INSTITUTO DEPARTAMENTAL DE DEPORTES DEL CAUCA
INDEPORTES CAUCA

POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

VIGENCIA 2022

PRESENTACION

El Instituto Departamental de Deportes del Cauca – Indeportes Cauca considera el valor de proteger los activos de información institucional dado que expuestos a perdida, daños y/o modificaciones por parte de terceros. Continuamente en la gestión de los procesos y procedimientos de acuerdo a la misión y visión de la Entidad se están procesando información valiosa que es generada desde cada una de las dependencias del Instituto que va desde información confidencial del personal de la Entidad, proveedores, usuarios, entrenadores, hasta datos de deportistas de alto rendimiento del Departamento que no debe ser divulgada a personal no autorizado, lo cual pondría en riesgo a la Entidad.

Por consiguiente INDEPORTES CAUCA asume la función de implementar el Sistema de Seguridad de la Información(SGSI), de acuerdo con la estructura organizacional y presupuestal, siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) de la Estrategia de Gobierno Digital.

La Entidad es consciente que la defensa y protección de los activos de información es una tarea fundamental para garantizar la continuidad y el desarrollo de nuestros objetivos institucionales, y para cumplir con las actividades contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013 y en la Política de Seguridad Digital.

CONTENIDO

INTRODUCCION

El Instituto Departamental de Deportes del Cauca – Indeportes Cauca es consciente de la importancia del manejo y seguridad de la información en condiciones apropiados garantizando su integridad, confidencialidad.

El modelo de seguridad que desee implementar El Instituto Departamental de Deportes del Cauca se basa en el modelo de seguridad y privacidad de la información entregado en el marco de la estrategia Gobierno Digital, incluye el eje de seguridad y privacidad de la información el cual es muy importante ya que funciona de manera transversal a los ejes de TIC para gobierno abierto, TIC para la gestión y TIC para servicios con el objetivo primordial de mantener en óptimos niveles de seguridad los datos manejados en Indeportes Cauca través de sus funcionarios y contratistas y los datos de trámites y servicios por parte de los ciudadanos.

1. OBJETIVO

Presentar el plan de seguridad y privacidad de la información de El Instituto Departamental de Deportes del Cauca, como marco de referencia para el establecimiento y regulación de lineamientos y medidas que permitan el aseguramiento de la protección y uso adecuado de la información y activos de información que la soportan al interior de la Entidad.

2. ALCANCE

El modelo de seguridad y privacidad de la información de El Instituto Departamental de Deportes del Cauca tiene como alcance para funcionarios, contratistas y visitantes en los casos que aplique. apunta a proteger y preservar las características de integridad, confidencialidad y disponibilidad de los activos de información que se identifiquen como parte de esta política.

3. NORMATIVIDAD

El modelo de seguridad y privacidad de la información se basa, principalmente, en las siguientes leyes, normas o decretos:

LEY, NORMA O DECRETO	CONCEPTO
Ley 1266 de 2008	Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales

Ley 1341 de 2012	Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC.
Ley 1581 de 2012	Protección de datos personales
Decreto 1377 de 2013	Reglamentación parcial de la Ley de datos personales
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones
Decreto único reglamentario 1078 de 2015	Define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL

4. GLOSARIO

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4). PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN .

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Administración Municipal y, en consecuencia, debe ser protegido. Se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Amenaza: es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los elementos de información. Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de riesgos de seguridad de la información: proceso sistemático de identificación de fuentes, estimación de impactos, probabilidades y comparación de dichas

variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Autenticación: es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701). PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3) PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Disponibilidad: es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3).

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, 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 de 2014. (Ley 1712 de 2014, art 6).

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, 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 2014. (Ley 1712 de 2014, art 6).

Integridad: es la protección de la exactitud y estado completo de los activos de información.
Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.

Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Propietarios de los activos de información: son los responsables de cada uno de los activos de información (archivos, bases de datos, contratos y acuerdos, documentación del sistema, manuales de usuario, material de formación, aplicaciones, software del sistema, equipos informáticos, equipos de comunicaciones, servicios informáticos y de comunicaciones, las personas, etc. Esta persona se hará cargo de mantener la seguridad del activo.

Recursos tecnológicos: son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo.

Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25).

Responsabilidad Demostrada: Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Sistema de información (SI): es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo. Dichos elementos pueden ser personas, actividades o técnicas de trabajo, datos y recursos materiales en general.

