INDEPORTES QUINDÍO

PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÒN

Contenido

1. INTRODUCCION

El Instituto Departamental de Deporte y Recreación del Quindío “INDEPORTES QUINDIO “, 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 Deporte y Recreación del Quindío, 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.

2. OBJETIVO

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores 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:

- *Minimizar el riesgo en las funciones más 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.*
- *Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de El Instituto Departamental de Deporte y Recreación del Quindío*
- *Garantizar la continuidad del negocio frente a incidentes.*
- *El Instituto Departamental de Deporte y Recreación del Quindío ha decidido **definir, implementar, operar y mejorar** de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.*

3. ALCANCE

Este directorio está dirigido a todos los funcionarios del Instituto Departamental de Deporte y Recreación del Quindío “INDEPORTES QUINDIO “que usan los servicios de TI, para que sean apropiados y permitan un mejor relacionamiento funcional con cada una de las áreas

4. DEFINICIONES

TI: Es la aplicación de ordenadores y equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos

VNP: Es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

FIREWALL: Un cortafuego (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

WIFI: Es una tecnología que permite la interconexión inalámbrica de dispositivos electrónicos. (Como una computadora personal, un televisor inteligente,

LAN: Es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.

SOFTWARE: Es un término genérico que designa al conjunto de programas de distinto tipo (Sistema operativo y aplicaciones diversas) que hacen posible operar con el ordenador.

HARDWARE: Conjunto de componentes materiales de un sistema informático. Cada una de las partes físicas que forman un ordenador, incluidos sus periféricos. Maquinaria y equipos (CPU, discos, cintas, modem, cables, etc.).

MESA DE AYUDA O HELPDESK: Se basa en un conjunto de recursos técnicos y humanos que permiten dar soporte a diferentes niveles de usuarios informáticos de una empresa, tales como: Servicio de soporte a usuarios de “sistemas microinformáticos” Soporte telefónico centralizado en línea (on-line)

VENTANILLA ÚNICA DE CORRESPONDENCIA: Área u Oficina donde se gestiona de manera centralizada y normalizada, los servicios de recepción, radicación y distribución de las comunicaciones

PQRS: El Sistema de Peticiones, Quejas, Reclamos y Sugerencias (PQRS) es una herramienta que nos permite conocer las inquietudes y manifestaciones que tienen nuestros grupos de interés para que tengamos la oportunidad de fortalecer nuestro servicio y seguir en el camino hacia la excelencia operativa.

AGENTE: es un programa de computación que actúa para un usuario u otro programa en una relación de entidad, un acuerdo para actuar en nombre propio. Tal "acción en nombre de" implica la autoridad para decidir cuál acción, si existe, es adecuada

POLÍTICA: Declaración de alto nivel que describe la posición de la Entidad sobre un tema específico.

REGLAMENTO POLITICA SEGURIDAD DE LA INFORMACION

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

AMENAZAS: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000)

ANÁLISIS DE RIESGO: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000)

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

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).

CIBERESPACIO: Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua Española)

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.

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).

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)

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).

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad, y disponibilidad de la Información. (ISO/IEC 27000)

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).

5. FINALIDAD

Finalmente es de gran ayuda incluir la descripción general de otras políticas relevantes para el cumplimiento de los Objetivos planteados dentro del proyecto del SGSI ya que éstas son el apoyo sobre el cual se desarrolla; éstas deben ser descritas de forma sencilla, puntual y muy efectiva.

Dentro de las temáticas que se tocan en este punto se encuentran por ejemplo la gestión de activos, seguridad física y ambiental, control de accesos, etc. Para abordar este punto es necesario remitirse a la “Guía de políticas específicas de seguridad y privacidad de la información” y mencionar aquellas que la Entidad haya establecido como necesarias y primordiales. De esta forma se presenta el siguiente ejemplo:

A continuación se establecen 12 principios de seguridad que soportan el SGSI de El Instituto Departamental de Deporte y Recreación del Quindío:

1. *El instituto departamental de deporte y recreación del Quindío ha decidido definir, implementar , operar y mejorar de forma continua un sistema de gestión de seguridad de la información, soportado en lineamientos claros alineados a las necesidades de la entidad y a los requerimientos regulatorios.*

