POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

INDERVALLE	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN **POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN** **PROCESO DIRECCIONAMIENTO ESTRATÉGICO**	CODIGO	PE-PO-100-009
		VERSIÓN	2
		APROBADO	10/MAR/2021

Contenido

1. INTRODUCCIÓN

Para el Instituto del Deporte, la Educación Física y la Recreación del Valle del Cauca - Indervalle, la información es un activo de alta prioridad que genera el desarrollo permanente de la misión y el cumplimiento de los objetivos, la cual puede ser de naturaleza legal, estratégica, financiera, etc., y es consciente de que las amenazas a que se enfrenta al no tomar las medidas adecuadas de seguridad, expone a la entidad a la vulneración de estos activos de información en cualquier estado en que se encuentre, como son: creación, procesamiento, almacenamiento, transmisión, utilización o destrucción y se pueden llegar a tener impactos legales, operacionales y de imagen.

Es por ello que esta Política pretende desarrollar acuerdos y controles para proteger la confidencialidad, integridad, disponibilidad, privacidad, continuidad, autenticidad y no repudio de los activos de información de la Entidad y que, dentro del proceso de Gestión de las comunicaciones, el área de Sistemas es la encargada de liderar y hacer seguimiento a la Política de Seguridad de la Información, orientados, siempre, a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información –SGSI.

2. OBJETIVOS

2.1. General

Establecer lineamientos que regulen la seguridad de la información en Indervalle, desde la emisión inicial, actualización y consulta, teniendo en cuenta que en todo momento la prioridad es salvaguardar los datos bajo los estándares internacionales de seguridad de la información, basado en la identificación y valoración de los riegos asociados a ellos, propendiendo por la protección de su confidencialidad, integridad, disponibilidad, privacidad, continuidad, autenticidad y no repudio y por el cumplimiento de la normatividad vigente aplicable

2.2. Específicos

a) Establecer los lineamientos que se consideren necesarios para seguir en materia de consulta y manipulación de los datos por parte de los diferentes funcionarios de la entidad.
b) Establecer las metodologías para el registro, control y seguimiento de los cambios que se realicen en los datos.
c) Definir las diferentes acciones a seguir cuando los datos se enfrentan a incidentes donde pongan en riesgo la integridad del contenido.
d) Desarrollar los controles estrictos que se deben consultar respecto a la vulneración de la información por parte de agentes externos y que no han sido autorizados.

3. ASPECTOS LEGALES

El Instituto del Deporte, la Educación Física y la Recreación del Valle del Cauca – Indervalle, se basa en las siguientes leyes, decretos y demás aspectos legales que regulan la Seguridad de la Información para implementar y divulgar la Política de Seguridad de la Información.

Ley 1273 de 2009. Por medio de la 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.

La constitución política de Colombia de 1992 donde reconoce en el artículo 15 el Habeas Data y **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, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales y **Decreto 1377 de 2013.** Por el cual se reglamenta parcialmente la Ley 1581 de 2012

Ley 594 de 2000. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.

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. y **Decreto 103 de 2015.** Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

El decreto 1599 de 2005. Por el cual se adopta el Modelo Estándar de Control Interno para el Estado Colombiano – MECI - para el estado de Colombia.

GLOSARIO

a) **Confiabilidad de la Información:** Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

b) **Confidencialidad:** Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

c) **Disponibilidad:** Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

d) **Estándar:** Lineamiento donde se da a conocer la acción a ejecutar cuando se dé una situación específica, estos estándares son instrucciones obligadas a seguir por parte de los funcionarios de la entidad ya que van a garantizar que una situación se resuelva de acuerdo a lo establecido.

e) **Equipos activos de red:** Son todos los dispositivos que hacen la distribución de las comunicaciones a través de la red de datos.

Guía: Con guía se refiere el camino o caminos sugeridos a seguir cuando se enfrente a problemas donde el enfoque sea la seguridad de la información, estas deben ser seguidas tal cual lo dicta el documento siempre y cuando no exista una justificación documentada y probada donde se detalle claramente el por qué no se debe seguir la guía.
Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la entidad.
Mejor practica: Regla de seguridad concreta o sistema que es aceptado, ya que esta proporciona el objetivo más concreto a una implementación concreta. Las mejores prácticas son establecidas para garantizar que los atributos de seguridad de los sistemas que se están utilizando cumplen de manera uniforme y que esto pueda brindar la confianza necesaria de saber que se está realizando según las normas estándares de seguridad de la información.
Procedimiento: Los procedimientos son los que definen claramente como las políticas, estándares, mejores prácticas usadas y las guías van a ser implementadas en una situación dada. Estos procedimientos tienen que ser independiente de la tecnología que se está usando. Estos definen a una área o dependencia los pasos a seguir para implementar la seguridad de la información con dicho proceso sistema en concreto. Se puede decir que los procedimientos son desarrollados, implementados y supervisados por el duelo del proceso o del sistema. Los procedimientos tienen que seguir las políticas, los estándares y las mejores prácticas tan al pie de la letra como les sea posible y a la vez tienen que ajustarse a los requerimientos de cada área o dependencia.
Política: Establecimiento por parte de los niveles directivos donde se describe la posición de la entidad respecto a un tema.
Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
Seguridad de la información: Establece los lineamientos para proteger los datos de una entidad o empresa garantizando la integridad de los datos y que estos no puedan ser manipulados ni corrompidos por ningún agente externo que pueda vulnerar la seguridad de estos independiente del sistema, tecnología que se está usando ni la cantidad de funcionarios que gestionan los datos diariamente.
Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

4. A QUIEN VA DIRIGIDA

En INDERVALLE, la estrategia de implementación de Políticas de Seguridad de la Información va dirigida a los todos funcionarios de planta (directivos, profesionales, asistenciales y personal técnico), así como a los contratistas y terceros que desempeñen alguna labor en la entidad y que trabajen con dispositivos tecnológicos como los que no manipulan información a través de estos. Esta se realiza a través de la inducción, reinducción y capacitaciones del personal.
El área de Sistemas de Indervalle es el responsable de dar soporte, adaptar, cumplir, hacer los respectivos controles, realizar el debido seguimiento y mediciones para ajustes posibles que se puedan evidenciar.

5. DECLARACIÓN DE POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Indervalle, es un establecimiento público de Orden Territorial, que maneja, fomenta y apoya el deporte en la región del Valle del cauca, con personería jurídica, autonomía administrativa y patrimonio independiente, comprendiendo la importancia que la seguridad de la información tiene para el desarrollo y buen funcionamiento de sus procesos internos, se toma la decisión de implementar un Sistema de Gestión de Seguridad de la Información (SGSI), basado en la norma internacional ISO 27001 de 2013 y un Modelo de Seguridad y Privacidad de la Información (MSPI), de Gobierno en Línea (GEL), suscribiendo la presente política.

Indervalle es quien establece, define y revisa los objetivos, dentro del SGSI y el MSPI de GEL, encaminados a mejorar su seguridad, entendiéndola como la preservación de la confidencialidad, integridad y disponibilidad de la información, así como de los sistemas que la soportan, incrementando los niveles de confianza en los servidores públicos, contratistas y otras partes interesadas, todo lo anterior, es fortalecido mediante el cumplimiento de todos los requisitos legales, reglamentarios y contractuales, que le sean de aplicación según la normatividad vigente Colombiana.

El diseño, implantación y mantenimiento del SGSI y el MSPI de GEL, se apoyará en los resultados de un proceso continuo de análisis y valoración del riesgo, del que se derivan las actuaciones a desarrollar, en materia de seguridad, dentro del alcance del SGSI y el MSPI de GEL, aprobado por la Alta Dirección de Indervalle, guardando una estrecha relación con la declaración de aplicabilidad vigente.

La Alta Dirección de Indervalle establecerá los criterios de evaluación del riesgo, de manera que todos aquellos escenarios, que impiden un nivel de riesgo aceptable, sean tratados adecuadamente y mitigados, adicional, la Alta Dirección desarrollará, implantará y mantendrá actualizado un Plan de Continuidad del Negocio, acorde a las necesidades de la entidad y dimensionado a los riesgos que le afectan.

