenecientes al Ministerio del Deporte o a otras entidades o instituciones públicas o privadas.
- Están totalmente prohibidos: el ingreso a páginas con contenidos sexuales, racistas o cualquier otro tipo de material ofensivo o discriminatorio; el ingreso a páginas de apuestas o juegos de suerte y azar en línea; la descarga de programas que permitan realizar conexiones automáticas o visores de sitios clasificados como pornográficos y la utilización de los recursos de la entidad para distribución o reproducción de este tipo de material ya sea vía Web o por medios magnéticos. Los usuarios que accidentalmente llegasen a conectarse a páginas de Internet que tengan estos contenidos, deberán

desconectarse inmediatamente e informar del hecho al GIT TIC´s, para proceder a su bloqueo en los equipos de seguridad informática de la entidad.

- Está prohibido descargar archivos de música o video, participar en juegos de entretenimiento en línea o utilizar los servicios de radio y TV por demanda; estas actividades generan un alto consumo de ancho de banda del canal de Internet causando afectación en la calidad del servicio para el resto de los usuarios.
- Está prohibida la descarga, instalación y uso de programas ajenos al licenciamiento de Mindeporte ya sea software libre (freeware o shareware), toolbars, hotbars, messenger o cualquier otro aplicativo o complemento que altere las configuraciones ya instaladas en los computadores de la entidad. Cualquier requerimiento para instalar una de estas aplicaciones o complementos deberá ser justificado y consultado con el GIT TIC´s quien realizará el correspondiente estudio técnico y de ser aprobada la solicitud, su instalación será llevada a cabo por el personal del GIT TIC´s
- Los accesos desde fuera de la entidad a través de Internet para utilizar los sistemas de información de Mindeporte o cualquier otra aplicación en forma remota y en tiempo real deben ser autorizados y supervisados por GIT TIC´s; no se permitirán en ningún caso los accesos externos para realizar soporte por parte de proveedores que no permitan ser monitoreados en tiempo real por el personal del GIT TIC's.

5.10.3 Seguridad de la intranet

- Cualquier archivo descargado a través de Internet, o recibido como adjunto en un correo electrónico, o proveniente de cualquier medio extraíble (disco externo, USB, CD, DVD), deberá revisarse con un software antivirus para garantizar que no contenga virus, adware, spyware, ransomware u otro tipo de código malicioso. La ejecución de estos programas podría comprometer la seguridad de la información de Mindeporte, afectar tanto el funcionamiento de los computadores como el rendimiento de la red o incluso llegar a destruir o dejar inutilizable la información del disco duro del computador. Antes de abrir cualquier archivo recibido por correo electrónico, el usuario debe asegurarse de que sea un archivo confiable; no deberán abrirse correos con adjuntos ni ingresar a enlaces que provengan de sitios aparentemente confiables sin antes verificar la autenticidad del mensaje. Antes de abrir un correo o archivo adjunto debe aplicarse la lógica de que ninguna entidad sea bancaria u oficial le pedirá datos ni le enviará archivos por medio de correo para solicitarle cualquier información de tipo personal. Todo equipo con acceso a Internet debe tener instalado un antivirus con sus bases de datos y agentes de detección actualizados y siempre debe estar activo.
- El nivel de seguridad del navegador de Internet debe estar configurado con un nivel medio-alto; de esta forma se controla la ejecución de secuencias de comandos, componentes, controles y complementos ActiveX provenientes de sitios de alto riesgo que puedan dañar o comprometer la información guardada en el computador. También de esta forma se controla la descarga automática de archivos y el bloqueo de ventanas emergentes.

- Está prohibido hacer uso de los servicios de Internet para interferir en los sistemas de información de Mindeporte mediante acciones deliberadas que disminuyan el desempeño o la capacidad de los equipos instalados. Así mismo, y en ninguna circunstancia se debe intentar burlar los esquemas de seguridad de los sistemas de Mindeporte mediante la instalación o uso de técnicas, dispositivos o programas que evadan o sobrepasen dichos esquemas de seguridad.