2. *Las **responsabilidades** frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de **los empleados, proveedores, socios de negocio o terceros**.*

3. *El Instituto Departamental de Deporte y Recreación del Quindío **protegerá la información** generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos **otorgados a terceros** (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.*

4. *El Instituto Departamental de Deporte y Recreación del Quindío **protegerá la información** creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un **uso incorrecto** de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.*

5. *El Instituto Departamental de Deporte y Recreación del Quindío **protegerá su información** de las amenazas originadas por parte **del personal**.*

6. *El Instituto Departamental de Deporte y Recreación del Quindío **protegerá las instalaciones** de procesamiento y la infraestructura tecnológica **que soporta sus procesos críticos**.*

7. *El Instituto Departamental de Deporte y Recreación del Quindío **controlará la operación** de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.*

8. *El Instituto Departamental de Deporte y Recreación del Quindío **implementará control de acceso** a la información, sistemas y recursos de red.*
9. *El Instituto Departamental de Deporte y Recreación del Quindío garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.*

10. *El Instituto Departamental de Deporte y Recreación del Quindío garantizará 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.*

11. *El Instituto Departamental de Deporte y Recreación del Quindío **garantizará la disponibilidad** de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.*

12. *El Instituto Departamental de Deporte y Recreación del Quindío garantizará el cumplimiento de las **obligaciones legales, regulatorias y contractuales establecidas.***

6. RIESGOS DE SEGURIDAD DE LA INFORMACION

Los riesgos en la seguridad de la información de la administración Municipal se pueden clasificar en tres grupos: Actos originados por la criminalidad común, Riesgos por sucesos de origen físico y riesgos por sucesos derivados de la impericia, negligencia de usuarios y decisiones institucionales

Actos originados por criminalidad común:	Riesgos por sucesos de origen físico:	Negligencia de usuarios y decisiones institucionales
• Sabotaje (ataque físico y electrónico) • Daños por vandalismo • Fraude /Estafa • Robo/hurto (físico) • Robo / Hurtoinformación electrónica • Virus /ejecución no autorizada de programas • Violación a derechos de autor	• Incendio • Sismo • Polvo • Sobrecarga eléctrica • Falla de corriente (apagones) • Falla de sistema /daño disco duro	• Falta de inducción, capacitación y sensibilización sobre riesgos • Mal manejo de sistemas y herramientas • Utilización de programas no autorizados /software ilegal • Falta de pruebas de software nuevo con datos productivos • Pérdida de Datos • Infección de sistemas a través de unidades portables sin escaneo • Manejo inadecuado de datos críticos (codificar, borrar, etc.) • Manejo inadecuado de contraseñas (inseguras, no cambiar ,compartidas) • Compartir contraseñas o permisos a terceros no autorizados • Trasmisión de contraseñas por teléfono • Acceso electrónico no autorizado a sistemas externos

7. PROCEDIMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

7.1 CONTROL DE ACCESO

El equipo de cómputo será asignado de acuerdo a las funciones de su contrato y será por parte del Jefe del área la asignación del mismo

En caso de presentar falla del equipo se deberá notificar al área de sistemas para su revisión y en ningún caso el usuario intentara reparar el equipo, la única área autorizada será el área de sistemas

El equipo de cómputo solo puede ser usado para las actividades de interés el área y no para uso personal

El área de sistemas realizara un sondeo de sus conocimientos de ofimática y manejo del equipo de computo y en caso de requerir capacitación se dará una inducción sobre el manejo básico de equipos

Toda Recepción de equipos de cómputo por adquisición o donación se realizara a través del área de inventarios con el área de sistemas

Cada equipo contiene el software necesario para las actividades del área lo cual no debe ser alterado de requerir algún software adicional se debe notificar al área de sistemas mediante oficio

Los usuarios no deben realizar la reubicación de los equipos de cómputo, instalar o desinstalar dispositivos, ni retirar sellos del mismo sin la autorización del área de sistemas en caso de requerir este servicio se solicitara por la mesa de ayuda de la entidad

Sera el usuario responsable de solicitar la capacitación de ser necesario para el manejo de herramientas informáticas que se utilizan en el equipo para así evitar riesgos por mal uso

