Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES

2025000825

POR MEDIO DE LA CUAL SE ADOPTA LA POLÍTICA DE ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN Y USO DE RECURSOS INFORMÁTICOS EN INDEPORTES ANTIOQUIA

El Gerente del Instituto Departamental de Deportes de Antioquia - de Indeportes Antioquia, en uso de sus atribuciones constitucionales, legales y reglamentarias, en especial las conferidas en la Ordenanza Departamental 8E del 1° de marzo de 1996,

CONSIDERANDO:

1. Que los activos de información son fundamentales, dada la importancia en la operación y en la gestión de la Entidad, como medio para alcanzar los objetivos estratégicos propuestos y que por ende traen inmersas grandes amenazas que comprometan la información tanto física como digital.

2. Que se deben implementar mecanismos para garantizar el cumplimiento de la normatividad vigente, en materia de derechos de autor y de la protección de la información y los datos.

3. Que Indeportes Antioquia, debe adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones.

4. Que los cambios en la configuración de la plataforma tecnológica de la Entidad y el cambiante panorama de riesgos y amenazas del sector TIC, hacen necesario la actualización de LA POLÍTICA DE ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN Y USO DE RECURSOS INFORMÁTICOS.

5. Que en virtud de la Resolución 2277 de 2025 del Ministerio de Tecnologías de la Información y las Comunicaciones, por la cual se actualizó el Anexo 1 de la Resolución 500 de 2021, INDEPORTES ANTIOQUIA adopta como referente la norma internacional ISO/IEC 27001:2022, en armonía con el principio de responsabilidad demostrada y reforzada.

6. Que, de igual forma, conforme al Decreto 1263 de 2022 y la Ley 2489 de 2025, se fortalece el enfoque de seguridad digital, transformación pública y protección integral de datos personales, garantizando la confidencialidad, integridad, disponibilidad y privacidad de la información administrada por la entidad.

7. Que las actualizaciones normativas refuerzan la estrategia de INDEPORTES ANTIOQUIA en seguridad digital, brindando un marco moderno y confiable para proteger los activos de información y asegurar la continuidad de servicios esenciales a la ciudadanía

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES

2025000825

8. Que la Resolución S 2025000814 DEL 03 DE SEPTIEMBRE DEL 2025 derogó la Resolución No. S 2025000448 del 16 de mayo de 2025 *"Por medio de la cual se deroga la resolución 2021000024 del 26 de junio de 2021 y la resolución 2023001322 del 29 de diciembre de 2023 y se adopta LA POLÍTICA GENERAL PARA LA SEGURIDAD DE LA INFORMACIÓN, LA SEGURIDAD DIGITAL, LA CIBERSEGURIDAD Y LA PROTECCIÓN DE LA PRIVACIDAD DE LOS DATOS PERSONALES DE INDEPORTES ANTIOQUIA.*".

9. Que mediante la Resolución S2025000814 DEL 03 DE SEPTIEMBRE DEL 2025 se incorpora el principio de responsabilidad demostrada y reforzada en el tratamiento de datos e información personal, como eje esencial para la fortalecer el Sistema de Gestión en Seguridad de la Información – SGSI y permita brindar el cumplimiento debido a las medidas técnicas, humanas y administrativas adoptadas en INDEPORTES ANTIOQUIA con destino a la seguridad.

10. Que al ser actualizada la política de tratamiento de datos en lo relativo a las medidas de seguridad que recaen sobre datos e información personal, debe ser objeto de articulación la política de seguridad de la información en pro de armonizarse como sistemas engranados, pero manteniendo su autonomía y alcance.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO 1. Adoptar la política de estándares de seguridad de la información y uso de recursos informáticos en INDEPORTES ANTIOQUIA

ARTÍCULO 2. OBJETIVO GENERAL: Actualizar el Sistema de Gestión de Seguridad de la Información en INDEPORTES ANTIOQUIA, determinando las políticas que lo rigen, con el fin de proteger la información contra una gran variedad de amenazas, minimizando el riesgo y asegurando la continuidad del servicio, acorde a los lineamientos definidos por el Departamento Administrativo de la Función Pública, el Ministerio de las TIC, el programa de Gobierno Digital y en coherencia con el Sistema de Gestión de Protección de Datos Personales – SGPDP.

ARTÍCULO 3. DEFINICIÓN DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN – SGSI: Las políticas institucionales son directivas con aceptación general, que constituyen un canal formal de actuación de los usuarios, en relación con los recursos y servicios tecnológicos disponibles en INDEPORTES ANTIOQUIA.

La política de seguridad de la información, en adelante, SGSI, constituye un compendio de procedimientos y compromisos de la Entidad, que le permiten actuar proactivamente ante situaciones que comprometan la integridad de los activos de información.

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

Las políticas por sí solas no constituyen una garantía para la seguridad; estas deben responder a intereses y necesidades organizacionales, que lleven a un esfuerzo conjunto de sus actores para administrar sus recursos y reconocer en los mecanismos de seguridad de la información, factores que faciliten la formalización y materialización de los compromisos adquiridos entre los usuarios y la Entidad.

ARTÍCULO 4. ALCANCE: Estas políticas están dirigidas al personal interno de la Entidad (servidores públicos, contratistas, entrenadores, deportistas, así como también a los residentes de las Villas deportivas: Antonio Roldán Betancur, Villa Náutica, CEDEP Urabá, Neiva-80 y las demás sedes que sean administradas por el Instituto). El alcance de dichos lineamientos también aplica a personas externas (usuarios no frecuentes y visitantes).

Todo usuario de los recursos tecnológicos, información y datos, en INDEPORTES ANTIOQUIA tiene un grado de responsabilidad a partir del momento que tiene autorización de acceso a la información y a los equipos o a los canales de comunicación Institucionales de los que hace uso. Acorde a lo descrito, los usuarios deberán conocer y aceptar estas directrices, por lo que el desconocimiento de este documento no exonerará a la persona de las responsabilidades adquiridas.

Además de las políticas generales dispuestas a cumplir en INDEPORTES ANTIOQUIA, se adoptarán las estrategias para la seguridad de la información definidas en la NTC ISO 27001:2022, y las que la Entidad disponga a partir del análisis de los riesgos de la seguridad de la Información.

La presente Política de Seguridad de la Información aplica a todos los procesos, dependencias, funcionarios, contratistas y terceros que tengan acceso, administren o utilicen activos de información de INDEPORTES ANTIOQUIA, en medios físicos o digitales, incluyendo plataformas externas vinculadas a la operación institucional (tales como sistemas de gestión documental, bases de datos en la nube o aplicativos de terceros).

ARTÍCULO 5. OBJETIVO ESPECÍFICO: El objetivo de este documento es implementar el sistema de gestión de seguridad de la información y, bajo la reglamentación del uso de los recursos tecnológicos, con el fin de incentivar mejores prácticas para su uso, minimizar los riesgos en materia de seguridad de la información y adoptar un código de conducta eficaz, con espíritu de autorregulación para el manejo y aprovechamiento de los recursos tecnológicos Institucionales.

Por lo tanto, la Entidad implementará, operará, monitoreará, revisará y mejorará permanentemente el sistema de gestión de seguridad de la información, en el contexto de su propia seguridad, para las actividades globales institucionales, de cara a los riesgos, buscando minimizar los impactos en la Entidad, en caso de cualquier tipo de interrupción de los servicios TIC.

Entre otras, la Entidad propende por:

- Establecer las políticas, procedimientos e instructivos en materia de seguridad

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

de la información.

- Fortalecer la cultura de seguridad de la información en los servidores de la Entidad, practicantes, contratistas y demás actores participes de la operación de la Entidad.
- Velar por la continuidad de los procesos de la Entidad.
- Minimizar los riesgos asociados a la seguridad de la información.
- Cumplir con los lineamientos establecidos por el Departamento Administrativo de la Función Pública, en lo concerniente al Modelo Integrado de Planeación y Gestión, y a la política de Gobierno en línea del Ministerio de Tecnologías de la Información y las Comunicaciones.
- Definir e implantar controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, y perdida de integridad, que respondan a la disponibilidad requerida por los usuarios o clientes externos de la Entidad.
- Proteger la información a la que se acceda y procese, para evitar su perdida, alteración, destrucción o uso indebido.
- Registrar y monitorear las violaciones a las políticas y controles de seguridad de la información, y a su vez reportarlas a la Oficina de Talento Humano, para que inicie las investigaciones pertinentes, de conformidad con el control disciplinario interno y con lo establecido en el Código Único Disciplinario.
- Incorporar prácticas de seguridad digital y ciberseguridad alineadas con la política de protección de datos personales.
- Fortalecer los procedimientos de gestión de incidentes de seguridad, asegurando coordinación con los responsables del SGPDP.
- Incluir al Equipo de Cumplimiento como instancia de verificación y seguimiento del cumplimiento normativo en materia de seguridad de la información.

ARTÍCULO 6. PRINCIPIOS FUNDAMENTALES DE LA SGSI: El sistema de gestión de seguridad de la información preserva la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo. Los siguientes son los conceptos sobre los cuales se diseñaron las políticas institucionales de seguridad de la información:

- **Responsabilidad en la contratación e individualización:** Este principio consiste en que cada persona es responsable de cada uno de sus actos, aun si tiene o no conciencia de las consecuencias, por lo que el Instituto deberá llevar a cabo las siguientes acciones:

    - Identificar los riesgos asociados al acceso, procesamiento, comunicación o gestión de la información y/o la infraestructura para su procesamiento, por parte de personas o Entidades externas, terceros y/o contratistas, con el fin de establecer los mecanismos de control necesarios para que la seguridad se mantenga.
    - Definir una cláusula de confidencialidad de la información, como parte integral de los contratos con personas o Entidades externas, terceros y/o contratistas, cuando deban tener acceso a la información y/o recursos de la Entidad; además, de no divulgar, usar o explotar la información confidencial

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información, teniendo en cuenta que cualquier violación a lo establecido en dicha cláusula será considerado como un "incidente de seguridad".
  - Identificar los riesgos a los que se encuentran expuestos los activos de información de la Entidad. Los riesgos de seguridad de la información analizados deben ser objeto de tratamiento (mitigar, transferir, evitar, aceptar), el cual debe ser coherente con los criterios de aceptación de riesgos.
  - Los riesgos deben ser monitoreados después de su tratamiento para asegurar que siguen estando en niveles aceptables para la Entidad.
  - Incluir este documento como parte integral del procedimiento de Inducción y reinducción de la Entidad y de la Oficina de Sistemas e Informática de INDEPORTES ANTIOQUIA.

- **Autorización:** Lo constituyen las reglas explícitas acerca de quién puede hacer qué. Es decir, de qué manera cada usuario puede utilizar los recursos informáticos. Los activos de información disponibles para los servidores públicos, contratistas y/o terceros, para su uso, operación y/o custodia, de acuerdo con las funciones específicas y necesidades del trabajo a realizar son propiedad exclusiva de la Entidad.

- **Mínimo privilegio:** Este principio indica que cada usuario debe estar autorizado a disponer únicamente de los recursos que requiera para realizar su trabajo, de acuerdo con sus funciones o actividades contractuales. Acoger este principio, además de constituirse en una medida de seguridad, facilita además la prestación de los servicios por parte del personal de la Oficina de Sistemas e Informática.

- **Separación de obligaciones:** Este principio establece que las actividades de un procedimiento deben ser distribuidas entre varias personas, con el fin de minimizar las posibilidades de error y/o ataques a la seguridad. Este principio facilita la aplicación de controles, el monitoreo y fortalece la transparencia administrativa.

- **Auditoría:** Todas las actividades y todas las personas que intervienen en las PSI deben poder ser auditadas, desde el inicio, hasta el final del proceso, e incluso, después de terminado, para garantizar que los datos no sean alterados durante o después de terminados los trámites.

- **Redundancia**: Este principio establece que la distribución y configuración de los recursos debe facilitar la restauración del servicio en caso de interrupciones fortuitas. Para eso, tanto los equipos como los programas y sus datos deben tener un respaldo. La configuración y el alcance de la redundancia se establece en el plan de contingencia y continuidad de la información. Se busca tener redundante lo que más afecte el servicio, por eso se configuran los servidores de autenticación como principal y secundario, se dispone de copias de respaldo por fuera de la Entidad y se establecen servicios en la nube, donde los proveedores garanticen su disponibilidad.

