RESOLUCIÓN No 20171300002585

IPSE-DO-F14

Fecha: 13-09-2017

"Por la cual el Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas-IPSE, adopta las políticas de Seguridad y Privacidad de la información para el IPSE"

EL DIRECTOR GENERAL DEL INSTITUTO DE PLANIFICACION Y PROMOCION DE SOLUCIONES ENERGETICAS PARA LAS ZONAS NO INTERCONECTADAS-IPSE

En uso de las facultades legales y en especial las conferidas por los Decretos 257 de 2004 y La Ley 1712 de 2014 en concordancia con el Decreto 103 de 2015 y,

CONSIDERANDO:

Que de conformidad lo establecido en la Ley 1273 de 2009, se estableció "*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*" tipificando penalmente las conductas contra la confidencialidad, integridad y la disponibilidad de datos de los sistemas informativos.

Que mediante Decreto 2573 de 2014, por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea, establece los componentes que facilitan la masificación de la oferta y la demanda del Gobierno en Línea, componente de Seguridad y privacidad de la información.

Que en el artículo 2.2.9.1.3.2 del Decreto 1078 del 2015, establece los plazos para la implementación del Manual de Gobierno en Línea.

Que dada la función establecida en el artículo 2.2.9.1.2.3 del decreto precitado, señala para el representante legal coordinar la implementación de la estrategia de gobierno en línea, y se hace necesario reestructurar la política de seguridad de la información del Instituto, para que se ajuste a las disposiciones de protección de datos personales contenidas en la ley 1581 de 2012 y de las normas de transparencia y de acceso a la información de la Ley 1712 del 2014.

Que el presente acto administrativo se encuentra sustentado con los siguientes anexos como la implementación Estrategia Gobierno en Línea, Tic para la Gestión, creación el comité de seguridad y privacidad de la información del IPSE, Sistema de Gestión Documental Orfeo, Seguridad de los Portales Web y sistema de los activos fijos, almacenes y nómina, pertenecientes al IPSE.

Que en acta de la Reunión Extraordinaria del Comité de Desarrollo Administrativo del día 12

"Por la cual el Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas-IPSE, adopta las políticas de Seguridad y Privacidad de la información para el IPSE"

de Septiembre del 2017, con radicado IPSE- 20171300003516 del día 13 de Septiembre del 2017, el comité de Desarrollo administrativo sometió y puso a consideración la política general de Seguridad y Privacidad de la Información del Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas no Interconectadas-IPSE.

RESUELVE:

ARTICULO PRIMERO: Objetivo: Adoptar las políticas de Sistema de Gestión de Seguridad Informática, Políticas de Seguridad y Privacidad de Información del Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas IPSE, contenida en el anexo que hace parte de la presente resolución.

ARTICULO SEGUNDO: Ámbito de Aplicación: Las disposiciones contenidas en el presente acto administrativo, aplica al Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas IPSE, y demás lugares donde se desarrollen el aspecto misional del Instituto.

ARTICULO TERCERO: Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas IPSE tendrá como políticas de Seguridad y Privacidad de la información, las siguientes:

1. Política de Seguridad y Privacidad de la información (Implementación Estrategia Gobierno en Línea, TIC´S para la Gestión.)
2. Políticas de Seguridad del Sistema de Gestión Documental "ORFEO"
3. Política de Seguridad Portales (página web, intranet y GLPI).
4. Política de Seguridad Sistemas de Activos Fijos, Almacenes y Nomina, versión 4.0
5. Política de Seguridad Sistema de Gestión Integral (SGI y Configuración General ITS-Gestión).

ARTICULO CUARTO: Difusión. La política de Seguridad y Privacidad de la información será socializada para conocimiento general, principalmente por medios electrónicos y será publicada en la página de intranet del Instituto.

ARTICULO QUINTO: Actualización. Las políticas de seguridad y privacidad de la información aquí adoptada por el IPSE, es un instrumento de gestión, el cual debe ser objeto de mejoramiento continuo.

Parágrafo: Será responsabilidad del área de sistemas y del comité de seguridad y privacidad de la información realizar la actualización de las políticas de seguridad y privacidad de la

"Por la cual el Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas-IPSE, adopta las políticas de Seguridad y Privacidad de la información para el IPSE"

información, conforme existan nueva necesidades y condiciones legales e institucionales previa aprobación por parte del comité de Desarrollo Administrativo.

ARTICULO SEXTO: Vigencia. El presente acto administrativo rige a partir de la expedición, es de obligatorio conocimiento y aplicación por todos y cada uno de los funcionarios y contratistas y deroga las disposiciones que le sean contrarias.

ARTICULO SEPTIMO: El presente acto administrativo será publicado en la página web e intranet del Instituto.

PUBLIQUESE Y CUMPLASE,

GERARDO DE JESUS CAÑAS JIMENEZ
Director General

Proyectó: Tathiana Leguizamón – Abogada Contratista OAJ
Revisó: Deyber Erickson Rodriguez Alvarez – Contratista TI
Revisó: Angelina Toloza Pabón – Coordinadora TI
Aprobó: Miembros del comité de Desarrollo Administrativo
Revisión Jurídica: Neila Baleta Mizar – Jefe Oficina Asesora Jurídica

MINMINAS

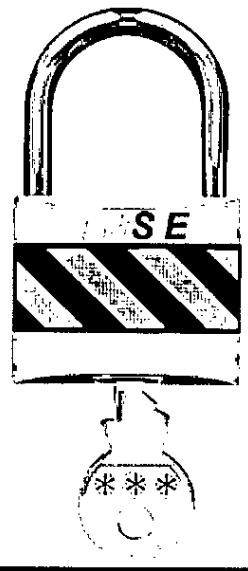
IPSE
Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Implementación Estrategia Gobierno el Línea
Tic para la Gestión

Mayo 2017



CONTRÓL DE CAMBIOS

VERSIÓN	FECHA	RESPONSABLE	DESCRIPCIÓN
1.0	04/6/2014	LEONARDO ANDRÉS ANCHIQUE LEAL	CREACION DE LA ESTRUCTURA DEL DOCUENTO
2.0	02/5/2017	DEYBER ERICKSON RODRIGUEZ ALVAREZ	ACTULIZACION GENERAL DEL DOCUMENTO
2.0			REVISIÓN Y OBSERVACIONES
			CORRECCIÓN DE OBSERVACIONES

DERECHOS DE AUTOR

CONTENIDO

TABLA DE IMÁGENES

2 INTRODUCCIÓN

El IPSE promueve soluciones energéticas sostenibles en las comunidades de las Zonas No Interconectadas (actualmente el 52% del país Aproximadamente), para ello cuenta con un equipo de trabajo comprometido y altamente calificado que debe trabajar en pro del crecimiento de los procesos misionales, en la modernización y unificación de las plataformas, así mejorar la gestión de la información y sus procesos internos, aprovechando la existencia de nuevas tecnologías, usándolas para contribuir al mejoramiento de las condiciones de vida de las comunidades en las Zonas No Interconectadas.

En la actualidad el punto de amenazas en cualquier entidad no se tipifica como personalizado, por el contrario estas amenazas se construyen de manera global, hecho que obliga a que las organizaciones se preparen para cualquier ataque y para eso cuente con elementos que prevengan los ataques como firewalls, antivirus, antispam, etc.

El IPSE debe crear, implantar, monitorear y evaluar las Políticas Seguridad y Privacidad de la Información, verificar su funcionalidad, cumplimiento, o modernización con respecto a las normas que las guíen o las certificaciones que la entidad considere necesarias, de esta manera proteger la información tangible e intangible creada, procesada, transmitida o resguardada en los diversos procesos, 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.

Para lograrlo, es necesario que los empleados, con tomen conciencia de los riesgos a los cuales están expuestos como parte de la organización, su rol en el desarrollo misional y la imagen pública del IPSE, de esta forma se le dé importancia a crear una cultura de Seguridad Informática, ligada a un trato seguro de la información, para que la implantación de las Políticas de Seguridad y Privacidad de la Información pueda generar sinergia al interior de la entidad y así el IPSE se pueda posicionar mejor.

1. OBJETIVOS

Objetivo Principal:

Adoptar por resolución, las nuevas Políticas de Seguridad y Privacidad de la Información en el Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas–IPSE, modernizando la Resolución No. 20131300004105 del 02/07/2013, alineándola a los requerimientos de privacidad y seguridad de la información solicitada a entes de orden nacional.

Objetivos Específicos:

1. Modernizar la Política de Seguridad Informática del IPSE implementada actualmente (Resolución No. 20131300004105 del 02/07/2013)
2. Dar cumplimiento a la Formulación e implementación de SGSI nombrado en la Política de Eficiencia Administrativa del Plan Estratégico Institucional del IPSE (2015-2018).
3. Exponer el buen uso de los recursos Informáticos y la Información Institucional dentro del contexto de confidencialidad, integridad y disponibilidad.
4. Proteger los activos de información del IPSE.
5. Adoptar la política de seguridad de la Información como un eje motivacional de cada funcionario, así lograr la satisfacción de los clientes internos y externos para mejorar la confianza.
6. Alinear las políticas seguridad y privacidad de la información a la continuidad del negocio frente a incidentes.
7. Cumplir con los principios de seguridad de la información (confidencialidad, integridad, disponibilidad) e infraestructura tecnológica.
8. Generar sinergia entre todos los procesos del IPSE para contribuir al desarrollo misional de la entidad, teniendo en cuenta la trazabilidad que tienen los procesos.
9. Concienciar a los funcionarios del IPSE sobre los riesgos a los cuales están expuestos como parte de la organización.
10. Apoyar la innovación tecnológica.
11. Dar cumplimiento a la normatividad que involucra a las entidades del estado.
12. Contribuir a mejorar la percepción que tienen los empleados del IPSE del Proceso de Gestión de TICS, para mejorar la visión que tiene del proceso las demás áreas.
13. Ayudar a posicionar la marca como una de las más seguras en el sector minas y energía.

2. ALCANCE

La Política de Seguridad y Privacidad de la información aplica a funcionarios, contratistas, proveedores, la ciudadanía en general, sistemas de información, terceros y la protección de activos de información del Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas -IPSE.

3. NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance deberán dar cumplimiento un 100% de la Política de Seguridad y Privacidad de la Información planteada en este documento, adicionalmente deben dar cumplimiento a los procedimientos y políticas internas específicas que difieren en cada uno de los Sistemas de Información del IPSE.

4. NORMATIVIDAD

Artículo 15 de la constitución política de Colombia de 1991, Derecho Intimidad Personal, Familiar y Habeas Data. (Constitucion_Politica_de_Colombia, 1991)

Decreto 1078 de 2015, Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. (Republica de Colombia, MINTIC, 2015)

Manual 3.1 Estrategia GEL, para la Implementación de la Estrategia de Gobierno en línea para entidades del Orden Nacional". (Ministerio de TIC, 2015)

1712 de 2014, Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. (Ley 1712, 2014)

Decreto 2473 de 2014, Estrategia de Gobierno en Línea. (Republica de Colombia, 2014)

Decreto 1377 de 2013, Por el cual se reglamenta parcialmente la Ley 1581 de 2012. (Republica de Colombia, Decreto 1377 de 2013 Nivel Nacional, 2013)

Ley 1581 de 2012, disposiciones generales para la protección de datos personales. (República de Colombia, LEY ESTATUTARIA 1581, 2012)

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. (República de Colombia, DECRETO 2693, 2012)

Ley 1273 de 2009, denominada "Protección de la información y los datos", Normas ISO 2700 Sistema de Gestión de Seguridad de la Información. (CONGRESO DE COLOMBIA, 2009)

Resolución 524 de 2007, se reglamenta el uso Sello Oficial de Gestión de la Calidad NTCGP 1000:2004 Sector Público, en el Estado colombiano. (RESOLUCION 524, 2007)

ISO 27001 del 2005, describe cómo gestionar la seguridad de la información en una empresa (requerimientos, técnicas y sistemas de gestión de seguridad). (ISO / IEC, 2005)

ISO 27002 del 2005, Guía de buenas prácticas de seguridad de la información. (iso27000.es, 2005)

ISO 27005, Guía para la Gestión de los riesgos de la seguridad de la información.