Es responsabilidad de los usuarios almacenar la información que manejan en la carpeta de el equipos “Mis Documentos “ya que hay se realizara la copia de seguridad mensual en caso de pérdida de información solo se podrá recuperar la información que se resguarde en dicha carpeta por el área de sistemas

Es responsabilidad del usuario mantener el área del equipo limpia y sin humedad para evitar posibles problemas del equipo a causa del mismo

Cuando se requiere realizar el cambio de múltiples equipos de cómputo debido a una reubicación de lugares físicos de trabajo, estos deberán ser notificados con una semana de anticipación al área de Sistemas a través de una solicitud la cual se podrá realizar por la mesa de ayuda del instituto o a través de oficio

Queda prohibido que el usuario abra o desarme los equipos de computo

Únicamente el personal autorizado por el área de sistemas y calidad podrá llevar a cabo los servicios y reparaciones al equipo informático

El usuario que tenga bajo su resguardo algún equipo de computo será responsable de su uso y por dice de acuerdo a la normativa vigente en caso de robo o perdida el responderá por el bien

El usuario que tenga dispositivos será responsable de su buen uso

REGLAMENTO POLITICA SEGURIDAD DE LA INFORMACION

El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario quien resguarda el equipo, se levantaran un reporte de incumplimiento de políticas de seguridad

Debe respetarse y no modificar la configuración de hardware y software establecida por el área de sistemas en caso de modificación se realizara su respectivo reporte por incumplimiento a las políticas de seguridad

Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseña alfanumérico de mínimo 8 caracteres y además deben configurar bloqueo de pantalla para que se lleve a cabo de 15 minutos de inactividad y requerir contraseña al reasumir la actividad, el usuario debe activarlo manualmente cada vez que se ausente de su oficina

Si un computador tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferiblemente por hardware

Para prevenir la intrusión de usuarios no permitidos a través de puerta traseras de la entidad, no está permitido el uso de modens en computadoras que tengan conexión a la red local, a menos que sea debidamente autorizado

A menos que se indique lo contrario los usuarios deben asumir que todo el software de la institución está protegido por derechos de autor y requiere licencias de uso. Por tal razón es ilegal y terminantemente prohibido hacer copias o usar ese software para fines personales.

Los usuarios no deben copiar a un medio removible como una USB, el software o los datos históricos en los computadores del instituto, sin la aprobación previa del área de sistemas o jefe inmediato

Cada equipo de computo debe contar con un herramienta de antivirus en caso de presentar virus se deberá tener el equipo en cuarentena hasta que se solucione el problema

Debe realizarse semanalmente el diagnostico de virus en cada equipo del instituto
No se debe utilizar software descargado de internet y en general software que provenga de una fuente no confiable, a menos que haya sido comprobado de forma rigurosa por el área de sistema y aprobada su uso

Para prevenir demandas legales o la introducción de cualquier virus informático se prohíbe la instalación de software no autorizado, incluyendo el que haya sido adquirido por el instituto, adicional no se permite uso de software de distribución gratuita o shareware, a menos que haya sido autorizado por el área de sistemas

En caso de restaurar programas dañados o infectados, se realizaran copias de seguridad de todo el software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro

No deben usarse USB u otros medios de almacenamiento en cualquier computador de la institución amenos que se haya sido previamente verificado que están libre de virus u otro programa dañado se tendrá un control de los dispositivos en los equipos para verificar que se cumpla

Periódicamente se deben hacerse copias de seguridad de la información vital para la operación del instituto y debe guardarse en un lugar seguro en caso de hurto, incendios, e inundaciones o virus

No se deben dejar las impresoras desatendidas en el momento de impresión por la información, adicional se deberá leer el instructivo cada usuario para el manejo de la

misma y así evitar daños de la impresora

El personal que utiliza un computador portátil que contenga información confidencial de la institución, no debe dejarlo desatendido, sobre todo

7.2 USO DEL INTERNET

Cada equipo de cómputo del instituto contara con un software para el bloqueo de acceso a páginas web no referentes con el trabajo en la entidad, por ende mejorar el ancho de banda al realizar trabajo en plataformas que lo requiere y evitar posibles daños a causa de páginas web con cualquier tipo de malware