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, Entidades o procesos no autorizados.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, Entidades o procesos autorizados cuando lo requiera.
- **Responsabilidad demostrada y reforzada**: la Entidad acredita y documenta permanentemente el cumplimiento normativo en seguridad de la información.
- **Prevención y gestión del riesgo**: las medidas de seguridad se diseñan con base en análisis de riesgos, mitigación y continuidad del negocio.
- **Interoperabilidad y seguridad digital**: se garantizan condiciones técnicas y organizativas para la protección de la información en entornos interoperables y digitales, conforme al Decreto 1263 de 2022.
- **Privacidad desde el diseño y por defecto**: se implementan mecanismos que aseguran la protección de datos personales y la privacidad en cada proyecto, proceso o sistema tecnológico desde su concepción.

ARTÍCULO 7. ROLES Y RESPONSABLES

7.1. Comité: El Comité de Gestión y Desempeño ejercerá la función de máximo órgano de dirección en materia de seguridad de la información, apoyado por el Subcomité de Protección de Datos Personales, el cual cuenta con un Equipo de Cumplimiento dependiente de la Oficina de Sistemas e Informática. Dicho equipo es responsable de liderar y coordinar, junto con contratistas especializados, el cumplimiento del Sistema de Gestión en Seguridad de la Información – SGSI y el Sistema de Gestión en Protección de Datos Personales – SGPDP.

7.2. Oficina de Sistemas e Informática: La Oficina de Sistemas e Informática asumirá el liderazgo operativo de la seguridad de la información, la seguridad digital y la gestión de incidentes, articulando las actividades del Equipo Técnico TIC y del Equipo de Cumplimiento. En desarrollo de este rol, coordinará el cumplimiento de las políticas, lineamientos y estándares internacionales (ISO/IEC 27001:2022) en toda la entidad.

7.3. Oficial de Seguridad de la Información: El Oficial de Seguridad de la Información dependerá funcionalmente de la Oficina de Sistemas e Informática. Tendrá como responsabilidad principal coordinar, implementar y supervisar el Sistema de Gestión de Seguridad de la Información – SGSI, asegurando su alineación con la normativa vigente y con el Sistema de Gestión de Protección de Datos Personales – SGPDP.

Sus funciones serán, entre otras:

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

- Elaborar y mantener actualizado el mapa de riesgos de seguridad de la información de la entidad.
- Coordinar la implementación de controles técnicos, organizativos y administrativos para proteger los activos de información.
- Gestionar, junto con el Equipo de Cumplimiento, los procesos de evaluación y auditoría del SGSI.
- Liderar la respuesta institucional ante incidentes de seguridad de la información, garantizando su adecuada documentación y cierre.
- Servir de enlace entre la Gerencia, el Subcomité de Protección de Datos Personales y las diferentes dependencias en materia de seguridad digital y ciberseguridad.
- Velar por la adopción de la norma ISO/IEC 27001:2022 en todos los procesos y sistemas de información de la entidad."

ARTÍCULO 8. MEDIDAS DE SEGURIDAD Y GESTIÓN DE INCIDENTES: INDEPORTES ANTIOQUIA adopta medidas administrativas, técnicas, físicas y jurídicas que garanticen la confidencialidad, integridad, disponibilidad y privacidad de la información, así como la resiliencia de los sistemas que la soportan. Estas medidas se implementan bajo un enfoque basado en riesgos y conforme a lo establecido en la norma ISO/IEC 27001:2022 y en la Resolución 2277 de 2025, asegurando que su aplicación sea proporcional a la criticidad del activo y al nivel de riesgo identificado.

ARTÍCULO 9. GESTIÓN DE INCIDENTES DE SEGURIDAD: Todo incidente de seguridad deberá ser reportado de manera inmediata al Oficial de Seguridad de la Información, quien coordinará su atención junto con el Oficial de Protección de Datos Personales cuando el incidente afecte información personal.

Los procedimientos internos garantizarán:

- La detección, reporte y registro oportuno de incidentes.
- La trazabilidad de las acciones adoptadas y de los responsables de su atención.
- La notificación a la Superintendencia de Industria y Comercio y a los titulares de la información, cuando la normativa lo exija.
- La documentación de lecciones aprendidas para fortalecer el SGSI y el SGPDP.
- El Equipo de Cumplimiento consolidará informes semestrales de incidentes para conocimiento del Subcomité de Protección de Datos y del Comité de Gestión y Desempeño."

ARTÍCULO 10. CONTROLES ESPECÍFICOS POR SISTEMAS Y BASES DE DATOS: Los controles de seguridad aplicarán de manera diferenciada según la naturaleza de los datos y activos de información:

- Para información institucional, se aplicarán mecanismos de seguridad digital, control de accesos, copias de seguridad, trazabilidad de transacciones y gestión documental segura.
- Para datos personales, se garantizarán medidas específicas de privacidad desde el diseño y por defecto, incluyendo cifrado de información sensible, autenticación reforzada, gestión de roles, acuerdos de confidencialidad y auditorías periódicas.
- En todos los casos, el diseño e implementación de sistemas, aplicativos o procesos tecnológicos deberán incorporar la seguridad de la información y la protección de datos

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

como requisitos desde su concepción."

ARTÍCULO 11. RESPONSABILIDAD DE USUARIOS EN LA SEGURIDAD: Todos los usuarios de la infraestructura tecnológica y de información institucional son responsables de custodiar sus credenciales, cumplir los protocolos de acceso seguro y reportar inmediatamente cualquier anomalía que pueda constituir un incidente de seguridad. El incumplimiento de estas obligaciones será considerado falta disciplinaria o contractual, de conformidad con la normatividad vigente y de acuerdo con los términos descritos a continuación:

1. RED CORPORATIVA:

La red Institucional esta segmentada para independizarla según los usuarios, conexiones con terceros y del servicio de acceso a Internet y determinar las conexiones y servicios. La red cableada es únicamente para uso exclusivo de los equipos propiedad de INDEPORTES. Para los diferentes usuarios, terceros y personal externo se cuenta con las redes inalámbricas empleados, invitados y expositores según el perfil y necesidad de cada uno.

Los equipos de cómputo de los servidores públicos de la Entidad deberán estar siempre conectados a la red CORPORATIVA, ya sea de forma inalámbrica o cableada. En el caso de los contratistas y demás usuarios, deben estar en la red corporativa únicamente si utilizan equipos propiedad de INDEPORTES ANTIOQUIA.

Cualquier tipo de conexión a la red CORPORATIVA de la Entidad ya sea cableado o wifi se realizará únicamente desde los equipos de cómputo asignados a los servidores públicos y/o contratistas por el personal de la Oficina de Sistemas e Informática. Los equipos personales, así como los invitados, y deportistas podrán conectarse únicamente a las redes wifi, disponibles para ellos.

La conexión a las aplicaciones de la Entidad como el ERP SICOF que no cuenten con conexiones con cifrado de seguridad, deberá realizarse siempre desde la red corporativa, directamente o por medio de VPN.

2. USO Y CUIDADO DE LOS ACTIVOS DE INFORMACIÓN:

Todos los funcionarios de la Entidad, para el desarrollo de sus funciones deberán utilizar únicamente los equipos asignados desde la Oficina de Sistemas e Informática. No está permitido utilizar equipos personales o diferentes a los asignados, por el riesgo asociado a la legalidad del uso de software y/o al hecho de no poder implementar los controles de seguridad establecidos por INDEPORTES ANTIOQUIA.

La instalación de los equipos de cómputo y/o accesorios (computadores, servidores, estaciones de trabajo, portátiles, impresoras, scanners, switches, APs, teléfonos, cables y puntos de red UTP), sean éstos propiedad de INDEPORTES ANTIOQUIA o en calidad de arrendamiento, sólo podrá realizarse por parte del personal de la Oficina de Sistemas e Informática de la Entidad, quien puede ser acompañado de personal técnico experto.

Ningún usuario está autorizado para hacer, por su propia cuenta, reubicación de los equipos de cómputo a su cargo, ni tampoco puede hacer una reasignación de estos, sin el aval técnico de la Oficina de Sistemas e Informática; una vez se cuente con dicho concepto, se

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

procederá a oficializar el traslado del bien con conocimiento del ALMACÉN, a través del procedimiento que este último tenga definido para tal fin.

En caso de requerir salida de equipos se acogerán las disposiciones de la subgerencia administrativa y financiera (Ver procedimiento para la salida de equipos y utilizar el Formato asociado). Todos los equipos de cómputo deben estar cubiertos por la póliza de todo riesgo de la entidad y tener cobertura móvil.

Los usuarios no deben intentar, por su cuenta, hacer reparaciones a los equipos de cómputo. No están autorizados para instalar, reemplazar o retirar partes de estos.

Cada usuario es responsable de apagar los equipos que estén a su cargo cuando finalice la jornada de trabajo.

Los usuarios deben bloquear y utilizar el protector de pantalla del computador durante los momentos en que se encuentre desatendido computador, el propósito es evitar el uso y acceso no autorizado de personal ajeno en su estación de trabajo y que pueda hacer uso indebido de los recursos informáticos en su nombre o consultar información, para la cual no están autorizados.

El procedimiento de bloqueo de pantalla se dicta en la inducción al personal. Además del bloqueo automático, está configurado un bloqueo automático después de diez (10) minutos de inactividad.

Los usuarios deben notificar a la Oficina de Sistemas e Informática, a través de la herramienta tecnológica mesa de servicios, cualquier solicitud, petición, incidente o problema con los recursos tecnológicos que operan, quien gestionará la intervención de personal interno o externo para la solución de la situación reportada.

No deben ponerse elementos como plantas, bebidas o alimentos cerca a los equipos de cómputo, ni bloquear las rejillas de ventilación.

En los tomas-regulados (color naranja) sólo deben conectarse los equipos de cómputo. En especial no pueden conectarse ventiladores, radios, planchas, neveras, tajalápiz ni extensiones eléctricas a dichos circuitos, toda vez que pueden causar interferencias o sobrecargas de energía que pueden afectar el buen funcionamiento de los equipos.

Los equipos asignados a los usuarios deben ser utilizados solamente para actividades propias de INDEPORTES ANTIOQUIA. Ningún equipo podrá usarse para actividades personales o académicas, tales como consultas de internet de carácter personal, redacción de documentos personales, capacitaciones virtuales que no sean de carácter institucional, con el fin de proteger los activos de información en términos de la integridad, confidencialidad y disponibilidad.

La Oficina de Sistemas e Informática, será la responsable de la identificación y clasificación de los activos de información, para establecer los mecanismos de protección correspondientes.

Se debe restringir el acceso a los documentos físicos y digitales según las normas

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

aplicables internas y/o externas, y a los permisos determinados de acuerdo con las funciones del perfil de cargos.

Toda la información de los procesos de la Entidad, así como los activos donde ésta se almacena y se procesa, están:

- Inventariados.
- Asignados a un responsable.
- Protegidos y clasificados; de acuerdo con la clasificación se deben establecer los niveles de protección, orientados a determinar a quién se le permite el manejo de la información, el nivel de acceso a la misma y los procedimientos para su manipulación.

La Oficina de Sistemas e Informática, deberá revisar la identificación y la clasificación de los activos de información anualmente y/o cuando se presenten cambios que puedan afectar las mismas.

Se deberán proteger adecuadamente todos los equipos que hacen parte de la infraestructura tecnológica de la Entidad para prevenir la pérdida, el daño, robo o los accesos no autorizados; y ubicarlos alejados de sitios que puedan tener amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética, vandalismo, entre otros. Los equipos de cómputo siempre deben estar asegurados con la respectiva guaya de seguridad.

Siempre que se reasigne un equipo de cómputo, se debe realizar previamente un borrado seguro de la información almacenada y realizar formateo en dichos equipos antes que sean entregados a los nuevos usuarios, a no ser que dicha información sea requerida para el desarrollo de las funciones del nuevo usuario a cargo del equipo.

