



INSTITUTO DEPARTAMENTAL DE DEPORTE Y RECREACION
DEL QUINDIO "INDEPORTES QUINDIO"

RESOLUCION No. 082
JULIO 16 DE 2020

"Por medio de la cual se adopta el Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI y El plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Instituto Departamental de Deporte y Recreación del Quindío "INDEPORTES QUINDIO"

EL GERENTE GENERAL DEL INSTITUTO DEPARTAMENTAL DE DEPORTE Y RECREACION DEL QUINDIO "INDEPORTES QUINDIO" en uso de sus facultades legales que le confieren sus estatutos, Acuerdo. 011 del 06 julio de 2009 y en especial las conferidas en la Ordenanza 027 del 14 de diciembre de 1998 el artículo 15 del acuerdo 011 del 06 julio de 2009, decreto 088 de enero 21 del 2020, y

CONSIDERANDO:

Que el Decreto 1078 de 2015 - Título 9 Políticas y Lineamientos de Tecnologías de la Información, Capítulo 1 Estrategia de Gobierno en Línea; en su artículo 2.2.9.1.1.1. define los lineamientos, instrumentos y plazos de la Estrategia Gobierno en Línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado Abierto, más eficiente, más transparente y más participativo, y que preste mejores servicios con la colaboración de toda la sociedad.

Que la Estrategia Anti trámite y Atención Efectiva al Ciudadano y la de Gobierno en Línea, buscan un mismo fin; el primero desde la racionalización del procedimiento y el segundo desde la automatización del mismo, siendo pertinente optimizar recursos y generar unidad de criterios.

Que el decreto 612 del 4 de abril de 2018 del Departamento Administrativo de la Función Pública señala: "La integración de los planes institucionales y estratégicos al Plan de Acción" para todas las entidades públicas.

Que la planeación estratégica de tecnologías de la información PETI, tienen como objetivo asegurar que las metas y objetivos de Tecnologías de Información estén vinculados y alineados con las metas y objetivos del Instituto Departamental de Deporte y Recreación del Quindío.

Que la Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración del Instituto Departamental de Deporte y la Recreación con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Modelo de Seguridad y Privacidad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

1



**INSTITUTO DEPARTAMENTAL DE DEPORTE Y RECREACION
DEL QUINDIO "INDEPORTES QUINDIO"**

Que, con mérito de lo expuesto,

RESUELVE:

ARTÍCULO PRIMERO: Adoptar para el Instituto Departamental de Deporte y Recreación del Quindío "INDEPORTES QUINDIO" el Plan Estratégico de Tecnologías de la Información y las comunicaciones PETI 2020-2023 y la Política General del Modelo de Seguridad y Privacidad de la Información del Instituto Departamental de Deporte y Recreación del Quindío deportes, los cuales están conformados de cuarenta y dos (42) folios, que hacen parte integral de la presente resolución.

ARTÍCULO SEGUNDO: El Plan Estratégico de Tecnologías de la Información y las comunicaciones - PETI y la Política General del Modelo de Seguridad y Privacidad de la Información que se adoptan, podrán ser modificados conforme a las circunstancias de tiempo, modo y lugar que corresponda a las necesidades de la Entidad.

ARTÍCULO TERCERO: Que el Plan Estratégico de Tecnologías de la Información y las comunicaciones PETI 2020-2023 y la Política General del Modelo de Seguridad y Privacidad de la Información podrá ser consultada a través del siguiente link: www.indeportesquindio.gov.co.

ARTICULO CUARTO: Realizar la socialización de los planes acá adoptados, y su publicación en la página WEB del instituto.

ARTICULO QUINTO: La presente Resolución rige a partir de la fecha de su expedición y deroga cualquier disposición que le sea contraria.

COMUNIQUESE, PUBLÍQUESE Y CÚMPLASE

FERNANDO AGÚSTO PANESO ZULUAGA
Gerente General

Proyectó y elaboró: Mauricio A.C / Contratista de Apoyo
Revisó: Orfa María Ruiz Agudelo / Jefe Área Administrativa y Financiera
Revisión jurídica: María Isabel rojas Vásquez / Jefe Área Jurídica

PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES PETI



**PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION Y LAS
COMUNICACIONES PETI**

Contenido

OBJETIVO.....	4
ALCANCE DEL DOCUMENTO.....	4
MARCO NORMATIVO	4
RUPTURAS ESTRATEGICAS	4
ANALISIS DE LA SITUACION ACTUAL.....	5
Naturaleza.....	5
Misión	5
Visión	5
ESTRATEGIA DE TI.....	6
USO Y APROPIACION DE LA TECNOLOGIA	6
Recursos TI: Humanos, financieros y tecnológicos.....	7
Tecnológicos.....	7
Servidor.....	7
Equipos de Escritorio y Portátiles	7
Red.....	7
Impresoras y Escáner.....	7
Software.....	7
SERVICIOS TECNOLOGICOS	11
Administración de los sistemas de información.....	11
LINEAMIENTOS DE SERVICIOS TECNOLÓGICO	11
AMBITO: ARQUITECTURA DE SERVICIOS TECNOLÓGICOS.....	11
AMBITO: OPERACIÓN DE LOS SERVICIOS TECNOLÓGICOS	12
ÁMBITO: SOPORTE DE LOS SERVICIOS TECNOLÓGICOS	12
ÁMBITO: GESTIÓN DE LA CALIDAD Y LA SEGURIDAD DE LOS SERVICIOS TECNOLÓGICOS	13
LINEAMIENTOS INFORMACION TI	13
ÁMBITO: PLANEACIÓN YGOBIERNO DE LOS COMPONENTES DE INFORMACIÓN	13
ÁMBITO: DISEÑO DE LOS COMPONENTES DE INFORMACIÓN.....	14
ÁMBITO: ANÁLISIS Y APROVECHAMIENTO DE LOS COMPONENTES DE INFORMACIÓN.....	15

PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES PETI

ÁMBITO: CALIDAD Y SEGURIDAD DE LOS COMPONENTES DE INFORMACIÓN	15
LINEAMIENTOS DEL DOMINIO SISTEMAS DE INFORMACIÓN	15
AMBITO: DISEÑO DE LOS SISTEMAS DE INFORMACION.....	15
ÁMBITO: CICLO DE VIDA DE LOS SISTEMAS DE INFORMACIÓN.....	17
ÁMBITO: SOPORTE DE LOS SISTEMAS DE INFORMACIÓN	18
ÁMBITO: GESTIÓN DE LA CALIDAD Y SEGURIDAD DE LOSSISTEMAS DE INFORMACIÓN	18
GOBIERNO DE TI	19
Entendimiento estratégico	19
ANÁLISIS FINANCIERO	19
Modelo de gestión de TI.....	20
Definición de los objetivos estratégicos de TI.....	20

PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES PETI

OBJETIVO

Establecer las estrategias para la gestión de las Tecnologías de la Información y las Comunicaciones PETI en el Instituto Departamental de Deporte y la Recreación del Quindío, acordes con las necesidades de la Entidad y los lineamientos del programa de Gobierno Digital, como eje de desarrollo institucional para el periodo comprendido entre el 2020 y 2023, que contribuya al logro de los objetivos y metas institucionales.

ALCANCE DEL DOCUMENTO

Este documento describe las estrategias, políticas y proyectos del ámbito de tecnología de información que se proponen ejecutar en el periodo 2020 – 2023 para apoyar en el cumplimiento de los objetivos misionales del instituto departamental de deporte y recreación del Quindío "INDEPORTES QUINDIO "

MARCO NORMATIVO

Ley 1712 de 2014: "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".

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

Decreto 1008 de 2018: "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la Parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario Del sector de Tecnologías de la Información y las Comunicaciones".

Decreto 415 de 2016: "Establece los lineamientos para el fortalecimiento Institucional en materia de tecnologías de la información y las Comunicaciones a través del posicionamiento de los líderes de tecnologías de la información (TI)".

Decreto 2573 del 12 de diciembre de 2014: "Por el cual Se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente La Ley 1341 de 2009 y se dictan otras disposiciones".

Decreto Nacional 1078 de 2015: "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"

RUPTURAS ESTRATEGICAS

El instituto departamental de deporte y recreación del Quindío "INDEPORTES QUINDIO "Las rupturas estratégicas nos permiten identificar las necesidades que se están presentando la entidad para poder realizar los cambios necesarios para la gestión de TI como son:

- Fortalecer el equipo humano de la institución pública y desarrollar sus capacidades de uso y apropiación de TIC.
- La tecnología debe ser considerada un factor de valor estratégico para la institución pública.
- La información debe ser más oportuna, más confiable y con mayor detalle.

PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES PETI

- Necesidad de aumento de la capacidad de análisis de información en todas las áreas de la institución pública.
- Necesidad de definir estándares de integración e interoperabilidad.
- La gestión de tecnología es más que un proceso de soporte, reparación y de provisión de equipos de cómputo, en el mundo de hoy TI es un factor Estratégico para la organización.
- Definir los estándares de integración de sistemas con el fin de facilitar la Transferencia de información entre ellos.
- Desarrollar e implementar soluciones de cara al ciudadano que den valor agregado y permitan mejorar la imagen de eficiencia y buen servicio.
- Fortalecer el equipo humano de la institución pública y desarrollar sus capacidades de uso y apropiación de TIC.

ANALISIS DE LA SITUACION ACTUAL

Naturaleza

El instituto departamental de deporte y recreación del Quindío Indeportes Quindío es un ente descentralizado de la gobernación del Quindío el cual se encarga de diferentes programas relacionados con el deporte y la recreación como son, inclusión social, deporte asociado hábitos de vida y estilo saludables (HEVS), supérate intercolegiados con los cuales se quiere fomentar el desarrollo deportivo y mejorar la calidad de vida de la comunidad Quindiana.

Misión

Somos una entidad que Garantiza en el Departamento del Quindío el fomento del deporte, la recreación y los hábitos y estilos de vida saludable como mecanismos para el aprovechamiento del tiempo libre, mejoramiento de la calidad de vida y la inclusión social a través, de nuestros recursos humanos, tecnológicos, físicos y financieros.

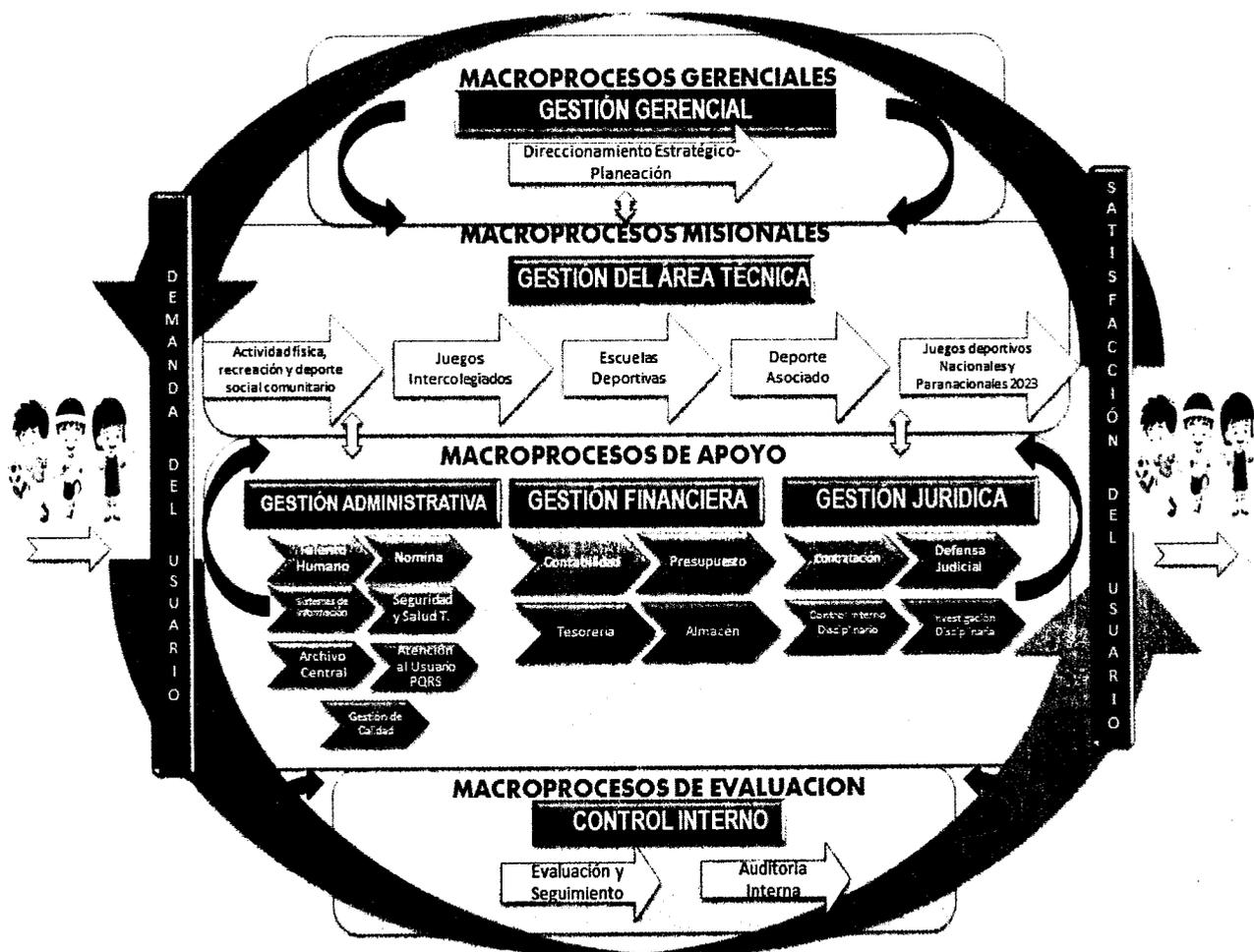
Visión

Ser al año 2023 una Institución fortalecida en la planificación, asesoría y fomento del deporte, la recreación y los hábitos y estilos de vida saludables en el Departamento del Quindío, coadyuvando al posicionamiento del deporte competitivo y altos logros en los XXII Juegos deportivos Nacionales y VI Juegos Paranales.

PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES PETI

ESTRATEGIA DE TI

Este dominio tiene el fin de apoyar el proceso de evolución de la Arquitectura en el Instituto Departamental de Deporte y Recreación del Quindío "INDEPORTES QUINDIO", en el siguiente cuadro se presenta los diferentes procesos con los que cuenta la entidad



USO Y APROPIACION DE LA TECNOLOGIA

Principales actividades que se llevan a cabo:

- Mantenimiento preventivo y correctivo de equipos tecnológicos
- Actualización e instalación de software
- Soporte de software
- Actualización e instalación de software antivirus
- Programación y ejecución de copias de seguridad de los equipos
- Administración del portal web www.indeportesquindio.gov.co
- Administración y seguimiento a correo institucionales

Productos y servicios que se prestan:

- Mantenimiento preventivo y correctivo de equipos tecnológicos
- Actualización e instalación de software
- Soporte e instalación de software
- Actualización e instalación de software antivirus

PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES PETI

- Programación y ejecución de copias de seguridad de los equipos
- Creación y administración de plataforma de correos institucionales
- Administración del portal web www.indeportesquindio.gov.co
- Administración y seguimiento a correo institucionales

Herramientas de TI que apoyan las actividades y la prestación de los servicios

Software aplicativo
Software utilitario

Recursos TI: Humanos, financieros y tecnológicos

Un (1) Técnico, contratista

Tecnológicos

Hardware

Servidor

Marca	Área	Característica
Hp Proliant	Administrativa	ML110 V4 GEN9

Equipos de Escritorio y Portátiles

Cantidad	Marca	Característica
1	Dell	Portatil
16	Hp	Computador de Mesa
8	Janus	Computador de Mesa
4	Compaq y clones	Computador de Mesa

Red

Cantidad	Marca	Característica
3	Tp link y Dlink	Switch

Impresoras y Escáner

Cantidad	Marca	Característica
3	Hp	Impresora Hp 1102w
2	Hp	Impresora hp 1212nf
1	Epson	Impresora Epson l220
2	HP	Escaner Scanjet Serie 8xxx y 7500