5.11 POLITICA DE GESTIÓN Y GOBERNABILIDAD DE SEGURIDAD DE LA INFORMACION

- Para poder establecer una estrategia de ciberseguridad efectiva, como parte integral de la seguridad de la información, se debe partir de una visión de alto nivel desde la Alta Gerencia alineada con los objetivos estratégicos de la organización. La ciberseguridad debe ser vista como un facilitador del negocio, no como gastos operacionales.
- El diseño e implementación de estas políticas, estándares, procesos y procedimientos pueden basarse en uno o más marcos de referencia de acuerdo con las necesidades de la organización o sus motivantes, tales como ataques inminentes, *compliance* (conformidad legal), visión de líderes mediante diferenciadores del negocio, ventaja competitiva, etc.
- Las organizaciones que buscan crecer en su curva de madurez en seguridad de la información implementan un SGSI (Sistema de Gestión de Seguridad de la Información) basado en la norma ISO 27001, con lo que establecerán el norte y los objetivos a cumplir en esta área. La Ciberseguridad al estar inmersa dentro de la Seguridad de la Información será cubierta por los controles establecidos por el SGSI (con un enfoque en la mitigación de riesgos más avanzados).

5.12 POLITICA DE DEFENSA EN PROFUNDIDAD

Es un enfoque de protección mediante mecanismos de seguridad por capas, en donde la protección funciona como un todo. Si un atacante ocasiona que uno de los mecanismos de protección falle, otro mecanismo debe estar presente para suplir la protección necesaria. Por ejemplo, si la capa más externa de firewalls es vulnerada, la protección por capas debe garantizar que haya otro mecanismo de protección en el camino hacia el activo de información, por ejemplo, firewalls internos, monitoreo de actividad de bases de datos (DAM) o protección de aplicaciones web (WAF).

Algunos controles que pueden ser implementados para proveer un enfoque de defensa en profundidad multicapa son:

- Firewalls (perimetrales, internos, de aplicaciones, de bases de datos)

- VPNs

- Intrusion Prevention Systems (IPSs)

- Filtrado de URL's

- Antivirus

- Web Application Firewalls (WAFs)

- NAC (Control de acceso a la red)

- EDR (Endpoint Detection and Response - una evolución del antivirus tradicional)

- Next Generation Firewalls (Firewalls con esquemas de seguridad adicionales)

- MDM (Gestión de seguridad en dispositivos móviles

- DAM (Monitoreo de actividad de bases de datos)

- SIEM + SOC (Gestión de eventos de seguridad + Centro de operación de seguridad)

5.13 POLITICAS DE SEGURIDAD DE LAS OPERACIONES

Estas políticas tienen como objetivo establecer directrices para garantizar la seguridad de las operaciones de Mindeporte, protegiendo la integridad, confidencialidad y disponibilidad de los sistemas, datos y recursos críticos.

Estas políticas se aplican a todas las operaciones y actividades realizadas en los sistemas, redes, activos y entornos de trabajo de la entidad.

Directrices:

- El personal de seguridad de la información y ciberseguridad definido en GIT TIC'S será responsable de supervisar y hacer cumplir estas políticas.
- Los usuarios y empleados deberán cumplir con estas políticas y reportar cualquier incidente o actividad sospechosa.
- Todo acceso a los sistemas y recursos de la entidad debe ser autorizado y estar basado en los principios de menor privilegio. Se deben establecer mecanismos de autenticación fuertes y actualizados.
- Implementar sistemas de monitoreo continuo para detectar actividades anómalas o no autorizadas en los sistemas. Esto incluye registros de eventos, auditorías y alertas de seguridad.