De forma previa al proceso de disposición final (por ejemplo: venta, donación o destrucción), se debe realizar borrado seguro de los equipos, verificar que no contengan información almacenada, para asegurar que cualquier dato sensible o software con licencia, haya sido retirado o sobrescrito en forma segura y verificar que los equipos no contengan el medio de almacenamiento, con información clasificada o confidencial.

Los medios de almacenamiento que contienen información confidencial o protegida por derechos de autor se deben destruir físicamente, eliminar o sobrescribir usando técnicas para hacer que la información original no sea recuperable, en vez de usar la función estándar borrar o formatear.

Los servidores deben estar ubicados de modo que se reduzcan los riesgos generados por amenazas del entorno (es decir, evitando daños derivados de situaciones como manifestaciones sociales, inundaciones, humedad o incendio), siempre en el cuarto técnico central de la Entidad en la sede administrativa, con las condiciones de temperatura y acomodación adecuadas.

Escritorios Limpios:

Pantalla limpia y equipo desentendido:

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

- La pantalla (escritorio) de los dispositivos de cómputo propiedad de INDEPORTES ANTIOQUIA debe estar libre de íconos y/o de accesos directos a información. Estos deben ser almacenados en el repositorio en nube, asignado por INDEPORTES ANTIOQUIA a cada funcionario.
- Los equipos de cómputo propiedad de INDEPORTES ANTIOQUIA, mantienen como política el bloqueo de sesión para un tiempo de inactividad de 10 minutos.
- Cuando están desatendidos, los computadores y terminales se deben dejar fuera del sistema o proteger con un sistema de bloqueo de la pantalla y el teclado, controlado por una contraseña y mecanismo similar de autenticación de usuario, y deben estar protegidos por bloqueo de teclas u otros controles, cuando no están en uso.
- Es responsabilidad del usuario del equipo de cómputo, realizar el bloqueo del equipo, cada vez que éste se vaya a ausentar de su puesto de trabajo a través del uso las teclas **Control+ Al t+ Suprimir al mismo tiempo.**
- Al ausentarse de su puesto de trabajo y al finalizar la jornada laboral, los funcionarios y contratistas de INDEPORTES ANTIOQUIA deben asegurarse que sus escritorios se encuentren libres de los documentos o medios removibles utilizados durante el desarrollo de sus funciones y que estos sean almacenados bajo la protección de seguridad necesarias conforme a la clasificación de la información.

3. INVENTARIO DE EQUIPOS:

La Oficina de Sistemas e Informática, lleva un registro o inventario de todos los equipos de cómputo, donde se especifican los datos del equipo, configuraciones, accesorios y el funcionario y/o contratista responsable, que es quien utiliza el equipo, constituyéndose en elemento de seguridad, control y apoyo a la gestión del almacén en material de circulación de los bienes tecnológicos.

La Oficina de Sistemas e Informática deberá hacer entrega formal del equipo al respectivo usuario y dejar registrada dicha entrega en un formato firmado y diligenciado por ambas partes.

El almacén es el encargado de realizar el registro de asignación del bien en el software ERP de la entidad. El usuario debe verificar que se le haga entrega de todos los elementos que componen el equipo y/o elemento que se reflejan en el documento. Los equipos de cómputo y demás elementos de tecnología quedan asignados a la cartera de cada Servidor Público y el Supervisor de cada contratista será el único responsable y quien deberá garantizar el buen uso de este.

Cualquier daño en los computadores debe ser reportado a la mesa de servicios, para que los técnicos procedan con su revisión y se asigne un equipo de forma provisional o permanente según el estado del bien afectado, mientras se ejecuta el procedimiento que se determine en la política de bienes de la Entidad, para definir la reparación o sustitución del bien según proceda.

Los activos de información dentro del alcance de la seguridad de la información están identificados y clasificados. Se definen responsabilidades sobre los activos de información de acuerdo con las necesidades de las partes interesadas y con la legislación aplicable, requisitos legales, técnicos, operativos y de gestión aplicables.

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

Los activos de información se caracterizan bajo una metodología de identificación, clasificación, valoración, disposición documental, publicación, seguimiento y mejora, de los activos de información arrendados o propios, los cuales desarrolla o produce y comparte INDEPORTES ANTIOQUIA, de acuerdo con las necesidades de las partes interesadas y de acuerdo con la legislación aplicable, requisitos legales, técnicos, operativos y de gestión aplicables.

4. MANTENIMIENTO DE EQUIPOS:

El mantenimiento preventivo y/o correctivo de los equipos será programado por la Oficina de Sistemas e Informática y se realizará sólo bajo la supervisión de los servidores públicos y/o contratistas de dicha Oficina.

5. UBICACIÓN DE EQUIPOS:

Los usuarios deben reportar a la Oficina de Sistemas e Informática, la necesidad de mover o reubicar equipos de cómputo y/o accesorios, quienes verificarán las condiciones mínimas para su funcionamiento (punto de red, corriente regulada, seguridad física) en el nuevo sitio indicado.

El acceso a los equipos especializados conectados a la red (servidores, discos duros de respaldo, switches, APs, entre otros), es exclusivo para los servidores públicos y/o contratistas de la Oficina de Sistemas e Informática.

Ningún usuario está autorizado para manipular los elementos de red o comunicaciones situados en áreas públicas, o los que estén situados cerca a su puesto de trabajo. Si se observa algo inusual, tal como ruido, fuego, desajustes, debe reportar inmediatamente a la mesa de servicios.

Para los equipos utilizados en teletrabajo se acogerá a lo establecido en la política de teletrabajo de la entidad.

6. SOFTWARE:

La Oficina de Sistemas e Informática, es la encargada y responsable de realizar seguimiento y control anual al licenciamiento del software y aplicaciones de la Entidad; y por ende los funcionarios adscritos a esta Oficina, son los únicos autorizados para instalar o desinstalar aplicaciones, software o cualquier tipo de software en los equipos institucionales.

Todas las compras, contrataciones, desarrollos o suscripciones de software o desarrollos que se requieran realizar en la Entidad, deberán ser realizadas desde la Oficina de Sistemas e Informática, independiente de la fuente de los recursos o del proyecto de inversión, y todas deben llevar el visto bueno del Jefe de la Oficina.

Todo software que deba ser instalado en la plataforma institucional, debe ser evaluado por la Oficina de Sistemas e Informática, sea éste en calidad de donación, prueba, convenio interinstitucional, adquisición o suscripción.

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

Los usuarios deberán reportar a la Oficina de Sistemas e Informática, las necesidades de software, con el fin de evaluar y tramitar el licenciamiento respectivo. Esta Oficina será la única autorizada para adelantar los procesos de contratación que tengan que ver con tecnologías de información o comunicaciones.

Los únicos servidores públicos y/o contratistas autorizados parar realizar instalación y desinstalación de programas, así como cambios de configuración en el Sistema Operativo, son los adscritos a la Oficina de Sistemas e Informática. En caso de detectar software instalado en los equipos de cómputo que no tenga licencia de uso, este será desinstalado y a su vez se reportará a la Oficina de Talento Humano, para que inicie las investigaciones pertinentes de conformidad con el control disciplinario interno y con lo establecido en el Código Único Disciplinario, por lo que las consecuencias de todo tipo serán asumidas por el servidor público responsable del equipo de cómputo.

Será responsabilidad de la Oficina de Sistemas e Informática generar periódicamente una revisión del software instalado en los equipos de cómputo, para validar que cumplan con los licenciamientos y/o autorizaciones respectivas. Toda instalación, configuración, mantenimiento y actualización de hardware y software, debe ser realizada o autorizada por la Oficina de Sistemas e Informática.

Es responsabilidad de la Oficina de Sistemas e Informática mantener actualizadas y vigentes las licencias del software instalado en los equipos.

Es responsabilidad de la Oficina de Sistemas e Informática mantener actualizado el antivirus en todos los equipos de cómputo y servidores.

7. CONTROL DE ACCESO:

La Oficina de Sistemas e Informática, es la encargada de crear los usuarios en el dominio de INDEPORTES ANTIOQUIA, así mismo, todos los equipos conectados a la red corporativa deben estar en el dominio.

El nombre del usuario del dominio Institucional se creará conformado por la inicial del primer nombre seguida por el primer apellido del respectivo usuario, en caso de que ya se encuentre creado un usuario que coincida con dichos valores, se buscará una combinación factible, usando el segundo nombre o apellido.

A los siguientes aplicativos institucionales se accederá utilizando las credenciales del dominio de forma unificada:

- Acceso a la red (Log-in del equipo).
- Office 365 (Correo electrónico, OneDrive, teams y herramientas ofimáticas).
- Plataforma Mesa de servicios.

Se definirán roles y responsabilidades, frente al nivel de acceso y los privilegios de los servidores públicos y contratistas que tengan acceso a la infraestructura tecnológica y a los sistemas de información de la Entidad, con el fin de reducir y evitar el uso y el acceso no autorizado o modificación sobre los activos de información de la Entidad.

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

Se implementarán reglas de control de acceso para todos los sistemas de disponibilidad crítica o media de la Entidad, de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

Se establecerán controles duales sobre el nivel de súper usuario de los sistemas de información, de tal forma que exista supervisión a las actividades realizadas por el administrador del sistema.

Se deben establecer medidas de control de acceso físico en el perímetro que puedan ser auditadas, así como procedimientos de seguridad que permitan proteger la información, el software y el hardware de daños intencionales o accidentales para todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones.

En general, el control de acceso se aplica así:

- Se cuenta con un proceso formal de registro y cancelación del registro del usuario.
- Para las aplicaciones de la Entidad se definen los requisitos de seguridad.
- Se debe establecer la coherencia entre los derechos de acceso y las políticas de clasificación de información de los sistemas y redes.
- La legislación pertinente y cualquier obligación contractual concerniente a la limitación del acceso a datos o servicios aparece en el normograma de la Entidad.
- La gestión de los derechos de acceso en un entorno distribuido y en red, que reconoce todos los tipos de conexiones disponibles como VPN, enlaces publicados por la Oficina de Sistemas e Informática.
- La separación de los roles de control de acceso, solicitud de acceso, autorización de acceso y administración del acceso las realiza la Oficina de Sistemas e Informática.

8. CONTROL DE ACCESO REMOTO:

La Oficina de Sistemas e Informática, es la única dependencia que puede autorizar el acceso remoto a los recursos de red cuando se requiera, para que los proveedores de los aplicativos específicos brinden asesoría, diagnostiquen la causa de algún mal funcionamiento, realicen labores de actualización de la plataforma o hagan algún ajuste en la configuración, indispensable para el buen funcionamiento y la disponibilidad de los servicios.

La Oficina de Sistemas e Informática, es la encargada de asignar las claves de acceso temporales y realizar la conexión con el proveedor respectivo.

INDEPORTES ANTIOQUIA utiliza certificados SSL/TLS en versión más reciente para proteger las conexiones remotas a la infraestructura tecnológica de la Entidad, las cuales serán otorgadas de acuerdo con las necesidades de seguridad de cada plataforma y previa autorización de la Oficina de Sistemas e Informática. Será responsabilidad de cada usuario velar por la seguridad, confidencialidad e integridad de la información a la que tiene acceso de forma remota.

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

El acceso remoto a los equipos y dispositivos de la plataforma de TI sólo está permitido para labores de soporte técnico autorizado.

El acceso remoto a plataformas de tecnología de la información de INDEPORTES ANTIOQUIA debe ser realizado a través de VPN u otros medios que garanticen la seguridad en la comunicación.

Los administradores de los sistemas de información y de la plataforma tecnológica, son los responsables de verificar periódicamente los privilegios de acceso. Para asignar o derogar permisos deben tener la aprobación del Jefe inmediato.

9. ACCESO A LOS SISTEMAS DE INFORMACIÓN:

A los Sistemas de Información sólo tendrán acceso los usuarios de INDEPORTES ANTIOQUIA que sean titulares de una cuenta del dominio y que tengan la autorización del área responsable de administrar el Sistema de Información en particular.