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

5. POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

La gerencia del Instituto Departamental de Deportes del Cauca, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para el Instituto Departamental de Deportes del Cauca, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a Indeportes Cauca según como se defina en el alcance, sus funcionarios, contratistas y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

Indeportes Cauca entiende la importancia y gestionará los temas críticos en cuanto a la seguridad de la información de la siguiente manera:

- Minimizar el riesgo en las funciones importantes de la Entidad
- Cumplir con los principios de seguridad de la información
- Cumplir con los principios de la función administrativa
- Mantener la confianza de sus clientes, socios y empleados
- Apoyar la innovación tecnológica
- Proteger los activos tecnológicos
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información

5.1. NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento a esta política.

Las políticas que soportan el plan de seguridad y privacidad de la información del Instituto Departamental de Deportes del Cauca son:

a) El Instituto Departamental de Deportes del Cauca ha decidido definir, implementar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, alineados a las necesidades de la entidad.

b) Las responsabilidades frente a la seguridad de la información deberán ser definidas, compartidas y aceptadas por cada uno de los funcionarios, contratistas o terceros.

c) Instituto Departamental de Deportes del Cauca protege los activos de información y la información generada, procesada o resguardada por los procesos de la entidad.
d) El Instituto Departamental de Deportes del Cauca implementa controles de acceso a la información, sistemas y recursos de red.
e) El Instituto Departamental de Deportes del Cauca del garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
f) El Instituto Departamental de Deportes del Cauca del a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
g) El Instituto Departamental de Deportes del Cauca del garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
h) El Instituto Departamental de Deportes del Cauca del garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
i) El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

5.2. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Justificación

El Instituto Departamental de Deportes del Cauca con el propósito de proteger y amparar la información de la entidad en todos sus aspectos ha establecido realizar un Plan de Seguridad y Privacidad de la información con el ánimo de que no se presenten pérdidas, robos y accesos no autorizados, igualmente promueve una política de seguridad de la información física y digital.

La seguridad de la información se entiende como la preservación de las siguientes características:

a) Confidencialidad: El acceso a la información debe darse sólo a personas autorizadas.

b) Integridad: La información debe ser protegida en su totalidad.

c) Disponibilidad: La información y los distintos recursos deben estar disponibles para los usuarios, de acuerdo a las autorizaciones.

Roles y Responsabilidades

Es responsabilidad del Proceso de Sistemas de El Instituto Departamental de Deportes delCauca, la implementación, aplicación, seguimiento y autorizaciones de la política del Plan de Seguridad y Privacidad de la información en las diferentes áreas y procesos de la entidad, como parte de su herramienta de gestión.

Es responsabilidad de la División Técnica que tiene a cargo el Proceso de Sistemas, supervisar, hacer seguimiento y garantizar el uso de la Política de Seguridad de laInformación, la cual debe ser aplicada de forma obligatoria por todos los funcionarios y contratistas para el cumplimiento de los objetivos.

Cumplimiento

El cumplimiento de la Política de Seguridad y Privacidad de la Información es obligatorio para las diferentes áreas y procesos de la entidad, por parte de funcionarios y contratistassin excepción.

Si los funcionarios de la entidad o terceros violan este plan, El Instituto Departamental de Deportes del Cauca se reserva el derecho de tomar las medidas correspondientes.

Comunicación

Todos los funcionarios, contratistas y/o terceros deben conocer la existencia de las políticas, la obligatoriedad de su cumplimiento y la ubicación física, igualmente estará alojados en la página de la entidad www.indeportescauca.gov.co

Monitoreo

Se crearán los indicadores correspondientes a la política de seguridad con el fin de determinar el cumplimiento de las mismas para establecer qué modificaciones o adicionesdeben hacerse, este monitoreo debe realizarse como mínimo una vez al año.

5.3. DESCRIPCIÓN DE LAS POLITICAS

Políticas para el cuidado de los equipos informáticos

El equipo de cómputo de propiedad del Instituto Departamental de Deportes del Cauca únicamente se podrá instalar y utilizar software o programas, sistemas de información, herramientas de software en equipos de cómputo de propiedad del Instituto de Deportes del Cauca que sean licenciados y autorizados por la Entidad.

Los Equipos de cómputo no podrán ser utilizados para actividades de divulgación, propagación o almacenamiento de contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso, o cualquier otro uso que no esté autorizado.

Organización y Clasificación de la información

Todo servidor público o persona entenderá y asumirá su responsabilidad de protección de la información a través de su acceso y uso apropiados.