- Establecer un proceso para aplicar parches y actualizaciones de seguridad de manera regular y oportuna en todos los sistemas y aplicaciones para mitigar vulnerabilidades conocidas.
- Aplicar mecanismos de encriptación y controles de acceso para proteger la confidencialidad e integridad de los datos sensibles, tanto en reposo como en tránsito.
- Mantener un plan de respuesta a incidentes que incluya procedimientos claros para identificar, contener, mitigar y recuperarse de cualquier incidente de seguridad.
- Realizar copias de respaldo regulares y almacenarlas de manera segura. Probar regularmente los procedimientos de recuperación de datos para asegurar su eficacia en caso de fallo o incidente.
- Establecer reglas y directrices claras sobre el uso aceptable de los sistemas y recursos de la entidad, incluyendo el uso de dispositivos personales, redes sociales y aplicaciones no autorizadas.
- Proporcionar capacitación regular a todo el personal sobre las políticas y procedimientos de seguridad, así como sobre las últimas amenazas y buenas prácticas de seguridad.
- Mantener medidas de seguridad física adecuadas para proteger los activos críticos, como la limitación de acceso a áreas sensibles y el uso de cerraduras, alarmas y controles de acceso.
- Estas políticas serán revisadas y actualizadas regularmente para mantener su relevancia y eficacia en respuesta a cambios en el entorno de seguridad y operativo.

5.14 POLITICAS DE MANEJO DE MEDIOS DE ALMACENAMIENTO

Esta política tiene la finalidad de establecer procedimientos y directrices para la gestión segura de los medios de almacenamiento de datos utilizados por Mindeporte, asegurando la protección de la información confidencial y sensible.

Esta política se aplica a todos los medios de almacenamiento de datos utilizados por empleados, contratistas y terceros que manejen información en la entidad.

Directrices:

- El personal del GIT TIC’S, será responsable de administrar y supervisar el cumplimiento de esta política. Así mismo, todo el personal que maneje medios de almacenamiento debe cumplir con las directrices y procedimientos establecidos en esta política, descritas a continuación:
- El GIT TIC’S, debe mantener un registro actualizado de todos los medios de almacenamiento utilizados por la entidad, incluyendo información sobre su tipo, capacidad, contenido y ubicación.
- Los medios de almacenamiento deben utilizarse solo para almacenar datos autorizados por la entidad. Se prohíbe el almacenamiento de datos personales o confidenciales sin autorización explícita.

- Todos los datos sensibles almacenados en medios extraíbles deben estar cifrados utilizando algoritmos de cifrado fuertes y aprobados por la entidad.
- Limitar el acceso a los medios de almacenamiento únicamente a personal autorizado. Los dispositivos deben estar protegidos mediante autenticación o contraseñas seguras.
- Salvaguardar los medios de almacenamiento físicamente mediante almacenamiento seguro en lugares controlados y restringidos, evitando el acceso no autorizado.
- GIT TIC'S debe etiquetar claramente cada medio de almacenamiento con información sobre su contenido, nivel de confidencialidad, fecha de creación y fecha de vencimiento (si corresponde).
- GIT TIC'S debe establecer procedimientos para la eliminación segura de datos de los medios de almacenamiento antes de su reutilización o disposición. Esto puede incluir el borrado seguro o la destrucción física según las normativas de seguridad.
- Las áreas encargadas deberán realizar auditorías periódicas para verificar el cumplimiento de las directrices establecidas en esta política y tomar medidas correctivas según sea necesario.
- Esta política debe ser revisada periódicamente para asegurar su relevancia y eficacia frente a los cambios en las tecnologías y las mejores prácticas de seguridad.

5.15 POLITICAS DE ESCRITORIO LIMPIO

5.15.1 Escritorio físico

- Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos físicos o en digital, con el fin de reducir riesgos de robo o pérdida de información.
- La documentación física que esté utilizando el funcionario a manera de consulta debe estar custodiada y reposar en los cajones asignados.
- El área de archivo de cada área debe permanecer bajo llave para evitar el robo o pérdida de información.

5.15.2 Escritorio lógico

- El escritorio (pantalla de inicio) del equipo de cómputo asignado debe estar despejado y ordenado, de tal forma que los íconos que se muestren en la pantalla del equipo sean estrictamente los necesarios para la labor desempeñada.