Los Jefes inmediatos de los Servidores Públicos o los Supervisores de los contratistas deben realizar las solicitudes de creación de usuario de los diferentes sistemas de la Entidad, por medio del aplicativo de mesa de servicios de la Entidad, especificando las necesidades de acceso a los respectivos sistemas de información. La Oficina de Talento Humano es la encargada de solicitar los permisos y accesos iniciales que requiere el funcionario, según el manual de funciones del cargo en que es nombrado.

Una vez recibido y validado el requerimiento, se procede a crear y/o modificar el usuario. La Oficina de Sistemas e Informática, coordinará las capacitaciones a los usuarios para el ingreso y operación de la respectiva aplicación.

El control de acceso a cada sistema de información será determinado de acuerdo con la Oficina responsable de generar y procesar los datos involucrados. La Oficina de Talento Humano y/o cada Supervisor es el responsable de informar a la Oficina de Sistemas e Informática, cuando los usuarios terminen el vínculo laboral o contractual con la Entidad por medio de la mesa de servicios, indicando la fecha de retiro del servidor público o el contratista, indicando si se requiere realizar y guardar copia del backup de la información.

10. GESTIÓN DE CONTRASEÑAS:

La Oficina de Sistemas e Informática, asignará una contraseña inicial que será informada al usuario para realizar el primer acceso al sistema. La primera vez que el usuario acceda a la red, deberá cambiar la contraseña, utilizando como mínimo seis (6) caracteres alfanuméricos y utilizando mínimo una (1) letra mayúscula, una (1) minúscula, números y caracteres especiales como por ejemplo @!#$%&*.

La gestión de contraseñas debe:

- Hacer cumplir el uso de identificaciones y contraseñas de usuarios individuales para mantener la rendición de cuentas.
- Permitir que los usuarios seleccionen y cambien sus propias contraseñas e incluyan un procedimiento de confirmación, cuando están conectados en la red corporativa

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

de la Entidad.

- Exigir que se escojan contraseñas de calidad utilizando como mínimo seis (6) caracteres alfanuméricos y utilizando mínimo una (1) letra mayúscula, una (1) minúscula, números y caracteres especiales como por ejemplo @!#$%&*.
- Obligar a los usuarios cambiar sus contraseñas cuando ingresan por primera vez.
- Exigir que se cambien las contraseñas en forma regular, cada treinta (30) días calendario.
- Llevar un registro de las contraseñas usadas previamente, e impedir su reúso.
- No permitir la visualización ni la predeterminación de las contraseñas en la pantalla cuando se está ingresando a cualquier plataforma.

La vigencia de dicha contraseña será de treinta (30) días calendario y/o en los intervalos que defina la Oficina de Sistemas e Informática. Después de este período, el sistema automáticamente solicitará cambio de contraseña. Durante el cambio de contraseña, el sistema no permite asignar la misma clave hasta después de seis (6) claves utilizadas previamente.

Las contraseñas no deben basarse en información personal como: fechas de cumpleaños, direcciones, números telefónicos, nombres de personas, números de documentos de identificación y/o nombre de la Entidad.

Las contraseñas de acceso a la red o de ingreso a los respectivos aplicativos (Intranet, Mercurio, ERP, entre otros), son de carácter personal e intransferible. El usuario se hace responsable del mal uso que pueda darse de los equipos de cómputo y/o accesorios o programas a su cargo, si divulga, comparte o deja en lugar público las contraseñas de acceso.

Los usuarios son responsables de todas las actividades realizadas con su cuenta de usuario, del dominio o cuenta de aplicativos y sus claves personales.

La Oficina de Sistemas e Informática, podrá restablecer la contraseña de un usuario sólo mediante solicitud del propio usuario o mediante solicitud de su Jefe inmediato o Supervisor, por medio de un requerimiento en la mesa de servicios. El Jefe inmediato que autorizó el cambio de contraseña debe notificarle al usuario cuando éste regrese a su sitio de trabajo, para que pueda ingresar nuevamente y asignársele una nueva contraseña.

La vigencia de la cuenta de dominio está determinada por el tiempo de vinculación del usuario con la Entidad. La Oficina de Sistemas e Informática, hará depuraciones periódicas para garantizar la desactivación de los usuarios que se desvinculan o terminan su contrato. La Oficina de Talento Humano será la encargada de notificar a la Oficina de Sistemas e Informática todas las novedades que se presenten para realizar las copias de seguridad, activaciones y/o desactivaciones, según corresponda. En el caso de contratistas, será responsabilidad de cada Supervisor notificar las novedades con el contrato.

Todo usuario que utilice los recursos de los sistemas y de red, tiene la responsabilidad de velar por la integridad, disponibilidad y confidencialidad de la información que maneje.

11. PRIVILEGIOS DE NAVEGACIÓN:

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

Todos los usuarios de INDEPORTES ANTIOQUIA estarán asociados a un GRUPO de navegación, el cual dispone de los servicios de internet requeridos de acuerdo con su cargo.

Los grupos establecidos en la Entidad son los siguientes:

- NAVEGACION_ORO.
- NAVEGACION_PLATA.
- NAVEGACION_BRONCE.

Cada grupo tiene configurado un perfil que le asigna las categorías permitidas y las URL específicas de ciertas categorías no permitidas que se autorizan, de acuerdo con los requerimientos institucionales.

Por defecto todos los usuarios se asignarán al perfil BRONCE, a excepción de los directivos que se asignarán al perfil ORO. En caso de requerir permisos adicionales de navegación, el Jefe directo del servidor público deberá realizar el respectivo requerimiento en la "mesa de servicios" de la Entidad, indicando el perfil al cual se debe asociar el usuario, la necesidad y justificación de esta.

La configuración de los grupos es dinámica y se actualiza conforme a las necesidades Institucionales y a las actividades particulares asignadas a los usuarios, con la debida sustentación de la necesidad.

Los usuarios no podrán consultar o actualizar las redes sociales o sitios de streaming de audio y video, excepto los que, por razón de sus actividades institucionales, estén encargados de dicha actividad. Para realizar la autorización el jefe inmediato del servidor público que requiera acceso deberá realizar la solicitud por medio del aplicativo de mesa de ayuda indicando la necesidad de acceder a este tipo de contenidos por parte del funcionario.

12. **ALMACENAMIENTO DE INFORMACIÓN:** La Entidad dispone de un servidor exclusivo para almacenar información de:

- Respaldo de la información de servidores públicos retirados.
- Respaldo de buzones de correo de servidores públicos retirados, entre otros.
- Respaldo en la nube para buzones de correo, cuentas de One Drive y sitios de SharePoint priorizados.

La información de trabajo de todos los usuarios deberá ser almacenada en la carpeta personal de OneDrive asignada con su cuenta de Office 365. Nunca se deberá almacenar información en el disco local del computador.

13. **PROTECCIÓN PERMANENTE CONTRA SOFTWARE MALICIOSO:**

Todos los recursos informáticos estarán protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware, antimalware y otras aplicaciones que brinden protección contra los diferentes tipos de amenazas actuales.

La protección contra los códigos maliciosos se deberá basar en software de detección de códigos maliciosos y de reparación, en toma de conciencia sobre la seguridad de la

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

información, y en controles apropiados de gestión de cambios y de acceso al sistema, por lo que se establecen las siguientes directrices:

- Se establece una política formal que prohíbe el uso de software no autorizado.
- Se implementan controles para evitar o detectar el uso de software no autorizado (sólo se autoriza por la Oficina de Sistemas e Informática).
- Se implementan controles para evitar o detectar el uso de sitios web maliciosos o que se sospecha que lo son (por ejemplo, listas negras).
- Se protege de manera formal para abordar los riesgos asociados con la obtención de archivos y de software, ya sea mediante redes externas o cualquier otro medio, indicando qué medidas externas se deben tomar.

Será responsabilidad de la Oficina de Sistemas e Informática, velar por la instalación y uso de las herramientas de seguridad, así como de su actualización permanente. Ningún usuario podrá deshabilitar o desinstalar en ninguna circunstancia dichos aplicativos.

Está totalmente prohibido escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.

14. CONTENIDO PÁGINA WEB E INTRANET:

La Oficina Asesora de Comunicaciones, es la responsable de realizar las publicaciones en los diferentes portales de la Entidad, y por tanto debe revisar todo el material que deba ser publicado en la Página Web o en la Intranet y realizar los ajustes de estilo pertinentes.

La Oficina Asesora de Comunicaciones, es la responsable de las redes sociales (Twitter, Facebook, YouTube, Instagram, LinkedIn, etc.), por lo que se deben tener reglas de seguridad habilitadas como tener el doble factor de autenticación habilitado y otras más que permitan blindar, el activo vital de la Entidad, como lo es la información publicada.

El usuario que genere cada contenido debe velar por el respeto de la Ley de derechos de autor, hacer las citas que referencien material creado por terceros y tramitar las autorizaciones pertinentes para citar, referenciar o hacer hipervínculos a dichos contenidos. Se debe cumplir con los mismos requisitos que se aplican a los contenidos impresos.

El usuario que genere cada contenido debe contar con el apoyo de la Oficina Asesora Jurídica referente al cumplimiento de la legislación aplicable como Ley de derechos de autor, Ley de protección de datos personales y las que se identifique en el NORMOGRAMA. El autor debe realizar las citas bibliográficas que referencien material creado por terceros y tramitar las autorizaciones pertinentes para citar, referenciar o hacer hipervínculos a dichos contenidos. Se debe cumplir con los mismos requisitos que se aplican a los contenidos impresos.

Cada área de la Entidad es responsable por la publicación de la información requerida de acuerdo con la Ley de transparencia y acceso a la información pública.

Únicamente la Oficina de Sistemas e Informática es la autorizada para comprar dominios, hostings y habilitar páginas web a nombre de INDEPORTES ANTIOQUIA o cualquiera de

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

sus programas.

15. CORREO ELECTRÓNICO INSTITUCIONAL:

Todos los funcionarios de la Entidad deberán enviar y recibir la información corporativa exclusivamente desde la cuenta de correo que la Oficina de Sistemas e Informática proporciona. El uso del correo electrónico proporcionado por el instituto es para uso exclusivamente de las funciones desarrolladas en el cargo.

La cuenta de correo electrónico institucional será solicitada por medio de la plataforma mesa de servicios, por la Oficina de Talento Humano detallando el nombre (anexar cédula de ciudadanía), dependencia donde labora y cargo a ocupar por la persona a la cual se le va a asignar la cuenta. De igual manera, dicha Oficina debe informar cuando la cuenta del usuario deba ser desactivada. Para el caso de los contratistas, dicha solicitud la debe realizar el Supervisor del contrato, con la misma información requerida, previa verificación de la necesidad de uso de dicha herramienta.

El usuario del correo institucional (usuario), coincidirá con el usuario del dominio descrito anteriormente.

La cuenta de correo estará conformada de la siguiente forma: (usuario@indeportesantioquia.gov.co).

El tamaño y la capacidad de los buzones de correo electrónico está definido para cada usuario; si un usuario requiere espacio adicional, deberá solicitarlo a la Oficina de Sistemas e Informática, quien determinará, la posibilidad de aceptar o no la solicitud de manera permanente o temporal.

Se recomienda a los usuarios no distribuir información innecesaria por correo electrónico y hacer uso racional del envío y almacenamiento de información en el correo. Así mismo, se orienta acerca de la depuración permanente de los correos que contengan información que no sea relevante para INDEPORTES ANTIOQUIA.

Todas las listas de distribución serán creadas y configuradas por la Oficina de Sistemas e Informática, previa solicitud de la Oficina de Comunicaciones o la Oficina de Talento Humano; todas las firmas predeterminadas y pie de página de los correos electrónicos, serán diseñadas y configuradas por la Oficina Asesora de Comunicaciones e implantadas por la Oficina de Sistemas e Informática.

Algunas áreas o proyectos que requieran un correo electrónico de uso genérico deberán solicitarlo a la Oficina de Sistemas e Informática, por medio de la plataforma mesa de servicios. Es responsabilidad del Jefe de área y éste podrá designar la atención de dicha cuenta de correo a un servidor público de su dependencia, sin eximirse de la responsabilidad por el cumplimiento de las presentes normas e independientemente del accionar del personal en el cual delegue tales funciones.