MECI 1000 de 2005, Modelo Estándar de Control Interno para el estado colombiano, determina las generalidades y la estructura necesaria para establecer, documentar, implementar y mantener un Sistema de Control Interno en las entidades y agentes obligados. (PRESIDENTE DE LA REPÚBLICA, 2005)

NTCGP1000 de 2004, norma que documenta los requisitos del sistema de gestión de calidad para la rama ejecutiva del poder público y otras entidades prestadoras de servicios. (REPUBLICA DE COLOMBIA, 2004)

LEY 734 DE 2002, Código Disciplinario Único. (LEY 734, 2002)

DECRETO 734 DE 2012, Reglamentación del Estatuto General de Contratación de la Administración Pública y se dictan otras disposiciones. (PRESIDENTE DE LA REPÚBLICA DE COLOMBIA, 2012)

5. POLÍTICA GENERAL

El IPSE, a través de su política de Seguridad y Privacidad de la Información se compromete velar por la Seguridad y privacidad de la información y la infraestructura en aras otorgar los recursos necesarios para garantizar la confidencialidad, disponibilidad e integridad de la información, utilizando mecanismos de protección que prevenga las posibles amenazas internas y externas, planteando lineamientos y procedimientos transversales que apoyen el desarrollo de los objetivos institucionales.

La Dirección General se compromete a cumplir con las disposiciones constitucionales y legales aplicables a la Entidad relacionadas con la seguridad de la información, además, a que se establezca, implemente, opere y mantenga la seguridad de la información como parte de la mejora continua de la Entidad, apoyando el logro de sus objetivos, Misión, Visión, Plan estratégico Institucional en concordancia con las actividades de Arquitectura empresarial que se realicen y los demás proyectos que se consideren competentes, en cumplimiento de los compromisos institucionales alineado a: la lucha anticorrupción, lucha antipiratería, confidencialidad de la información, la circulación y divulgación adecuada de la información, estrategia de Gobierno en Línea, Ley de Transparencia y mejores prácticas.

6. DEFINICIONES

Activo: Cualquier cosa que tiene valor para la organización. (NTC 5411-1, 2006)
En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO - ICONTEC, 2006.)

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO - ICONTEC, 2006.)

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO - ICONTEC, 2006.)

Autenticidad: Es la propiedad de garantizar la identidad de un sujeto o recurso declarado. La autenticidad se aplica a entidades tales como usuarios, procesos, sistemas e información.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO - ICONTEC, 2006.)

Backup: Es la copia total o parcial de información importante del disco duro, CD´s, bases de datos u otro medio de almacenamiento, la cual puede recuperarse en caso de pérdida de la copia original.

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).

Confidencialidad: Es la propiedad de determinar que la información no esté disponible ni sea revelada a individuos, entidades, procesos o procedimientos no autorizados.

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

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

Dirección IP (Dirección de protocolo de Internet): Etiqueta numérica que identifica a un equipo que esté conectado a una red que utilice el protocolo IP (Internet Protocol). La dirección IP consta de cuatro segmentos de números separados por puntos y cada número es menor de 256.

Disponibilidad: Es la propiedad de la información de ser accesible y utilizable por solicitud de una Entidad o funcionarios autorizados.

DNS (Domain Name System): Es una base de datos distribuida, con información que se usa para traducir los nombres de dominio, fáciles de recordar y usar por las personas, en números de protocolo de Internet (IP) que es la forma en la que las máquinas se encuentran en Internet.

Firewall: Es un ordenador, software o dispositivo físico que se conecta en una red con salida a Internet con el fin de impedir el acceso no autorizado, incorporando elementos que garantizan la privacidad, autentificación, etc., conforme a las políticas de seguridad de quien los instala.

Forefront: es un producto de seguridad que permite proteger los puestos de trabajo, portátiles y servidores de la empresa de las nuevas amenazas que aparecen, como spyware y rootkits, así como virus y otras modalidades de ataque más tradicionales.

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 - ICONTEC, 2006.)

GLPI: Es un software libre distribuido bajo licencia GPL, que facilita la administración de recursos informáticos. GLPI es una aplicación basada en Web escrita en PHP, que permite registrar y administrar los inventarios del hardware y el software de una empresa, optimizando el trabajo de los técnicos gracias a su diseño coherente. (Ginioux Jean-Mathieu Doléans y Frederic, 2017)

Hardware (Hw): Son las partes físicas y tangibles de una computadora, sus componentes eléctricos, electrónicos, electromecánicos y mecánicos, sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

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

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las

circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712, 2014)

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712, 2014)

Integridad: Es la propiedad de salvaguardar la exactitud y estado completo de los activos.

Intranet: Red privada de computadoras que permite compartir recursos entre ellas y se encuentra enlazada para uso exclusivo dentro de una empresa u hogar. Puede o no tener acceso a Internet.

ISO (International Organization for Standardization): Deriva del griego isos, que significa "igual"; Organización creada el 23 de Febrero de 1947, en Ginebra, Suiza, con el fin de "facilitar la coordinación internacional y unificación de normas industriales". Actualmente son miembros 165 países.

LAN (Local Area Network): Red de Área Local, es una interconexión de computadoras y periféricos que forman una red dentro de una empresa u hogar. Con esta Red, se pueden intercambiar datos y compartir recursos entre las computadoras que la conforman.

ORFEO: El sistema de gestión documental ORFEO, se encuentra conectado a un servidor Institucional con capacidad para almacenar toda la información digitalizada de los documentos físicos, internos y externos relacionados con el IPSE. Para tener acceso a esta información digitalizada se cuenta con modelos jerárquicos de seguridad (I-II-III-IV-V).

Phishing: Es la obtención de información importante como números de tarjetas de crédito, claves, datos de cuentas bancarias, etc., al ingresar a un sitio que presume ser legal o auténtico.

Red lógica: Hace referencia a la forma en que los medios físicos (Cables –cobre, fibra óptica, switches, computadoras, impresoras y demás dispositivos) establecen una conexión lógica o comunicación mediante direcciones IP.

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 - ICONTEC, 2006.)

Router: Determina (basado en diversos parámetros) la mejor ruta para el envío de datos a través de una red interconectada y luego redirige los paquetes hacia el segmento y puerto de salida adecuados.

SAN (Storage Area Network): Es una red concebida para conectar servidores, matrices de discos y librerías de soporte. Permite conectar de manera rápida, segura y fiable los distintos elementos que la conforman, también transportar datos entre servidores y recursos de almacenamiento. La tecnología SAN permite conectividad de alta velocidad de servidor a almacenamiento, almacenamiento a almacenamiento, o servidor a servidor.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad. (ISO - ICONTEC, 2006.)

SFI (Sistema Financiero Integrado): Software que permite transacciones en línea entre sus módulos, con capacidad de manejar varias estructuras de cuentas, empresas, periodos, lugares geográficos, centros de costos y multiusuario (Súper usuario financiero y Súper usuario informático).

SIGMA: Herramienta que permite el manejo y administración del Sistema de gestión integrado del IPSE, que facilita el acceso a una fuente de datos de un plan de mejoramiento continuo. Cuenta con 3 modelos jerárquicos de seguridad: Básico, directivo y administrativo.

Sniffing: Programa encargado de obtener datos que circulan por una red que detecta problemas de congestión, mediante la búsqueda de cadenas numéricas o de caracteres en los paquetes.

Spoofing: Suplantación de la dirección IP de otro sistema.

Software (Sw): Equipamiento lógico de una computadora digital, comprende el conjunto de componentes lógicos como aplicaciones informáticas, sistema operativo, funcionamiento de programas, interacción con los componentes físicos, interfaz del usuario y demás aplicaciones debidamente licenciadas.

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO - ICONTEC, 2006.)

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO - ICONTEC, 2006.)

Comité de seguridad y privacidad de la información: Hace referencia a los encuentros de un grupo de personas seleccionadas por el Grupo Tecnologías y Sistemas de Información, que se encarga de definir el alcance, planificar, controlar y verificar los procesos de las Políticas de Seguridad y Privacidad de la Información en el IPSE. Control Interno, la Oficina Asesora Jurídica, Talento Humano, Financiera U otras

11 áreas que se consideren necesarias deberán ser llamados a comité si se considera necesaria su participación. (Anexo 1)

7. ESQUEMA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - IPSE

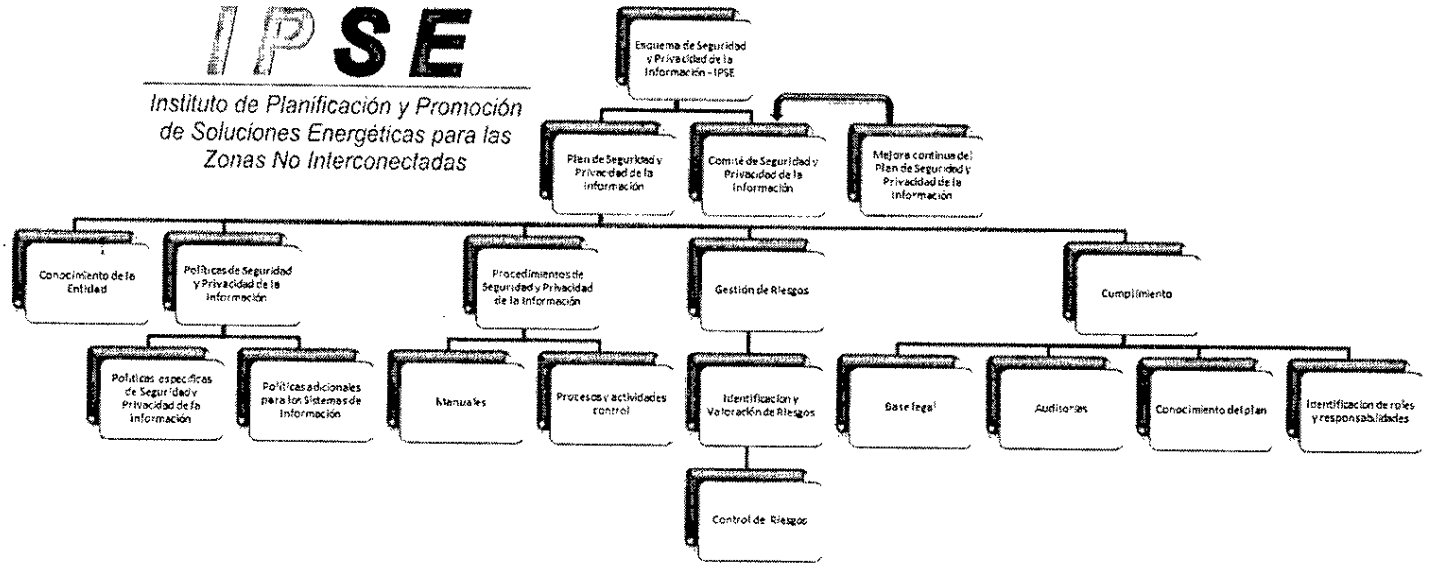


Imagen 1 Esquema de Seguridad y Privacidad de la Información IPSE.