5.16 POLÍTICAS PARA ADMINISTRADORES DE SISTEMAS

- Usuario con rol de administrador: En los sistemas de información, servidores, equipos de cómputo y portátiles debe configurarse un usuario con privilegios de administrador con el único fin de realizar las tareas administrativas y de gestión que requieran permisos elevados sobre dichos equipos o sistemas. Los demás usuarios que se definan no podrán tener ese nivel y se les deberá configurar un rol limitado a las actividades que deban realizar.
- Almacenamiento de contraseñas de usuarios con rol de administrador: Los usuarios con rol de administrador deberán registrar su lista de contraseñas, ya sea en forma impresa o en un medio digital, dentro de un sobre sellado y marcado que deberá entregarse para su custodia bajo llave al Coordinador del GIT TIC´s.
- Intentos errados de ingreso a equipos: El número máximo de intentos errados consecutivos al tratar de ingresar a los equipos de cómputo deberá establecerse en tres (3) intentos; si luego del tercer intento no se logra establecer conexión, se deshabilitará el usuario y se debe solicitar al GIT TIC´s su desbloqueo. La contraseña debe ser cambiada por el usuario al realizar el próximo ingreso.
- Contraseñas por defecto: Las contraseñas que traen por defecto de sistemas de información, software base y equipos de cómputo deberán ser cambiadas tan pronto se instale o configure el sistema o equipo; la nueva contraseña asignada debe cumplir con los requerimientos de contraseñas fuertes que establece la entidad y se almacenará en sobre sellado bajo llave por el Coordinador del GIT TIC´s.
- Revisión de los registros del sistema: El administrador asignado deberá revisar regularmente los registros (logs) de cada uno de los diferentes sistemas de información y servidores a fin de tomar acción preventiva oportuna sobre los eventos relevantes de seguridad informática y realizar el reporte respectivo de acuerdo con el procedimiento Reporte de Incidentes de Seguridad de la Información.
- Habilitación de logs en sistemas y aplicaciones: Se debe habilitar el registro de logs en los servidores, sistemas de información y aplicaciones críticas que así lo permitan; se debe también configurar la gestión y mantenimiento de logs de manera que el tamaño de los archivos de registro de eventos se mantenga bajo crecimiento controlado.
- Monitoreo de sistemas: Se debe mantener configurada una adecuada aplicación de monitoreo que identifique problemas o alertas en el funcionamiento de los servidores, sistemas de información y aplicaciones críticas.
- Sincronización de relojes: Todos los servidores, equipos de cómputo y de red deberán configurarse para que sus relojes internos se mantengan sincronizados con el controlador de dominio del Directorio Activo de la entidad; el controlador de dominio a su vez deberá mantenerse sincronizado contra una fuente de tiempo externa confiable preferiblemente de estrato (stratum) 1 o 2 o en su defecto contra un pool de proveedores de servicios NTP abierto multiservidor (por ejemplo, pool.ntp.org).

5.17 POLITICAS DE GESTION DE VULNERABILIDADES

La política de gestión de vulnerabilidades tiene como objetivo establecer procedimientos y directrices para identificar, evaluar, mitigar y gestionar las vulnerabilidades en los sistemas y activos de Mindeportes, garantizando así la seguridad de la información y la continuidad del negocio.

Estas políticas se aplican a todos los sistemas, aplicaciones y activos digitales críticos para las operaciones de la entidad, incluyendo infraestructuras de red, servidores, dispositivos móviles y software.

Directrices:

El personal de seguridad de la información y ciberseguridad definido en GIT TIC'S será responsable de ejecutar, supervisar y coordinar la gestión de vulnerabilidades. Así mimos, los administradores de sistemas, desarrolladores y el personal de TI serán responsables de aplicar las correcciones de seguridad y seguir los procedimientos establecidos. En este orden se deberán seguir las siguientes directrices:

- Mantener un inventario actualizado de todos los activos de la entidad, identificando sus características y su función en el entorno.
- Realizar evaluaciones periódicas de riesgos de seguridad para identificar y priorizar las vulnerabilidades potenciales.
- Utilizar herramientas de escaneo y pruebas de penetración para identificar y catalogar las vulnerabilidades conocidas y desconocidas.
- Clasificar las vulnerabilidades según su gravedad, probabilidad de explotación y relevancia para el entorno de la entidad.
- Establecer un proceso para aplicar parches de seguridad y actualizaciones de software de manera regular y sistemática.
- Implementar y mantener estándares de configuración segura para sistemas y aplicaciones.
- Monitorización continua:
- Utilizar herramientas de monitoreo y detección de intrusiones para identificar y responder a nuevas vulnerabilidades o actividades sospechosas.
- Establecer procedimientos para evaluar y gestionar las vulnerabilidades en productos de terceros utilizados por la entidad.
- Fomentar la divulgación responsable de vulnerabilidades para permitir su corrección antes de su divulgación pública.
- Ofrecer capacitación regular al personal sobre las mejores prácticas de seguridad y la importancia de identificar y reportar vulnerabilidades.
- Desarrollar y mantener un plan de respuesta a incidentes que incluya acciones específicas para gestionar y mitigar vulnerabilidades explotadas o posibles ataques.

5.18 POLITICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD

- Todos los colaboradores son responsables de identificar y reportar los incidentes de seguridad.
- La atención de los incidentes está a cargo del GIT TIC´s como grupo de primera respuesta. Dependiendo del tipo de incidente, puede ser requerido el apoyo de otras dependencias de la Entidad.
- Los colaboradores deben reportar los eventos que sean considerados como posibles incidentes de Seguridad de la Información a través del correo electrónico del Grupo de Soporte del GIT TIC´s.
- Posterior de reportar los eventos que sean considerados como posibles incidentes de Seguridad de la Información, el GIT TIC´s registrará el evento en la bitácora de incidentes y determinará si se trata de un incidente de Seguridad de la Información para proceder con su gestión.
- Todos los colaboradores deben participar en las actividades de sensibilización, capacitación y socialización de Seguridad de la Información a las cuales sean convocados.
- El GIT TIC´s es responsable de realizar pruebas de vulnerabilidad (test y retest) a los sistemas de información con los que cuenta Mindeporte, en el momento que considere pertinente y/o se requiera ya sean de manera interna, y/o con los servicios adquiridos a través de pólizas de seguro que realice estas pruebas.
- El GIT TIC´s como primer respondiente a los resultados de las pruebas de vulnerabilidad y/o simulaciones de ciberseguridad, implementará las actualizaciones del sistema operativo y parches de seguridad que se requieran para mitigar los riesgos detectados. Para tal efecto, se debe contar con un cronograma para el desarrollo de estas actividades.
- El GIT TIC´s estará en contacto con las autoridades y grupos de interés de manera inmediata en un lapso inferior a 24 horas, en caso de que se presente un incidente de Seguridad de la Información. Tales como: ColCert: Grupo de Respuesta a Emergencia Cibernéticas de Colombia, CSIRT: Centro de Coordinación Seguridad Informática Colombia y MINTIC: Ministerio de las Tecnologías y las Comunicaciones.

5.19 POLITICAS DE PROVEEDORES O TERCEROS TECNOLÓGICOS

- El Ministerio del Deporte debe garantizar el relacionamiento con los terceros y/o proveedores de tecnología no afecte negativamente el desempeño de la operación y misionalidad de la entidad.
- El GIT - TIC´s realizará la gestión de los proveedores para garantizar una relación eficaz y sobre todo segura de los bienes y servicios tecnológicos que ofrecen a la entidad, gestionando los riesgos ciberseguridad que se identifiquen con cada una de las actividades.

- El GIT - TIC´s con el supervisor del contrato estará velando por el cumplimiento estricto de la ley y/o normativas vigentes del orden nacional en ciberseguridad.
- En caso de que el bien o servicio tecnológico suministrado esté a cargo de otro proceso, GIT, área o dirección, debe contar con el acompañamiento y aval del GIT - TIC´s y los responsables de la ciberseguridad de la entidad.
- El coordinador del GIT - TIC´s con el supervisor del contrato, en caso de algún incidente de ciberseguridad con el proveedor y/o terceros de los servicios tecnológicos deberá reportar al equipo de ciberseguridad de la entidad para evaluar la situación, el impacto y la remediación.
- El supervisor del contrato identificará y exigirá los controles de ciberseguridad a tener en cuenta, en el acceso de los proveedores a la información propiedad del Ministerio del Deporte.
- El coordinador del GIT - TIC´s gestionará la inclusión en los acuerdos de confidencialidad con los proveedores en los documentos contractuales tales como (contratos, ordenes de servicio, etc.).