Software

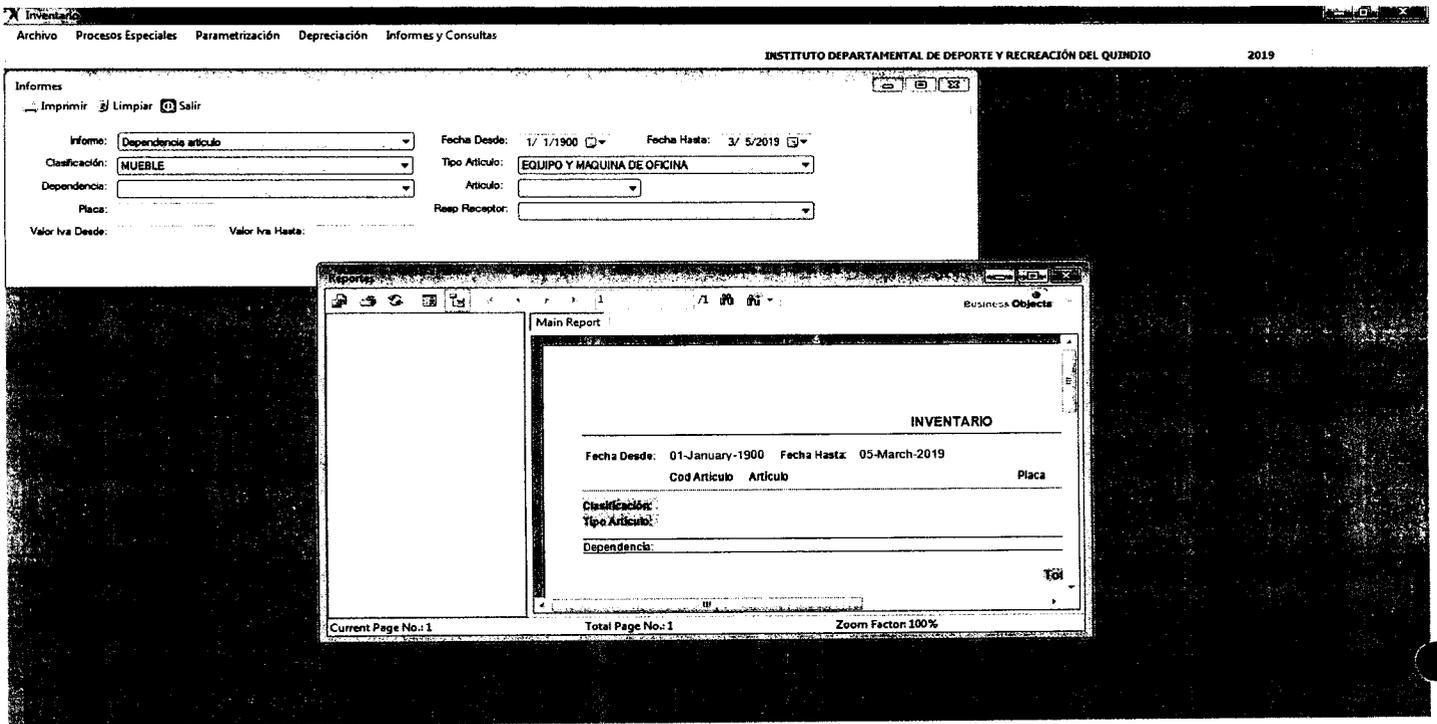
SOFTWARE FINANCIERO (SIAS SAS PUBLIFINANZAS)

SOPORTE DE USUARIOS (MESA DE AYUDA GLPI)

PORTAL WEB www.indeportesquindio.gov.co

VENTANILLA UNICA www.indeportes.micorrespondencia.com/index.php

PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES PETI



Nombre del sistema de información: SIAS SAS PUBLIFINANZAS

Descripción detallada de la funcionalidad: Publi-Finanzas es un software económico, amigable y de fácil manejo con capacidad de integrar todos los módulos del área financiera de los entes oficiales, proporcionando así confiabilidad y rapidez en el ingreso de la información, oportunidad y eficacia en la utilización de la misma. Actualizado a Normas Internacionales de Información Financiera NIIFS.

Módulos que componen el sistema SIAS Publifinanzas

- MODULO DE INVENTARIOS
- MODULO DE NOMINA
- MODULO DE PRESUPUESTO
- MODULO DE CONTABILIDAD
- MODULO DE BANCOS
- MODULO DE INGRESOS
- SISTEMA DE INFORMACION



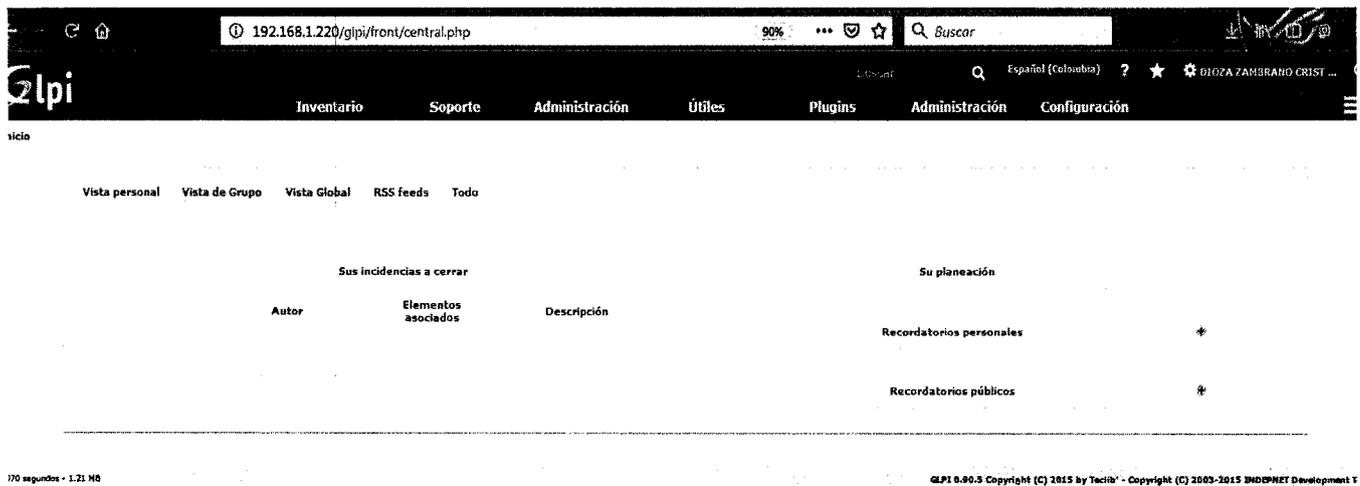
PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES PETI

Nombre del sistema de información: GLPI MESA DE AYUDA

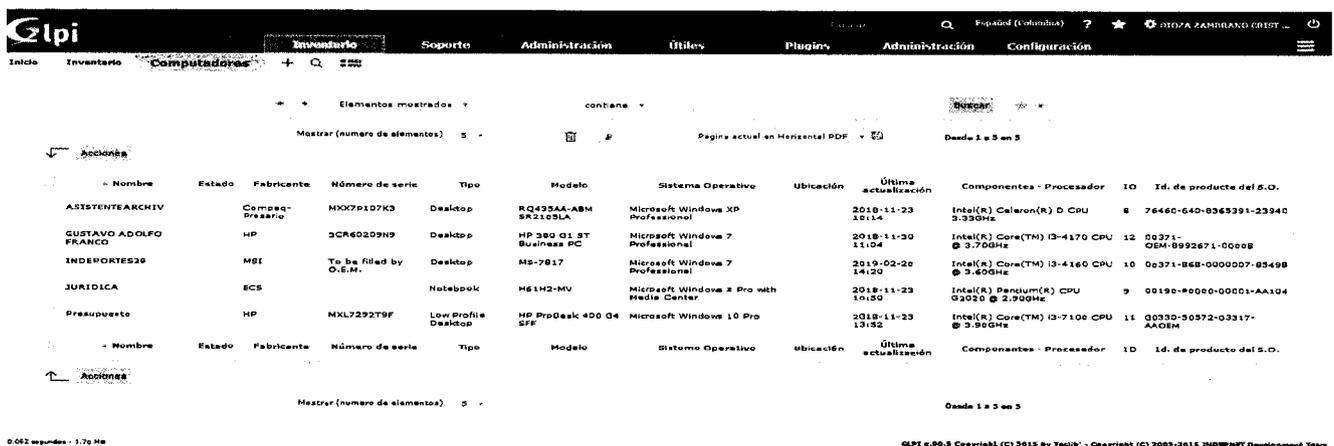
Descripción detallada de la funcionalidad: GLPI es una solución libre de gestión de servicios de tecnología de la información, un sistema de seguimiento de incidencias y de solución service desk. Este software de código abierto está editado en PHP y distribuido bajo una licencia GPL.

Módulos que componen el sistema GLPI

- MODULO DE INVENTARIO DE EQUIPOS DE COMPUTO (FUSION INVENTORY)
- MODULO DE INCIDENCIAS Y REPORTES



The screenshot shows the GLPI dashboard interface. At the top, there is a navigation bar with links for 'Inicio', 'Inventario', 'Soporte', 'Administración', 'Útiles', 'Plugins', 'Administración', and 'Configuración'. Below this, there are options for 'Vista personal', 'Vista de Grupo', 'Vista Global', 'RSS feeds', and 'Todo'. The main content area is titled 'Sus incidencias a cerrar' and contains a table with columns for 'Autor', 'Elementos asociados', and 'Descripción'. To the right, there are sections for 'Su planeación', 'Recordatorios personales', and 'Recordatorios públicos'. The footer indicates '170 segundos - 1.21 Mb' and 'GLPI 0.90.5 Copyright (C) 2015 by Teclib® - Copyright (C) 2009-2015 INDEPNET Development Team'.