La cuenta de correo asignada a un usuario es personal e intransferible. Queda estrictamente prohibido intentar o apoderarse de claves de acceso de otros usuarios, acceder y/o suplantar la identidad de otro usuario. Ningún usuario está autorizado para

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

divulgar su clave a otros y permitir que ellos hagan en su nombre tareas que están bajo su responsabilidad.

Queda estrictamente prohibido tanto el uso del correo electrónico Institucional como el personal, para divulgar información confidencial de la Entidad o información catalogada como sensible.

Queda estrictamente prohibido el uso del correo electrónico Institucional para cualquier propósito personal, comercial, financiero, político, religioso, delictivo o temas similares, ni para atentar contra el buen nombre de Instituciones o personas. Los usuarios no podrán utilizar el correo institucional para suscripciones a servicios o envío de correos personales o comerciales.

El buzón de correo no es un lugar de almacenamiento, sólo es utilizado para el envío y recepción de correos, por lo cual es importante que se depure de manera continua la información, acorde al nivel de importancia para el desarrollo de sus funciones.

No está permitido:

- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, xenófobo, homófobo, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y/o la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Entidad; de igual forma mensajes malintencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
- Utilizar la dirección de correo electrónico corporativa como punto de contacto ante instituciones, servicios o comunidades interactivas de contacto social, tales como Facebook y/o Twitter o cualquier otro sitio que no tenga que ver con las actividades laborales.
- Enviar archivos que contengan extensiones ejecutables, en ninguna circunstancia.
- Enviar y/o recibir archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por la mesa de servicios de INDEPORTES.
- Entregar la lista de correo electrónico de los servidores públicos de la Entidad, a usuarios externos que la utilicen para fines comerciales o políticos.
- Abrir correos electrónicos de remitentes desconocidos o que sean sospechosos de tener contenido malintencionado como virus o programa malicioso.
- Intercambiar información no autorizada de propiedad de INDEPORTES y/o de sus usuarios con terceros.
- Queda estrictamente prohibido el uso del correo electrónico institucional, para propagar mensajes de tipo cadena, no importa el contenido del mensaje divulgado. Si el Instituto recibe quejas, denuncias o reclamaciones por estas prácticas, se tomarán las medidas disciplinarias pertinentes.

Dado que el correo electrónico es un recurso tecnológico de INDEPORTES ANTIOQUIA, puede ser monitoreado en caso de que el Jefe inmediato o un ente de control que así lo demande con el concepto previo de la Oficina Asesora Jurídica y la autorización del usuario;

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

por lo cual el servidor público no debe considerar que la información almacenada, enviada o recibida es privada.

16. INTERNET:

Se controlará, verificará y monitorear para el uso y la navegación en internet de todos los usuarios conectados a la red de la Entidad de manera permanente, con el fin de garantizar el uso eficiente del canal corporativo y mantener la seguridad de la información.

La Oficina de Sistemas e Informática, podrá en cualquier momento inspeccionar los tiempos de navegación, páginas visitadas y evaluar las actividades realizadas durante la navegación, de acuerdo con la legislación nacional vigente por los usuarios de la Entidad en los canales institucionales. No está permitido deshabilitar o evadir los controles de navegación en internet. La instalación de herramientas que permitan evadir estos controles será vigiladas y sancionadas.

La Entidad reconoce que los usuarios de la red pueden usar esporádicamente los recursos de internet que les han sido asignados, o a los que tienen acceso, para uso personal y ocasional, pero nunca para uso comercial. Los canales de internet institucionales no deben usarse para promover sistemas multiniveles como: esquemas de pirámide, o conducir a rifas o sorteos en los que haya que pagar por el acceso. Tal uso personal y ocasional no debe ser excesivo y no debe interferir con la operación eficiente de los canales y servicios de la Institución, ni con los deberes y obligaciones de las personas establecidas en los diferentes reglamentos y manuales.

Está prohibido descargar intercambiar, usar y/o instalar música, juegos, películas, fondos de pantalla que cambien lo institucional, software de libre distribución, información y/o productos que atenten contra la propiedad intelectual o cualquier otro software que comprometa la integridad y disponibilidad de la plataforma tecnológica de la Entidad.

Está prohibido consultar páginas de carácter pornográfico o sexual, violencia en línea, software ilegal, drogas, alcohol, hacking y/o cualquier otra página que vaya en contra de la ética, las leyes vigentes o políticas establecidas en el presente documento.

Está prohibida la consulta de las páginas de redes sociales o de streaming de audio y video durante la jornada laboral, excepto para el personal que actualiza Información Institucional en estos sitios o por autorización del Jefe inmediato que su perfil requiera acceso permanente a dichos sitios para consulta de información ligada con sus funciones.

Se prohíbe la distribución intencional de virus, gusanos, troyanos o la realización de cualquier tipo de actividad destructiva en calidad de hacker o similar.

Se prohíbe usar los servicios de la red para propósitos fraudulentos o para la propagación de mensajes destructivos u obscenos.

17. OPERACIONES BANCARIAS VÍA INTERNET:

La gestión del Instituto en seguridad informática exige conexiones seguras, con prácticas como direcciones IP estáticas propias de la red local de INDEPORTES ANTIOQUIA, control

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

de firewall, políticas de seguridad en dominio, plataformas web con certificaciones de seguridad, acceso al aplicativo con doble factor de autenticaciones, cifrado extremo – extremo y adhesión de clavija o centinela, entre otros.

18. COPIAS DE SEGURIDAD:

Se debe asegurar que la información con nivel de clasificación, contenida en la plataforma tecnológica de la Entidad, sea resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad, disponibilidad y confiabilidad.

Se debe establecer una política de copias de respaldo para definir los requisitos de INDEPORTES ANTIOQUIA para copias de respaldo de información, software y sistemas.

La política de copias de respaldo debe definir los requisitos de retención y de protección.

Se debe proporcionar instalaciones adecuadas para copias de respaldo, para asegurar que la información y el software esenciales se puedan recuperar después de un desastre o falla.

Se diseñará un plan de elaboración de copias de respaldo, para esto, se deberán tener en cuenta los siguientes aspectos:

- Se deben producir registros exactos y completos de las copias de respaldo, y procedimientos de restauración documentados.
- La cobertura (por ejemplo, copias de respaldo completas o diferenciales) y la frecuencia con que se hagan las copias de respaldo deben reflejar los requisitos del negocio de INDEPORTES ANTIOQUIA, los requisitos de la seguridad de la información involucrada, y la criticidad de la información para la operación continua de INDEPORTES ANTIOQUIA.
- Las copias de respaldo se deben almacenar en un lugar remoto, a una distancia suficiente que permita escapar de cualquier daño que pueda ocurrir en el sitio principal;
- A la información de respaldo se le debe dar un nivel apropiado de protección física y del entorno, de coherencia con las normas aplicadas en el sitio principal.
- Los medios de respaldo se deben poner a prueba regularmente para asegurar que se puede depender de ellos para uso de emergencia en caso de ser necesario; esto se debe combinar con una prueba de los procedimientos de restauración.
- En situaciones en las que la confidencialidad tiene importancia, las copias de respaldo deben estar protegidas por medio de encriptación.
- Definir en conjunto con el Centro de Administración de documentos - CADA y de acuerdo con lo determinado por la Ley, los períodos de retención de las copias de seguridad y disponer de los recursos necesarios para identificar los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos, permitiendo un rápido y eficiente acceso a los medios que contienen la información resguardada.
- Asegurar el servicio de sincronización en la nube (OneDrive), de la información que se encuentre en las carpetas Mis Documentos, Mis Imágenes, en el Escritorio o carpetas propias de la nube en el equipo de los usuarios. Información almacenada en una ubicación diferente no será respaldada.
- Excluir del proceso de respaldo la información personal de fotos, videos y archivos

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

con extensiones .exe, .mp3, entre otras.

19. SEGURIDAD DE LA INFORMACIÓN PARA LOS MEDIOS EXTRAÍBLES:

Implementar los controles necesarios para asegurar que en los equipos de cómputo institucionales sólo los servidores públicos y contratistas autorizados puedan hacer uso de los medios de almacenamiento extraíbles.
Asegurar física y lógicamente los dispositivos extraíbles, con el fin de no poner en riesgo la información de la Entidad contenida en los mismos.

20. SERVICIOS DE IMPRESIÓN:

La Entidad tiene distribuido el servicio de impresión en zonas, que permiten a los usuarios utilizar por defecto la impresora más cercana a su puesto de trabajo, todas ellas están en red, de manera que los usuarios pueden usar otra, en caso de alguna falla o situación atípica de congestión en su dependencia.

Cada impresora es un equipo multifuncional que permite además copiar, escanear y enviar las imágenes al correo electrónico.

Los usuarios manejan una contraseña de retención, por medio de la cual pueden utilizar los servicios, esta se digita en el panel de control de la impresora.

La Entidad, por medio de la Resolución S 202000406 del 03 de julio de 2020, ordenó adoptar e implementar en INDEPORTES ANTIOQUIA las buenas prácticas del uso del papel, orientadas a la implementación de la Política Cero Papel, por medio del aprovechamiento, de las tecnologías de la información y comunicaciones TIC, aplicando los principios de Gestión Documental.

Como gestión en esta política, la Entidad tiene implementada la plataforma MERCURIO, sistema que cumple a cabalidad e integra en su total el flujo de documentos basado en procesos, rutas y workflow con cobertura total de transversalidad.

La Oficina de Sistemas e Informática con el apoyo de la Oficina de Control Interno cada mes revisan el informe de impresiones que permite identificar los trabajos impresos, la cantidad de impresión, así como otros datos que permiten controlar los documentos que se imprimen en la Entidad.

Se deben considerar las siguientes directrices:

- Se debe evitar el uso no autorizado de fotocopiadoras y otra tecnología de reproducción (por ejemplo, escáneres, cámaras digitales, entre otros).
- Los medios que contienen información sensible o clasificada se deben retirar de las impresoras inmediatamente.
- La información sensible o crítica del negocio, por ejemplo, sobre de papel o en un medio de almacenamiento electrónico, se debe guardar bajo llave (idealmente, en una caja fuerte o en un gabinete u otro mueble de seguridad), cuando no se requiera, especialmente cuando la Oficina esté desocupada.
- Todas las impresoras deben tener la función de código con PIN, de manera que los

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

originadores son los únicos que pueden hacer impresiones y sólo cuando están al lado de la impresora liberar las mismas.

21. CLASIFICACIÓN DE LA INFORMACIÓN:

El esquema de clasificación de información debe incluir las convenciones para la clasificación y los criterios para la revisión de la clasificación en el tiempo. El nivel de protección en el esquema se debe valorar analizando la confidencialidad, la integridad y la disponibilidad, y cualquier otro requisito para la información considerada. El esquema se debe alinear con la política de control de acceso y los documentos archivísticos de la Entidad como las tablas de retención documental, el índice de información clasificada, entre otros, por lo cual esta actividad se realizará siempre en conjunto con el personal del Centro de Administración de documentos - CADA.

Los propietarios de los activos deben determinar las reglas de control de acceso apropiadas, los derechos de acceso y las restricciones para los roles de usuario específicos con relación a sus activos, con la cantidad de detalle y severidad de los controles, que reflejen los riesgos de seguridad de la información asociados. Los propietarios de la información deben garantizar la seguridad de la información y los sistemas que le dan soporte.

La Oficina de Sistemas e Informática es responsable de asegurar la confidencialidad, integridad y disponibilidad de los activos de información, datos y los servicios de TI, mediante el monitoreo de portales, equipos, tráfico de información en la red, antivirus, usuarios y cualquier otra herramienta utilizada para preservar la seguridad de la información.