6. POLITICAS NORMATIVAS Y REGULATORIAS DEL ESTADO COLOMBIANO

El Ministerio del Deporte, en calidad de entidad del estado colombiano del orden nacional, adopta las normativas regulatorias (leyes, decretos, directivas presidenciales, etc.) publicadas por el estado para su debido cumplimiento. En este orden, la entidad sigue las siguientes directrices definidas en los siguientes apartados de esta política.

6.1 Plan de transición para la adopción de ipv6 en coexistencia con ipv4

- De acuerdo con la circular expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones, insta a las entidades de la administración pública, Ramas y Organismos del Estado y al Sector TIC en general a:
- Exigir en las compras de equipos TIC, aplicaciones, plataformas TIC y servicios prestados a través de TIC, que estén desarrollados e implementados sobre IPv6 con compatibilidad o soporte total IPv4.
- Incluir en sus administraciones un "PLAN DE TRANSICIÓN PARA LA ADOPCIÓN DE IPv6 EN COEXISTENCIA CON IPv4". Que tengan por lo menos diagnóstico, plan de inversión, cronograma de implementación, formación en IPv6 de los funcionarios, evaluación de resultados y demás aspectos técnicos de implementación.

6.2 Lineamientos de gobierno digital (antes gobierno en línea)

Mediante el decreto 1008 de 2018, MinTIC estableció la política de Gobierno Digital (antes Estrategia de Gobierno en Línea) en la cual se erigen los lineamientos generales de dicha política y se dispone el Manual de Gobierno Digital como instrumento que permite adelantar las acciones que corresponde ejecutar a los sujetos obligados en lo referente a elementos habilitadores e indicadores de cumplimiento de IPv6 dentro de su arquitectura empresarial.

6.3 Lineamientos de la dirección de gobierno digital del MINTIC

El Viceministerio de Economía Digital del Ministerio de TICs, a través de la Dirección de Gobierno Digital y como ente encargado de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones, presentó durante el primer semestre de 2019 un documento actualizado que apoya a las entidades en los lineamientos técnicos que se requieren tener en cuenta para seguir el proceso de transición de IPv4 a IPv6 con éxito, teniendo en cuenta su aplicación para todo el ciclo de desarrollo por fases que requiere el nuevo protocolo, en un ambiente controlado y seguro que permita consolidar una adopción del protocolo IPv6 con éxito en el país, documento que es adoptado por Mindeporte en cabeza del GIT TIC´s a fin de consolidar la ruta de adopción del protocolo IPv6.

7. LINEAMIENTOS GENERALES

7.1 Inducción en seguridad de la información

El Grupo de Talento Humano deberá notificar al Grupo TIC´s sobre la vinculación de nuevos funcionarios con el fin de que éste realice la respectiva inducción en seguridad de la información durante el mes siguiente al proceso de vinculación. Para el caso de contratistas el supervisor del contrato debe informar al GIT TIC´s una vez legalizado el contrato para igualmente dar la inducción respectiva.

7.2 Supervisión y monitoreo

El GIT TIC´s podrá monitorear las actividades de los usuarios relacionadas con el ingreso a los sistemas de información y el uso de la red, el correo electrónico institucional y el servicio de Internet mediante logs de auditoría, para garantizar el cumplimiento de las políticas de seguridad de la información y prevenir cualquier riesgo de seguridad en la operación, servicio y funcionalidad de los sistemas informáticos de Mindeporte.

Para efectos de que Mindeporte disponga de una red con alto grado de confiabilidad, el GIT TIC's realizará el monitoreo de todos y cada uno de los equipos, sistemas y servicios informáticos. Los sistemas considerados críticos estarán bajo monitoreo permanente.