8. METODOLOGIA

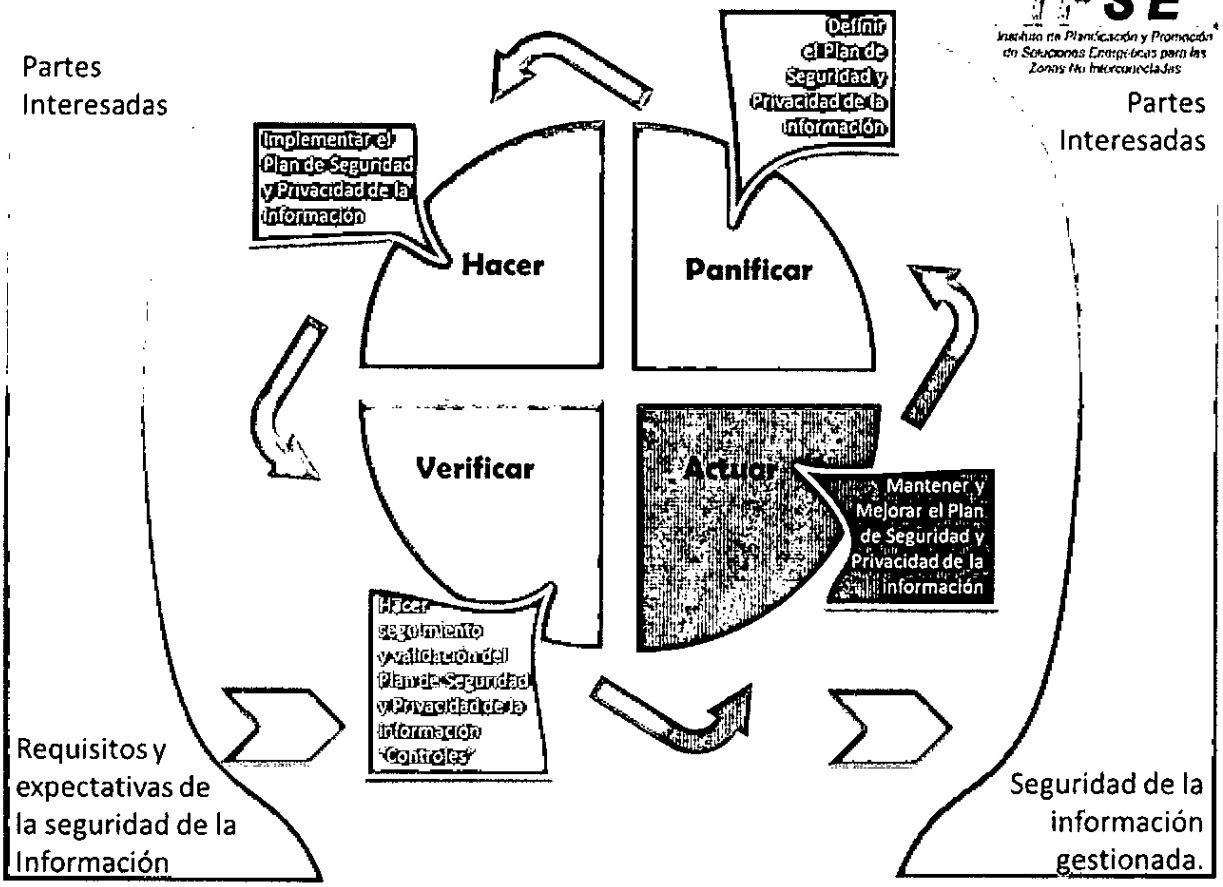


Imagen 2 Modelo PHVA aplicado a la Gestión de Seguridad y Privacidad de la información del IPSE. (ISO - ICONTEC, 2006.)

9. POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

9.1 Organización de la Información.

EL IPSE debe tener un documento que contenga los procedimientos para organizar y clasificar la información en los diferentes niveles que la entidad maneje, basándose en las normas que se deben aplicar, para esto se necesita la cooperación y la colaboración de los usuarios en los diferentes procesos, incluyendo los auditores y los encargados de gestión de riesgos, el proceso de clasificación de la información (sensibilidad y disponibilidad), es independientemente sobre cada uno de los procesos que tiene el IPSE pero aplica la misma metodología.

Todos los empleados IPSE, reciben una capacitación inicial de los procesos de manipulación de la información al interior y exterior del IPSE, donde se expone la reglamentación y se informan las políticas y lugares permitidos (carpetas privadas o públicas), donde se debe almacenar la información, estableciendo de esta manera, roles y responsabilidades, para mantener un control de documentos responsable, actualizado y seguro.

La oficina asesora jurídica debe garantizar que exista un compromiso de confidencialidad e integridad de la información en cada contrato, convenio, acuerdo, etc, para que todo empleado o entidad que maneja información del IPSE cumpla con la política de seguridad reglamentada en este documento, para garantizar que toda información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información, además de prestar la asesoría legal de la seguridad de la información en las actualizaciones que se le realicen en vigencias futuras a las políticas y el plan de seguridad y privacidad de la información del IPSE.

Se debe garantizar que las versiones de los documentos más recientes sean legibles e identificables, además se encuentren disponibles en los lugares donde se ha establecido, si se observa algún documento obsoleto debe ser reportado para realizar la actualización o eliminación (Procedimientos, tramites, formatos, inventarios, tablas, organigramas, estructuras, artículos, políticas, reportes, directorios, normatividad, etc.).

La infraestructura tecnológica y la información como equipos de cómputo, dispositivos electrónicos, sistemas de información, todo lo que se comparte entre los mismos y los documentos físicos, pertenecen al IPSE, por esto ningún funcionario puede compartir, duplicar o divulgar dicha información, sin previa autorización, podrán hacerlo estrictamente en cumplimiento de sus funciones.

9.2 Control de Acceso

- ✓ **Solo accede Personal Autorizado**

  Los Funcionarios, Contratistas o integrantes del IPSE en calidad de trabajadores, personal provisional, personal de planta, asesores, pasantes, que se encuentren vinculados por medio de un contrato laboralmente con el IPSE, pueden realizar una solicitud de acceso al Grupo Tecnologías y Sistemas de Información si han sido autorizados por el líder del proceso (Formato, creación y administración cuentas de usuarios), la asignación de privilegios sobre el acceso a información debe ser evaluada por el líder del Grupo Tecnologías y Sistemas de Información. Los privilegios difieren para algunos Sistemas de Información, reglamentado en las políticas internas adicionales, Los casos específicos deben ser reevaluados.

- ✓ **Ingreso y uso de equipo fotográfico**

  No se permite el ingreso y uso de equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con autorización para ello.

- ✓ **Documentación de acceso**

  El Grupo Tecnologías y Sistemas de Información debe documentar toda la información de administración de Contraseñas de Usuario y lo que respecta al acceso a los sistemas de información de todas las plataformas o software que posee la entidad, (Formato, creación y administración cuentas de usuarios).

- ✓ **Acceso de administradores**

  Se deben establecer combinaciones de caracteres especiales (números, símbolos, letras mayúsculas y minúsculas), en las claves de cuentas de acceso para usuarios administradores de las plataformas.

- ✓ **Documentación acceso a la red**

  El Grupo Tecnologías y Sistemas de Información debe documentar el control de acceso la red, ya que cada funcionario debe tener solamente un usuario de red a su nombre, asignado por el Grupo Tecnologías y Sistemas de Información, así evitar usuarios duplicados, verificar los intentos de acceso remoto y a los sistemas de información no autorizados.

- ✓ **Acceso a escritorios virtuales del IPSE**

  Basándose en la Política de Seguridad del año 2013, la herramienta de virtualización VmWare fue adoptada por el IPSE, con el objeto de permitir el acceso a los escritorios virtuales de los funcionarios y/o Contratistas desde una red externa (Internet),

obteniendo mayor seguridad de la información, disponibilidad, agilidad de los servicios de escritorio y experiencia de usuario en todas las sesiones, dispositivos y ubicaciones.

- ✓ **Acceso de equipos con información sensible**

  El líder de cada proceso junto con la Grupo Tecnologías y Sistemas de Información deben priorizar los equipos o las cuentas que contienen información sensible o privada, para mejorar configuraciones adicionales que le brinden más seguridad.

- ✓ **Acceso al servidor de almacenamiento (file server) institucional**

  Quien tiene acceso a los escritorios virtuales del IPSE, también lo tienen acceso al servidor de almacenamiento. Las políticas de instalación, administración o modificación los perfiles de acceso, solo puede ser alterada por el Grupo Tecnologías y Sistemas de Información, con previo aviso según sea su dependencia. El fin del servidor es conservar, organizar, centralizar y respaldar la Información Institucional, bajo un esquema de seguridad granular y de acceso para cada usuario de la entidad, el cual consta de tres (3) carpetas (1 privada, 1 publica del grupo de trabajo y 1 pública general del IPSE).

- ✓ **Acceso al data center y centros de cableado del IPSE**

  El Grupo Tecnologías y Sistemas de Información es el encargado de configurar, administrar y otorgar privilegios referentes a modificaciones, pruebas, auditorías, visitas, ingresos y mantenimiento del Data Center, personas que necesiten ingresar deben diligenciar el formato acceso data center, acceso que debe ser revisado, autorizado y monitoreado, los accesos están regulados por un sistema de control biométrico, la manipulación se fundamentan en la ética profesional y confidencialidad de la información, por ello el acceso a servidores es restringido, solo pueden ingresar los líderes del Grupo Tecnologías y Sistemas de Información.

- ✓ **Acceso de equipos externos a la plataforma institucional del IPSE**

  Para otorgar el ingreso externo, se debe diligenciar el Formato "Formato, Ingreso red institucional equipos externos", Entiéndase Equipo externo como todo aquel que no se encuentre registrado bajo la propiedad del IPSE-, donde se consignan los datos del Usuario externo, especificaciones del Equipo, tipo de acceso y el Funcionario de Área que autoriza. Los Equipos externos se someterán a los lineamientos provistos en el presente documento, a fin de cumplir y mantener las Políticas de Seguridad Informática establecidas en el IPSE.

- ✓ **Acceso responsable a internet (www - world wide web)**

  El uso de Internet es de carácter laboral y debe permitir cumplir con el objeto y/o dar alcance a cada Contrato.

- Está prohibido el ingreso a páginas con contenido sexual, erótico y videos, entiéndase como consultas y contenidos inadecuados en el ámbito laboral, por tal motivo el uso de software que permita acceder a páginas bloqueadas está prohibido.
- El uso del chat es exclusivamente de tipo laboral.
- La descarga de software está prohibida por motivos de seguridad y vulnerabilidad de los sistemas de Información, si el software o el acceso a páginas bloqueadas es necesario se debe informar al Grupo Tecnologías y Sistemas de Información.
- El uso de redes sociales y YouTube es de carácter laboral.

✓ **Firewall**

Se debe limitar el tráfico de la información por medio de las reglas o funcionalidades del firewall para bloquear el acceso no autorizado, la configuración depende de los administradores de sistemas.

✓ **Bloqueo de sesión**

El usuario debe boquear su sesión de trabajo una vez se aleje de su máquina virtual o física, el usuario es responsable de la seguridad, del acceso y uso de la máquina virtual protegiendo sus contraseñas, bloqueando el acceso.

9.3 Organización de la seguridad

✓ **Administración de plataformas y sitios WEB**

Se debe garantizar la administración, actualización y soporte del sitio Web del IPSE y la intranet, brindando estabilidad y disponibilidad del servicio, al mismo tiempo proporcionar un uso adecuado en las herramientas de gestión de acceso seguro tanto a nivel de administración como de los mismos usuarios.