La información en INDEPORTES ANTIOQUIA está clasificada de acuerdo con su impacto de seguridad:

- **Información pública**: Toda información que INDEPORTES ANTIOQUIA genere, obtenga, adquiera, o controle en su calidad de obligado.
- **Información pública clasificada:** Toda información que estando en poder o custodia de INDEPORTES ANTIOQUIA en su calidad de obligado, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica, por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 del 6 de marzo de 2014 (Ley de transparencia y del derecho de acceso a la información pública nacional).
- **Información reservada**: Información que estando en poder o custodia de INDEPORTES ANTIOQUIA en su calidad de obligado, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 6 de marzo de 2014 (Ley de transparencia y del derecho de acceso a la información pública nacional).
- Los servidores públicos deben cumplir las políticas para el manejo de información reservada y clasificada, los cuidados que debe recibir este tipo de información incluyen:
- No dejarla desatendida ni a la vista de personas no autorizadas, como por ejemplo en los puestos de trabajo y zonas de impresión.
- Debe encontrarse almacenada únicamente en los sistemas de información

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

suministrados por la Entidad.

- Siempre se debe utilizar clave de seguridad para su impresión. Si lo anterior no es posible, se debe tener una persona atendiendo todo el proceso de impresión.
- Los servidores públicos son responsables de proteger la información de su trabajo y solicitar a la Oficina de Sistemas e Informática el almacenamiento seguro de la información, cuya pérdida pueda causar incumplimientos legales y/o la interrupción de los procesos de la Entidad.
- Sólo se permite la transferencia de información clasificada o reservada cuando exista un acuerdo de confidencialidad o compromiso contractual que lo regule.
- La información específica sobre incidentes o vulnerabilidades de seguridad de la información, así como el detalle de las medidas para proteger las plataformas de TIC, debe ser tratada como información reservada.

22. TERMINACIÓN DEL CONTRATO, CAMBIO DE CARGO O RETIRO:

Los Servidores públicos y/o contratistas que finalicen su relación laboral o contractual con INDEPORTES ANTIOQUIA deben entregar a su jefe inmediato o Supervisor responsable, la información de la Entidad producida o conocida que se encuentre bajo su responsabilidad y/o manejo.

Al retiro definitivo de la Entidad, las Oficinas de Talento Humano u Oficina Asesora Jurídica o en su defecto el Supervisor del contrato, notificarán a la Oficina de Sistemas e Informática, por medio de la mesa de servicios, los servidores públicos y/o contratistas que se retirarán de la Entidad mínimo con cinco (5) días hábiles de anterioridad, para realizar las respectivas copias de seguridad y la desactivación del usuario.

La información y el conocimiento desarrollado por los servidores públicos de INDEPORTES ANTIOQUIA y dentro de la vigencia del contrato es propiedad de la Entidad, por lo tanto, se prohíbe el borrado o la copia de dicha información por parte de servidores públicos en proceso de retiro o por personal retirado.

Ante la finalización de la relación laboral o cambio de funciones de un servidor público, el jefe respectivo es responsable de solicitar la suspensión o cambio de los permisos de acceso a las plataformas de TIC de la Entidad.

La Oficina de Talento Humano, o quien haga sus veces, debe informar inmediatamente a la Oficina de Sistemas e Informática, los retiros o traslados de los servidores públicos, contratistas y practicantes, con el fin de revocar o modificar los privilegios de acceso asignados a dicho personal.

El jefe inmediato es el responsable de gestionar el respaldo de la información de los equipos de cómputo de los servidores públicos en proceso de retiro. Los contratos celebrados entre INDEPORTES ANTIOQUIA y contratistas con acceso a la información de la Entidad deben incluir cláusulas para mitigar riesgos de seguridad de la información.

Adicionalmente, se debe gestionar la documentación de entrega referenciada en los formatos F-TH-75 Informe de entrega del cargo, F-TH-17 Constancia por dependencia establecidos en el SGC.

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

23. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:

En INDEPORTES ANTIOQUIA los eventos e incidentes de seguridad informática son gestionados oportunamente, con el fin de minimizar el impacto sobre la Entidad. Reporte de eventos, incidentes y debilidades de la seguridad de la información.

Los servidores públicos y/o contratistas, entrenadores, deportistas y practicantes deben reportar inmediatamente a la mesa de servicios, todas las situaciones que puedan afectar la seguridad de la información sobre Incidentes o vulnerabilidades de seguridad informática, así como el detalle para poder tomar medidas y proteger las plataformas TIC.

Debe conformarse y mantenerse un equipo multidisciplinario para la respuesta y tratamiento a los incidentes de seguridad de la información.

Cuando un evento de seguridad sea declarado como incidente de seguridad de la información, debe seguirse el procedimiento de gestión apropiado de reporte de incidentes de seguridad de la información, aprobado en el sistema de gestión de calidad.

24. POLÍTICA DE COMUNICACIÓN CON PRENSA, RADIO Y TELEVISIÓN:

Ningún servidor público y/o contratista diferente a la Oficina Asesora de Comunicaciones, está autorizado para divulgar información oficial de la Entidad por medios electrónicos o escritos, a medios de comunicación, clientes o proveedores, a excepción de aquellos funcionarios a los cuales las directivas de la Entidad hayan delegado para tal fin.

No se podrá entregar información oficial de la Entidad si no existe una solicitud por escrito que especifique el objetivo de la información solicitada; esta solicitud deberá ir acompañada de cláusulas de confidencialidad, de acuerdo con el objetivo expuesto por el solicitante de la información.

En ninguna circunstancia podrá entregarse información personal, familiar, de domicilio o correspondencia de los empleados, deportistas o entrenadores, salvo en aquellos casos que sea solicitada por una autoridad competente mediante una orden judicial en los casos y formalidades que establezca la Ley.

25. MANEJO DE EXCEPCIONES:

Las excepciones de la política están definidas en la sección de Correo Electrónico, Internet y comunicaciones y sólo pueden ser autorizadas por la Oficina de Sistemas e Informática. En estos casos, se deben ejecutar procedimientos específicos para manejar la solicitud y la autorización de excepciones.

Debe usarse en aquellas circunstancias en que las necesidades de la Entidad justifiquen la ejecución. La validez de la excepción se determinará mediante el correspondiente análisis de los riesgos. Una excepción implica la exposición a uno o varios riesgos, por lo tanto, para hacer efectiva la excepción, es necesario el entendimiento y la aceptación de dichos riesgos por parte del área interesada.

26. TELETRABAJO / CONEXIÓN REMOTA / TRABAJO EN CASA:

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

Cuando se tengan archivos o sistemas de información pertenecientes a INDEPORTES ANTIOQUIA con sesiones abiertas, el servidor público, contratista y/o practicante en trabajo en casa, deberá impedir el uso del equipo de cómputo por personal no autorizado lo que incluye: familiares, amigos y clientes, entre otros.

Los equipos de cómputo suministrados por la Entidad para trabajo en casa sólo deben ser utilizados por el servidor público, contratista y/o practicante al que le fue asignado.

Evitar establecer conexiones a redes inalámbricas desconocidas o que estén habilitadas sin seguridad, es decir, que no solicite claves de ingreso.

Usar la conexión VPN para acceder a los sistemas de información que se encuentren en la red interna de INDEPORTES ANTIOQUIA, así como a los servicios web que no cuentan con conexión cifrada o certificados de seguridad.

Cambiar periódicamente las credenciales para el establecimiento de la VPN. Dichas solicitudes se registran en la mesa de servicios. Las credenciales asignadas para el establecimiento de la VPN son de uso personal e intransferible, por tanto, no se comparten o divulgan. El uso inadecuado es responsabilidad exclusiva del usuario asignado.

Para el trabajo en casa siempre se debe utilizar el equipo de cómputo asignado por la Entidad, para garantizar el proceso de actualización del sistema Operativo (parches) y tener instalado una consola de Antivirus actualizada, así como las herramientas corporativas para permitir el correcto desarrollo de las funciones y ofrecer el soporte técnico remoto requerido.

Para la actividad de trabajo en casa, será obligatorio que se almacene la información en el repositorio corporativo definido por la Entidad (OneDrive o SharePoint del Office 365).

Los funcionarios, contratistas o terceros, no podrán solicitar servicios para mantenimiento o formateo de sus equipos personales, dado que éste no es propiedad de la Entidad; tampoco podrán solicitar licenciamiento de Office o del sistema Operativo, o instalación de software gratuito, todo esto debe correr por cuenta del propietario del equipo.

El equipo de cómputo para trabajo en casa cuenta con placa y es propiedad de INDEPORTES ANTIOQUIA, por tanto, cubre todo el soporte técnico del equipo, además de las instalaciones aprobadas por el personal que autoriza el licenciamiento.

Se implementa esta política y medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo/conexión remota.

Cuando se considere aplicable, se deben considerar las siguientes actividades:

- La seguridad física existente en el sitio del teletrabajo y/o trabajo remoto/trabajo en casa, teniendo en cuenta la seguridad física de la edificación y del entorno local
- Los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de INDEPORTES ANTIOQUIA, la sensibilidad de la información a la que se tendrá acceso y que pasará a través del

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

enlace de comunicación y la sensibilidad del sistema interno.
- La amenaza de acceso no autorizado a información o a recursos, por parte de otras personas que usan el mismo alojamiento, por ejemplo, familia y amigos.
- El uso de redes domésticas y requisitos o restricciones sobre la configuración de servicios de red inalámbrica.
- Acuerdos de licenciamiento de software, de tal forma que INDEPORTES ANTIOQUIA pueda llegar a ser responsable por el licenciamiento de software de terceros en estaciones de trabajo de propiedad de los empleados o de usuarios externos.
- Requisitos de firewall/WAF y de protección contra código malicioso.

27. DISPOSITIVOS MÓVILES:

Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles cuando esto aplica.

Cuando se usan dispositivos móviles, se debe asegurar que no se comprometa la información del negocio. Por tal razón, la política de dispositivos móviles debe tener en cuenta los riesgos de trabajar con dispositivos móviles en entornos no protegidos.

La política de dispositivos móviles debe considerar los siguientes ítems:

- El registro de los dispositivos móviles.
- Las restricciones para la instalación de software.
- La restricción de la conexión a servicios de información.
- Técnicas de cifrado cuando se requiera proteger la confidencialidad del activo.
- Protección contra código malicioso utilizando el software de la Entidad.
- Copias de respaldo si el activo lo requiere.
- Uso de servicios y aplicaciones web.

Es importante resaltar que se debe tener cuidado cuando se usan dispositivos móviles en lugares públicos, salas de reuniones y áreas no protegidas, hoteles, entre otros lugares. Se debe contar con protección para evitar el acceso o la divulgación no autorizada de la información almacenada y procesada por estos dispositivos.

Los dispositivos móviles también deben estar protegidos contra robo mediante pólizas de aseguramiento.

- **Información adicional:** Las conexiones inalámbricas para dispositivos móviles son similares a otros tipos de conexión de red, pero tienen diferencias importantes que se deben considerar cuando se identifican controles. Las diferencias típicas son:

    - Algunos protocolos de seguridad inalámbricos no están desarrollados suficientemente, y tienen debilidades conocidas;
    - La información almacenada en los dispositivos móviles no esté copiada en discos de respaldo, debido a limitaciones en el ancho de banda o porque los dispositivos móviles no estén conectados en los tiempos en que se programa la elaboración de copias de respaldo.

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

En consecuencia, los dispositivos móviles generalmente comparten funciones comunes con los dispositivos de uso fijo, por ejemplo, trabajo en red, acceso a internet, correo electrónico y manejo de archivos. Los controles de seguridad de la información para los dispositivos móviles generalmente consisten en los controles adoptados en los dispositivos de uso fijo, y en los controles para tratar las amenazas que surgen por su uso fuera de las instalaciones de INDEPORTES ANTIOQUIA.

28. TRANSFERENCIA DE INFORMACIÓN:

Se debe mantener la seguridad de la información transferida dentro de la Entidad y con cualquier entidad externa. Está prohibido compartir información desde el repositorio de OneDrive con usuarios externos a la organización. Cualquier excepción deberá ser solicitada a la Oficina de Sistemas e Informática, quien la analizará para conceder o negar el permiso.