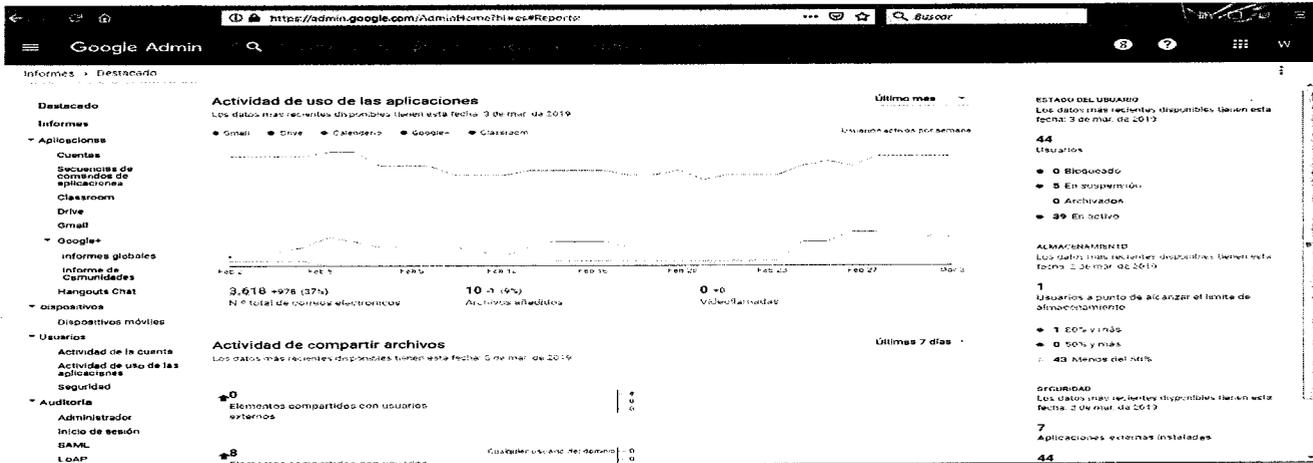


The screenshot shows the GLPI inventory management interface. The navigation bar includes 'Inicio', 'Inventario', 'Computadores', 'Soporte', 'Administración', 'Útiles', 'Plugins', 'Administración', and 'Configuración'. The main content area displays a table of computer assets with columns for 'Nombre', 'Estado', 'Fabricante', 'Número de serie', 'Tipo', 'Modelo', 'Sistema Operativo', 'Ubicación', 'Última actualización', 'Componentes - Procesador', and 'Id. de producto del S.O.'. The table lists several computers, including one from 'ASISTENTEARCHIV' and another from 'GUSTAVO ADOLFO FRANCO'. The footer indicates '0.062 segundos - 1.76 Mb' and 'GLPI 0.90.5 Copyright (C) 2015 by Teclib® - Copyright (C) 2009-2015 INDEPNET Development Team'.

Nombre del sistema de información: CORREO INSTITUCIONAL GSUITE

Descripción detallada de la funcionalidad: Correo institucional de la plataforma de google los cuales se cuenta con las diferentes aplicaciones de Gmail como es google, hangouts, visualizador de texto, visualizador de cálculo, y visualizador de presentaciones para su uso en la institución.

PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES PETI



Usuarios

Usuarios | Todos los usuarios

+ Añadir un filtro

Nombre	Correo electrónico	Estado	Último acceso	Uso del correo electrónico	Uso de Drive
administrador indeportes	administradorweb@indeportesquindio.gov.co	Activo	Hace 1 semana	0.75 GB	0 GB
ADRIANA PATRICIA GIRALDO VA...	presupuesto@indeportesquindio.gov.co	Activo	Hace 1 mes	0.22 GB	0 GB
ALBA LILIANA PRIETO	asistencias@indeportesquindio.gov.co	Activo	Hace 1 día	4.07 GB	0.39 GB
ALEXANDER ALZATE LOPEZ	logistica@indeportesquindio.gov.co	Activo	Hace 4 días	0.12 GB	0 GB
BRIGADIER ARIAS ALZATE	conductor@indeportesquindio.gov.co	Activo	Hace 9 meses	0.08 GB	0 GB
capacitacion gerencia deportiva	capacitaciongerenciadeport@indeportesquindio.gov.co	Suspendido por el administ...	Hace más de 1 año	0.02 GB	0 GB
CHRISTIAN CAMILD GALVEZ	promotor@indeportesquindio.gov.co	Activo	Hace 8 meses	0.1 GB	0.03 GB
CLARA JANNETH MENDEZ CAL...	procesosgerencia@indeportesquindio.gov.co	Activo	Hace 1 mes	0.05 GB	0 GB
Contactenos indeportes Quindio	contactenos@indeportesquindio.gov.co	Activo	Hace 1 día	1.96 GB	0.15 GB

Files por página: 50

Página 1 de 1

Nombre del sistema de información: MI CORRESPONDENCIA

Descripción detallada de la funcionalidad: Plataforma informática especializada en servicios de gestión, administración y control a la correspondencia de Entidades Públicas y Privadas, que permite:

- Administra toda la correspondencia tanto interna como externa, ya sea enviada o recibida. Reemplazar el uso de documentos físicos por documentos electrónicos.
- Automatizar el proceso de registro, asignación y tratamiento de la información.
- Controla los tiempos de respuesta de las peticiones, quejas, denuncias, tutelas y derechos de petición.
- Notificar actividades por correo electrónico.
- Facilita la radicación y gestión electrónica vía Web, de la correspondencia.
- Administra la distribución física y agiliza la trazabilidad de la información

independientes.micorrespondencia.com/u/index.php

Aplicaciones Autenticación de U... Inicio Iniciar Sesión Editor PDF - Editor... Editor fácil de usar... Liquidación y Pago... EDL-APP v2.3.2 MICORRESPONDE...

MAURICIO ALVARADO CALDERON
Correo de Notificación: contactenos@indeportesquindio.gov.co

Cambiar Vigencia: 2020

MENU

- Correspondencia Recibida
- Correspondencia Enviada
- Correspondencia Pendiente de Respuesta

CONFIGURACION

- Cambiar Clave
- Cambiar Correo Electronico de Notificación de correspondencia

CORRESPONDENCIA RECIBIDA 2020

Tipo de Documento: Todos

Palabra a Buscar:

No Radicación	Fecha de Registro	Asunto	Remitente	Destinatario	Reenviar A	Tiempo de Respuesta	Consultar
00105	2020-04-22	Con motivo de la pandemia covid 19 se hace revisión de correspondencia pendiente por contestar por lo que aparece a su nombre, en caso de haber dado respuesta oportuna, haga caso omiso de este mensaje.	ZULMA TORO	MAURICIO ALVARADO CALDERON	<input type="button" value="Reenviar A"/>	<input type="button" value="Tiempo de Respuesta"/>	<input type="button" value="Consultar"/>

PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES PETI

APLICATIVO	TIPO DE SISTEMA
SIAS SAS PUBLIFINANZAS	SISTEMA MISIONAL DE PRESTACION
GLPI	SISTEMA DE APOYO
PORTAL WEB	SISTEMA MISIONAL DE INFORMACION DIGITAL
CORREO ELECTRONICO INSTITUCIONAL	SISTEMA MISIONAL DE INFORMACION DIGITAL
MI CORRESPONDENCIA	SISTEMA MISIONAL DE INFORMACION DIGITAL

SERVICIOS TECNOLOGICOS

La gestión de los servicios tecnológicos en el instituto departamental de deporte y recreación del Quindío Indeportes Quindío es realizado por el área de sistemas de información que hace parte del área administrativa. El instituto Cuenta con un servidor en el cual se hace manejo del servicio de Publifinanzas donde se hace todo el manejo administrativo.