El Instituto Departamental para la Recreación y el Deporte será el dueño de la propiedad intelectual de los avances desarrollados por los contratistas, servidores públicos o terceros, derivados del objeto y en cumplimiento de las funciones o tareas asignadas bajo acuerdo contractual.

Todos los contratistas, servidores públicos o terceros deberán firmar el acuerdo de confidencialidad y transparencia, en el cual se establece la responsabilidad de confidencialidad de la información de la entidad bajo su responsabilidad.

Los usuarios deben recoger de las impresoras, escáneres y fotocopiadoras inmediatamente los documentos confidenciales para evitar su divulgación no autorizada o mal intencionada.

Los usuarios no deberán almacenar información en discos duros de los equipos de cómputo o virtuales disponibles de archivos de video, música, fotos o cualquier tipo de archivo que no sea de carácter institucional.

Política de Seguridad De Recursos Humanos

Todos los contratistas deberán realizar la devolución de cada uno de los activos de información asignados, y realizar el proceso de diligenciamiento de paz y salvo de la Entidad con los tramites al día a la terminación del contrato.

El Instituto Departamental de Deportes del Cauca se asegurará acerca de la aceptación de las responsabilidades del acceso y uso de información o activos de información en aseguramiento de la confidencialidad de la información y transparencia mediante la firma de formato definido por la Entidad.

Seguridad Física y Ambiental

Los funcionarios y contratistas deben portar el carné que los identifica como contratistas o funcionarios en un lugar visible mientras se encuentren en las instalaciones de Indeportes Cauca. Aquellos contratistas, funcionarios o personal externo que realice alguna prestación de servicio, deben utilizar prendas distintivas que faciliten su identificación.

Se deberán definir e implementar programas de mantenimiento preventivo y correctivo de los equipos instalados en las áreas seguras del Instituto Departamental de Deportes del Cauca.

El Proceso de Sistemas debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado.

Política de Uso de Internet

El Instituto Departamental de Deportes del Cauca permitirá el acceso a servicios de internet, con lineamientos que garanticen la navegación y uso controlados de componentes del servicio.

Se restringirá toda posibilidad de descarga de software no autorizado o código malicioso en los equipos de cómputo del Instituto Departamental para la Recreación y el Deporte a través de internet.

El acceso y uso del servicio de internet se concederá solo para propósitos laborales o fines particulares definidos y aprobados por El Instituto Departamental de Deportes del Cauca para los propósitos de almacenamiento de archivos e información, El Instituto Departamental de Deportes del Cauca dispone de discos para realizar backup. En dichos discos no se almacenará información personal, música, videos, ni información que no concierna a Indeportes Cauca.

Se restringirá el acceso a sitios web dedicados a compartir material audiovisual fotos, videos, streaming tales como Facebook, Youtube, Flickr, TeamViewer, Twitter, y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias de la Entidad.

No se permitirá el acceso a sitios web con contenidos que están en contra de la ley, principios de ética moral del Instituto Departamental de Deportes del Cauca tales como, pornografía, terrorismo, contenidos obscenos, discriminación racial o similar.

Política de Gestión De Control De Acceso

Instituto Departamental de Deportes del Cauca definirá las pautas y criterios generales para controlar y asegurar la asignación de derechos de acceso lógico a usuarios sobre los sistemas operativos, datos o información, servicios de información de la plataforma tecnológica o red de datos que sea concedida.

Toda asignación de derechos de acceso lógico a usuarios se realizará bajo el cumplimiento de un protocolo y diligenciamiento de solicitud y autorización Contraseñas de usuarios de acceso a información o servicios de red deberán mantenerse confidenciales bajo buenas prácticas de protección de confidencialidad de estas.

Toda conexión inalámbrica deberá ser establecida bajo las condiciones y medidas de seguridad basadas en la configuración y el monitoreo de las redes locales inalámbricas y de los dispositivos allí conectados para la conexión a dichas redes.

Los equipos de cómputo que se conecten o deseen conectarse a las redes de datos de la Empresa deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

	NOMBRE	CARGO	FIRMA
ELABORÓ	**ISABEL FERNANDEZ**	Contratista - Sistemas	**Original firmado**
REVISO	**ANYELA M. PALACIOS**	Subgerente administrativa y financiera	**Original firmado**
REVISO	**DIANA MARCELA FABARA**	PU PLANEACION	**Original firmado**
APROBO	**OLIVER CARABALI BANGUERO**	Gerente	**Original firmado**