- **Políticas y procedimientos de transferencia de información:** Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación. Los procedimientos y controles que se siguen cuando se usan instalaciones de comunicación para la transferencia de información deben tener en cuenta los siguientes elementos:

    - Los procedimientos diseñados para proteger la información transferida contra interceptación, copiado, modificación, enrutado y destrucción.
    - Los procedimientos para la detección de software malicioso y protección contra éste, que puede ser transmitido mediante el uso de comunicaciones electrónicas.
    - Los procedimientos para proteger información electrónica sensible comunicada que están como adjuntos.
    - La política o directrices que presentan el uso aceptable de las instalaciones de comunicación.
    - Las responsabilidades del personal, las partes externas y cualquier otro usuario, no comprometen a INDEPORTES ANTIOQUIA, por ejemplo, por difamación, acoso, suplantación, envío de cadenas, compras no autorizadas, etc.
    - Las directrices sobre retención y disposición para toda la correspondencia del negocio, incluidos mensajes, de acuerdo con la legislación y reglamentaciones locales y nacionales.
    - Los controles y restricciones asociadas con las instalaciones de comunicación, por ejemplo, el reenvío automático de correo electrónico a direcciones de correo externas.
    - Brindar capacitación al personal de INDEPORTES ANTIOQUIA, para que tome las precauciones apropiadas acerca de no revelar información confidencial

- **Acuerdos sobre transferencia de información:** Los acuerdos deben tener en cuenta la transferencia segura de información del negocio entre INDEPORTES ANTIOQUIA y las partes externas. Para esto se deben establecer las políticas, procedimientos y estándares para proteger la información y los medios físicos en

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

tránsito, y se deben referenciar en los acuerdos de transferencia.

El contenido de seguridad de la información de cualquier acuerdo debe reflejar el carácter sensible de la información involucrada.

Los acuerdos de transferencia de información deben incluir lo siguiente:

- Las responsabilidades de la dirección para controlar y notificar la transmisión, despacho y recibo.
- Certificados digitales requeridos.
- Estándares de identificación de mensajería.
- Las responsabilidades y obligaciones en el caso de incidentes de seguridad de la información, tales como pérdidas de datos.
- El uso de un sistema de etiquetado acordado para información sensible o crítica.
- Cualquier control especial que se requiera para proteger elementos críticos, tales como criptografía aplicada a la información que va a ser transmitida.

- **Información adicional:** Los acuerdos pueden ser electrónicos o manuales y pueden ser contratos formales. Para información confidencial, los mecanismos específicos usados para la transferencia de esta información deben ser coherentes con las políticas de INDEPORTES ANTIOQUIA.

29. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS:

INDEPORTES ANTIOQUIA debe asegurar que los datos e infraestructura y las instalaciones de procesamiento estén protegidas contra códigos maliciosos, para mantener la seguridad de la información, por lo que se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.

La protección contra los códigos maliciosos se debe basar en software de detección de códigos maliciosos y de reparación, en toma de conciencia sobre la seguridad de la información, y en controles apropiados de gestión de cambios y de acceso al sistema. Se deben considerar las siguientes directrices:

- Establecer una política formal que prohíba el uso de software no autorizado.
- Implementar controles para evitar o detectar el uso de software no autorizado, un ejemplo fundamental, son las listas blancas de aplicaciones.
- Implementar controles para evitar o detectar el uso de sitios web malicioso o que se sospecha que lo son, un ejemplo para este ítem, son las listas negras.
- Establecer una política formal para proteger contra riesgos asociados con la obtención de archivos y de software, ya sea mediante redes externas o cualquier otro medio, indicando qué medidas externas se deben tomar.
- Reducir las vulnerabilidades de las que pueda aprovecharse el software malicioso, por ejemplo, por medio de la gestión de la vulnerabilidad técnica.
- Llevar a cabo revisiones regulares del software y del contenido de datos de los sistemas que apoyan los procesos críticos del negocio; se debe investigar formalmente la presencia de archivos no aprobados o de enmiendas no

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

autorizadas.
- La instalación y actualización regular del software de detección y reparación del software malicioso en los computadores y medios como una medida de control, en forma rutinaria.

Gestión de las vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de INDEPORTES ANTIOQUIA a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.

Es importante resaltar que un inventario actualizado y completo de los activos, es un prerrequisito para una gestión eficaz de la vulnerabilidad técnica.

Es importante obtener información oportuna del grado de vulnerabilidad al que está asociada al activo y el riesgo impactante sobre este activo de propiedad de INDEPORTES ANTIOQUIA.

Se deben tomar acciones apropiadas y oportunas en respuesta a la identificación de vulnerabilidades técnicas potenciales.

Los siguientes aspectos se deben seguir para establecer un proceso de gestión eficaz para las vulnerabilidades técnicas:

- INDEPORTES ANTIOQUIA debe definir y establecer los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica, incluido el seguimiento de la vulnerabilidad, la valoración de riesgos de vulnerabilidad, la colocación de parches, el seguimiento de activos y cualquier responsabilidad de coordinación requerida.
- Los recursos de información que se usarán para identificar las vulnerabilidades técnicas pertinentes y para mantener la toma de conciencia acerca de ellos se deben identificar para el software y otra tecnología (con base en la lista de inventario de activos, estos recursos de información se deben actualizar con base en los cambios en el inventario o cuando se encuentran otros recursos nuevos o útiles).
- Se debe definir una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas pertinentes potencialmente.
- Una vez que se haya identificado una vulnerabilidad técnica potencial, INDEPORTES ANTIOQUIA debe identificar los riesgos asociados y las acciones por tomar; esta acción puede involucrar la colocación de parches de sistemas vulnerables o la aplicación de otros controles.
- Dependiendo de la urgencia con la que se necesite tratar una vulnerabilidad técnica, la acción tomada se debe llevar a cabo de acuerdo con los controles relacionados con la gestión de cambios, o siguiendo los procedimientos de respuesta a incidentes de seguridad de la información.
- Si está disponible un parche de una fuente legítima, se deben valorar los riesgos asociados con la instalación del parche (los riesgos que acarrea la vulnerabilidad se deben comparar con el riesgo de instalar el parche).
- Los parches se deben probar y evaluar antes de su instalación, para asegurarse de que son eficaces y no producen efectos secundarios que no se puedan tolerar; si no hay parches disponibles, se deben considerar otros controles como:

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

- Dejar de operar los servicios o capacidades relacionados con la vulnerabilidad.
- Adaptar o adicionar controles de acceso, por ejemplo, cortafuegos, en los límites de la red.
- Incrementar el seguimiento para detectar ataques reales.
- Hacer tomar conciencia sobre la vulnerabilidad.
- Se debe llevar un log de auditoría para todos los procedimientos realizados.
- Se debe hacer seguimiento y evaluación regulares del proceso de gestión de vulnerabilidad técnica, con el fin de asegurar su eficacia y eficiencia
- Se deben abordar primero los sistemas que están en alto riesgo.
- Un proceso de gestión eficaz de la vulnerabilidad técnica debe estar alineado con las actividades de gestión de incidentes para comunicar los datos sobre vulnerabilidades a la función de respuesta a incidentes y suministrar los procedimientos técnicos para realizarse si llegara a ocurrir un incidente
- Definir un procedimiento para hacer frente a una situación en la que se ha identificado una vulnerabilidad, pero no hay una contramedida adecuada. En esta situación, INDEPORTES ANTIOQUIA debe evaluar los riesgos relacionados con la vulnerabilidad conocida y definir las acciones de detección y correctivas apropiadas.

30. CRIPTOGRAFÍA:

Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.

Cuando se desarrolla una política sobre el uso de la criptográfica, es conveniente tener en cuenta lo siguiente:

- El enfoque de la dirección con relación al uso de controles criptográficos en toda INDEPORTES ANTIOQUIA, incluyendo los principios generales bajo los cuales se debe proteger la información del negocio.
- Con base en la valoración de riesgos, se debe identificar el nivel de protección requerida, teniendo en cuenta el tipo, fortaleza y calidad del algoritmo de encriptación requerido.
- El uso de encriptación para la protección de información de acuerdo con la valoración del riesgo se clasifica en:
  - Certificado SSL/TLS.
  - Cifrado de discos duros.
  - Cifrado de información en tránsito.
  - Cifrado de información que proceso un software, por ejemplo, nomina o contabilidad.

31. PRIVACIDAD Y PROTECCIÓN DE INFORMACIÓN DE DATOS PERSONALES:

Cuando sea aplicable, se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

Se debe desarrollar e implementar una política relativa a datos de INDEPORTES ANTIOQUIA, para la privacidad y la protección de datos personales. Esta política se debe comunicar a todas las personas involucradas en el procesamiento de información de datos personales.

El cumplimiento de esta política y de toda la legislación y reglamentación pertinente concerniente a la protección de la privacidad de las personas y a la protección de los datos personales, requiere una estructura y control de gestión apropiados. Con frecuencia, la mejor manera de lograrlo es nombrando una persona responsable.

La responsabilidad por el manejo de información sobre datos personales y por asegurar la toma de conciencia sobre los principios de privacidad se debe abordar de acuerdo con la legislación y las reglamentaciones pertinentes. Se deben implementar medidas técnicas y organizacionales para proteger la información de datos personales.

32. SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES:

Asegurar la protección de los activos de INDEPORTES ANTIOQUIA que sean accesibles a los proveedores.

- **Política de seguridad de la información para las relaciones con proveedores:** Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de INDEPORTES ANTIOQUIA, se deben acordar con estos y se deben documentar.
- **Aplicación de la política:** INDEPORTES ANTIOQUIA debe identificar y exigir controles de seguridad de la información para tener en cuenta en una política específicamente el acceso de los proveedores a la información.

Estos controles deben tener en cuenta los procesos y procedimientos que va a implementar INDEPORTES ANTIOQUIA, al igual que los procesos y procedimientos que el Instituto debe exigir a sus proveedores, que implementará, incluidos:

- La identificación y documentación de los tipos de proveedores, por ejemplo, servicios de TI, utilidades logísticas, servicios financieros, componentes de la infraestructura de TI, a quienes INDEPORTES ANTIOQUIA permitirá acceso a su información.
- La definición de los tipos de acceso a la información que se permitirá a diferentes tipos de proveedores, y el seguimiento y el control del acceso.
- Los controles de exactitud y totalidad, para asegurar la integridad de la información o del procesamiento de la información realizado por una tercera parte.
- Los tipos de obligaciones aplicables a los proveedores para proteger la información de INDEPORTES ANTIOQUIA.
- El manejo de incidentes y contingencias asociadas con el acceso de proveedores, incluidas las responsabilidades tanto de INDEPORTES ANTIOQUIA como de los proveedores.
- Las condiciones bajo las cuales los requisitos y controles de seguridad de la información se documentarán en un acuerdo firmado por ambas partes.

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de INDEPORTES ANTIOQUIA.

El seguimiento y la revisión de los servicios de los proveedores deben asegurar que los términos y condiciones de seguridad de la información de los acuerdos se cumplan, y que los incidentes y problemas de seguridad de la información se gestionen apropiadamente.

La Oficina de Sistemas e Informática, monitoreará de forma permanente que los sistemas y recursos de la red operen adecuadamente y que los usuarios estén acatando las directrices emanadas en este documento.

La Oficina de Control Interno realizará auditorías internas para determinar si los controles, sus objetivos, los procesos y procedimientos continúan de conformidad con este documento y para analizar y planificar acciones de mejora.

ARTÍCULO 12. GENERALIDADES: Todos los usuarios de INDEPORTES ANTIOQUIA son responsables del cumplimiento de cada una de las políticas de seguridad y los Jefes de las dependencias deberán supervisar el cumplimiento de estas.

ARTÍCULO 13. MARCO NORMATIVO:

- **Ley 23 de 1982** - Derechos de Autor.
- **Ley 599 de 2000 -** Código Penal.
- **Ley 1032 de 2006** - Por la cual se modifican los artículos 257, 271, 272 y 306 del Código Penal: Artículo 257. De la prestación, acceso o uso ilegales de los servicios de telecomunicaciones. Artículo 271. Violación a los derechos patrimoniales de autor y derechos conexos.
- Artículo 272. Violación a los mecanismos de protección de derecho de autor y derechos conexos, y otras defraudaciones.
- **Ley 679 de 2001** - Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución.
- **Ley 1273 de 2009 -** Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado *"De la Protección de la información y de los datos*" - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

ARTÍCULO 14. SANCIONES: Ante la evidencia del incumplimiento de lo establecido en el presente documento, la administración podrá iniciar los procesos disciplinarios a que haya lugar o aplicar las sanciones administrativas correspondientes, o dar traslado a la autoridad competente para que se haga la respectiva investigación de tipo penal, de acuerdo con la normatividad vigente.