Se prohíbe el uso de programas de intercambio de archivos de programas de internet, deberá estar autorizado por el área de sistemas su uso

Se prohíbe el uso de sitios de chat, diferente al prestado localmente para la comunicación del instituto

Se prohíbe el uso de internet para actividades ilícitas o descargas que no cumplan con la normativa vigente

Se prohíbe el acceso a los sitios de material amenazador, pornográfico, con contenido racista, sexista o cualquiera que vulnere la calidad de ser humano

No se debe compartir claves de sus correo electrónico es para uso personal

No permitir que el navegador guarde la contraseña automáticamente porque así programas de terceros podrían robar esa información

Evitar el entretenimiento o juegos en línea en los equipos del instituto

Si no se encuentra navegando por internet, cierre las ventanas abiertas para reducir el bando de ancha en toda la red

Cualquier archivo descargado de una fuente que no sea confiable debe revisarse para confirmar que no cuentas con virus que puedan ocasionar un daño en la entidad
Los usuarios de internet de la institución tienen que reportar todos los incidentes sin excepción de seguridad informática al área de sistema inmediatamente después de su identificación

Los usuarios del servicio de internet del instituto, al aceptar el servicio están aceptando que sean: Serán sujetos de monitoreo de las actividades que realiza en internet y el uso de dispositivos extraíbles, ya saben que se cuenta con prohibición de acceso a páginas y descargas sin autorización del área de sistemas

Los servidores de red y los equipos de contabilidad (Routers, swiches, etc.) deben estar ubicados en lugares apropiados, protegidos contra daños y robos. Y se debe restringir el acceso de personal no autorizado

7.3 MANEJO DE REDES SOCIALES

Las redes sociales estarán bloqueadas para así mejorar la velocidad en demás plataformas que requieran el instituto como son bancos, y publicación estatal de contratos Los usuarios que requieran estos medios deberán informar porque deben habilitarse al área de sistemas La información que se publique o divulgue por cualquier medio de internet de cualquier funcionario contratista o colaborador del instituto que sea creado a nombre personal, como redes sociales, twitter, facebook, youtube, likedlink o blogs, se considera

fuera del alcance de SGSI y por lo tanto su confiabilidad, integridad y disponibilidad de daños y perjuicios que puedan llegar a causar será de completa responsabilidad de la personal que las haya generado

7.4 MANEJO DE IMPRESORA

Los documentos que se impriman en las impresoras serán de carácter institucional

Es responsabilidad del usuario conocer el adecuado manejo de equipos de impresión (escáner y fotocopiadora) para que no se afecte su correcto funcionamiento

Ningún usuario debe realizar labores de reparación y /o mantenimiento de las impresoras
En caso de reportar falla se reportara la falla por la mesa de ayuda

7.5 CORREO ELECTRONICO

El uso del correo institucional es de uso explicito para actividades de la misma

Se prohíbe él envió de información o almacenamiento de información ilegal, sexual, pornográfica o demás degrade la identidad de las personas
Se prohíbe el almacenamiento de videos, música que no sea de uso para las actividades

Se realizara un cambio de contraseñas semestral e informar al área de sistemas del cambio
No abrir correos electrónicos sospechosos que tengan enlaces u archivos de dudosa procedencia al notar eso se debe informar al área de sistemas

Se eliminaran correos no deseados o spam semanalmente

Si cuentan con correos institucionales se recomienda su uso para toda la comunicación interno o externo, o per medio del chat del instituto para así evitar el gasto de papel y tinta, igualmente el uso de carpetas compartidas por LAN para mover y compartir información

Cada trimestre se entregara un informe de los incidentes de las cuentas de correo de cada funcionario para así tener un registro de posibles fallas de seguridad

7.6 CUENTAS DE USUARIO

Toda cuenta de acceso que requiera modificar su nombre u contraseña deberán solicitar a el área de sistemas
El procedimiento de creación de cuentas de usuario deberá ser informado a través de mesa de ayuda
En caso de tener algún problema al acceder a la cuenta de usuario encargado del equipo deberá informar al área de sistema por medio de mesa de ayuda para su solución
El área de sistemas tendrá a su disposición las contraseñas de los equipos que cuenta la entidad