La Alta Dirección de la Indervalle se compromete a la implantación, mantenimiento y mejora del SGSI y el MSPI de GEL, dotándolos de aquellos medios y recursos que sean necesarios e instando a todos los servidores públicos, contratistas y partes interesadas, para que asuman este compromiso. Para ejecutar esto, Indervalle implantará las medidas requeridas para la formación y concienciación de los servidores públicos, contratistas y partes interesadas, en temas de seguridad de la información. A su vez, cuando exista una violación de las políticas de seguridad de la información, aprobadas por la Alta Dirección, Indervalle se reserva el derecho de aplicar las medidas disciplinarias, acordes a los compromisos laborales de los servidores públicos, contratistas y partes interesadas, dentro del marco legal aplicable y dimensionada al impacto que tengan sobre la entidad.

Indervalle entiende la importancia y gestionara los temas críticos en cuanto a la seguridad de la información de la siguiente manera.

a) Minimizar el riesgo en las funciones importantes de la entidad

b) Cumplir con los principios de seguridad de la información

c) Cumplir con los principios de la función administrativa

d) Mantener la confianza de sus clientes, socios y empleados

e) Apoyar la innovación tecnológica

f) Proteger los activos tecnológicos

g) Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información

6. NIVEL DE CUMPLIMIENTO

Todos los funcionarios y contratistas deben dar estricto cumplimiento a la actual política de seguridad de la información. A continuación, se establecen las 12 políticas de seguridad de la información que deben soportar el SGSI de Indervalle

a) Indervalle decide definir, implementar, operar y mejorar de forma continua su SGSI, de manera que soporte los lineamientos claros que estén encaminados a las necesidades del negocio de la entidad, y a los requerimientos que regulan y se aplican a esta naturales.
b) Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los contratistas, contratistas y toda persona que haga uso de los activos de información de Indervalle.
c) Indervalle protegerá la información que se genere, que se procese o sea resguardada por los procesos del negocio y activos de información relacionados.
d) Indervalle debe proteger la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar los impactos financieros, operativos o legales debido al uso incorrecto de estos.
e) Indervalle protegerá su información de las amenazas originadas por parte del personal.
f) Indervalle protegerá las instalaciones de procesamiento y la infraestructura Tecnológica que soporta sus procesos críticos.
g) Indervalle controlara la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
h) Indervalle implementara control de acceso a la información, sistemas y la red de la entidad.
i) Indervalle garantizara que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
j) Indervalle garantizara a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información.
k) Indervalle garantizara la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
l) Indervalle debe garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

m) El incumplimiento de estas políticas de seguridad de información, traerá consigo las consecuencias legales que dicta la Ley, que se apliquen a la normatividad vigente colombiana, incluyendo lo establecido por el gobierno nacional y territorial en cuanto a seguridad de la información y privacidad de esta.

7. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información, se va a encargar de coordinar, centralizar y monitorear toda la gestión que se realice entorno a la seguridad informática de Indervalle.

8.1. Funciones

Las funciones de las que serán responsables los miembros del comité de la seguridad de la información serán las siguientes:

a) Dar forma, promover y coordinar los proyectos de seguridad de todos los procedimientos de la entidad Indervalle.
b) Impulsar la creación de las diferentes directrices que tengan que ver con la seguridad de la información.
c) Definir la estructura con la que se va a organizar la seguridad de la información de la entidad Indervalle y que va a ser gestiona por el Área de Sistemas de la entidad.
d) Definir las responsabilidades de todo el personal que va a estar involucrado, incluyendo, funcionarios de carrera administrativa, asesores, contratistas, provisionales y personal de libre nombramiento y remoción de la organización.
e) Administrar las decisiones de seguridad, normas, políticas, planes de continuidad del negocio, análisis de riesgos, recuperación de desastres, entre otros temas relacionados.
f) Aprobar las medidas de política de seguridad de la información.
g) Dar el visto bueno y adoptar los procesos que sean necesarios para formalizar el uso de todos los sistemas y servicios de información y deben establecer las correspondientes revisiones que se necesiten sobre esto.
h) Coordinar todos los esfuerzos debidos y necesarios asignando las diferentes responsabilidades sobre la seguridad de la información de la entidad.
i) Dar el visto bueno a los acuerdos de confidencialidad que se establezcan con terceros, contratistas, ya sean sobre servicios o personal.
j) Administrar todos los cambios, actualizaciones o mejores que se vayan a realizar en cuanto a la seguridad de la información de los diferentes servicios informáticos de Indervalle.

8.2. Conformación

El Comité de Seguridad de la Información está conformado por los siguientes miembros.

a) Presidencia: Gerente de Indervalle o quien este designe para su representación.

b) Vocerías: Un representante de las siguientes áreas de la entidad Indervalle:
   - Subgerencia de Fomento
   - Subgerencia de Competición
   - Subgerencia de Planeación
   - Centro de Medicina Deportiva
   - Secretaria General
   - Cada una de las áreas que conforman la Subgerencia Administrativa y Financiera (Almacén, Recursos Humanos, Tesorería, Presupuesto, Contabilidad, Sistemas, Recaudo)

c) Secretaria general del comité.

d) La persona responsable de la seguridad de la información que debe ser designado por el área de Sistemas de Indervalle entre los integrantes de dicha área.

8.3. Funcionamiento del comité

a) El comité se debe reunir una vez cada seis meses de carácter ordinario y de carácter extraordinario cada vez que su presidente lo requería.

b) Socializar incidentes de seguridad graves que afecten a cualquiera de las áreas que hacen parte de Indervalle.

c) Identificar nuevas necesidades dentro de la entidad que se haga necesaria la participación del comité.

d) El comité puede crear de forma independiente las ponencias técnicas que se hagan necesarias para el normal desarrollo dentro de sus funciones.

e) A las reuniones que tenga el comité pueden asistir en calidad de asesores las personas que crea conveniente para cada caso el presidente.

f) El comité se debe ajustar a los reglamentos internos de la entidad Indervalle y los que dicte la ley para su normal funcionamiento.

8. GESTIÓN DE ACTIVOS

El alcance de la Gestión de Activos incluye la administración y la responsabilidad que se debe tener frente a los activos de información, como son:

8.1 Identificación de activos:

Indervalle a través del área de Sistemas identifica los activos en el Registro Inventario de Activos de Información, el cual debe ser actualizado cada seis meses en las dependencias de la entidad.

8.2 Clasificación de activos:

Indervalle conoce la importancia de usar la información, gestionarla y define la clasificación en el Registro Inventario de Activos de Información, a través de, Objetivo de la excepción, fundamento constitucional o legal, fundamento jurídico de la excepción, excepción total o parcial, fecha de la calificación, plazo de la clasificación o reserva.

Se considera información cualquier forma de comunicación o representación de los conocimientos o datos digitales que se hayan escrito en cualquier medio, ya sea medios físicos, medios magnéticos, medios visuales entre otros que genera Indervalle como, por ejemplo:

a) Formularios, comprobantes propios o de terceros que lleguen a Indervalle.
b) Datos en los sistemas de información, equipos informáticos de la entidad, partes electrónicas o magnéticas y los considerados medios físicos como el papel.
c) Soportes magnéticos que sean de carácter removible o fijos.
d) Todo tipo de información que sea transmitido de forma verbal o por cualquier otro medio de comunicación.

8.3 Etiquetado de la información:

El Registro Inventario de Activos de Información, establece la siguiente información para cada activo: dependencia, nombre de la información, descripción, idioma, medio de conservación y/o soporte, formato, información de disponibilidad, responsable de la producción de la identidad, frecuencia de producción de la información, frecuencia de la generación de información, tipo de información.

Para verificación de los cambios en el tiempo, Indervalle utiliza el formato Control de cambios.