✓ **Procedimientos de control de acceso a la red**

El Grupo Tecnologías y Sistemas de Información debe trabajar transversalmente para mejorar y aplicar los procedimientos de control de acceso a la red, con el fin de minimizar el riesgo de acceso no autorizado, de esta forma tener un control más estable.

✓ **Denuncias de acceso no autorizados y ataques**

El Grupo Tecnologías y Sistemas de Información debe generar la denuncia y recolectar la información sobre los accesos no autorizados o ataques, para ser reportados a las entidades competentes.

✓ **Claves privadas intransferibles**

Todos los acuerdos o contratos que realice el IPSE con otra entidad, contratistas, pasantes o empleado IPSE, debe incluir un acuerdo de confidencialidad, donde se

informa del uso o manejo que se debe dar a la información, de esta manera se establecen sanciones disciplinarias por incumplimiento a las políticas de seguridad y privacidad de la información y ley vigente en Colombia.

- ✓ **Derechos de Autor**

  Los empleados, contratistas y pasantes no pueden descargar, utilizar o compartir información protegida por derechos de autor (libros, software, archivos, imagen, sonido, entre otras) sin recibir la aprobación de quien figure como autor.

- ✓ **Revisión de virus**

  Toda la información que proviene de un nuevo hardware (Discos de almacenamiento extraíble, USB, HDMI), o el exterior de la entidad debe ser analizada por el antivirus, para minimizar la posibilidad de intrusión, daño el sistema de archivos, robo o secuestro información, en los equipos físicos o virtuales la verificación por medio de los antivirus la debe realizar el usuario.

- ✓ **Configuración de Puertos**

  La configuración de Puertos corresponde y debe ser solo y únicamente editada por el Grupo Tecnologías y Sistemas de Información del IPSE, o la persona que los mismos hayan autorizado para la labor.

- ✓ **Asignación de Usuarios**

  Los usuarios son asignados por el Grupo Tecnologías y Sistemas de Información con su respectiva autorización (Formato, creación y administración cuentas de usuarios), firmado y fechado, cada empleado puede tener una sola cuenta de acceso para el escritorio remoto (Máquina Virtual), las cuentas de usuarios antiguos o activos no pueden ser reasignadas o puestas a nombre de otras personas.

- ✓ **Conexiones remotas**

  Las conexiones remotas y el intercambio de información con otros equipos de cómputo utilizando los diferentes protocolos de transferencia de archivos o información, debe ser autorizado, monitoreado y evaluado por el Grupo Tecnologías y Sistemas de Información. Los usuarios que se conecten a su escritorio remoto deben tener en cuenta que se deben cumplir absolutamente todas las políticas de seguridad y privacidad de la información establecidas por el IPSE.

- ✓ **Acceso a información no autorizada**

  La ejecución de acciones y manipulación de información no autorizadas al cargo específico que desempeña el empleado o la entidad contratada o al alcance del contratista, se considera falta grave y es sancionada disciplinariamente.

- ✓ **Archivos libres de virus**

El Grupo Tecnologías y Sistemas de Información trabaja activamente en los controles para minimizar los riegos de infección de virus, pero no garantiza que los archivos que se transfieran por la red de Internet estén libres de los distintos tipos de virus de computadoras, Lombrices, worm o gusanos, Bomba de Tiempo, caballos de Troya, Hijackers, Keylogger o demás códigos de infección, Los empleados IPSE deben hacer un análisis en busca de virus de todos los medios extraíbles que se inserten en el equipo de cómputo asignado (USB, SD, CD´S, DVD´S) mediante el Antimalware Institucional, antes de hacer uso de ellos,

- ✓ **Aplicaciones para empleados**

  El IPSE actualmente entrega a cada empleado las cuentas de usuarios para acceder a las aplicaciones básicas internas (Mesa de ayuda, Sistema de gestión de Documental, Correo institucional, máquina virtual, etc), dichas cuentas poseen los siguientes parámetros de seguridad (encriptación, claves de acceso, bases de datos de autenticaciones, entre otros); el acceso al Sistema Financiero Integrado (SFI) u otros aplicativos que sean necesarios para cada proceso en específico cuenta con unas políticas diferentes que deben ser revisadas por el Grupo Tecnologías y Sistemas de Información.

- ✓ **Configuraciones Sistema de información y Sistema Operativo**

  La configuración general de los sistemas de información y de los sistemas Operativos solo la pueden realizar los empleados asignados al Grupo Tecnologías y Sistemas de Información con previa autorización, o estrictamente en cumplimiento de las funciones específicas de su contrato, especialmente aquellas modificaciones específicas de seguridad (Antivirus, Firewall, Puertos de Acceso, contraseñas de equipo para administrador, entre otras)

- ✓ **Responsabilidad Perdida de Información**

  Si los empleados no cumplen las políticas y los procedimientos establecidos por el IPSE, el Grupo Tecnologías y Sistemas de Información no se hace responsable de la perdida de Información (no debe por ningún motivo alojar información en el escritorio, mis documentos, únicamente se responde por la información alojada en la carpeta asignada al usuario) el grupo de tecnología y sistemas de información no se hace responsable de la información contenida en las carpetas públicas pues estas carpetas son solo de trasferencia de archivos temporales.

- ✓ **Asignación de IT y responsabilidad de uso**

  A los empleados se les asigna una Tink client (Computador) y una impresora a la cuenta de red, a los cuales solo se les puede dar uso institucional, es responsabilidad del

usuario dar un uso adecuado a los equipos (escáner y fotocopiado y demás) brindando un correcto funcionamiento, por tal motivo los documentos que se impriman en las impresoras deben ser de carácter institucional, las fallas que presenten los equipos deben reportarse al Grupo Tecnologías y Sistemas de Información o Recursos Físicos, quien asignara el personal indicado para realizar la reparación o mantenimiento.

9.4 Gestión de activos de información

- ✓ Se deben clasificar los Activos de Información basándose en la normatividad actual vigente en el país, impartida por las diferentes entidades de control.
- ✓ El IPSE se reserva el derecho de restringir el acceso a la Información que se considere prudente o necesario, se encuentra priorizado el acceso a servidores.
- ✓ El inventario de activos de información se actualiza cada vez que se considere necesario, el comité de seguridad o quien haga sus veces, debe revisar su inclusión.
- ✓ Los activos de información son etiquetados cuando entran al sistema de gestión documental (Orfeo), con una información básica que contiene el año, área, consecutivo e identificador.
- ✓ El intento no autorizado de intrusión o inhabilitación de los controles establecidos por el Plan de seguridad y privacidad de la Información está sujeto a medidas legales, como se encuentra reglamentado por la ley o las entidades que lo regulen.
- ✓ Los activos de Información, están ligados al derecho de confidencialidad, integridad, disponibilidad, el habeas data, y la protección de los datos de sus propietarios, para ello se planea la inclusión de firmas digitales para el personal por secciones, definidas por el Grupo Tecnologías y Sistemas de Información.
- ✓ Los controles de revisión, actualización y validación según el nivel de protección que la Información necesite tanto física como lógicamente, deben ser aplicados durante el ciclo de vida de la Información, con un tiempo establecido, basado en la necesidad de la entidad, o la necesidad que tienen los empleados que los utilizan.
- ✓ No está permitido dejar documentos en espera (documentos en las impresoras y fotocopiadoras, así como en sitios de paso o de atención al público).
- ✓ El personal del Grupo Tecnologías y Sistemas de Información debe mantener una BD actualizada que contenga el inventario de licencias y Software instalado o disponible para los equipos del IPSE (Pagos o free).
- ✓ El personal del Grupo Tecnologías y Sistemas de Información debe mantener el registro actualizado del inventario de usuarios activos.
- ✓ El IPSE implementó un sistema para la administración de recursos físicos donde se le agrega a cada equipo una placa identificadora, de esta manera se asignan los equipos a un

responsable (Solo personal de planta del IPSE), adicionalmente se debe llevar un registro de las personas que usan los equipos pero que no pueden figurar como responsables (contratistas, pasantes o empresas contratadas).

9.5 Seguridad en el recurso humano

Se debe informar al personal nuevo de la entidad sobre la existencia del plan de gestión de seguridad y privacidad de la información, por este motivo se adiciona en los contratos, el compromiso de confidencialidad de la información y la responsabilidad que conlleva manejar información del IPSE en materia de seguridad, de esta forma se implementan capacitaciones y avisos informativos didácticos, en procedimientos de seguridad de información, gestión de incidencias y demás, el desconocimiento de la política de seguridad y privacidad de la información no exonerará al personal de los procesos disciplinarios con respecto a la norma, ya que quien posea o este incurso en alguna relación con el IPSE debe solicitar y cumplir con las políticas establecidas en este documento.
El uso adecuado de la Infraestructura tecnológica para garantizar la seguridad de la información le compete a toda la entidad, los riesgos a los cuales los empleados están expuestos voluntaria o involuntariamente deben ser documentados para mitigarlos o eliminarlos.

El Grupo Tecnologías y Sistemas de Información del IPSE debe realizar campañas didácticas de las políticas de seguridad y privacidad de la información, las vulnerabilidades, amenazas y controles a los que están expuestos los clientes como recurso humano del IPSE, de esta forma crear confianza, incentivar una cultura de política segura y responsable para la manipulación de la infraestructura tecnológica y los activos de información.

Los Equipos informáticos de la Institución deben estar ubicados en sitios adecuados que cumplan con todos los requerimientos instalación, actualización, reasignación referente a la Seguridad industrial, física y ambiental, Conexión eléctrica regulada y Conectividad a la Red lógica, con el ánimo de garantizar a los Funcionarios y/o Contratistas del IPSE, herramientas para desempeñar labores asertivas y eficientes.

El IPSE debe realizar una verificación de antecedentes de los candidatos al empleo que sea ofertado, contratistas y terceros en concordancia con las regulaciones, ética y leyes relevantes, las medidas deben ser proporcionales a los requerimientos del negocio y a la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.
Cuando a un empleado o entidad se le termina el contrato o acuerdo, se le eliminaran todos los derechos de acceso para garantizar que el acceso a la información e Infraestructura Tecnológica no le estará disponible.

9.6 Seguridad física y del Entorno.

- ✓ En las sedes del IPSE, se deben garantizar unas condiciones de acceso físico seguras, limitando el acceso a personas no autorizadas o dispositivos no autorizados, por medio de herramientas que mejoren o maximicen la seguridad de la Infraestructura, por ejemplo: Validación de visita con el empleado, controles biométricos, creación de registros, detector de metales, revisión de bolsos, o los que la entidad considere necesarios.
- ✓ La ubicación, instalación y traslado de la infraestructura tecnológica debe ser analizada por Recursos Físicos y el Grupo Tecnologías y Sistemas de Información o el Comité de Seguridad, para garantizar su seguridad, especialmente la Infraestructura que suministra energía o la que permite acceder a los activos más importantes o sensibles,(Servidores, Cableado, Router, Switches), e incluir niveles de seguridad adicionales y espacios con características ambientales necesarias si son requeridas, esta información se debe manejar por Orfeo, especialmente si los equipos van a salir de las instalaciones donde se encuentran ubicados, el traslados lo debe realizar el personal o la entidad que se haya asignado puntualmente.
- ✓ Cada empleado es responsable tener una buena conducta enmarcada en el respeto y buen uso de contenidos que se publiquen bajo su registro, en lo que compete a información que pueda perturbar la tranquilidad de sus compañeros o demás empleados del IPSE.
- ✓ Cada empleado debe contribuir al desarrollo de espacios limpios y ordenados en el IPSE, manteniendo sus escritorios o dispositivos asignados aseados y organizados.
- ✓ El personal dentro de la entidad no puede comer, consumir líquidos y fumar en cercanías de las instalaciones de procesamiento de información o equipos de cómputo (computadores, impresoras, scanner, switches, Router, modem, y demás equipos del IPSE).
- ✓ La Infraestructura Tecnológica no debe ser usada para provecho personal o diversión que involucre actividades como juegos, contenido sexual o erótico, Redes sociales, You Tube y videos etc, ya que estas actividades podrían volver vulnerable la red o incomodar, distraer o perjudicar al personal.
- ✓ El uso de bebidas alcohólicas o sustancias psicoactivas puede maximizar los riesgos por equivocación del usuario, el daño en los dispositivos o cableado que podrían volver vulnerable la red de la misma manera podría causar afectaciones a quien las use o al resto del personal, por esto son prohibidas.
- ✓ Los controles contra daño por desastres naturales como inundaciones, terremoto, explosiones entre otros, deben ser monitoreados anualmente o cuando se considere necesario por la entidad, para planificar mejoras.