Una infracción o falta de estas políticas por parte de un contratista o proveedor puede resultar en la terminación de su contrato con INDEPORTES ANTIOQUIA.

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES

2025000825

A continuación, se referencia algunas de las sanciones establecidas por la Ley:

La protección de la Información y de los Datos, está contemplada en el código penal, a través de la Ley 1273 de 2009, 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:

- ***Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO**: **El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.***
- ***Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.** El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.*
- ***Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS**. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.*
- ***Artículo 269D: DAÑO INFORMÁTICO.** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*
- ***Artículo 269E: USO DE SOFTWARE MALICIOSO.** El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*
- ***Artículo 269F: VIOLACIÓN DE DATOS PERSONALES.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*
- ***Ley 679 de 2001: ARTÍCULO 7. PROHIBICIONES.** Los proveedores o servidores, administradores y usuarios de redes globales de información no podrán:*

  - *Alojar en su propio sitio imágenes, textos, documentos o archivos audiovisuales que impliquen directa o indirectamente actividades sexuales con menores de edad.*
  - *Alojar en su propio sitio material pornográfico, en especial en modo de imágenes*

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

o videos, cuando existan indicios de que las personas fotografiadas o filmadas son menores de edad.

- *Alojar en su propio sitio vínculos o links, sobre sitios telemáticos que contengan o distribuyan material pornográfico relativo a menores de edad.*

- ***Artículo 312B. Omisión de denuncia.*** *El que, por razón de su oficio, cargo, o actividad, tuviere conocimiento de la utilización de menores para la realización de cualquiera de las conductas previstas en el presente capítulo y omitiere informar a las autoridades administrativas o judiciales competentes sobre tales hechos, teniendo el deber legal de hacerlo, incurrirá en multa de diez (10) a cincuenta (50) salarios mínimos legales mensuales vigentes.*
  Si la conducta se realizare por servidor público, se impondrá, además, la pérdida del empleo.
- ***Ley 1336 de 2009:*** *La Ley 1336 de 2009 especifica en su Capítulo VI, artículo 24, una modificación al artículo 218 de la ley 599, referente a la pornografía con personas menores de 18 años:*
- ***Artículo 218. Pornografía con personas menores de 18 años.*** *El que fotografíe, filme, grabe, produzca, divulgue, ofrezca, venda, compre, posea, porte, almacene, trasmita o exhiba, por cualquier medio, para uso personal o intercambio, representaciones reales de actividad sexual que involucre persona menor de 18 años, incurrirá en prisión de 10 a 20 años y multa de 150 a 1.500 salarios mínimos legales mensuales vigentes.*
  Igual pena se aplicará a quien alimente con pornografía infantil bases de datos de Internet, con o sin fines de lucro.
  La pena se aumentará de una tercera parte a la mitad cuando el responsable sea integrante de la familia de la víctima.

ARTÍCULO 15. SANCIONES ADMINISTRATIVAS: INDEPORTES ANTIOQUIA tomará medidas a partir de las denuncias formuladas, y sancionará a los proveedores o servidores, administradores y usuarios responsables que operen sucesivamente, con la cancelación o suspensión de la correspondiente página electrónica.

Para la imposición de estas sanciones se aplicará el procedimiento establecido en el Código Contencioso Administrativo con observancia del debido proceso y criterios de adecuación, proporcionalidad y reincidencia.

PARÁGRAFO: INDEPORTES ANTIOQUIA tendrá competencia para exigir, en el plazo que este determine, toda la información que considere necesaria a los proveedores de servicios de internet, relacionada con la aplicación de la Ley 679 de 2001 y demás que la adicionen o modifiquen. En particular podrá:

- Requerir a los proveedores de servicios de internet a fin de que informen en el plazo y forma que se les indique, qué mecanismos o filtros de control están utilizando para el bloqueo de páginas con contenido de pornografía con menores de edad en Internet.
- Ordenar a los proveedores de servicios de internet incorporar cláusulas obligatorias en los contratos de portales de internet relativas a la prohibición y bloqueo consiguiente de páginas con contenido de pornografía con menores de edad.
- Los proveedores de servicios de internet otorgarán acceso a sus redes a las autoridades judiciales y de policía cuando se adelante el seguimiento a un número IP desde el cual se produzcan violaciones a la presente ley.

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

ARTÍCULO 16. GLOSARIO:

Activo: Buen que tiene valor para INDEPORTES ANTIOQUIA, se requiere para las actividades y requiere protección.

Activos de información: Activo que dispone de información de INDEPORTES ANTIOQUIA, corresponde a elementos tales como infraestructura, sistemas de información, bases de datos, documentación, manuales de usuarios, planes de continuidad, etc.

Activos de software: Son elementos tales como: Aplicaciones de software, herramientas de desarrollo, y utilidades adicionales.

Activos físicos: Se consideran activos físicos elementos tales como: Computadores, laptops, módems, impresoras, escáner, equipos de comunicaciones, teléfonos, cintas, discos extraíbles, UPS, swiches, apps, routers, etc.

Amenaza: Potencialidad que puede provocar un evento/incidente en INDEPORTES ANTIOQUIA que podría producir daños o pérdidas materiales y/o inmateriales.

Borrado seguro: Procedimiento de eliminación de archivos que no permite la recuperación posterior de éstos.

Cifrado: Que está escrito con letras, símbolos o números que sólo pueden comprenderse si se dispone de la clave (llave criptográfica) necesaria para descifrarlos.

Correo masivo: Expresión usada en el presente documento para referirse a mensajes de correo electrónico enviado a 100 o más destinatarios que no formen parte de los dominios “@indeportesantioquia.gov.co”.

Confidencialidad: Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado 2.13 ISO 27000

Datos Sensibles: Información catalogada como pública clasificada o pública reservada.

Derechos / Privilegios de acceso / Roles: Conjunto de permisos otorgados a un usuario o a un sistema para acceder a un determinado recurso (repositorio información, aplicativo, datos).

Disponibilidad: Propiedad que la información sea accesible y utilizable por solicitud de los autorizados 2.10 ISO 27000.

Hacking: Es un conjunto de técnicas utilizadas para introducirse en un sistema informático vulnerando las medidas de seguridad, con independencia de la finalidad con la cual se realice, puede ser lícito y solicitado.

Hardware: Son los componentes físicos que forman parte de sistema informático como son: Servidores, impresoras, monitores, la CPU, teclados, mouse, etc.

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y/o amenazar la seguridad de la información. Todo incidente es un evento, más no todo evento es un incidente.

Integridad: Propiedad de salvaguardar la exactitud y el estado completo de los activos 2.36 ISO 27000.

Mesa de servicios de INDEPORTES ANTIOQUIA: Equipo responsable de gestionar las solicitudes de servicio relacionadas con las plataformas de tecnologías de información y comunicaciones de la Entidad.

Software: Son los programas y archivos que tiene un computador y que son necesarios para su funcionamiento.

Usuario: Todas aquellas personas que utilicen sistemas software, equipos informáticos y los servicios de Red provistos por la Entidad.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información. Adicionalmente, otras propiedades como la autenticidad, trazabilidad, no repudio y confiabilidad pueden estar relacionadas.

Seguridad informática: Mediciones y controles que garantizan la seguridad de la información en los dispositivos tecnológicos como equipos de cómputo, tales como servidores, equipos de escritorio, portátiles, tabletas, móviles, dispositivos de red, software aplicaciones y sistemas operativos.

Servidores públicos: Término que se usa en el presente documento para identificar a empleados públicos, provisionales, de carrera, libre nombramiento, contratistas y practicantes de INDEPORTES ANTIOQUIA.

Software malicioso (código malicioso): Es un tipo de software que tiene como objetivo infiltrar o dañar un equipo de cómputo o sistema de información sin el consentimiento de su propietario.

Usuario: Persona, proceso o aplicación autorizada para acceder a la información de la Entidad o a los sistemas que se utilizan para habilitar los procesos.

VPN (Virtual Private Network): Una Red Privada Virtual es una tecnología de red de computadores que permite tener una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.

ARTÍCULO 17. COMUNICACIÓN: El Jefe de la Oficina de Sistemas e Informática, dará a conocer este documento por todos los medios de comunicación internos: Correo electrónico, Intranet, SharePoint y hacer firmar de cada uno de los usuarios el documento de compromiso con estas políticas.

De igual forma, se realizarán campañas de sensibilización y jornadas de capacitación al personal de INDEPORTES ANTIOQUIA, para fortalecer y mejorar la conciencia de auto

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

cuidado y de seguridad de la información.

Toma de conciencia, educación y formación en la seguridad de la información:

Todos los empleados de INDEPORTES ANTIOQUIA, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.

Todo el programa de toma de conciencia en seguridad de la información debe apuntar a que los empleados, y en donde sea pertinente, los contratistas, tomen conciencia de sus responsabilidades de seguridad de la información, y de los medios por los cuales se cumplen estas responsabilidades.

Se debe establecer un programa de toma de conciencia en seguridad de la información, en línea con las políticas y procedimientos pertinentes de seguridad de la información de INDEPORTES ANTIOQUIA, teniendo en cuenta la información de INDEPORTES ANTIOQUIA que se va a proteger, y los controles que se han implementado para proteger la información.

El programa de toma de conciencia debe incluir varias actividades para toma de conciencia, tales como campañas (por ejemplo, el “día de la seguridad de la información”) y la elaboración de folletos y boletines de noticias.

La formación en toma de conciencia se debe llevar a cabo según se exija en el programa de toma de conciencia en seguridad de la información. Para la formación en toma de conciencia se pueden usar diferentes medios, dentro de los que se incluyen clase en aula, aprendizaje a distancia, aprendizaje basado en la web, aprendizaje autónomo, y otros.

La educación y la formación en seguridad de la información también debe comprender aspectos generales tales como:

- La afirmación del compromiso de la dirección con la seguridad de la información en toda INDEPORTES ANTIOQUIA.
- La necesidad de familiarizarse con las reglas y obligaciones de seguridad de la información aplicables y de cumplir con ellas, como se definen en las políticas, normas, leyes, reglamentos, contratos y acuerdos.
- La rendición personal de cuentas, por las acciones y omisiones propias, y las responsabilidades generales con relación a asegurar o proteger la información que pertenece a INDEPORTES ANTIOQUIA y a las partes externas.
- Los procedimientos básicos de seguridad de la información (tales como el reporte de incidentes de seguridad de la información) y los controles de línea base (tales como la seguridad de las contraseñas, los controles del software malicioso, y los escritorios limpios).
- Los puntos de contacto y los recursos para información adicional y asesoría sobre asuntos de seguridad de la información, incluidos los materiales de educación y formación sobre seguridad de la información.

ARTÍCULO 18. REVISIÓN: Esta resolución será revisada de forma anual por la Oficina de Sistemas e Informática y la alta Dirección de la Entidad, o antes si ocurren cambios

Radicado: S 2025000825
Fecha: 05/09/2025
Tipo:
RESOLUCIONES
2025000825

significativos, para asegurar su conveniencia, adecuación y eficacia continuas.

ARTÍCULO 19. VIGENCIA: La presente resolución rige a partir de la fecha de su publicación y deroga todas las disposiciones que le sean contrarias.

PUBLÍQUESE Y CÚMPLASE

LUIS GIOVANY ARIAS TOBÓN
Gerente

	NOMBRE	FIRMA	FECHA
Aprobó:	Juliana Bermúdez Henao Jefe Oficina de Sistemas e Informática		05/09/2025
Revisó:	Maria Teresa Muñoz PU Oficina Asesora Jurídica		05/09/2025
Proyectó:	Ana María Mesa Elneser Contratista – Oficina de Sistemas e Informática		05/09/2025
Aprobó:	León David Quintero Restrepo Jefe Oficina Asesora Jurídica		05/09/2025
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para firma.			