8.4 Devolución de los activos:

Los activos de información son procesados, gestionados y actualizados por los funcionarios y contratistas de INDERVALLE en las diferentes áreas teniendo en cuenta:

a) Identificar los activos que se estaban usando: inventario personal de activos que estaba manipulando de tal manera que se pueda evidenciar como le fue entregada la información y como la está devolviendo.

b) Verificación de los cambios en el tiempo: se evidencia a través de cambios, ya sea en físico, por escrito o en el sistema de información de apoyo para este proceso donde se pueda ver claramente todos los cambios que se realizó en el activo

c) Cambios de acceso a los activos de información: se realiza el proceso de los respectivos cambios de acceso de tal manera que el usuario no pueda tener acceso nuevamente a estos archivos, esto debe quedar evidenciado tanto en el software o

informando a los responsables de los activos de información en la oficina respectiva.

d) Empalme con nuevo usuario si es necesario Se realiza el empalme de entrega y recibimiento de los activos por parte del usuario que los devuelve y de parte del usuario que los recibe para seguir su debida gestión, esto es solo necesario en caso que alguien vaya a seguir manteniendo la información, si el ciclo de vida de ese activo termina con la entrega del anterior usuario no se hace necesario este paso.

e) Responsabilidad del proceso se asigna un responsable por cada área que la representa en el comité de seguridad de la información de Indervalle y lidera la gestión de devolución de los activos.

f) Instrumento de evidencia: Todos los anteriores pasos quedan registrados en el sistema de gestión de activos de información que Indervalle haya dispuesto para tal fin, de manera que pueda ser ingresado en este software.

8.5 Gestión de medios removibles:

Dado que prácticamente todos los equipos tecnológicos hablando de computadores tienen acceso vía lectores de USB y acceso vía bandejas lectoras de CD-ROM se hace indispensable tener claro cómo se debe acceder y bajo que riesgos debe tener el introducir uno de estos dispositivos. Debemos tener contemplado las políticas de acceso y copiado de información con este tipo de instrumentos.

8.5.1 CD-ROM

En todos los computadores que pertenezcan a la entidad se debe realizar el proceso de bloque de las bandejas de CD- ROM, esto nos va a garantizar que los usuarios no copien mediante este instrumento y que no instalen ningún programa adicional o software que venga contenido en un CD. Para lo cual se realiza mediante bloqueo desde el editor de registros y mediante el usuario Administrador del computador, es decir que debe hacerse en cada uno de los computadores. Para justificar su activación esta debe ser redactada por el funcionario y comunicada al vocero del área en cuestión que pertenezca al comité de seguridad de la información con el cual realizara el debido tramite en la oficina del área de sistemas al secretario general del comité que pertenece a esta área, el cual debe proceder a su correspondiente análisis de la justificación y posterior activación de esta funcionalidad en el computador concreto, teniendo en cuenta que esta activación tiene un rango de tiempo límites para lo cual debe volver a desactivarse por cuestiones de seguridad.

8.5.2 Dispositivos de almacenamiento masivo USB

Para este tipo de dispositivos debe aplicar la misma regla anterior donde debe estar bloqueado el acceso mediante USB a estos, realizar este mismo procedimiento para cada uno de los computadores que hagan parte de la entidad Indervalle.

Se debe realizar el respectivo procedimiento involucrando al vocero del comité de la seguridad de información quien debe ser el enlace para este tipo de requerimientos, el cual tramitará los respectivos accesos y permisos para el computador que se necesita habilitar.

8.5.3 Dispositivos de almacenamiento externo USB

En caso que la información a gestionar en los anteriores puntos este contenida en un dispositivo de almacenamiento masivo como las memorias USB, discos duros memorias extraíbles, debe considerarse realizar los mismos pasos anteriormente delimitados, siguiendo al pie de la letra las instrucciones y dejando evidencia de este proceso en las diferentes actas para lo cual se ha designado.

Cuando el dispositivo sea borrado en el último punto, se debe realizar un formateo a bajo nivel para garantizar que los datos anteriores no sean posibles recuperarlos en caso que se trate de información sensible o reservada y que el dispositivo se siga usando.

8.5.4 Dispositivos móviles

Indervalle comprende que los dispositivos móviles inteligentes son cada vez más usados para muchas gestiones y para ello se dicta la política clara frente a esto respecto al buen uso y abuso de la información enviada a través de estos por las diferentes aplicaciones que hay para ello.

La entidad bloquea la conexión a todos los puntos de conexión WIFI que se tengan en la entidad de este tipo de dispositivos, mediante configuración y bloqueos por dirección MAC de los equipos se realiza este filtrado, desde allí se verifica y se niega el acceso a la red de Indervalle.

Si algún dispositivo se requiere ingresar a la red se debe tramitar con el vocero de cada área que pertenezca al comité de seguridad de la información, el cual a su vez debe realizar el trámite de permisos antes el subgerente de cada dependencia justificando el porqué de la conexión del móvil, tiempos de conexión, rango de fechas de autorización y su debida identificación del dueño del dispositivo y sus características internas de fabricación.

Si la entidad cuenta con dispositivos móviles propios se puede realizar el debido registro de estos antes los diferentes routers e identificarlos para tener claridad cuáles son, quien los usa y su debida gestión que se realiza con estos.

Realiza también a los funcionarios que tienen dispositivos móviles conectados a la red WIFI que debe hacer uso racional de la red en términos de descargas, multimedia ejecutada en páginas de videos, audios ejecutados ya que son recursos que consumen

mucha cantidad de red y puede quitar ancho de banda a otras áreas que lo necesitan y por lo tanto ralentizar la red de internet.
Realiza la recomendación de no enviar archivos de texto, audios y videos por la aplicación de WhatsApp que sean contemplados como sensibles, reservados ello para evitar perdida, filtraciones de estos dentro de esta red de la aplicación que pertenece a terceros, esto mismo aplica para todo tipo de aplicaciones similares a WhatsApp o que se use con el mismo fin.

8.5.5 Disposición final de los activos:

Cada vez que se vaya a realizar el retiro de un dispositivo tecnológico en el cual se encuentre información con la cual se halla trabajado o gestionado durante un periodo de tiempo por funcionarios internos o externos, este debe ser procesado mediante la política de retiro de dispositivos donde se contemple estrictamente las medidas a seguir en torno a los archivos, backups, usuarios, logs de cambios y todo lo relacionado con información que pudiera haberse gestionado en dicho aparato. Se debe contar con las medidas necesarias para salvaguardar la información de esta, de ser posible trasladarla a otro equipo similar o resguardarla en dispositivos de almacenamiento para su posterior consulta de datos.

El procedimiento para realizar esta gestión de retiro de uno de los equipos tecnológicos de la entidad es la siguiente en estricto orden de cumplimiento.

- Responsable del proceso: Por cada área debe tomar la responsabilidad el vocero del comité de la seguridad de información quien debe tramitar, gestionar, comunicar, entre otros, el debido proceso ante el secretario general del comité del área de Sistemas quien hará las veces de supervisor del proceso y encargado de verificar que todos los pasos se estén cumpliendo bajo lo acá destinado en las políticas de seguridad de información.

- Identificación del equipo a retirar: Se debe realizar la debida caracterización y búsqueda en el inventario del equipo sé que se está retirando, con esto vamos a realizar la ubicación en el sistema de información donde debe estar consignado toda la información respectiva de uso, funciones, roles y los usuarios que están involucrados en la gestión de información en dicho equipo tecnológico.

- Identificación de la información gestionada: Se debe verificar el estado de la información que se usaba en el dispositivo tecnológico, para confirmar el uso, los cambios y los debidos respaldos de seguridad con los que se cuenta en los repositorios generales, de esta forma conocemos y damos el visto bueno de los datos que se estaban administrando desde allí.

- Disposición de copias de seguridad o traslado de la información: Realizar las debidas copias de seguridad de información actualizadas en los contenedores de información para salvaguardar una última versión de los datos en caso que no se vaya a usar más, en caso que sea necesario realizar el traslado de esta hacia otros dispositivos tecnológicos este proceso se debe realizar teniendo en cuenta todas las medidas que implica trasladar datos de manera que no se vayan a dañar, perder o corromper en el camino hacia el nuevo contenedor de estos.

- Borrado seguro de la información: Cuando la información haya sido traslada hacia el nuevo destino, sea confirmada verificando que sea copia exacta del anterior, debe realizarse el procedimiento de borrado de esta, reiterando que debe realizarse una confirmación ultima de seguridad antes de borrar los datos. La única persona autorizada para borrar la información es el secretario del comité de seguridad de la información.

9. CONTROL DE ACCESO

Indervalle cuenta con sistemas de información misionales, con sistemas de información para la gestión documental, además de sistemas de trámites y servicios, al igual que sistema donde se gestiona toda la parte financiera de la entidad y otros sistemas de información de apoyo para tareas concretas, en cuanto a los equipos de cómputo cuentan con usuario y contraseña, según política de seguridad de acceso de tal manera que solo es posible ingresar por el usuario al cual fue asignado el equipo.