- ✓ La implementación de virtualización de máquinas, permite dar seguridad en la información cuando un Tink client se daña, ya que toda la información se almacena cumpliendo con parámetros seguros y no se resguarda directamente en el equipo físico de cada usuario.
- ✓ Anualmente se debe planificar, desarrollar y evaluar un plan de mantenimiento físico para todos los equipos, de esta manera garantizar la disponibilidad y e integridad de los mismos y unas condiciones ambientales óptimas para los empleados y las personas que visitan el IPSE.
- ✓ El grupo de Tecnologías y Sistemas de Información no se hace responsable por el uso de equipos que se estén usando en cada una de las áreas sin su consentimiento (quienes no hayan reportado el ingreso (Formato, Ingreso red institucional equipos externos), por ello cada área es responsable de informar sobre el ingreso de equipos y no permitir el uso de los cuales no están registrados, si se usaran en su espacio físico (Área).
- ✓ Racionalizar el consumo eléctrico y contribuir con el medio ambiente al apagar su equipo y/o monitor cuando no se requiera su uso.

9.7 Gestión de comunicaciones y operaciones

Los usuarios pueden operar los equipos si han recibido la capacitación previa necesaria para operarlos. La compra, eliminación y mantenimiento de equipos de almacenamiento deberá ser planeada conjuntamente por las diferentes áreas, asignando labores, basándose en los procedimientos y políticas que hayan sido establecidos para los activos de información.

La información de acceso de usuarios a las diferentes plataformas que operan activamente en el IPSE, debe ser almacenada e informada al Grupo Tecnologías y Sistemas de Información, quienes debe planificar la disponibilidad de los sistemas en el futuro, igualmente proyectar la inclusión de actividades o nuevas plataformas que involucren el acceso de más usuarios, para mejorar la capacidad de equipos y evitar sobrecargas.

Teniendo en cuenta la importancia que tienen los Sistemas de Información, los empleados IPSE deben aplicar los controles de seguridad básicos para manipular, abrir, descargar y compartir la información, mejorando las políticas del buen uso de la información que se ha implementado, la mejora o adaptación que deba realizarse.

El Grupo Tecnologías y Sistemas de Información debe tener un lugar disponible en el servidor para almacenar las carpetas Backup que permitirán realizar recuperación de los datos, por este motivo los

empleados IPSE deben aplicar y respetar los lugares asignados para el almacenamiento, los procedimientos y cumplir las políticas, de esta manera evitar perdida de información.

Los empleados IPSE se comprometen a no divulgar, modificar, retirar o destruir activos si no han sido autorizados, adicionalmente todos los datos sensibles o valiosos antes de ser transportados deben ser encriptados.

La información correspondiente al diseño, fallas, manejo específico y desarrollo de los Sistemas de Información como el sistema de gestión documental, la mesa de ayuda, el portal WEB, el sistema financiero u otros sistemas de información que maneja el IPSE para la administración, solo la puede acceder el personal autorizado o especializado y encargado para la labor.

El registro de fallas de procesamiento y de seguridad se debe alojar internamente en los servidores, adicionalmente debe tener un registro de hora actualizada para todas las máquinas virtuales (tiempo que se actualiza desde el servidor), la revisión la realizaran los administradores.

9.8 Adquisición, desarrollo y mantenimiento de sistemas de información (sistema, programación o aplicación)

- ✓ El Grupo Tecnologías y Sistemas de Información debe documentar las necesidades técnicas que tiene la entidad, para la adquisición, compra, desarrollo, implementación y monitoreo de un software, para uso general de todos los empleados o el necesario en actividades específicas, incluyendo procedimientos y políticas de seguridad específicas.
- ✓ El Grupo Tecnologías y Sistemas de Información debe analizar la clasificación de la información a trabajar en los software que necesite el IPSE, para definir los métodos de protección a ser implementados, utilizados o solicitados, de esta manera se de una viabilidad técnica estructural y se revisen los impactos que se pueden presentar.
- ✓ Con las necesidades documentadas, el proyecto debe ser viabilizado por los procesos correspondientes al interior del IPSE, para realizar un estudio de mercados que incluya todas las necesidades anteriormente documentadas, posteriormente se toma una decisión de actualización, compra o desarrollo.
- ✓ Antes de implementar nuevos software en la organización se deben realizar y documentar pruebas del mismo, determinadas por el Grupo Tecnologías y Sistemas de Información como se haya establecido en los procedimientos de la política de seguridad o contratos, de esta manera eliminar o minimizar los posibles riesgos y las posibles fallas.

- ✓ Las aplicaciones de mensajería instantánea o de correos electrónicos están reguladas por las políticas y procedimientos seguridad y privacidad planteados por la entidad que provee el servicio.
- ✓ La calidad del cifrado de las claves criptográficas debe ser validado y autorizado por el Grupo Tecnologías y Sistemas de Información para su implementación, también la forma de autenticar la identidad del usuario o empresa, de forma electrónica, ante terceros.
- ✓ Es necesario asegurar el sistema usado para la gestión de usuarios y claves, etiquetándolo como de uso restringido, solamente lo podrá acceder el personal líder del Grupo Tecnologías y Sistemas de Información.
- ✓ El Grupo Tecnologías y Sistemas de Información debe asignar un software a un empleado de la entidad, para que haga responsable de la verificación de pruebas e implementación y acompañe la implementación del mismo a los ambientes de producción de una forma controlada, basándose en los parámetros que hayan sido establecidos por la entidad.
- ✓ La verificación y evaluación de pruebas se realiza en compañía del proceso o responsable del proceso que haya realizado la solicitud.
- ✓ Se debe realizar un plan de capacitación para los empleados, cuando las actualizaciones o el nuevo software se considere apto para la implementación, posteriormente se realizaran las actividades que este conlleve.
- ✓ El IPSE debe reglamentar cuando lo considere necesario la adquisición de Software, incluyendo los deberes y derechos que deben cumplir las dos partes (Comprador-Proveedor), de esta manera crear acuerdos más transparentes, que permitan evaluar calidad, mejorar las garantías y permitir auditorías más eficientes que promuevan la mejora continua de seguridad y privacidad.
- ✓ Con previa solicitud evidenciada en la Mesa de Ayuda GLPI, el Grupo de tecnología y sistemas de información, puede autorizar la instalación y uso de Software Free al Usuario interesado, de demostrarse que su finalidad se ajusta a las metas de la entidad y no es de beneficio personal.

9.9 Gestión de los incidentes de seguridad de la información

- ✓ Se deben identificar, analizar, clasificar, evaluar los riesgos, vulnerabilidades, amenazas y controles de Seguridad y Privacidad de la Información, basándose en la clasificación de activos de información y su correspondiente monitoreo.
- ✓ Los incidentes de seguridad que se presenten deben ser reportados a la mesa de ayuda (GLPI), la cual permite hacer gestión de incidentes, para clasificar y validar el impacto y control que se debe aplicar, así realizar las acciones correctivas oportunas, basándose en los

procedimientos del Plan de Seguridad y Privacidad e la Información vigentes en la entidad o actividades que estén definidas.

- ✓ Se debe tener actualizado el servicio de Antivirus, que permita tener la información de incidencias de seguridad en la primera línea donde se presenten, así mismo generar reportes para saber en qué sector del ente se deben tener más precauciones.
- ✓ La entidad debe disponer de un grupo de atención de incidentes, quienes se encargaran de manejar las relaciones con entes internos y externos además de empleados, para dar respuesta, recolectar evidencia, crear anuncios, investigar y detectar las nuevas vulnerabilidades, riesgos o actualizaciones y recomendaciones de seguridad, de esta manera informar a los funcionarios periódicamente y evitar la propagación de amenazas.
- ✓ La Sincronización de Relojes debe ser optimizada, para facilitar el análisis de los eventos y la información, y mejorar la trazabilidad que se debe dar a la gestión del riesgo, basándose en los diferentes elementos y herramientas que están a disposición del personal que realiza el análisis.(Alertas en sistemas de seguridad, Caídas de servidores, Reportes de usuarios, informes Software antivirus, registro de acceso de usuarios, Logs servidores, Logs de aplicaciones y Logs de herramientas de seguridad)
- ✓ La recolección de evidencias y la sincronización de relojes permite al IPSE tener información exacta de los incidentes, cuando es necesario hacer un monitoreo especifico de una persona en un proceso que conlleve una acción legal (civil o penal).
- ✓ El Grupo Tecnologías y Sistemas de Información debe dar prioridad a los incidentes por criticidad de impacto, impacto actual o impacto futuro para asignar tiempos de respuesta rápidos y soluciones eficientes.
- ✓ Ante un riesgo de intrusión, se debe capacitar al personal líder del Grupo Tecnologías y Sistemas de Información, el encargado de la Seguridad o quien se considere necesario, en la implementación de una estrategia de orden oportuno, para evitar la propagación del incidente y así disminuir los daños a los recursos de TI, garantizando los principios de confidencialidad, integridad y disponibilidad basándose en estrategias de contención, erradicación y recuperación de un incidente.
- ✓ Es necesario realizar reevaluación de los Riesgos para proyectar posteriores soluciones y garantizar la mejora continua en la seguridad de la Información.

9.10 Gestión de la continuidad del negocio

Se deben proyectar eventos futuros que afecten al IPSE, en los procesos o en la infraestructura tecnológica, para planificar formas de recuperación de desastres y garantizar la continuidad del negocio,

además de Crear un mantener una Arquitectura Empresarial, observando y proyectando las diferentes FODA (Fortalezas, Oportunidades Debilidades y Amenazas), así como los impactos a los que se le daría lugar, de esta manera mantener un flujo de operatividad constante en toda la entidad.

Para todo Funcionario los Jefes de Área y para todo Contratista los Supervisores de Contrato, son responsables de hacer seguimiento de las diferentes estrategias estadísticas que tiene el IPSE, para monitorear el cumplimiento de la Gestión que realizan sus colaboradores, orientándolos en lo importante que son para el futuro de la Entidad.

Los controles preventivos y correctivos se deben mantener actualizados, principalmente se debería tener un BCP (Plan de Continuidad del Negocio), un DRP (Plan de Recuperación de Desastres), enfocándose en la administración, capacitación y distribución de tareas a los encargados de aplicar dichos planes, de esta forma garantizar la puesta en marcha de la operatividad nuevamente ante alguna eventualidad.

Se deben realizar las diferentes actividades planteadas en cada uno de los cronogramas que se proyecten, para respaldar que cada uno de los proyectos o estrategias nuevas se cumplirán, de esta manera no generar retrasos que afecten el desarrollo de otras actividades, en consecuencia aumenten los riesgos que puedan afectare la continuidad del negocio.