7.7 CONTRASEÑAS Y ACCESO

El usuario no debe guardar la contraseña en medio lógico o en físico donde pueda ser encontrado, tampoco el uso de información personal para la contraseña tampoco el uso de contraseñas que ya hayan sido utilizadas anteriormente

No se debe compartir las contraseñas con otros usuarios al hacerlo el usuario se expone

a que las acciones de terceros hagan con la misma y asume las consecuencias por daños

El cambio de contraseña se realiza mensual y se notifica al área de sistemas del cambio

La contraseña inicial emitida a un nuevo usuario solo debe ser válida para la primera sesión En ese momento el usuario deberá escoger otra

No se debe usar la función de recordar contraseña de los navegadores

Los usuarios que intenten violar los sistemas de seguridad de acceso, considerándose una violación a las políticas de la compañía puede ser causal de despico

Para tener evidencias de casos o de acciones disciplinarias u judiciales, cierta clase de información debe capturarse y grabarse para ser usado en caso de abuso fraude u otro crimen que involucre los sistemas

7.8 SEGURIDAD INFORMATICA

El área de sistemas para identificar tendencias del uso de los equipos en la entidad podrá implementar mecanismos de control y si se evidencia un mal uso se generara un reporte del mismo

Esta absolutamente prohibido el uso de herramientas de hardware o software que violen los controles de seguridad informática

Ningún usuario de la entidad probara fallas de seguridad a menos que se tenga un control por parte del área de sistemas para mejorar la calidad del servicio

Los jefes de cada área serán los encargados de que todos los procedimientos de seguridad funcionen correctamente

Se prohíbe absolutamente la escritura generación, compilación, copia, propagación, ejecución o intentos de propagar cualquier tipo de código potencialmente dañino y así capturar la información o afectar el rendimiento de los equipos de la entidad

8. MANEJO DE INCIDENTES MESA DE AYUDA

En caso de suceder cualquier incidente o requerimiento referente a los equipos de cómputo por ejemplo (soporte técnico, mantenimiento preventivo, mantenimiento correctivo, etc.) el procedimiento a realizar el ticket a la mesa de ayuda lo podrán visualizar en el documento que se les entregara en medio electrónico o cada dependencia contara con el instructivo del mismo cuando necesite hacer inducción del mismo
En el caso de no poder realizarlo con el procedimiento anterior puede acercarse al área de sistemas y el tomara le ayudara a generar el ticket del problema y enviarlo al técnico respectivo

En caso de realizarse el mantenimiento anual se debe tener un cronograma de actividades de los mantenimientos donde se evidencie las fechas como también la actividad realizada y a realizar Lo anterior con autorización del área de sistemas

Se deben utilizar formatos determinado para la realización del procedimiento y en caso de realizar cambio de hardware o software del equipo debe ser colocado en la ficha técnica del equipo

9. MANEJO IMAGEN INSTITUCIONAL

Los equipos de cómputo tendrán de salva pantallas y fondo de escritorio imagen relacionadas con el instituto o en su defecto logo institucional

Cada usuario res responsable del cuidado de su herramienta de trabajo así vez se recomienda limpiar continuamente el equipo externamente (monitor, teclado, mouse) el cual se podrá limpiar con alcohol isopropilico

10. POLITICAS GENERALES

Los jefes de cada área deberán apoyar el cumplimiento de las políticas antes mencionadas, el no cumplir con estas políticas se hará acreedor de una sanción que se designará por nivel directivo

11. REFERENCIAS

Elaboración de la política general de seguridad y privacidad de la información. Ministerio de las Tic

Ley 1450 de 2011, por el cual se expide el Plan Nacional de Desarrollo 2010

Ley 1341 de 2009 Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones en el artículo 38 sobre Masificación del uso de las TIC y cierre de la brecha digital

Decreto 2693 de 2012, por el cual se establecen los lineamientos generales de laestrategia de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones

Capítulo IV referente a la Gestión de Documentos Electrónicos de Archivo del decreto 2609 de 2012, por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del estado.

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.

Ley 1581 de 2012, reglamentada parcialmente por el Decreto 1377 de 2013, por la Cual se dictan disposiciones generales para la protección de datos personales.