9.1 Control de acceso con usuario y contraseña

Cada usuario que tenga acceso a los sistemas de información o tenga asignado un equipo de cómputo debe tener un usuario y contraseña única e irrepetible para su correspondiente control. La asignación de esta debe corresponder con el debido procedimiento PR-330-005 Gestión de las TICS el cual explica detalladamente como debe hacerse la solicitud de un usuario y clave de acceso detallando el objetivo sistemas de información o equipo de cómputo.

Es de aclarar las responsabilidades que debe tener el usuario ya sea funcionario interno, funcionario externo o contratista de la entidad, independiente de la anterior caracterización debe tener claro las implicaciones de tener estos datos. Entre las diferentes responsabilidades que se debe tener es que un usuario y contraseña asignado es de carácter confidencial y por lo tanto se vuelve obligatorio no compartir esta información con nadie ni mucho menos transferirla a otro usuario ya que puede poner en riesgo la información que gestiona por medio de estos.

Se aclara de igual manera que el procedimiento para modificación corresponde con el PR-330-005 gestión de las TICS el cual dictamina los pasos para relacionar todos los cambios que se realicen en las contraseñas.

Para realizar el procedimiento de suspensión o eliminación del correspondiente usuario debe realizarse mediante el PR-330-005 gestión de las TICS, el cual nos guía sobre los pasos a seguir para realizar la suspensión de estos datos ya sea en el sistema de información o el equipo de cómputo.

9.2 Suministro de control de acceso

La designación de roles de los usuarios en los sistemas de información debe también tener una política clara que seguir para realizar este procedimiento, por lo tanto, se dicta la guía a seguir cuando un usuario requiere privilegios adicionales, cuando se requiere

remover estos privilegios, en cualquier de estos casos se debe dirigir al procedimiento PR-330-005 gestión de las TICS, el cual nos aclara y guía dentro de este proceso.

Es de aclarar que todo este proceso debe hacerse por intermedio del vocero del comité de la seguridad de información quien debe comunicar la petición a el secretario general del comité del área de Sistemas el cual recepciona, verifica y ejecuta los cambios debidos donde haya lugar, ya sea el sistema de información objetivo o el equipo de cómputo, agregando o removiendo privilegios.

9.3 Gestión de contraseñas

En este apartado se debe garantizar la total calidad de la contraseña asignada, siguiendo los parámetros mínimos de seguridad en cuanto a la robustez de la contraseña, se debe evitar totalmente la fragilidad de estas claves, la contraseña como mínimo debe ser de 8 caracteres los cuales deben contar entre sus caracteres con 1 letra mayúscula, 1 letra minúscula, 2 números y 1 carácter especial para de esta manera cumplir con la normativa a nivel internacional de claves seguras.

Por lo anterior se dictamina que la contraseña sea generada automáticamente por un algoritmo autómata el cual tenga integrado entre su parametrización los requisitos mínimos.

El funcionario al que se le haya asignado dicha contraseña debe responsabilizarse de esta y prevenir a toda costa que sea conocida por alguien diferente, en caso dado que la contraseña sea puesta en riesgo de seguridad, inmediatamente debe realizar el procedimiento de cambio de la misma realizando el debido proceso para ello. Es responsabilidad total del funcionario si pasan más de 24 horas desde el incidente de seguridad y puesta en riesgo de la contraseña asignada, el cual tiene que hacerse responsable por cualquier vulneración de los datos que tiene asignados y de los sistemas de información o equipos tecnológicos que use.

Todas y sin excepción, ya sean contraseñas de sistemas de información o contraseñas de equipos de cómputo deben tener una periodicidad de cambio de 6 meses en los cuales el secretario general del comité debe ser el responsable de contactar a los voceros de cada área para informarle del cambio en el usuario de su correspondiente área y vincularse con el debido procedimiento para actualizar dicha clave y entregar los nuevos datos, quedando evidencia de todo en la bitácora de las políticas de seguridad de la información.

9.4 Perímetros de seguridad

Teniendo en cuenta que toda la información resguardada es importante ya sea datos en medios físicos o medios digitales, y que esta información debe estar resguardad en lugares seguros y en óptimas condiciones para su conservación, se dictan las políticas para el acceso al perímetro de dichos lugares ya que no todos los funcionarios pueden tener acceso a estos lugares, solo pueden estar las personas involucradas y autorizadas.

Para la información que se encuentra relacionada y salvaguardad en formatos físicos esta debe estar en lugares, armarios o habitaciones dispuestas para ello y en estar área que en Indervalle es área de archivo, solo puede acceder el jefe de esta área, ningún documento puede salir de este lugar, por lo tanto, este lugar es totalmente restrictivo para cualquier persona diferente al responsable del área en cuestión. En caso de ser estrictamente necesario acceder por cuestión de daños en el lugar o adecenamientos que se tenga que hacer por parte del personal de servicios generales, se debe hacer uso del PR-330-005 gestión de las TICS en el cual se dicta la norma para ingreso de personal al archivo de resguardo.

La información que se guarda a nivel digital y que se encuentra resguardada en los servidores de la entidad Indervalle, estos que deberían estar en el cuarto o habitación de máquinas tecnológicas solo puede ser accesado por el personal autorizado del área de sistemas, recordando que para entrar y estar en este lugar se debe seguir las recomendaciones de limpieza, libre de humo, entre otros teniendo en cuenta que se trata de un lugar refrigerado.

Cualquier persona incluidos los propios funcionarios del área de sistemas que quieran ingresar deben diligenciar el formato del PR-330-005 gestión de las TICS el cual da la guía de como ingresar y el tiempo que mantendrá dentro de esta habitación, solo de esta manera se puede ingresar, aclarando de nuevo que solo los responsables del área de sistemas lo pueden hacer, ningún otro funcionario diferente va a poder entrar, si es necesario que personal de aseo, de reparaciones deba entrar estos deben diligenciar el formato anteriormente nombrado además que debe entrar acompañado de algunos de los funcionarios del área de sistemas para que supervise las funciones que se están realizando en dicha habitación.

9.5 Áreas de carga:

La importancia del área donde se realiza la carga de paquetes físicos para bodegas debe tener las condiciones especiales de seguridad, limpieza, estandarización para que el trabajo se realice correctamente, especificando los atributos que sean convenientes para ello. Indervalle cuenta con área de bodega donde se realiza este procedimiento el cual debe seguir las normas básicas para este fin.

Los responsables de esta política deben tener el acompañamiento del jefe de bodega el cual debería estar en condiciones de brindar todas las especificaciones siguiendo la normatividad para estas áreas. Estas áreas deben contar con el control de acceso debido para que ninguna persona no autorizada ingrese a este espacio. Se cuenta con el PR-330-005 gestión de las TICS en el cual se especifica la guía para ingreso de personal no autorizado a esta área de la entidad.

10 NO REPUDIO

Indervalle por su características y filosofía enfocada en el deporte gestiona muchos datos día a día, en el cual se ven involucrados muchos actores con diferentes roles, estos actores de los sistemas que los conforman los contratistas, funcionarios de planta, contratistas externos, entre otros. Dada la cantidad de usuarios que hacen parte

de los sistemas de información con los que cuenta la entidad, se debe contar con estrictos protocolos de comunicación entre estos usuarios dentro de las aplicaciones de tal forma que todo el proceso que se haga quede registrado.

Los sistemas de información que se usan tanto misionales, como gestor documental, sistema de trámites y servicios debe garantizar y tomar en cuenta los siguientes aspectos a tener en cuenta. Igualmente, todos los procedimientos y procesos que se hagan de forma manual tienen que cumplir con las políticas de no repudio.

Trazabilidad:

Todos los procesos que se gestionen dentro de los procedimientos que están establecidos deben contar su correspondiente registro de trazabilidad el cual permite hacer seguimiento desde el inicio del procedimiento hasta su actual estado. Este debe permitir realizar la consulta sin restricciones y garantizar la integridad de esta información la cual no debe poder dejarse modificar ya que este sirve de sustento legal según las leyes establecidas para cualquier discrepancia frente a estos datos que se tenga.