Se debe crear y mantener un comité de seguridad y privacidad de la información, el cual contara con una distribución de roles, funciones, responsabilidades e integrantes, para dar apoyo al cumplimientos y gestión de la políticas de seguridad y privacidad de la información.

9.11 Escritorio despejado

Todos los usuarios deben mantener su escritorio o interfaz de pantalla limpia, pues por usabilidad, rendimiento y eficiencia en los equipos cliente es una necesidad, además de mantener un ambiente cómodo al ingresar a su cuenta de usuario sobre la aplicación de VmWare.

10. CUMPLIMIENTO DE POLÍTICAS DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- ✓ Todos los empleados, contratistas, pasantes y empresas contratadas con el IPSE deben dar cumplimiento a las políticas adicionales de los sistemas de información (documentos anexos al presente documento) y las demás políticas que sean impartidas por el comité de

seguridad y privacidad de la información (documento anexo al presente documento), como se haya establecido en las reuniones de comité.

- ✓ Al interior de la entidad se hace necesario que las Políticas de Seguridad de la Información sean aproadas por la Dirección General.
- ✓ El Comité de seguridad y privacidad de la Información se encargara de socializar en todos los procesos del IPSE los lineamientos aprobados y procedimientos para la clasificación de activos de información, teniendo en cuenta la planeación que el mismo haya establecido.
- ✓ Todos los empleados, contratistas, pasantes y empresas contratadas con el IPSE deben adoptar una cultura del uso responsable de activos de información, planteada en el plan de seguridad y privacidad de la información, aprobado por la Dirección General.
- ✓ El grupo de talento humano debe trabajar con el Grupo Tecnologías y Sistemas de Información para realizar las capacitaciones de conocimiento y concientización a todo el recurso humano, sobre los riesgos y amenazas que pueden tener los activos de información, en especial los más sensibles y la relación entre la implantación del plan de políticas de seguridad y privacidad de la información y el papel que juegan como empleados para el cumplimiento de la misión, la visión del IPSE y el posicionamiento de la marca en el estado u sector minas y energía.
- ✓ Mejorar la percepción de las partes interesadas del IPSE (clientes, proveedores, contratistas, comunidades, funcionarios y organismos de control) con respecto a los productos y servicios que ofrece el instituto enmarcados dentro de una política de seguridad y privacidad que cumpla los requerimientos u normatividades vigentes.
- ✓ El área asesora de Control interno deben realizar las auditorias correspondientes para validar cumplimiento y mejorar las condiciones de seguridad con las que debe contar el IPSE, entregando e informando los resultados de las auditorias.
- ✓ El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa del IPSE (Resolución de la presente Política), incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere (NORMATIVIDAD del presente documento).

11. ANEXOS

1. Documento para la creación del Comité de Seguridad y Privacidad de la información para el Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas no Interconectadas.
2. Políticas específicas para ORFEO
3. Políticas específicas para PORTALES
4. Políticas específicas para SFI
5. Políticas específicas para SISTEMA DE GESTIÓN INTEGRAL

12. REFERENCIAS

RESOLUCION 524. (27 de 07 de 2007). Recuperado el 02 de 05 de 2017, de RESOLUCION 524: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=27859

CONGRESO DE COLOMBIA, _. (2009). *LEY 1273.* Recuperado el 02 de 05 de 2017, de LEY 1273: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Constitucion_Politica_de_Colombia. (1991). *Constitucion_Politica_de_Colombia*. Recuperado el 02 de 05 de 2017, de https://www.procuraduria.gov.co/guiamp/media/file/Macroproceso%20Disciplinario/Constitucion_Politica_de_Colombia.htm

Ginioux Jean-Mathieu Doléans y Frederic. (2017). *Gestionnaire libre de parc informatique.* Recuperado el 02 de 05 de 2017, de Gestionnaire libre de parc informatique: http://glpi-project.org/spip.php?article87

ICONTEC. (22 de 03 de 2006). *NORMA TÉCNICA NTC-ISO/IEC.* Recuperado el 02 de 05 de 2017, de NORMA TÉCNICA NTC-ISO/IEC: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

ISO - ICONTEC, I. C. (2006.). *Sistema de Gestión de la Seguridad de la Información (SGSI).* Colombia: XPRESS ESTUDIO GRTAFICO Y DIGITAL - ICONTEC.

ISO / IEC. (15 de 10 de 2005). *ISO / IEC 27001.* Recuperado el 02 de 05 de 2017, de ISO / IEC 27001: https://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf

iso27000.es. (2005). *http://www.iso27000.es.* Recuperado el 02 de 05 de 2017, de http://www.iso27000.es: http://www.iso27000.es/download/ControlesISO27002-2013.pdf

Ley 1712, a. 6. (06 de 03 de 2014). Ley 1712 de 2014, art 6. *Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.* Colombia.

LEY 734. (2002). *Procuraduria General de la Nacion.* Recuperado el 02 de 05 de 2017, de www.procuraduria.gov.co: https://www.procuraduria.gov.co/guiamp/media/file/Macroproceso%20Disciplinario/L-734-02.htm

Ministerio de TIC, _. (2015). *http://www.mintic.gov.co.* Recuperado el 02 de 05 de 2017, de http://www.mintic.gov.co: http://programa.gobiernoenlinea.gov.co/apc-aa-files/eb0df10529195223c011ca6762bfe39e/manual-3.1.pdf

NTC 5411-1, -1. (2006). NTC 5411-1. Colombia.

PRESIDENTE DE LA REPÚBLICA. (20 de 05 de 2005). *http://www.alcaldiabogota.gov.co.* Recuperado el 02 de 05 de 2017, de http://www.alcaldiabogota.gov.co: DECRETO 1599 DE 2005

PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. (13 de 04 de 2012). *http://wsp.presidencia.gov.co.* Recuperado el 28 de 04 de 2017, de http://wsp.presidencia.gov.co: http://wsp.presidencia.gov.co/Normativa/Decretos/2012/Documents/Abril/13/dec73413042012.pdf

REPUBLICA DE COLOMBIA. (2004). *NTCGP 1000:2004.* Recuperado el 02 de 05 de 2017, de NTCGP 1000:2004: https://www.usco.edu.co/contenido/ruta-calidad/documentos/anexos/66-Norma%20tecnica%20de%20calidad%20en%20la%20gestion%20publica%20NTCGP%201000%20de%202004.pdf

República de Colombia, _. (2012). *DECRETO 2693.* Recuperado el 26 de 04 de 2017, de DECRETO 2693: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=51198

República de Colombia, _. (2012). *LEY ESTATUTARIA 1581.* Recuperado el 02 de 05 de 2017, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981#0

Republica de Colombia, _. (2013). *Decreto 1377 de 2013 Nivel Nacional.* Recuperado el 02 de 05 de 2017, de Decreto 1377 de 2013 Nivel Nacional: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646

Republica de Colombia, _. (2014). Recuperado el 2017 de 04 de 25, de http://wp.presidencia.gov.co/sitios/normativa/decretos/2014/Decretos2014/DECRETO%202473%20DEL%2002%20DE%20DICIEMBRE%20DE%202014.pdf

Republica de Colombia, _. (26 de 05 de 2015). *MINTIC.* Recuperado el 02 de 05 de 2017, de MINTIC: http://www.mintic.gov.co/portal/604/articles-9528_documento.pdf

MINMINAS

IPSE
Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

POLITICAS DE SEGURIDAD DEL SISTEMA DE GESTION DOCUMENTAL "ORFEO"

"La presente Política aplica para el sistema de gestión documental Orfeo.

Mayo 2017

CONTROL DE CAMBIOS

VERSIÓN	FECHA	RESPONSABLE	DESCRIPCIÓN
1.0	10/5/2017	JORGE ENRIQUE LOPEZ TIMANA	CREACIÓN DOCUMENTO
1.0	10/5/2017	DEYBER ERICKSON RODRIGUEZ ALVAREZ	AJUSTE DEL FORMATO
1.0			REVISIÓN Y OBSERVACIONES
			CORRECCIÓN DE OBSERVACIONES

DERECHOS DE AUTOR

CONTENIDO

1. DERECHOS DE AUTOR DE LOS CONTENIDOS - COPYRIGHT.

Licencia de Orfeo: Licencia AGPL V3

Licencia que se encontrara en la http://www.gnu.org/

Este sistema de colaboración para el licenciamiento es un esfuerzo de la "Free Software Fundation".

En la Raiz del Aplicativo podra encontrar la Licencia Licencia AGPL o en la página http://www.gnu.org/licenses/agpl

La Affero GPL es íntegramente una GNU GPL con una cláusula nueva que añade la obligación de distribuir el software si éste se ejecuta para ofrecer servicios a través de una red de ordenadores. La Licencia AGPL La licencia AGPL fue diseñada para cerrar la evasión de los proveedores de servicios de aplicación a la licencia GPL ordinaria, que no obliga la distribución del código fuente cuando el software licenciado con GPL sea usado para dar un servicio, típicamente aplicaciones web.

Correlibre.org es una Fundación que se encarga de promover el software y conocimiento libre (GNU/GPL). Actualmente se encuentra administrando de la Comunidad OrfeoGPL.org.

2. NIVELES DE ACCESO A ORFEO

NIVEL	DESCRIPCIÓN
1	Contratistas, SENA, Pasantes.
2	Secretario Ejecutivo
3	Técnicos Administrativos
4	Coordinadores, Profesionales Universitarios/Especialistas
5	Dirección General, Secretaria General, Jefes de Oficina, Subdirectores

3. ADMINISTRACION DE CUENTAS DE USUARIO DE ORFEO

a. La creación y modificación de los datos de usuarios, corresponde al funcionario designado como Administrador de Orfeo en IPSE, es importante tener en cuenta que para dicho procedimiento de traslado todas las carpetas del usuario Orfeo deben estar vacías y solo se permiten radicados en informados.

b. No se pueden crear usuarios con ñ - Ñ, ni con caracteres especiales.

Los nombres de cuentas de usuario para los funcionarios de libre nombramiento y remoción deben ser asignados por el Grupo de Tecnologías y Sistemas de Información del IPSE.

c. El acceso a la bandeja de usuarios ausentes de manera temporal por fuerza mayor debe ser autorizado por el propietario de la cuenta y en casos excepcionales por el director de la dependencia.
d. Antes de pasar la última cuenta de un contrato de prestación de servicios, el interventor o supervisor debe exigir paz y salvo documental físico y electrónico (bandeja del aplicativo).
e. Se deben inactivar Usuarios en el Sistema cuando estos se encuentren en periodo de vacaciones o finalicen parcial o totalmente el vínculo laboral con el IPSE, esta solicitud se realiza a través de la Oficina de Talento Humano; Igualmente aplica para cuando se reintegran a la Entidad.

4. MANEJO DEL DOCUMENTO FISICO

a. Todo trámite del documento debe realizarse a través de Orfeo: reasignaciones, envíos ha Visto Bueno (Vo.Bo.) y su respectiva revisión, un documento solo será impreso cuando esté en firme y se deba pasar para la firma.
b. Toda dependencia debe crear la Unidad de correspondencia donde reposarán los documentos físicos hasta que termine el trámite.
c. La unidad de correspondencia será la encargada de marcar como impreso, marcar como enviado, adjuntar firmado y notificado y archivar al finalizar el trámite de las comunicaciones de salida y aquellos que no generan respuesta (invitaciones)
d. El documento físico debe pasar de ventanilla de radicación directamente al Centro de Documentación de la dependencia, y podrán ser solicitados solo en calidad de préstamo, cuando no sean legibles o por su volumen no hayan sido completamente digitalizados.
e. Las comunicaciones internas no se imprimirán, sin embargo se exigirá en formato PDF con su correspondiente firma mecánica, dando cumplimiento a la Directiva Presidencial 04 de 2012, de cero papel.