Administración de los sistemas de información

La administración del sistema Publifinanzas está a cargo de SIAS SAS los cuales dan el soporte a incidencias que se presenten con el aplicativo, actualizaciones y creación de cuentas el equipo donde se encuentra instalada la aplicativo tiene las siguientes características técnicas:

MONITOR JANUS 19"
CPU HP 280 HP PROLIANT ML110 V4 GEN9
PROCESADOR INTEL CORE XEON E5-2603V4 - 1.7GHz 15 MB L3 CACHE
RAM 8GB
DISCO DURO 500GB

LINEAMIENTOS DE SERVICIOS TECNOLÓGICO

AMBITO: ARQUITECTURA DE SERVICIOS TECNOLÓGICOS

Código	Nombre	Descripción	Implementación
LI.ST.01	DIRECTORIO DE SERVICIOS TECNOLÓGICOS	El área de sistemas de información debe contar con un directorio actualizado de sus Servicios Tecnológicos, que le sirva de insumo para administrar, analizar y mejorar los activos de TI.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.
LI.ST.02	ELEMENTOS PARA EL INTERCAMBIO DE INFORMACIÓN	El área de sistemas de información debe incluir dentro de su arquitectura de Servicios tecnológicos los elementos necesarios para poder realizar el intercambio de información entre las áreas de la institución y las organizaciones externas a escala sectorial y nacional. Las instituciones que son productoras de información geográfica deben incorporar los elementos dentro de la arquitectura de Servicios tecnológicos para constituirse en nodos de la ICDE (Infraestructura Colombiana de Datos Espaciales), de tal forma que se asegure el intercambio de información geo-espacial y geo-referenciada.	No se requiere el software para el intercambio de la información debido a que no se intercambia ninguna clase de datos privados.

PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES PETI

LI.ST.03	GESTIÓN DE LOS SERVICIOS TECNOLÓGICOS	El área de sistemas de información, debe gestionar la operación y el soporte de los servicios tecnológicos, en particular, durante la implementación y paso a producción de los proyectos de TI, se debe garantizar la estabilidad de la operación de TI y responder acorde al plan de capacidad.	No se cuenta con la gestión de servicios tecnológicos directorio de servicios tecnológicos para final del 2 semestre de 2021 se tendrá realizado.
LI.ST.04	ACCESO A SERVICIOS EN LA NUBE	El área de sistemas de información debe evaluar como primera opción la posibilidad de prestar o adquirir los Servicios Tecnológicos haciendo uso de la Nube (pública, privada o híbrida), para atender las necesidades de los grupos de interés.	El área de sistemas se encarga de monitorear el uso del servicio en la nueve de los correos institucionales
LI.ST.15	DISPOSICIÓN DE RESIDUOS TECNOLÓGICOS	La institución debe implementar un programa de correcta disposición final de los residuos tecnológicos, teniendo en cuenta los lineamientos técnicos con los que cuente el gobierno nacional.	El instituto actualmente estudia el programa de disposición de residuos tecnológicos

AMBITO: OPERACIÓN DE LOS SERVICIOS TECNOLÓGICOS

LI.ST.05	CONTINUIDAD Y DISPONIBILIDAD DE LOS SERVICIOS TECNOLÓGICOS	El área de sistemas de información debe garantizar la continuidad y disponibilidad de los servicios Tecnológicos, así como la capacidad de atención y resolución de incidentes para ofrecer continuidad de la operación y la prestación de todos los servicios de la entidad y de TI.	Actualmente se cuenta con ups en los equipos del área administrativa, gerencia y servidor del instituto, adicional se cuenta con un sistema de detección de incendios En el monitoreo de software se cuenta con Forticlient el cual brinda control de las páginas y medios extraíbles en los diferentes equipos del instituto
LI.ST.06	ALTA DISPONIBILIDAD DE LOS SERVICIOS TECNOLÓGICOS	El área de sistemas de información debe implementar capacidades de alta disponibilidad para las infraestructuras críticas y los Servicios Tecnológicos que afecten la continuidad del servicio de la institución, las cuales deben ser puestas a prueba periódicamente.	El área de sistemas cuentan con cronograma de mantenimiento de los equipos de cómputo para su óptimo funcionamiento además de contar con un BACKUP mensual de la información
LI.ST.07	CAPACIDAD DE LOS SERVICIOS TECNOLÓGICOS	El área de sistemas de información debe velar por la prestación de los servicios de TI, identificando las capacidades actuales de los Servicios Tecnológicos y proyectando las capacidades futuras requeridas para un óptimo funcionamiento.	El área de sistemas es responsable de prestar el servicio de mantenimiento preventivo y correctivo de los equipos del instituto

ÁMBITO: SOPORTE DE LOS SERVICIOS TECNOLÓGICOS

LI.ST.08	ACUERDOS DE NIVEL DE SERVICIOS	El área de sistemas de información debe velar por el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) establecidos para los Servicios Tecnológicos.	No se cuenta con un acuerdos de nivel de servicio, se reprograma el estudios para la elaboración del ANS para el 2 semestre de 2021.
LI.ST.09	SOPORTE A LOS SERVICIOS TECNOLÓGICOS	El área de sistemas de información debe definir e implementar el procedimiento para atender los requerimientos de soporte de primer, segundo y tercer nivel, para sus servicios de	El área de sistemas está encargado de prestar el servicio de Se cuenta con el aplicativo GLPI para el soporte de servicios tecnológicos para el final del primer semestre de

PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES PETI

		TI, a través de un único punto de contacto como puede ser una mesa de servicio.	2019 se socializara con los funcionarios de la entidad
LI.ST.10	PLANES DE MANTENIMIENTO	El área de sistemas de información debe implementar un plan de mantenimiento preventivo y evolutivo sobre toda la infraestructura y demás Servicios Tecnológicos de la institución.	El área de sistemas cuenta ya con plan de mantenimiento preventivo y correctivo, el cual se socializo a los funcionarios del instituto por medio de correo institucional.

ÁMBITO: GESTIÓN DE LA CALIDAD Y LA SEGURIDAD DE LOS SERVICIOS TECNOLÓGICOS

LI.ST.11	CONTROL DE CONSUMO DE LOS RECURSOS COMPARTIDOS POR SERVICIOS TECNOLÓGICOS	El área de sistemas de información debe identificar, monitorear y controlar el nivel de consumo de los recursos críticos que son compartidos por los Servicios Tecnológicos y administrar su disponibilidad.	El área de sistemas implemento para el monitoreo de los equipos de cómputo el software gratuito Forticlient el cual hace control de las páginas web, dispositivos USB y función de antivirus
LI.ST.12	GESTIÓN PREVENTIVA DE LOS SERVICIOS TECNOLÓGICOS	El área de sistemas de información debe asegurarse de que la infraestructura y demás recursos tecnológicos de la institución cuenten con mecanismos de monitoreo para generar alertas tempranas ligadas a los umbrales de operación que tenga definidos.	El software Forticlient entrega alertas de incidentes que tenga el equipo de cada funcionario
LI.ST.13	RESPALDO Y RECUPERACIÓN DE LOS SERVICIOS TECNOLÓGICOS	El área de sistemas de información debe contar con mecanismos de respaldo para los servicios tecnológicos críticos de la entidad así como con un proceso periódico de respaldo de la configuración y de la información almacenada en la infraestructura tecnológica, incluyendo la información clave de las estaciones de trabajo de los funcionarios de la entidad. Este proceso debe ser probado periódicamente y debe permitir la recuperación íntegra de los Servicios Tecnológicos.	Se cuenta con el BACKUP mensual de los equipos de cómputo además de las copias diarias del servidor
LI.ST.14	ANÁLISIS DE RIESGOS	El área de sistemas de información debe realizar el análisis y gestión de los riesgos asociados a su infraestructura tecnológica haciendo énfasis en aquellos que puedan comprometer la seguridad de la información o que puedan afectar la prestación de un servicio de TI.	Se cuenta con el mapa de riesgos del área de sistemas y se cuenta con el tratamiento de riesgos de seguridad y privacidad de la información
LI.ST.15	SEGURIDAD INFORMÁTICA	El área de sistemas de información debe implementar controles de seguridad informática para gestionar los riesgos que atenten contra la disponibilidad, integridad y confidencialidad de la información.	Se cuenta con la política de seguridad y privacidad de la información la cual detalla los controles que se tiene en cada área

LINEAMIENTOS INFORMACION TI

ÁMBITO: PLANEACIÓN Y GOBIERNO DE LOS COMPONENTES DE INFORMACIÓN

LI.INF.01	RESPONSABILIDAD Y GESTIÓN DE COMPONENTES DE INFORMACIÓN	El área de sistemas de información debe definir las directrices y liderar la gestión de los Componentes de información durante su ciclo de vida.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado
-----------	---	--	--

PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES PETI

		Así mismo, debe trabajar en conjunto con las dependencias para establecer acuerdos que garanticen la calidad de la información.	para los funcionarios del instituto.
LI.INF.02	PLAN DE CALIDAD DE LOS COMPONENTES DE INFORMACIÓN	El área de sistemas de información debe contar con un plan de calidad de los componentes de información que incluya etapas de aseguramiento, control e inspección, medición de indicadores de calidad, actividades preventivas, correctivas y de mejoramiento continuo de la calidad de los componentes.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.
LI.INF.03	GOBIERNO DE LA ARQUITECTURA DE INFORMACIÓN	El área de sistemas de información debe definir, implementar y gobernar la Arquitectura de Información, estableciendo métricas e indicadores de seguimiento, gestión y evolución de dicha arquitectura.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.
LI.INF.04	GESTIÓN DE DOCUMENTOS ELECTRÓNICOS	El área de sistemas de información debe definir, implementar y gobernar la Arquitectura de Información, estableciendo métricas e indicadores de seguimiento, gestión y evolución de dicha arquitectura.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.
LI.INF.05	DEFINICIÓN Y CARACTERIZACIÓN DE LA INFORMACIÓN GEOREFERENCIADA	El área de sistemas de información debe acoger la normatividad, los estándares relacionados de la Infraestructura Colombiana de Datos Espaciales (ICDE), los lineamientos de política de información geográfica y demás instrumentos vigentes que rijan la información geográfica según el Comité Técnico de Normalización, y disponer en el Portal Geográfico Nacional aquella información oficial útil para el desarrollo de proyectos de interés nacional y estratégicos.	El instituto no cuenta con un sistema de georeferenciación

ÁMBITO: DISEÑO DE LOS COMPONENTES DE INFORMACIÓN

LI.INF.06	LENGUAJE COMÚN DE INTERCAMBIO DE COMPONENTES DE INFORMACIÓN	Se debe utilizar el lenguaje común para el intercambio de información con otras instituciones. Si el lenguaje no incorpora alguna definición que sea requerida a escala institucional o sectorial, la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces deberá solicitar la inclusión al Ministerio de las TIC para que pueda ser utilizada por otras instituciones y quede disponible en el portal de Lenguaje común de intercambio de información del Estado colombiano.	El instituto cuenta con el intercambio de información Colombia compra eficiente (SECOP), SIA OBSERVA
LI.INF.07	DIRECTORIO DE SERVICIOS COMPONENTES DE INFORMACIÓN	El área de sistemas de información debe crear y mantener actualizado un directorio de los Componentes de información. La institución es responsable de definir el nivel de acceso de este directorio teniendo en cuenta la normatividad asociada. Este directorio debe hacer parte del directorio de Componentes de información sectorial, el cual debe ser consolidado a través de la cabeza de sector, con el fin de promover y facilitar	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.

PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES PETI

		el consumo, re-uso, ubicación y entendimiento, entre otros de los Componentes de información.	
LI.INF.08	PUBLICACIÓN DE LOS SERVICIOS DE INTERCAMBIO DE COMPONENTES DE INFORMACIÓN	El área de sistemas de información debe publicar los servicios de intercambio de información a través de la Plataforma de Interoperabilidad del Estado colombiano	El instituto cuenta con el intercambio de información Colombia compra eficiente (SECOP), SIGEP, SIA OBSERVA
LI.INF.09	CANALES DE ACCESO A LOS COMPONENTES DE INFORMACIÓN	El área de sistemas de información debe garantizar los mecanismos que permitan el acceso a los servicios de información por parte de los diferentes grupos de interés, contemplando características de accesibilidad, seguridad y usabilidad	El instituto cuenta con redes sociales , pagina web del instituto correo electrónico para la atención de la comunidad adicional en el portal del instituto se publica la información que establece la ley 1712 del 2014

ÁMBITO: ANÁLISIS Y APROVECHAMIENTO DE LOS COMPONENTES DE INFORMACIÓN

LI.INF.10	MECANISMOS PARA EL USO DE LOS COMPONENTES DE INFORMACIÓN	El área de sistemas de información debe impulsar el uso de su información a través de mecanismos sencillos, confiables y seguros, para el entendimiento, análisis y aprovechamiento de la información por parte de los grupos de interés.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.
LI.INF.11	ACUERDOS DE INTERCAMBIO DE INFORMACIÓN	El área de sistemas de información debe establecer los Acuerdos de Nivel de Servicio (ANS) con las dependencias o instituciones para el intercambio de la información de calidad, que contemplen las características de oportunidad, disponibilidad y seguridad que requieran los Componentes de información.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.
LI.INF.12	FUENTES UNIFICADAS DE INFORMACIÓN	El área de sistemas de información debe garantizar la existencia de fuentes únicas de información, para que el acceso sea oportuno, relevante, confiable, completo, veraz y comparable.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.

ÁMBITO: CALIDAD Y SEGURIDAD DE LOS COMPONENTES DE INFORMACIÓN

LI.INF.13	HALLAZGOS EN EL ACCESO A LOS COMPONENTES DE INFORMACIÓN	El área de sistemas de información debe generar mecanismos que permitan a los consumidores de los Componentes de información reportar los hallazgos encontrados durante el uso de los servicios de información.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.
LI.INF.14	PROTECCIÓN Y PRIVACIDAD DE COMPONENTES DE INFORMACIÓN	El área de sistemas de información debe incorporar, en los atributos de los Componentes de información, la información asociada con los responsables y políticas de la protección y privacidad de la información, conforme con la normativa de protección de datos de tipo personal y de acceso a la información pública.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.

LINEAMIENTOS DEL DOMINIO SISTEMAS DE INFORMACIÓN

AMBITO: DISEÑO DE LOS SISTEMAS DE INFORMACION

LI.SIS.01	DEFINICIÓN ESTRATÉGICA DE LOS	El área de sistemas de información debe definir y documentar la arquitectura de los sistemas de	Se encuentra en proceso de construcción, se estima que para el segundo semestre del
-----------	-------------------------------	---	---

PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES PETI

	SISTEMAS DE INFORMACIÓN	DE	información de la institución identificando los diferentes componentes y la forma en que interactúan entre sí, así como la relación con los demás dominios de la Arquitectura Empresarial.	2021 se tendrá socializado para los funcionarios del instituto.
LI.SIS.02	DIRECTORIO DE SISTEMAS DE INFORMACIÓN	DE DE	El área de sistemas de información debe definir y documentar la arquitectura de los sistemas de información de la institución identificando los diferentes componentes y la forma en que interactúan entre sí, así como la relación con los demás dominios de la Arquitectura Empresarial.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.
LI.SIS.03	ARQUITECTURAS DE REFERENCIA DE SISTEMAS DE INFORMACIÓN	DE DE DE	El área de sistemas de información es la responsable de definir y evolucionar las arquitecturas de referencia de los sistemas de información, con el propósito de orientar el diseño de cualquier arquitectura de solución bajo parámetros, patrones y atributos de calidad definidos.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.
LI.SIS.04	ARQUITECTURAS DE SOLUCIÓN DE SISTEMAS DE INFORMACIÓN	DE DE	El área de sistemas de información debe garantizar la documentación y actualización de la arquitectura de solución de los sistemas de información de la institución bajo los parámetros de las arquitecturas de referencia definidas.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.
LI.SIS.05	METODOLOGÍA DE REFERENCIA PARA EL DESARROLLO DE SISTEMAS DE INFORMACIÓN	DE DE DE	El área de sistemas de información debe definir una metodología formal para el desarrollo y mantenimiento de software, que oriente los proyectos de construcción o evolución de los sistemas de información que se desarrollen a la medida, ya sea internamente o a través de terceros.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.
LI.SIS.06	DERECHOS PATRIMONIALES SOBRE LOS SISTEMAS DE INFORMACIÓN	LOS	Cuando se suscriban contratos con terceras partes bajo la figura de "obra creada por encargo" o similar, cuyo alcance incluya el desarrollo de elementos de software, la entidad debe incluir en dichos contratos, la obligación de transferir a la institución los derechos patrimoniales sobre los productos desarrollados.	En caso de presentarse se aplicaran los derechos patrimoniales sobre los sistemas de información.
LI.SIS.07	GUÍA DE ESTILO Y USABILIDAD		El área de sistemas de información debe definir o adoptar una guía de estilo y usabilidad para la institución. Esta guía debe estar aplicada de acuerdo a la caracterización de usuarios y según el canal utilizado por los sistemas de información y, así mismo, debe estar alineada con los principios de usabilidad definidos por el Estado colombiano, asegurando la aplicación de la guía en todos sus sistemas de información. Para los componentes de software, que sean propiedad de terceros, se debe realizar su personalización hasta donde sea posible de manera que se pueda brindar una adecuada experiencia de usuario.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.

PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES PETI

LI.SIS.08	APERTURA DE DATOS	El área de sistemas de información debe asegurar que en el diseño e implementación de sus sistemas de información se incorporen funcionalidades que faciliten la generación de datos abiertos. Así mismo, se deben automatizar los procesos de extracción de los sistemas de información fuente, para la generación y publicación de conjuntos de datos abiertos.	se encuentra en estudio, en el caso que aplique para la entidad, se empezará el proceso de diseño
LI.SIS.09	INTEROPERABILIDAD	El área de sistemas de información, debe desarrollar los mecanismos necesarios para compartir su información haciendo uso del Modelo de Interoperabilidad definido por el Estado a partir de las necesidades de intercambio de información con otras entidades.	se encuentra en estudio, en el caso que aplique para la entidad, se empezará el proceso de diseño
LI.SIS.10	SOPORTE A LOS COMPONENTES DE INFORMACIÓN	El área de sistemas de información, debe garantizar que los sistemas de información soporten la arquitectura y componentes de información establecidos por la entidad.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.
LI.SIS.24	ACCESIBILIDAD	Los sistemas de información que estén disponibles para el acceso a la ciudadanía o aquellos que de acuerdo a la caracterización de usuarios lo requieran, deben cumplir con las funcionalidades de accesibilidad que indica la estrategia de Gobierno en Línea.	El instituto cuenta actualmente con la página web institucional, donde el usuario tiene acceso a toda la información de interés. El SECOP I y SIA OBSERVA son plataformas las cuales sirven para la transparencia en la contratación.

ÁMBITO: CICLO DE VIDA DE LOS SISTEMAS DE INFORMACIÓN

LI.SIS.11	AMBIENTES INDEPENDIENTES EN EL CICLO DE VIDA DE LOS SISTEMAS DE INFORMACIÓN	El área de sistemas de información debe identificar y mantener la independencia de los ambientes requeridos durante el ciclo de vida de los sistemas de información, ya sea directamente o través de un tercero. Ejemplos de ambientes son: desarrollo, pruebas, capacitación, producción.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.
LI.SIS.12	ANÁLISIS DE REQUERIMIENTOS DE LOS SISTEMAS DE INFORMACIÓN	El área de sistemas de información debe incorporar un proceso formal de análisis y gestión de requerimientos de software en el ciclo de vida de los sistemas de información de manera que se garantice su trazabilidad y cumplimiento.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.
LI.SIS.13	INTEGRACIÓN CONTINUADURANTE EL CICLO DE VIDA DE LOS SISTEMAS DE INFORMACIÓN	El área de sistemas de información debe garantizar que dentro del proceso de desarrollo de sistemas de información, se ejecuten estrategias de integración continua sobre los nuevos desarrollos de sistemas de información.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.
	PLAN DE PRUEBAS DURANTE EL CICLO DE VIDA DE LOS SISTEMAS DE INFORMACIÓN	En el proceso de desarrollo y evolución de un sistema de información, la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con un plan de pruebas que cubra lo funcional y lo no funcional. La aceptación de cada una de las etapas de este plan debe estar vinculada a la transición del sistema de información a través de los diferentes ambientes.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.

PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES PETI

LI.SIS.15	PLAN DE CAPACITACIÓN Y ENTRENAMIENTO PARA LOS SISTEMAS DE INFORMACIÓN	El área de sistemas de información debe realizar constantemente capacitación y entrenamiento funcional y técnico a los usuarios, con el fin de fortalecer el uso y apropiación de los sistemas de información.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.
LI.SIS.16	MANUAL DEL USUARIO, TÉCNICO Y DE OPERACIÓN DE LOS SISTEMAS DE INFORMACIÓN	El área de sistemas de información debe asegurar que todos sus sistemas de información cuenten con la documentación técnica y funcional debidamente actualizada.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.
LI.SIS.17	GESTIÓN DE CAMBIOS DE LOS SISTEMAS DE INFORMACIÓN	El área de sistemas de información debe definir e implementar formalmente un procedimiento de control de cambios para los sistemas de información de la institución.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.

ÁMBITO: SOPORTE DE LOS SISTEMAS DE INFORMACIÓN

LI.SIS.18	ESTRATEGIA DE MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	Para el mantenimiento de los sistemas de información, la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe hacer un análisis de impacto ante cualquier solicitud de cambio en alguno de sus componentes, con el fin de determinar la viabilidad del cambio y las acciones a seguir.	El área de sistemas cuenta ya con plan de mantenimiento preventivo y correctivo, el cual se socializa a los funcionarios del instituto por medio de correo institucional.
LI.SIS.19	SERVICIOS DE MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN CON TERCERAS PARTES	El área de sistemas de información debe establecer criterios de aceptación y definir Acuerdos de Nivel de Servicio (ANS) cuando se tenga contratado con terceros el mantenimiento de los sistemas de información. Los ANS se deben aplicar en las etapas del ciclo de vida de los sistemas de Información que así lo requieran y se debe velar por la continuidad del servicio.	El área de sistemas cuenta ya con plan de mantenimiento preventivo y correctivo, a cargo del contratista del área administrativa y financiera

ÁMBITO: GESTIÓN DE LA CALIDAD Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

LI.SIS.20	PLAN DE CALIDAD DE LOS SISTEMAS DE INFORMACIÓN	El área de sistemas de información debe implementar un plan de aseguramiento de la calidad durante el ciclo de vida de los sistemas de información.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.
LI.SIS.21	CRITERIOS NO FUNCIONALES Y DE CALIDAD DE LOS SISTEMAS DE INFORMACIÓN	En la construcción o modificación de los Sistemas de Información, el área de sistemas de información, debe identificar los requisitos no funcionales aplicables, garantizando su cumplimiento una vez entre en operación el sistema.	Se encuentra en proceso de construcción, se estima que para el segundo semestre del 2021 se tendrá socializado para los funcionarios del instituto.
LI.SIS.22	SEGURIDAD Y PRIVACIDAD DE LOS SISTEMAS DE INFORMACIÓN	Durante todas las fases del ciclo de vida de los sistemas de información, El área de sistemas de información debe analizar e incorporar aquellos componentes de seguridad y privacidad de la información que sean necesarios.	El software Forticlient bloquea el ingreso a paginas no institucionales así como entrega alertas de incidentes que tenga el equipo de cada funcionario De igual manera cada equipo cuenta con un usuario administrador que solo es manejado por el área de sistemas.
LI.SIS.23	AUDITORÍA Y TRAZABILIDAD DE LOS SISTEMAS DE INFORMACIÓN	El área de sistemas de información debe desarrollar mecanismos que aseguren el registro histórico de las acciones realizadas por los usuarios	El área de sistemas de información actualmente cuenta con las hojas de vida actualizadas de los

PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES PETI

		sobre los Sistemas de Información, manteniendo la trazabilidad y apoyando los procesos de auditoría	ordenadores del instituto (30 ordenadores)
LI.SIS.24	ACCESIBILIDAD	Los sistemas de información que estén disponibles para el acceso a la ciudadanía o aquellos que de acuerdo a la caracterización de usuarios lo requieran, deben cumplir con las funcionalidades de accesibilidad que indica la estrategia de Gobierno en Línea.	El instituto cuenta actualmente con la página web institucional, donde el usuario tiene acceso a toda la información de interés. El SECOP I y SIA OBSERVA son plataformas las cuales sirven para la transparencia en la contratación.

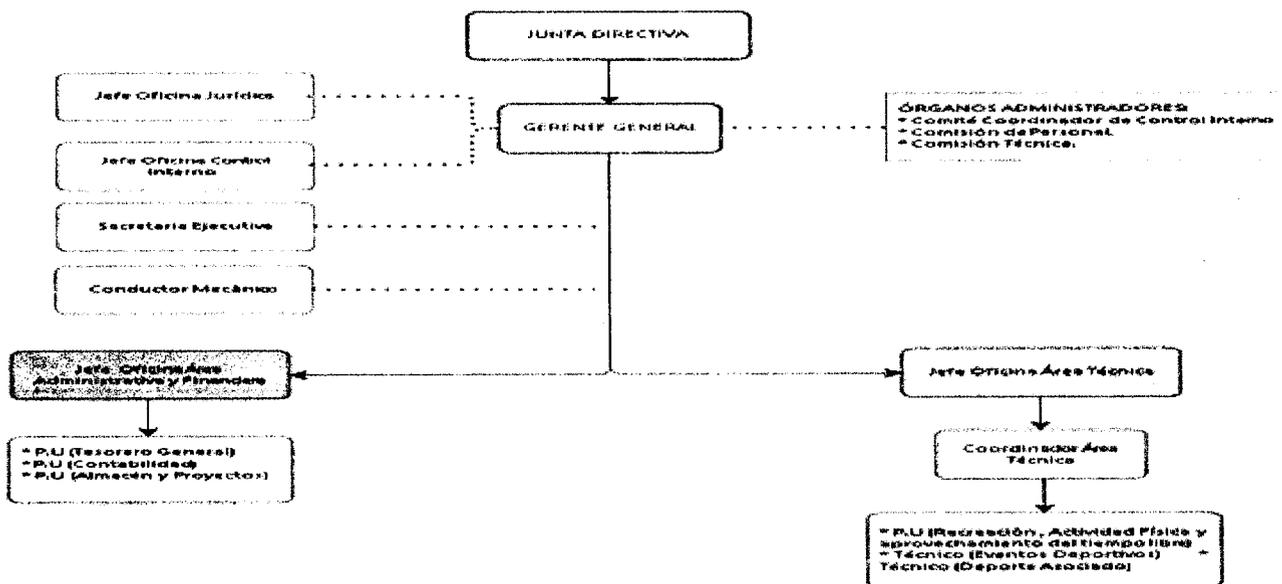
GOBIERNO DE TI

Entendimiento estratégico

Estructura del área TI dentro del instituto departamental de deporte y recreación del Quindío:

El cargo del área TI dentro de la entidad no se encuentra en la planta de personal del instituto por lo cual por medio de contratos de prestación de servicio de apoyo a la gestión para ejercer las funciones de gobierno digital, de manejo de redes sociales, mantenimiento preventivo y correctivo de equipos de cómputo y demás funciones relacionadas con el área de TI

ORGANIGRAMA DEL INSTITUTO



ANÁLISIS FINANCIERO

CONTRATOS AREA DE SISTEMAS 2019		
CONTRATO	OBJETO	VALOR
CTTO -006	PRESTAR LOS SERVICIOS PROFESIONALES DE ASISTENCIA Y SOPORTE TÉCNICO AL SOFTWARE "PUBLIFINANZAS" QUE APOYA LOS DIFERENTES PROCESOS DEL ÁREA FINANCIERA (CONTABILIDAD, PRESUPUESTO, TESORERÍA, NOMINA, INVENTARIOS) DE INSTITUTO DEPARTAMENTAL DE DEPORTE Y RECREACIÓN DEL QUINDÍO.	\$17.738.245

PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES PETI

CTTO-008	PRESTAR LOS SERVICIOS DE APOYO A LA GESTION EN EL AREA ADMINISTRATIVA Y FINANCIERA EN EL INSTITUTO DEPARTAMENTAL DE DEPORTE Y RECREACION DEL QUINDIO INDEPORTES QUINDIO	\$9.540.000
CTTO-013	PRESTAR SÉRVICIOS DE APOYO A LA GESTION EN EL AREA ADMINISTRATIVA Y FINANCIERA DEL INSTITUTO DEPARTAMENTAL DE DEPORTE Y RECREACION DEL QUINDIO INDEPORTES QUINDIO.	\$9.010.000
CTTO-093	PRESTAR SERVICIOS DE APOYO A LA GESTION EN EL AREA ADMINISTRATIVA Y FINANCIERA DEL INSTITUTO DEPARTAMENTAL DE DEPORTE Y RECREACION DEL QUINDIO INDEPORTES QUINDIO.	\$8.109.000
CTTO-101	PRESTAR SERVICIOS DE APOYO A LA GESTION EN EL AREA ADMINISTRATIVA Y FINANCIERA DEL INSTITUTO DEPARTAMENTAL DE DEPORTE Y RECREACION DEL QUINDIO INDEPORTES QUINDIO.	\$8.586.000

Modelo de gestión de TI

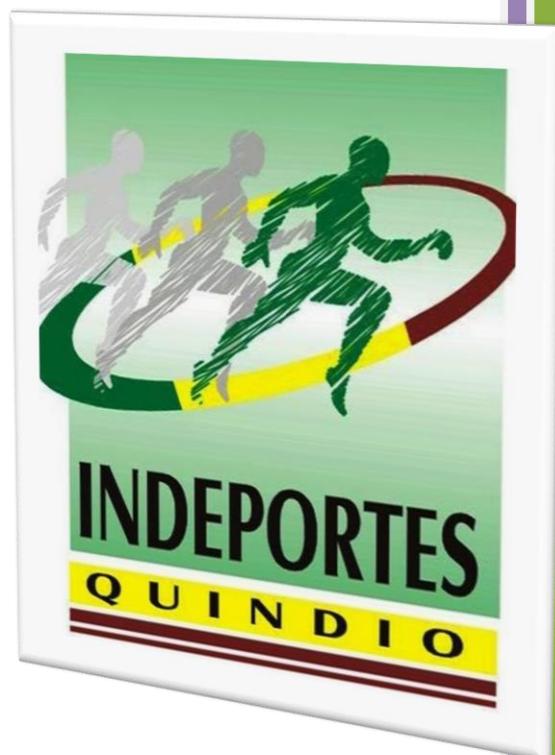
Las metas propuestas para el periodo 2020-2023 son prestar servicios eficientes en lo relacionado con la atención al público en PQRS de forma virtual y con la mayor rapidez, realizan la implementación de un software de gestión documental y publicación de datos abiertos por parte del instituto

Definición de los objetivos estratégicos de TI

Objetivo	Implementar sistemas y mecanismo de información para usuarios internos, recurriendo al uso de las Tecnologías de la Información
Actividades	Buscar el mejor mecanismo para el acercamiento de la comunidad ya sea por medio de la página web, por medios de las redes sociales.
Indicadores	Número de solicitudes realizadas en la ventanilla única del instituto / Número de solicitudes respondidas por el instituto
GESTION PUBLICA EFECTIVA Y TRASPARENTE	
Objetivo	Apoyar y fortalecer el proceso de Tecnología de Información y Comunicaciones (TIC) en las actividades que realiza la entidad, ofreciendo procesos más eficientes para el desarrollo de las actividades del instituto.
Actividades	Adecuar e incrementar la plataforma tecnológica con la que cuenta el instituto para su adecuado desarrollo. Garantizar los mantenimientos preventivos de soporte mínimos a la plataforma tecnológica de la entidad
Indicadores	Número de funcionarios los cuales se socializo las políticas de TI que implemente el instituto Número de equipos, impresoras y componentes tecnología adquiridos mediante contrato o convenios de manera anual.

EL PETI debe ser socializado con los funcionarios y contratistas de la entidad de forma virtual mediante la implementación de correo electrónico institucional o el portal web: www.indeportesquindio.gov.co y presencial mediante socialización al personal del instituto.

REGLAMENTO POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION



REGLAMENTO POLITICA SEGURIDAD DE LA INFORMACION

Contenido

1. INTRODUCCION	3
2. OBJETIVO	3
3. ALCANCE	3
4. DEFINICIONES	4
5. FINALIDAD	6
6. RIESGOS DE SEGURIDAD DE LA INFORMACION	7
7. PROCEDIMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	8
7.1 CONTROL DE ACCESO	8
7.2 USO DEL INTERNET	10
7.3 MANEJO DE REDES SOCIALES	10
7.4 MANEJO DE IMPRESORA	11
7.5 CORREO ELECTRONICO	11
7.6 CUENTAS DE USUARIO	11
7.7 CONTRASEÑAS Y ACCESO	11
7.8 SEGURIDAD INFORMATICA	12
8. MANEJO DE INCIDENTES MESA DE AYUDA	12
9. MANEJO IMAGEN INSTITUCIONAL	13
10. POLITICAS GENERALES	13
11. REFERENCIAS	13

REGLAMENTO POLITICA SEGURIDAD DE LA INFORMACION

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

REGLAMENTO POLITICA SEGURIDAD DE LA INFORMACION

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).

REGLAMENTO POLITICA SEGURIDAD DE LA INFORMACION

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.*

REGLAMENTO POLITICA SEGURIDAD DE LA INFORMACION

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
<ul style="list-style-type: none"> • Sabotaje (ataque físico y electrónico) • Daños por vandalismo • Fraude /Estafa • Robo/hurto (físico) • Robo / Hurto información electrónica • Virus /ejecución no autorizada de programas • Violación a derechos de autor 	<ul style="list-style-type: none"> • Incendio • Sismo • Polvo • Sobrecarga eléctrica • Falla de corriente (apagones) • Falla de sistema /daño disco duro 	<ul style="list-style-type: none"> • 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

REGLAMENTO POLITICA SEGURIDAD DE LA INFORMACION

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 levantarán 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 modems 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

REGLAMENTO POLITICA SEGURIDAD DE LA INFORMACION

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, linkedlink o blogs, se considera

REGLAMENTO POLITICA SEGURIDAD DE LA INFORMACION

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 fotocopidora) 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 explícito para actividades de la misma

Se prohíbe el envío 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

REGLAMENTO POLITICA SEGURIDAD DE LA INFORMACION

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 despido

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

REGLAMENTO POLITICA SEGURIDAD DE LA INFORMACION

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 designara 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 la estrategia 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.