Los procedimientos que se realicen bajo la modalidad de registros físicos el cual deben registrarse en bitácoras y libros tienen que contar con la garantía que se deban resguardar en lugares donde se pueda proteger en cuanto a pérdidas, deterioros de estos y posible manipulación que se tengan sobre estos de parte de los funcionarios encargados.

Los sistemas de información que se usan para la gestión de los datos en la entidad de Indervalle deben contar con la parametrización necesaria y demostrable que pueda grabar cada movimiento, registro y acción que haga los usuarios dentro de este. El software debe permitir verificar que tipo de acción y sobre qué tipo de datos realizo determinada acción los diferentes usuarios del sistema. Igualmente se tiene que brindar la garantía que los datos no pueden ser modificados por lo cual brinda el atributo de confiabilidad de los datos.

Estos registros tienen que quedar guardados en tablas de datos donde se pueda realizar fácilmente auditorias tecnológicas y que estas solo puedan ser accesados por roles y usuarios específicos de los sistemas de información.

Retención:

La información que generan las diferentes acciones en todos los procesos que hagan los usuarios de los sistemas de información y los procedimientos de gestión de datos que se realizan de forma física debe resguardarse en la plataforma segura para que esta pueda ser consultada cuando sea necesario, pero igualmente esta debe ser garantizada en su total integridad para evitar el deterioro de la información.

La información guardada para estos fines y que se resguardan en los contenedores de información seguros en los servidores de Indervalle debe tenerla garantía de brindarnos el resguardo perpetuamente ya que al tratarse de información pública debe poder consultarse en cualquier momento y por lo tanto se debe utilizar todos los medios

posibles para tener controlado este aspecto, ya sea que se haga sobre los servidores principales, en la nube o en dispositivos de almacenamiento masivo como discos duros de larga duración.

Lo anterior significa que Indervalle establece la política de resguardo de la información de forma perpetua con esto se garantiza la consulta de esta y la disponibilidad de la misma.

10.1 Auditoria:

Todos los procesos y procedimientos establecidos mediante las políticas de seguridad de la información deben tener su correspondiente elemento de auditoria y que esta se pueda realizar cuando así lo designe el secretario general del comité de seguridad.

Aleatoriamente en fechas y en procesos aleatorios deben realizarse las pruebas de auditoria a los datos que generan los sistemas de información, igualmente los procesos que se hagan en forma física tienen que poder realizar su correspondiente auditoria en las fechas señaladas y de la forma señalada. Por lo tanto, es de obligación del secretario general del comité realizar estas auditorías y generar el correspondiente informe socializándolo en la reunión del comité principal de seguridad donde se discutirá los resultados obtenidos y las acciones a mejorar para garantizar el no repudio de los procesos.

10.2 Intercambio electrónico de información:

Todas las comunicaciones que se realicen en formato digital, deben garantizar el no repudio de ellas, en este apartado están los envíos de correo electrónico por medio de los servidores institucionales, los envíos de correo electrónico enviado por cuentas de terceros como Hotmail, Gmail, Yahoo, entre otros. Al igual que los datos que se envíen por medio de aplicaciones de chat de terceros tienen que brindar esta garantía de no repudio.

La actual política declara que este tipo de información anteriormente mencionado debe ingresar dentro de la confianza que debe brindar este tipo de aplicaciones de mensajería y brindar la característica de no repudio, por lo tanto, todas estas sirven como pruebas para discrepancias donde se lleguen a identificar por parte de los funcionarios. Igualmente aclara que estas también deben ser parte de objeto de auditorías para cumplimiento de no repudio.

11 PRIVACIDAD Y CONFIDENCIALIDAD

Indervalle conoce y respeta las leyes de protección de datos dictadas por el gobierno nacional de Colombia por lo cual establece las siguientes políticas en materia de protección de datos siguiendo las recomendaciones en las leyes nacionales.

Se establece que todos los datos recolectados tienen que ser valorados y tratados como tal y garantizar a las personas o empresas involucradas sus derechos sobre estos.

Ámbito de aplicación

Los datos que son registrados en los diferentes sistemas de información con los que cuenta Indervalle así mismo la información de personas o empresas que se retengan de forma física debe regirse por la normatividad vigente por lo cual se establece este alcance a todo los relacionado con datos que se resguarden en los servidores propios de Indervalle, servidores alquilados por parte de la entidad, servidores de contratistas donde se tenga aplicativos instalados. También se alcanza a proteger toda información personal de empresas o personas naturales que hagan parte de archivos físicos que sean recolectados en las diferentes áreas que componen la institución.

11.1 Excepción al ámbito de aplicación de las políticas de tratamiento de datos personales

Entendiendo que toda información personal su correspondiente dueño tiene su total derecho sobre esta para restaurar, modificar, actualizar y borrar, Indervalle no deja como excepción ningún dato ya que estamos ante datos que los usuarios deben proteger por ser dueños de ellos mismos.

Siendo así, la información recolectada en todos los sistemas y de cualquier tipo, su origen ya sea persona o empresa dispone enteramente de estos para gestionar cualquier tipo de acción derivada de las leyes de protección que así lo dictamina el gobierno nacional de Colombia dentro de todo su territorio.

11.2 Principios del tratamiento de datos personales

11.2.1 Principio de legalidad

Todos los datos como se dice anteriormente deben ser tratados y vistos mediante la lupa de las leyes concernientes en materia de protección de datos personales regidos por medio del gobierno nacional de Colombia. Esto debe garantizar la totalidad de los derechos sobre los datos según la información recolectada por cada sistema de información de Indervalle y donde se involucren estos.

11.2.2. Principio de finalidad

La actual política establece que los sistemas de información deben informar claramente el objetivo de los datos recolectados, esto debe realizarse siempre con opciones de menú emergentes donde se muestre esta información, y dentro de los documentos de privacidad de los datos. Así mismo en las áreas donde se registra y recolecta información de personas

o empresa, estas deben tener claro y disponible los objetivos de los mismos dentro de dicha área. Lo anterior es de estricto cumplimiento.

11.2.3. Principio de libertad

Todos los sistemas de información que se utilicen dentro de Indervalle deben generar la opción la cual debe marcarse en caso de estar de acuerdo con las políticas de tratamiento de los datos personales, esta tiene que estar a la vista y donde fácilmente se pueda ubicar en el formulario que se está diligenciando de forma virtual, el sistema debe poder desplegar las políticas de tratamiento de información de forma obligatoria para que se pueda habilitar los botones de envío de información o de guardado de los datos correspondientes en la interfaz gráfica.

Así mismo en la recolección de los datos de forma física, siempre se debe tener a la mano las políticas de tratamiento de datos personales en un formato adjunto, donde la persona pueda leer sin problemas y correspondiente marcar la opción de acepto el tratamiento de los datos que se están recolectando. Lo anterior debe ser de estricto cumplimiento dentro de las áreas y los sistemas de información que se están usando para los diferentes fines.

11.2.4. Principio de veracidad o calidad

Toda la información que se recolecte independiente del medio ya sea físico o formato digital, debe poder comprobarse su calidad de esta mediante la exactitud, lo actualizado que se encuentre, el atributo de comprensible y que tan comprobable es, esto debe poder realizarse por la persona origen de los datos es decir el dueño de estos si así lo requiera o lo disponga.

11.2.5. Principio de transparencia

La actual política de seguridad de la información establece que el titular de los datos recolectados, en este caso podemos identificar a: técnicos, deportistas, funcionarios, ciudadanía general, empresas, clubes deportivos, entre otros que pueden verificar, solicitar y analizar la información recolectada de estos para confirmar el tratamiento que se le está dando a sus datos y de qué manera se está haciendo por parte de Indervalle.

11.2.6. Principio de acceso y circulación restringida

Se establece que los datos solo pueden ser tratados, revisados por personas autorizadas por el titular de los datos, y por los dictaminados por las leyes vigentes relacionadas para tal fin, esto debe cumplirse en estricto orden y disponerse tanto en los sistemas de información como en la recolección de datos de forma física.

11.2.7. Principio de seguridad

Indervalle mediante este documento de políticas de seguridad de la información establece de forma clara y rotunda que la información recolectada será tratada y resguardada bajo todos los protocolos de seguridad que sean debidos y garantiza al titular de los datos que estos estarán seguros para evitar pérdidas, posibles corrupciones de la información y se le garantizara la integración de estos brindando la confiabilidad de los datos personales que son tratados.