5. MANEJO DE LA CUENTA POR PARTE DEL USUARIO FINAL

a. Todo Servidor que tenga la facultad de firmar documentos debe gestionar su firma mecánica en el sistema.

b. Todo usuario es responsable de los eventos que se ocasionen desde su cuenta y deberá velar por la seguridad de su contraseña y/o accesos no autorizados que se den sobre ella.
c. El funcionario, contratista o practicante que posea una cuenta de Orfeo asignada por el IPSE, debe dar trámite a todos los radicados que posea en su cuenta si finaliza su contrato con el IPSE o antes de salir a vacaciones, para dejar a paz y salvo su Orfeo, además debe avisar al área de TIC para que sea tramitado con tiempo su paz y salvo (por lo menos se debe avisar el día hábil anterior mas próximo).

6. PROCESOS ASOCIADOS AL MANEJO DE ORFEO

a. En adelante se incluirá en el proceso de inducción y reinducción de nuevos funcionarios, la socialización de todo el manejo de Gestión Documental, y programar por lo menos 1 vez al mes, una capacitación en Orfeo, para los nuevos funcionarios incorporados, tanto Contratistas como Nombrados.
b. La tabla de Retención Documental debe mantenerse actualizada por el líder del Grupo de Archivo.

7. SOPORTE TECNICO DE ORFEO

El soporte técnico sobre el manejo de la herramienta se atenderá directamente por el Grupo de Tecnologías y Sistemas de Información del IPSE.

8. MANEJO DE DOCUMENTOS A TRAVÉS DE ORFEO

a. En Orfeo se radicará toda la documentación que ingrese al IPSE, exceptuando los documentos anónimos, que si se deben relacionar en la planilla de envíos de la documentación física.
b. Al ingresar los nuevos datos de un ciudadano o empresa al sistema, se debe escribir claramente sin la utilización de caracteres especiales, específicamente comilla simple, doble comillas.
c. La tipificación de entrada debe realizarse en los despachos y la tipificación de respuesta y\o comunicaciones internas o de salida la realizará el responsable del trámite que elabora o proyecta
d. Una comunicación interna, se responde a través de una comunicación interna nueva, a la cual se le "anexa/asocia" el radicado padre (también interno).
e. Para realizar el trámite de radicados que requieren respuesta compartida hay que tener presente lo siguiente:

- ✓ Si la respuesta es unificada, el funcionario que recibe el requerimiento y consolida (funcionario_1), debe enviar una comunicación interna a los otros responsables, solicitando dar respuesta (a los ítems correspondientes o de su competencia) y asociando el requerimiento del ciudadano, los otros funcionarios responden (al funcionario_1) con comunicaciones internas, y dicho funcionario al recibir las respuestas consolida y generar un solo radicado de respuesta (salida).
- ✓ Si la respuesta no es unificada y cada uno responde al ciudadano, el funcionario que recibe el requerimiento (funcionario_1) genera una comunicación interna a los otros responsables, solicitando dar respuesta (a los ítems correspondientes por competencia) y asociando el requerimiento del ciudadano. Cada uno de esos funcionarios genera una radicación de salida (nueva) asociando el radicado que se está dando respuesta. La comunicación interna recibida de parte del funcionario_1, puede ser archivada por los otros.

f. Una vez un documento o registro ha sido radicado, este no puede ser borrado o eliminado del Sistema, en este caso el procedimiento es archivar dicho documento y escribir en la observación, los motivos por los cuales se desiste de dicho radicado.

g. Un documento solo puede ser modificado por el usuario que lo anexó o por su jefe inmediato antes de que se le haya asignado el radicado.

h. Para quienes no están autorizados al uso de firma mecánica y requieran adjuntar el documento firmado, se debe realizar a través de la opción "Asociar imagen", no se recomienda la opción de Anexar otro archivo.

i. Un radicado que no tiene imagen asociada, no se debe devolver, sin antes verificar si por su naturaleza (web, telefónica, etc.), no requiere imagen adjunta.

j. Cuando un radicado no sea de competencia del funcionario al que fue asignado se debe remitir al competente natural o en su defecto ante el desconocimiento devolverlo al origen con la debida observación aclaratoria.

k. El conteo de días de un radicado termina cuando se le anexa la respuesta notificada y se archiva por el Centro de Documentación.

l. Cualquier radicado que no requiera respuesta debe ser enviada al usuario del centro de documentación con la debida observación aclaratoria para su respectiva acción de archivo.

m. Un documento que se ha archivado puede ser retornado solo a la bandeja del usuario que lo archivó, previa solicitud de dicho procedimiento al funcionario lider de Orfeo en su dependencia.

n. Cuando llegan requerimientos a los correos corporativos del Sr. Director o Secretario, estos deben ser ingresados al sistema ORFEO anexando una impresión pdf del mensaje de datos original para que quede registrada la trazabilidad de la solicitud. Se le debe responder el correo al ciudadano con el número con el que quedó radicada su solicitud para que pueda consultarla vía web.

o. Para la elaboración de una resolución, el funcionario que proyecta debe generar una comunicación interna con el contenido del texto y enviarlo al usuario de Despacho; cualquier modificación sobre el texto, se realiza sobre dicha comunicación interna. Cuando el documento está aprobado, en el despacho se toma el texto proyectado y se elabora y radica dicha resolución.

9. A TENER EN CUENTA...

- ✓ Para modificar a un Usuario en Orfeo, se requiere tener las carpetas sin Documentos.
- ✓ Se realizarán auditorias y seguimiento a los Documentos que no han sido archivados y que llevan un periodo de tiempo prolongado en las carpetas.
- ✓ El Sistema de Gestión Documental Orfeo, no permite reservar números de Radicados.
- ✓ Los Documentos físicos que requieran ser consultados, deben ser solicitados a través de Orfeo y dirigidos al Proceso Gestión Documental, quien registrará y realizará seguimiento de los Documentos en calidad de préstamo usando de manera obligatoria su contraseña del Usuario.
- ✓ El grupo de Gestión Documental realizará el seguimiento de los Documentos en préstamo a través del Sistema.
- ✓ Los usuarios del IPSE que tienen a cargo Contratos o Convenios deben asociar los Documentos en Orfeo a los expedientes virtuales.
- ✓ Gestión Documental tendrá bajo su responsabilidad el Módulo de archivo, donde se realizará la depuración y alimentación de expedientes físicos.
- ✓ El Módulo Devolución de Correos y el Módulo Envíos, son de uso exclusivo del Grupo de Gestión Documental quien verificará el descargue a través del Sistema, además la entrega y recepción de los Documentos a las empresas de mensajería.
- ✓ Toda la documentación generada dentro de la Entidad debe ser entregada al Grupo de Gestión Documental para su digitalización.
- ✓ Será función de Control Interno, auditar los tiempos transcurridos entre la radicación y digitalización del documento, teniendo en cuenta el volumen de documentos que ingresan a la Entidad lo nombrado.
- ✓ Se solicitará a los ciudadanos y empresas hacer referencia en la documentación al número del expediente asociado al proceso que se lleva en el IPSE.
- ✓ Se radica como Anexo cuando el Documento que se va a generar es la respuesta al Documento principal o al radicado de entrada, y pertenecen al mismo expediente.

- ✓ Radicación Masiva es un Módulo por el cual se pueden generar varios Radicados con una plantilla creada previamente por el usuario, que contiene el mismo Contenido. (Ver Manual Interno de Radicación Masiva)
- ✓ El Usuario con perfil de Jefe en Orfeo, es el único que puede reasignar o recibir Radicados de otras dependencias porque es principio de Orfeo que el Jefe este informado de toda la documentación que llega o sale a la Dependencia.
- ✓ El Usuario con perfil normal (que no es Jefe) solo puede reasignar Radicados a Funcionarios de su misma Dependencia.
- ✓ El usuario que es Jefe puede reasignar Radicados a Jefes de otras Dependencias o Funcionarios de su misma dependencia.
- ✓ Un expediente es la representación virtual de un expediente físico que contiene en orden cronológico los Documentos que han sido incorporados dentro de un trámite y/o proceso.
- ✓ Se debe archivar un radicado cuando el trámite ha finalizado, la tipificación es la adecuada y esta digitalizado con firma y/o firma digital.
- ✓ Después de creado un expediente en Orfeo, cualquier persona que tramite un Radicado, puede incluirlo al expediente.
- ✓ OrfeoScan es el aplicativo de Orfeo por el cual se digitalizan los Documentos.
- ✓ Cualquier usuario puede acceder a las estadísticas.
- ✓ Los usuarios con nivel de acceso 1 en Orfeo no pueden generar radicados.

MINMINAS

IPSE
Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

POLÍTICA DE SEGURIDAD PORTALES

"La presente Política aplica para los siguientes sitios web: Página web del IPSE, Intranet y GLPI."

Mayo 2017

CONTROL DE CAMBIOS

VERSIÓN	FECHA	RESPONSABLE	DESCRIPCIÓN
1.0	17/3/2017	LILIANA MORAN RODRIGUEZ	CREACIÓN DOCUMENTO
1.0	17/3/2017	DEYBER ERICKSON RODRIGUEZ ALVAREZ	AJUSTE DEL FORMATO
1.0			REVISIÓN Y OBSERVACIONES
			CORRECCIÓN DE OBSERVACIONES

DERECHOS DE AUTOR

CONTENIDO

1. DERECHOS DE AUTOR DE LOS CONTENIDOS - COPYRIGHT.

Los contenidos de los portales son de propiedad intelectual del IPSE. Es posible descargar material de ellos para uso personal y no comercial, siempre y cuando se haga expresa mención de la propiedad en cabeza del IPSE. Respecto a los contenidos que aparecen en los portales, el usuario se obliga a:

a) Usar los contenidos de forma diligente, correcta y lícita.
b) No suprimir, eludir, o manipular el copyright (derechos de autor) y demás datos que identifican los derechos del IPSE.
c) No emplear los contenidos y en particular la información de cualquier otra clase obtenida a través del IPSE o de los servicios para emitir publicidad.
d) El IPSE no será responsable por el uso indebido que hagan los usuarios del contenido de sus portales.
e) El visitante o usuario de los portales se hará responsable por cualquier uso indebido, ilícito o anormal que haga de los contenidos, información o servicios de los sitios del IPSE.
f) El visitante o usuario del sitio, directa o por interpuesta persona, no atentará de ninguna manera contra los portales del IPSE, contra su plataforma tecnológica, contra sus sistemas de información ni tampoco interferirá en su normal funcionamiento.
g) El visitante o el usuario del sitio no alterará, bloqueará o realizará cualquier otro acto que impida mostrar o acceder a cualquier contenido, información o servicios de los sitios del IPSE, o que estén incorporados en las páginas web vinculadas.
h) El visitante o el usuario de los sitios web del IPSE no enviará o transmitirá en este sitio o hacia el mismo a otros usuarios o a cualquier persona cualquier información de alcance obsceno, difamatorio, injuriante, calumniante o discriminatorio.
i) El visitante o el usuario de los sitios web del IPSE no incurrirá en y desde el mismo en conductas ilícitas, como daños o ataques informáticos, interceptación de comunicaciones, infracciones a los derechos de autor, uso no autorizado de terminales, usurpación de identidad, revelación de secretos o falsedad en los documentos.