7.3 Responsabilidades

Todos los usuarios de los equipos, sistemas y servicios informáticos de Mindeporte son responsables del cumplimiento de cada una de las políticas de seguridad de la información y los jefes de las áreas deberán supervisar su cumplimiento.

Toda información confidencial de Mindeporte relacionada con los sistemas de información, deberá ser tratada bajo estricta seguridad y el personal a cargo de su manejo no está autorizado para revelarla a terceros.

Todos los empleados deberán observar y atender la normatividad sobre uso restringido de información confidencial, tal como información de personas naturales contemplada en la ley de habeas data y demás disposiciones sobre el tratamiento de datos personales.

Todos los empleados de Mindeporte deberán aplicar las recomendaciones dadas por el GIT TIC's sobre buenas prácticas de manejo de los equipos, sistemas y servicios informáticos de la entidad con el objetivo de minimizar la ocurrencia de incidentes de seguridad de la información en la entidad.

7.4 Sanciones

El incumplimiento de la política general de seguridad de la información aquí presentada puede acarrear consecuencias, tales como: la cancelación temporal de la cuenta de usuario del dominio cuenta de correo, servicio de Internet; y en algunos casos la suspensión definitiva de la misma.

En otros casos y dependiendo de la naturaleza de la acción se analizará el caso en particular y se adoptarán las medidas necesarias ante las instancias competentes de control disciplinario de la entidad.

Todas las acciones en las que se vea comprometida la seguridad de los sistemas informáticos de Mindeporte podrán ser sancionadas, aunque no estén previstas en esta política.

La protección de la información y de los datos está contemplada en el código penal colombiano mediante la Ley 1273 del 5 de enero de 2009 (Ley de Delitos Informáticos), con la que se pretende preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones penalizando conductas inapropiadas y sancionándolas penalmente.

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	26/Nov/2021	Se crea este nuevo documento en remplazo del GT-MN-002 Políticas de Seguridad de la Información con el fin alinearlo al nuevo modelo MIPG. Se realizan ajustes al documento en cuanto a redacción. Modificación del numeral 4.4.4., versión ISO 27001, capacidad envío correo. Se migra plantilla tipo "manual" a plantilla tipo "política". Se incorporan nuevos lineamientos, controles y consideraciones que se deben cumplir en materia de Seguridad de la información para la Entidad.
2	30/Sep/2022	Se realizó una actualización a la versión generada en el año 2021; ya que se debían incorporar nuevos controles y consideraciones que se deben cumplir en materia de Seguridad de la información para la Entidad; así como modificar algunos en su redacción.
3	06/Dic/2023	Se realizó actualización a la versión generada en el año 2022, dada la necesidad de actualizar algunas políticas, reorganizar la estructura de esta para mayor entendimiento y adicionar tres políticas adicionales que son: Política de Operaciones, Políticas de medios de almacenamiento y políticas de Gestión de Vulnerabilidades. Se elimina la política de acceso al sistema de información financiero SOA, dado que sobra porque hay una política ya establecida para el acceso a los sistemas.
4	27/May/2025	Se realizó una revisión a la versión generada en el año 2023; así como modificar el nombre de grupo de trabajo Mesa de Ayuda por Grupo de Soporte.

ELABORÓ	REVISÓ	APROBÓ
Ing. Carolina Rodríguez Forero Líder Seguridad de la Información	Ing. Leonardo Mejía Lobo Coordinador GIT TIC´s	Fabio Alberto Álzate Carreño Secretario General
Ing. Lorena Patricia Suárez Sierra Líder Seguridad de la Información y Ciberseguridad	Ing. Rocío Pabón Santana Coordinadora GIT TIC´s	Luis David Garzón Chaves Secretario General
Ing. Bernardo Angel Rios Santana Líder Seguridad de la Información y Ciberseguridad	Ing. Rene Mauricio Pinto Pedraza Coordinador GIT TIC´s	Miguel Antonio de la Hoz García Secretario General (E)