11.2.8. Principio de confidencialidad

De la misma manera Indervalle garantiza y provee todas las herramientas necesarias para que los funcionarios que son gestores de estos datos en los sistemas de información usados o asignados para cualquier tarea así mismo como la información que pueda tratarse en los diferentes formatos físicos debe guardarse la confidencialidad de la misma, garantizando con esto que los datos no pueden divulgarse por ninguna persona que los está tratando en su debido momento, estos deben acogerse a dicha regla y brindar esta seguridad a los titulares de la información.

Los funcionarios o personal externo que realice dicho tratamiento de información deben antes haber firmado la cláusula de confidencialidad donde establezca que se somete a estas políticas enfrentando los diferentes castigos a que haya lugar en caso de ir en contra de estas y someterse a las sanciones pertinentes que se diera el caso.

11.3. Derecho de los titulares

Se establece que todos los titulares que tengan información en los sistemas de información y contenedores de datos físicos sin excepción tienen los siguientes derechos:

- Conocer, actualizar y rectificar sus datos personales.
- Solicitar la prueba de su autorización para el tratamiento de sus datos personales.
- Ser informado respecto del uso que se les da a sus datos personales
- Revocar la autorización y/o solicitar el borrado de sus datos personales de las diferentes bases de datos o archivos cuando el titular lo considere necesario, siempre y cuando no se encuentre vigentes procesos relacionados con dicha autorización.
- Presentar quejas ante la entidad administrativa encargada de la protección de los datos personales.

11.4. Autorización del titular

Para Indervalle es crucial que todo el tratamiento de los datos por parte de los sistemas de información tenga que estar sustentado con la correspondiente autorización por parte del titular. Los sistemas de información deben brindar la opción obligatoria de tener que dar clic en la opción de ver políticas de seguridad y poder leerlas sin prejuicio a perder

lo procesado hasta el momento, luego debe poder habilitarse el botón o procedimiento para guardar los datos, de esta forma se da obligatoriedad a los funcionarios que están usando el sistema y a los usuarios que lo están manipulando para poder enterarse de dicha política, igualmente esta política debe poder reenviarse vía correo electrónico al autor de los datos.

En cuanto a los procedimientos que se realicen mediante formatos físicos en las diferentes áreas, estas deben contar con el formato donde este impreso la política de seguridad de la información en lo referente al tratamiento de datos y debe ser firmada y autorizada por el titular que en ese momento se encuentre en el área realizando dicho proceso. Estas políticas de tratamiento de datos deben poder darse una copia idéntica de la firmada para resguardo de los titulares de la información.

11.5. Deberes de los responsables del tratamiento

Los funcionarios que están al frente de los sistemas de información y de las áreas donde recoge datos en formato físico deben tener las responsabilidades sobre el uso y tratamiento de estos datos, para lo cual se establece claramente cuáles son estas.

- Guardar total confidencialidad de la información
- Garantizar el buen uso de los datos
- No cambiar, ni actualizar ni borrar sin el consentimiento del titular de los datos
- No compartir la información con agentes externos o personas no autorizadas
- No descuidar su equipo de trabajo donde se evidencie dichos datos.
- Resguardar con todas las medidas de seguridad posible contra deterioro para evitar la pérdida de estos datos hablando de formatos físicos, formularios y carpetas guardadas en las diferentes áreas correspondientes.
- Todos los concernientes a garantizar la privacidad de los datos según las normas y leyes establecidas por la normatividad vigente de Colombia.
- Firmar la cláusula de confidencialidad de los datos que está gestionando sin previa autorización y debe establecerse dicha cláusula a partir del momento que empieza su trabajo relacionado con dichos datos o asignación de los mismos.

11.6. Política de controles criptográficos

Debido a la importancia y criticidad de muchos documentos que son generados bajo la modalidad virtual y electrónicamente se debe establecer las políticas que garanticen que dichos documentos son genuinos, para ello se debe contar con el mecanismo de firma digital el cual sea generado mediante software que muestre claramente el código único creado a partir de dicho documento electrónico y con esto poder realizar la comprobación en los sistemas informáticos cuando sea requerido que realmente es auténtico y no hay cabida al engaño o manipulación de estos.

13. INTEGRIDAD

La actual política avalada por todo el comité que hace parte de la seguridad de información comprender que la información es lo más importante y esta debe ser protegida siguiendo todos los estándares regulares para esto y pretende que igualmente todos los funcionarios involucrados en la entidad Indervalle, conozcan detalladamente, sepan cómo reaccionar frente a los incidentes que nos genera diariamente la tecnología y sobre todo tengan los conocimientos para salvaguardar los datos de tal manera que se proteja la integridad de los mismos.

Los funcionarios ya sean contratistas, personal de planta, personal externo y contratistas deben dar la importancia a tomar todas las medidas necesarias para que los datos no pierdan su integridad y retengan toda la información original sin ningún perjuicio, a menos que esta sea autorizada por el o los autores de los datos para que pueda ser modificada, teniendo este consentimiento validado, por escrito o digitalmente firmado, debe poder darse esta última opción de modificación, de lo contrario es entera responsabilidad de la persona encargada de la custodia de los datos en los equipos tecnológicos asignados o contenedores físico de datos encargado para tal fin.

13.1. Responsabilidad

Si los datos, en los planes de evaluación de la calidad de estos, es comprobado que han perdido sus atributos de calidad como la integridad, se debe realizar una investigación por parte del secretario general del comité de seguridad de información con ayuda del vocero del área donde sucedió el incidente de tal forma que pueda verificarse el momento exacto donde se halla perdido la integridad, detectando el directo custodio de la información, el por qué se generó el incidente e identificar la dimensión del daño causado por el problema.

Se debe realizar una investigación laboral para confirmar o descartar la culpabilidad del funcionario que tenía a cargo los datos, en caso de que haberse realizado la identificación de esta culpa, deben tomarse todas las sanciones necesarias para este funcionario, teniendo en cuenta que los datos es lo más importante y recurriendo hasta en las últimas instancias, intentando recuperar los datos a su estado inicial y original de acuerdo a los cambios sucedidos gracias al incidente.

13.2. Medidas a tomar después del incidente

Una vez que se haya detectado el incidente y que se realizó todo lo posible por recuperar la información a su estado anterior gracias a los Logs, herramientas de extracción y recuperación de información, tablas y sistemas de auditorías, se debe proceder a tomas las medidas en torno a el problema que surgió.

Se debe realizar un estricto plan de calidad de todos los datos contenidos en los sistemas de información siguiendo las pautas del documento plan de calidad de datos, esto debe

arrojar los respectivos informes donde indique posibilidad de pérdida de integración de otros conjuntos de información.

En caso que el problema surgido sea a causa de errores comprobables en los sistemas de información se deben tomar las medidas necesarias inmediatamente con la persona encarga del sistema o si es por medio de un proveedor se debe citar a reunión con las personas del comité de seguridad de información que están haciendo seguimiento al incidente presentado. Todo lo anterior en aras de entender lo sucedido, tomas las medidas preventivas necesarias y correcciones al software en caso de necesitarlo, con sus correspondientes pruebas posteriores para confirmar que el incidente no se vuelva a ocurrió de la misa manera.

Lo anterior debe quedar correctamente documentado y digitalizado en la bases de datos encargada de gestionar los incidentes ocurridos en la plataforma digital o en los formatos físicos encargados de salva guardar la información requerida para este fin

14. DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN

Indervalle debe estar preparado para cualquier incidente que se pueda presentar y que ello no afecte el negocio, es decir que se pueda seguir trabajando sin perdidas mayores de tiempo ni procesos deberían estar represados durante mucho tiempo según las políticas de seguridad de información.

Para lo anterior, Indervalle ha creado el documento donde se da prioridad a este tema llamado continuidad del negocio, es de aclarar que para más detalles se debe remitir a este documento donde se especifica claramente los procedimientos a seguir en caso de volverse realidad los riesgos del negocio que se han identificado con anterioridad. En el presente documento se dictan las políticas a seguir en materia de la disponibilidad de los servicios y de la información de forma general.

Indervalle define la disponibilidad de los servicios y de la información la cual debe seguir prestando sus diferentes tareas de la siguiente manera que se ha organizado.