2. CONDICIONES DE CONFIDENCIALIDAD Y SEGURIDAD

Es interés del IPSE la salvaguardia de la privacidad de la información personal del usuario obtenida a través de los sitios web de la entidad, para lo cual se compromete a adoptar una política de confidencialidad de acuerdo con los siguientes lineamientos:

a) Información personal: el usuario o visitante reconoce que el ingreso de información personal lo realiza de manera voluntaria y ante la solicitud de requerimientos específicos por el IPSE para realizar un trámite, presentar una petición, queja, reclamo, sugerencia o denuncia, o para acceder a los mecanismos interactivos. El usuario también comprende que los datos por él consignados harán parte de un archivo y/o base de datos.

b) Uso de la clave de acceso: la información personal proporcionada por el usuario está asegurada por una clave de acceso que sólo él conoce. Por tanto, es el único responsable de mantener en secreto su clave y realizar el cambio periódicamente, utilizar una clave segura en lo posible con letras, números y símbolos. El IPSE se compromete a no acceder ni pretender conocer dicha clave. Debido a que ninguna transmisión por Internet es absolutamente segura ni puede garantizarse dicho extremo, el usuario asume el hipotético riesgo que ello implica, el cual acepta y conoce.

c) Ingreso a la información personal por terceros: El IPSE no responderá en ningún caso y bajo ninguna circunstancia por los ataques o incidentes contra la seguridad de sus sitios web o contra sus sistemas de información o por cualquier exposición o acceso no autorizado, fraudulento o ilícito a su sitio web y que puedan afectar la confidencialidad, integridad o autenticidad de la información publicada o asociada con los contenidos y servicios que se ofrecen en él. Tampoco se responsabilizará por cualquier consecuencia derivada del ingreso indebido de terceros a la base de datos y/o por cuando alguna falla técnica en el funcionamiento y/o conservación de datos en el sistema en cualquiera de los menús de su página web.

d) Seguridad de la información: El IPSE ha adoptado los niveles de seguridad de protección de los datos personales legalmente requeridos, instalando las medidas técnicas y organizativas necesarias para evitar en lo posible la pérdida, mal uso, alteración, acceso no autorizado y robo de los datos facilitados. El IPSE no controla ni garantiza, al 100%, la ausencia de virus ni de otros elementos en los contenidos que puedan producir alteraciones en su sistema informático (software y hardware) o en los documentos electrónicos y ficheros almacenados en su sistema informático. En consecuencia, el IPSE no se hará responsable de ningún daño ocasionado en virtud de cualquier alteración que se haya efectuado a los materiales o archivos de descarga suministrados directamente por la entidad.

e) Confidencialidad de la información: El IPSE no compartirá ni revelará la información confidencial con terceros, excepto que tenga expresa autorización de quienes se suscribieron, o cuando ha sido requerido por orden judicial o legal, o para proteger los derechos de propiedad intelectual u otros derechos.

MINMINAS

IPSE
Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

POLÍTICA DE SEGURIDAD SISTEMAS DE ACTIVOS FIJOS, ALMACENES Y NÓMINA

"Aplica a los Sistemas de Activos Fijos, Almacenes y Nómina, versión 4.0."

Mayo 2017

CONTROL DE CAMBIOS

VERSIÓN	FECHA	RESPONSABLE	DESCRIPCIÓN
1.0	31/5/2017	WINSTON RUIZ HOYOS	CREACIÓN DOCUMENTO
1.0	31/5/2017	DEYBER ERICKSON RODRIGUEZ ALVAREZ	AJUSTE DEL FORMATO
1.0			REVISIÓN Y OBSERVACIONES
			CORRECCIÓN DE OBSERVACIONES

DERECHOS DE AUTOR

CONTENIDO

Estos Sistemas están diseñados para Cliente-Servidor, con herramientas Developer de Oracle, las cuales funcionan en Windows 7, 8, 8,1 y 10, y Windows server 2012. Estos sistemas, derivados de versiones anteriores del mismo autor, están protegidos por la Oficina de Derechos de Autor del Ministerio del Interior.

1. BASE DE DATOS

a. Los Sistemas de Solgein suministrados a IPSE están diseñados para la base de datos Oracle 11g y 12c.
b. Todas las tablas están normalizadas, con sus llaves primarias, índices, referencias de integridad, chequeos, índices.
c. Actualmente, IPSE tiene instaladas la versión 3.0 de Activos Fijos, la versión 4.0 de Activos Fijos y Almacenes, en los esquemas SOLGEIN_SUIMAX30 y SOLGEIN_SUIMAX40 respectivamente. Ambas versiones comparten muchos nombres de objetos iguales, pero la estructura de ambas varia de muchas formas.
d. Como ambas versiones están en la misma base de datos, los sinónimos públicos y los grants de los objetos a los usuarios solo pueden apuntar a una versión a la vez. Es por esto que cuando entra en producción la versión 4.0, la versión 3.0 queda inutilizada.
e. El Sistema de nómina que está instalado en IPSE es Nómina Solgein v 3.0, el cual está en el esquema SGH30. La versión de nómina que antes utilizaba el IPSE (versión Construsoft) está en el esquema SRH.
f. Las tablas están organizadas en Tablespaces, uno para la versión 3.0 de RRFF, otro para la 4.0 de RRFF y otro para Nómina 3.0
g. Actualmente, el servidor de BD tiene automatizado el backup de la base de datos
h. Dicho backup exporta todo el contenido de la base de datos, el cual incluye los siguientes esquemas:
    - ✓Activos Fijos Solgein v 3.0
    - ✓Activos Fijos y Almacén Solgein v 4.0
    - ✓Nómina Solgein v 3.0
    - ✓SFI de Construsoft para Windows v 1.0 (Contabilidad, Presupuesto, CxP y Tesorería)
    - ✓Compras y Contratos
    - ✓Costos ABC
    - ✓Administración de Menús Solgein v 4.1

i. Se recomienda que el área de Sistemas copie regularmente los archivos comprimidos en otro lugar.
j. A cada usuario del Sistema le corresponde un usuario de la base de datos.

2. REDES

a. Los Sistemas, al ser Cliente-Servidor, comparten con los usuarios finales una carpeta desde el Servidor de Aplicaciones.
b. Los usuarios no tienen acceso directo al servidor de BD.
c. Los usuarios solo se comunican con la base de datos a través de las formas y reportes diseñadas para su uso.
d. Actualmente, solo se dan privilegios de acceso a usuarios de Nómina, Recursos Físicos y a la Contadora.
e. Si los usuarios intentan ingresar a la carpeta de red la encontrarán vacía, para evitar cualquier daño accidental.

3. PROGRAMAS FUENTE

a. La licencia otorgada al IPSE es para uso privado, por tiempo indefinido de los programas fuentes y ejecutables.
b. Por ser licencia privada, el IPSE podrá leer o modificar, solo para usos de mantenimiento.
c. IPSE no podrá divulgar ni publicar parte o la totalidad del contenido de la información fuente a terceros.
d. La responsabilidad de la custodia de los programas fuente es del IPSE y del personal externos que haya sido asignado para trabajar en los programas fuente.

4. FONT-END

a. Los usuarios acceden al Sistema a través de un ícono que abre una ventana de bienvenida, la cual les solicita el nombre del alias y la clave de seguridad.
b. Todas las opciones tienen un diseño homogéneo y minimalista, lo que agiliza el trabajo.

c. Como la carpeta compartida del servidor de aplicaciones está como solo lectura, no hay riesgo de propagación de virus al servidor por este medio.
d. Las formas cuentan con mensajes de advertencia en caso que el usuario desee borrar algún registro.
e. Las formas cuentan con un registro de la fecha de creación y modificación de la información por parte de los usuarios.

5. ADMINISTRACIÓN DE MENÚS

a. Los Sistemas de Solgein se acceden a través del Sistema de Administración de Menús, versión 4.1.
b. Este Sistema cuenta con la opción de crear usuarios y sincronizarlos con los usuarios Oracle de la BD.
c. La contraseña queda encriptada.
d. Cuando el Administrador crea un usuario le puede asignar una contraseña temporal.
e. Cuando el usuario entra por primera vez, el Sistema le solicita cambio de clave. De esta manera, el Administrador nunca conoce las claves de los usuarios.
f. Si un usuario olvida la clave, el Sistema le da tres oportunidades antes de cerrar la ventana.
g. Cuando persiste la equivocación de la clave, el Sistema de Menús bloquea el usuario cuando supera los intentos permitidos.
h. La cantidad de intentos para cerrar la ventana o para bloquear al usuario pueden ser configurados por el Administrador del Sistema.
i. El Sistema de Menús otorga los permisos con base en roles o perfiles asignados a las diferentes opciones de la aplicaciones.
j. El Sistema de Menús guarda la historia de todos los inicios de sesión y accesos a todas las opciones de los Sistemas.
k. El Administrador del Sistema puede configurar el tiempo en que debe ser guardada la información histórica de todos los accesos.
l. El Administrador puede crear roles y definir si los usuarios asignados pueden entrar a consultar o modificar la información.
m. Todos los históricos de Menús pueden ser consultados por el administrador del software

MINMINAS

IPSE
Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

POLÍTICA DE SEGURIDAD SISTEMA DE GESTIÓN INTEGRAL

"La presente Política aplica SGI del IPSE"
CONFIGURACIÓN GENERAL ITS- GESTIÓN"

Mayo 2017

CONTROL DE CAMBIOS

VERSIÓN	FECHA	RESPONSABLE	DESCRIPCIÓN
1.0	18/5/2017	LINA VANNESA PERDOMO - ITS SOLUCIONES ESTRATÉGICAS	CREACIÓN DOCUMENTO
1.0	22/5/2017	DEYBER ERICKSON RODRIGUEZ ALVAREZ	AJUSTE DEL FORMATO
1.0			REVISIÓN Y OBSERVACIONES
			CORRECCIÓN DE OBSERVACIONES

DERECHOS DE AUTOR

CONTENIDO

1. CONFIGURACIÓN GENERAL ITS- GESTIÓN

Para garantizar la seguridad de la aplicación ITS-GESTION, se sugiere realizar un seguimiento y evaluación a la seguridad de la aplicación y en el servidor dónde está alojada.

Con el fin de evitar brechas de seguridad ITS-SOLUCIONES ESTRATÉGICAS desarrolló el siguiente plan de trabajo, el cual está planteado para evitar accesos y modificaciones no autorizadas en la aplicación.

2. CONDICIONES DE CONFIDENCIALIDAD Y SEGURIDAD

Los puntos a realizar para los servidores y la aplicación serán los siguientes:

- Mover la carpeta del document root a una unidad donde no esté instalado el sistema operativo, por default se instala la carpeta en la unidad del sistema (normalmente la unidad C). La idea es instalar la carpeta a una partición diferente a la que contiene el sistema operativo esto es para mejorar la seguridad y evitar daños al sistema operativo del servidor de aplicaciones.
- Retirar archivos de configuración que estén en la raíz del código fuente del sistema con el fin de no presentarle opciones a intrusos, mediante archivos que en tiempo de desarrollo son útiles pero que en tiempo de producción son grandes brechas de seguridad.
- Aislar las carpetas temporales de PHP, con el fin que un intruso no pueda acceder por ejemplo a datos de sesión.
- Utilizar el principio de publicación Web, que consiste en dar privilegios mínimos a usuarios no administradores.
- Configurar IIS para evitar que liste la información de las carpetas en Web.
- Aislar la aplicación web y que no se comparta el sitio web con ninguna otra aplicación.
- Revisar que el servidor tenga antivirus y esté activo el Firewall debidamente configurado.