Niveles de disponibilidad

Todas las áreas que componen Indervalle deben acogerse a las políticas que están consignadas en este documento, por lo cual es importante remitirse a estas en caso de los incidentes que puedan presentarse, también es claro que los niveles de disponibilidad se encuentran establecidos con anterioridad en los documentos pertinentes, para el caso de disponibilidad del negocio, se debe remitir al documento continuidad del negocio que hacer parte de la estrategia de seguridad de la información requerida para tal fin y donde se identifica junto al análisis de riesgos lo que se debería tener en cuenta en caso de fallos.

El documento análisis de riesgos nos muestra claramente como están identificados estos para la empresa Indervalle, este documento debe tener una periodicidad de 6 meses

antes de volver a realizar un diagnóstico en cuantos los riesgos actuales, riesgos nuevos que se puedan incluir en la documentación.

El plan de continuidad del negocio nos califica, identifica los riesgos, los funcionarios que están encargados de cada proceso en caso de incidente y no guiar para saber qué acción tomar cuando se ha vuelto realidad un riesgo programado dentro de este, este documento continuidad del negocio es el único documento que va a servir de guía para solventar el problema presentado. Por lo tanto, queda como política establecida acudir solo a este documento para tener una correcta continuidad del negocio.

El comité de seguridad de la información encomienda al secretario general del comité del área de sistemas que sirva de apoyo para especificar, recomendar, explicar las diferentes acciones a seguir que se encuentran consignadas dentro de esta documentación que hace parte del bloque archivístico del plan de seguridad de la información.

Planes de recuperación

Cada que se encuentre un incidente de seguridad que ponga en riesgo la prestación ideal o dentro de los parámetros establecidos el normal aseguramiento de los procesos y procedimientos que se están ejecutando, quien haga parte como vocero del comité de las diferentes áreas serán los encargados de dar los primeros avisos y tendrá que ponerse al frente del tema sin descuidarlo hasta que no se halla subsanado el problema. El vocero del comité tiene que realizar los respectivos procedimientos, dar aviso rápidamente al secretario general del comité para que este sea quien interprete finalmente mediante el documento de continuidad del negocio el paso a seguir en plan de recuperar el proceso que se ha caído o procedimiento afectado por el incidente presentado.

Interrupciones

Todos los procesos, sistemas de información y procedimientos que conforman la plataforma de datos de la entidad Indervalle están sujetos de acuerdo al plan de mantenimiento a realizar pequeñas interrupciones para realizarse dicho proceso. Por lo cual la política de seguridad de la información establece que estas interrupciones deben realizarse en tiempo que no afecten el libre funcionamiento de la información por toda la entidad, debe realizarse en días no hábiles y en horarios donde el posible uso de información sea lo más bajo posible.

Cuando se vaya a presentar un evento de este tipo debe ser comunicado mediante formato especifico, firmado por el jefe del área en cuestión, para que este sea evaluado de los alcances de la interrupción, todo con el ámbito de estar preparados para lo que pueda ocurrir, esto debe ser notificado a los directamente implicados. Si los afectados es la ciudadanía en especial, debe realizarse con días antelación una comunicación pública donde se indique que efectivamente se va a pagar, pausar o tumbar algunos de los servicios prestados por Indervalle.

Acuerdos de nivel de servicio

Cuando los procesos o procedimientos son interrumpidos por cualquier razón que haga que esto suceda, debe realizarse la comunicación pertinente con los implicados en esta información que se gestiona por medio de estos.

Se debe tener en cuenta que los contratistas que manejan varios de los servicios, sistemas de información que tiene Indervalle deben respetar los ANS ya que estos nos dan la pauta cuando se necesite algún tipo de interrupción. Los contratistas que incumplan con esta política deben someterse a las sanciones que están establecidas en los contratos de prestación de servicios y en donde se tiene que haber especificado dichos temas.

Los ANS deben ser revisados con una periodicidad de 1 vez cada aña para confirmar que de acuerdo a los cambios empresariales están cumpliendo con lo pactado según estos acuerdos, en caso dado que no sea así, deben replantearse junto con el proveedor en cuestión para que sea actualizado y vuelto a ingresar dentro de los documentos que se tienen para estos procesos.

Segregación de ambientes

Todos los nuevos productos, desarrollos que se estén creando por parte de contratistas, funcionarios de plan o contratistas deben tomar las respectivas medidas para prevenir el impacto negativo de estos nuevos sistemas de información que se estén creando.

Se deben hacer uso de ambientes de desarrollo, pruebas, con el objetivo que no ocasionen problemas a los servicios que ya están funcionando y se encuentran estables dentro de la institución Indervalle.

Indervalle debe proveer las herramientas necesarias para que esto se lleve a cabo con la misma rigurosidad, estas herramientas deben estar claramente separadas de los sistemas de información que están en producción con el alivio de que estos no puedan realizar interrupciones sobre ellos, una vez que se hallan realizado las respectivas pruebas se debe pasar a los sistemas reales, realizando instalaciones nuevas o actualizando los software existentes, teniendo en cuenta las medidas preventivas para no realizar en horarios hábiles a menos que se trate de una actualización critica donde esté en riesgo la continuidad del negocio y donde dicho documento lo designa de esta manera.

Gestión de cambios

Cuando se trate de creación de nuevos productos de software, actualizaciones de los mismos con nuevas funcionalidades por parte de desarrollos dentro de la entidad, también cuando esto mismo aplique para contratistas de sistemas de información que estén realizando algún proyecto de software se debe tomar las medidas necesarias para cuando tengan que realizar cambios en los sistemas que ya se encuentran instalados.

Nadie puede realizar algún cambio en los sistemas de información sin la autorización del secretario general del comité de seguridad de información ya que este debe validar el procedimiento que se piensa realizar, se debe diligenciar ya sea por escrito físico o documento virtual el formato adecuado para cambios de este tipo, comunicársele al encargado y proceder luego a autorizar dicho cambio.

Se debe tener en cuenta que los cambios deben quedar en bitácoras de cambio y utilizar repositorios de versiones, software de versiones para que los problemas que se puedan presentar respecto a esto sean mínimos.

15. REGISTRO Y AUDITORIA

Todos los procesos deben tener un registro auditable el cual se pueda verificar su integridad, cambios en el tiempo, estado anterior, estado actual y los responsables directos de dichos procedimientos sobre los datos.
La actual política de seguridad de la información establece que se debe contener dentro de registros seguros dichos cambios que se realicen en los sistemas de información, cambios que se realicen en los datos, las evidencias que surjan de

estos procesos deben resguardarse en contenedores de información al cual solo tengan permisos los roles específicos sin que ello afecte la información guardada.
Los registros de auditoria deben tener obligatoriamente y cumplir con lo especificado a continuación donde se dictan las pautas a tener en cuenta para todos los funcionarios y responsables de los procesos.

Responsabilidad

Todas las entidades públicas cuentan con la oficina de control interno la cual para este caso debe velar porque se cumplan las auditorias planeadas según cada área y para cada proceso que se esté ejecutando dentro de la entidad Indervalle.

La actual política de seguridad informática establece que la oficina de control interno debe realizar dichas actividades y estas deben ser comunicadas mediante escrito físico o escritos digitales al vocero de dicha área dentro del Comité de seguridad informática. A su vez el vocero debe presentarlas durante las reuniones ordinarias que se establezcan para tal fin, en caso de verificar anormalidades en los resultados que indiquen de posibles fallos de seguridad, este debe convocar una reunión extraordinaria para dar a conocer dicha situación con el objetivo de encontrar solución prontamente.

Almacenamiento de registros

Todos los registros de auditoras que se establezcan deben resguardarse en sitios y contenedores de datos verificados, esta regla debe abarcar a toda la información resultante de dichas auditorias sin excepción a la regla, se debe tener en cuenta la calidad del dispositivo que estará albergando la información, la confiabilidad de este para que se evite perdidas irreversibles.

El comité de seguridad de la información establece que se debe hacer seguimiento periódico a estos objetivos de archivos para establecer si son fielmente confiables a los requerimientos de tiempo, de espacio que se pueda dañar, deteriorar dicha información y por la cual se pueda perder completamente o perder parcialmente.

Normatividad
Indervalle debe garantizar que todas las disposiciones planteadas en los registros de auditoria deben ajustar según las normas vigentes del gobierno central para entidades públicas como esta, por lo cual debe verificarse los estatutos, leyes y artículos relacionados para comprobar que se esté cumpliendo con lo establecido por la ley.

Este proceso se debe llevar a cabo por todo el comité de seguridad de información y el cual se debe poner de acuerdo en caso que se esté incumpliendo con alguna normatividad el realizar el ajuste correspondiente y que este sea verificable en el tiempo.

Garantía de cumplimiento
Todos los procesos que se resuelvan por medio de los registros de auditoria, todos los resultados obtenidos sobre este tipo de evaluación deben verificarse y garantizarse que efectivamente se está cumpliendo según las recomendaciones dadas por estas.
Indervalle por medio de su comité de seguridad de la información deben velar que efectivamente estos registros de auditoria como sus resultados están siendo tenido en cuenta y procesados de tal manera que se esté subsanando en caso de encontrar algún incidente de seguridad de la información por medio de estas evaluaciones.
Debe quedar por escrito que efectivamente se están realizando los cambios y avances en subsanar estos problemas que encontramos gracias a las auditorias planteadas.

Periodicidad
El comité de seguridad de la información, advierte y establece que se deben revisar cada 6 meses los resultados de las auditorias, así como los avances que se estén realizando en torno a estos. Se debe tener en cuenta que las auditorias también deben realizarse cada 6 meses y que el vocero de cada área que pertenezca al comité debe apersonarse y estar de veedor que se están realizando según el plan estipulado para tal fin.
En caso de encontrar algún incidente, discrepancia respecto a los tiempos de las auditorias que se realizan a los procesos donde implica activos de información esta debe resolverse por parte del comité de seguridad de la información por medio de una reunión extraordinaria si así lo amerita la situación, teniendo en cuenta que se debe documentar todos los procesos que se están realizando en torno al tema de registros de auditoria y procesos auditables.

16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

El comité de seguridad de la información debe velar porque todos los incidentes sean procesados, analizados bajo los estándares que, adecuados para ellos, igualmente debe garantizar que todos los incidentes se van a ver gestionados durante el tiempo parametrizado para tal fin, igualmente se debe garantizar que todos los incidentes se deben resolver de acuerdo a las políticas planteadas dando cumplimiento estricto a estas y a la normatividad vigente para tales eventos de seguridad informática.

La actual política define claramente lo que se debe seguir, el plan con el cual guiarse para tener en cuenta los incidentes que se puedan presentar y los funcionarios igual deben estar seguros que los problemas surgidos de estos se van a ser resueltos de acuerdo a estas políticas acá definidas.

La política de la seguridad de información debe contar con el cumplimiento mínimo de las siguientes condiciones de acuerdo a lo planteado por el Comité que lo genera y lo aprueba.

Compromiso de la alta dirección

La alta dirección de Indervalle debe tener aprobada la política actual de tal forma que esta pueda ser socializada con total compromiso y apoyo por parte de los jefes de las subgerencias y gerencia principal.

Dado el apoyo sobre estas políticas se deben comprometer a conocer los avances, resultados de auditorías que se realicen, dedicar tiempo para conocer por menores de los beneficios y cifras las cuales respaldan la implementación de dicho documento a toda la entidad por lo tanto, el comide de seguridad de información debe garantizar que este compromiso sea real con el documento y que pueda ser llevado a cabo cada renglón de este con el total apoyo de la alta dirección.

Visión general

Todos los procesos que se hagan de acuerdo a estas políticas que se implemente a la entidad Indervalle deben arrojar informes y reportes pormenorizados sobre lo implementado, sobre el suceso que se hayan resuelto y los incidentes que se pudieron haber resuelto.
Estos informes deben ser conocidos por todo el comité de seguridad de información de Indervalle el cual debe conocer los detalles de estos.

Todos los reportes e informes que se puedan generar, que se deben crear son implementados en formato digital ya que estos deben quedar en bases de datos digitales para posteriores consultas, incluso los incidentes que tengan que ver con información física que se resuelvan por medio de este documento debe quedar en forma digital en los diferentes formatos y mediante los sistemas de información respectivo.

Definir responsables

Los responsables de los procesos de seguridad informática como ya se ha venido mencionando en todo el documento son los voceros de cada área que pertenezcan al comité de seguridad de la información, estos deben estar atentos, recepcionar los incidentes y comunicarlos a la Secretaria General del Comité que es del área de Sistemas.

El secretario general del comité que debe ser un funcionario del área de sistemas es quien se encarga de realizar los monitoreo, auditorias de registros, recepción de incidencias desde las diferentes áreas de Indervalle, dar trámite a estos incidentes, así como su correspondiente solución con ayuda de los demás expertos profesionales del área de TI. Este debe verificar también que los salvaguardas se estén llevando a cabo coherentemente y que se esté cumpliendo dado las políticas de seguridad de la información, debe velar porque lo consignado en este documento se cumpla al pie de la letra y llevar los reportes al comité de seguridad de informática presentando, reportes detallados según el periodo a analizar. Igualmente debe realizar lo concerniente y explicar en lenguaje no técnico la importancia de los diferentes temas que se tengan que gestionar por medio de las políticas de seguridad de la información.

El director principal del comité debe velar porque las políticas se cumplan, debe estar pendiente sobre los incidentes mayores y brindar todo su apoyo para que se resuelvan de la mejor manera posible.

Actividades

Todos los incidentes que sucedan en la entidad de Indervalle tiene un flujo de gestión el cual se debe seguir al pie de la letra cumpliendo con las debidas políticas de seguridad informática, este flujo debe mostrarnos todos los estados actuales, anteriores y posibles posteriores para validar que el incidente se está resolviendo de la mejor manera posible

El flujo de gestión empieza cuando el incidente es identificado desde las diferentes áreas de la entidad, luego debe ser informado al vocero que pertenece al área con el cual se debe empezar a realizar la documentación del mismo para llevarlas al secretario general del comité el cual es el experto en seguridad informática del área de sistemas, este funcionario debe seguir documentando, obtener pruebas del incidente antes y después del suceso y buscar la manera de proteger la información para que no se deteriore más en caso dado. Por consiguiente, se debe buscar la solución dentro de lo presupuestado dentro del análisis de riesgos y plan de continuidad para que la entidad no se detenga por el problema, controlar, resolver y luego debe documentar todo lo gestionado en bases de datos digitales para luego en evaluar la severidad del problema y si es necesario convocar a una reunión extraordinaria para dar a conocer el problema y la documentación realizada que se hizo por esta razón.

Se toman las medidas pertinentes para que no vuelva a suceder y se debe archivar el caso según sea dado.

Documentación

El sistema de gestión de calidad de la entidad Indervalle debe estar en concordancia con las políticas de seguridad de información las cuales deben comprobar y estar a la par de las situaciones presentadas, poniendo a disposición de estas los diferentes formatos que se encuentra relacionados con la seguridad informática.

Se debe realizar la correcta implementación de coherencias con los diferentes procedimientos que tiene contemplado la empresa durante su continuo manejo de la información en la entidad. Se debe realizar la completa gestión de la compenetración de estos informes para evaluar los seguimientos que se puedan dar de acuerdo a estos. La documentación de los procesos debe ser íntegros y ser fieles a lo relacionado que se pueda dar con los procedimientos establecidos en la entidad.

Descripción del equipo que manejara los incidentes

Los usuarios funcionarios encargados de manejar y gestionar los eventos de los incidentes que se presentan en la entidad Indervalle deben ser contratistas, personal de planta, para que se haga un correcto trabajo y continuidad del trabajo realizado bajo este esquema.

La resolución de incidentes está encabezada por el director del comité de seguridad de información quien a su vez empodera al experto en informática que es el secretario general del comité y el cual basa sus soluciones y seguimientos a los incidentes de acuerdo a la información suministrada por los voceros que conforman las diferentes áreas de la entidad Indervalle.

Elaboró:	Revisó:	Aprobó	Incorporó SGI
Nombre: Stella Jiménez Pimentel	Nombre: Rafael Pérez Manquillo	Nombre: Carlos Felipe López López	Nombre: Rodrigo Martínez Cruz
Cargo: Técnico Sistemas	Cargo: Subgerente Administrativo y Financiero	Cargo: Gerente	Cargo: Jefe Oficina Asesora de Planeación
Firma:	Firma:	Firma:	Firma: