	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Páginas
		15-09-2022	Pág. 1 de 36

INSTITUTO DE PLANIFICACIÓN Y PROMOCIÓN DE SOLUCIONES ENERGÉTICAS PARA ZONAS NO INTERCONECTADAS (IPSE)

MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

PROCESO DE GESTIÓN DE TIC


	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Paginas
		15-09-2022	Pág. 2 de 36

TABLA DE CONTENIDO


INTRODUCCIÓN.....	4
1. OBJETIVO	4
2. ALCANCE	4
3. DEFINICIONES	5
4. MARCO LEGAL	8
5. POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL.	9
6. POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	10
6.1 POLITICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.....	10
6.1.1 ORGANIZACIÓN INTERNA.....	10
6.1.2 DISPOSITIVOS MOVILES	10
6.1.3 TELETRABAJO – TRABAJO EN CASA	11
6.2 POLITICA DE SEGURIDAD DE LOS RECURSOS HUMANOS.....	11
6.2.1 ANTES DE ASUMIR EL EMPLEO.....	11
6.2.2 DURANTE LA EJECUCIÓN DEL EMPLEO.....	12
6.2.3 TERMINACIÓN Y CAMBIO DE EMPLEO	12
6.3 POLITICA DE GESTIÓN DE ACTIVOS.....	13
6.3.1 RESPONSABILIDAD POR LOS ACTIVOS	13
6.3.2 CLASIFICACIÓN DE LA INFORMACIÓN	14
6.3.3 MANEJO DE MEDIOS	14
6.4 POLITICA CONTROL DE ACCESOS	15
6.4.1 REQUISITOS DE LA ENTIDAD PARA EL CONTROL DE ACCESO	15
6.4.2 GESTIÓN DE ACCESO DE USUARIOS	16
6.4.3 RESPONSABILIDADES DE LOS USUARIOS	17
6.4.4 CONTROL DE ACCESOS A SISTEMAS Y APLICACIONES	17
6.5 POLITICA SEGURIDAD PARA EL USO DE RECURSOS CRIPTOGRÁFICOS.....	18
6.5.1 CONTROLES CRIPTOGRÁFICOS.....	18
6.6 POLITICA FIRMA DIGITAL.....	19
6.7 POLITICA SEGURIDAD FÍSICA Y DEL ENTORNO.....	20
6.7.1 ÁREAS SEGURAS.....	20



MANUAL DE LA POLÍTICA DE
SEGURIDAD Y PRIVACIDAD DE LA
INFORMACIÓN Y SEGURIDAD DIGITAL

Código	Versión
IPSE-TIC-M04	1
Fecha:	Páginas
15-09-2022	Pág. 3 de 36

6.7.2 EQUIPOS	22
6.8 POLITICA SEGURIDAD DE LAS OPERACIONES	23
6.8.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	23
6.8.2 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS.....	24
6.8.3 COPIAS DE RESPALDO	25
6.8.4 REGISTRO DE EVENTOS Y SEGUIMIENTO.....	26
6.8.5 CONTROL DE SOFTWARE OPERACIONAL	27
6.8.6 GESTIÓN DE VULNERABILIDADES TÉCNICAS.....	27
6.8.7 CONSIDERACIONES SOBRE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	28
6.9 POLITICA SEGURIDAD DE LAS COMUNICACIONES.....	28
6.9.1 GESTIÓN DE SEGURIDAD DE LAS REDES.....	28
6.9.2 TRANSFERENCIA DE INFORMACIÓN.....	29
6.9.3 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.....	31
6.9.4 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	32
6.9.5 PROTEGER LOS DATOS USADOS PARA PRUEBAS	34
6.10 POLITICA SEGURIDAD DE RELACIÓN CON PROVEEDORES.....	35
6.11 POLITICA GESTIÓN DE INCIDENTES DE SEGURIDAD.....	36
6.12 POLITICA GESTIÓN CONTINUIDAD DEL NEGOCIO.....	36
6.12.1 CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN	36
6.13 POLITICA DE PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES.....	36
6.14 POLITICA DE CUMPLIMIENTO.....	42
6.14.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES	42
BIBLIOGRAFÍA.....	43

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Paginas
		15-09-2022	Pág. 4 de 36

INTRODUCCIÓN

El instituto de Planificación y Promoción de Soluciones Energéticas para Zonas No Interconectadas (IPSE) reconoce la importancia de la información que gestiona, debido a que es uno de los activos más significativos para su funcionamiento y que ésta puede ser de naturaleza legal, estratégica, financiera, operativa y en algunos casos corresponder a datos personales de servidores públicos, contratistas y grupos de valor.

De igual manera, es consciente de las amenazas que enfrenta la información y de las consecuencias a las que se expone cuando no cuenta con las medidas de seguridad y protección adecuadas. En ese sentido, El IPSE debe tener una visión general de los riesgos de seguridad digital que pueden afectar la seguridad y privacidad de la información, donde se podrán establecer controles y medidas efectivas, viables y transversales con el propósito de realizar el aseguramiento de la disponibilidad, integridad y confidencialidad tanto de la información del negocio como de los datos de los servidores públicos, contratistas y partes interesadas. Es indispensable que el instituto realice una adecuada identificación, clasificación, valoración, gestión y tratamiento de los riesgos de seguridad digital que puedan afectar la información de la entidad, con el propósito de implementar medidas y controles efectivos que permitan estar preparados ante situaciones en las que se vea comprometida tanto la seguridad física y lógica de sus instalaciones, personas, recursos y sistemas, como la seguridad de su información.

Teniendo en cuenta lo anterior, la presente política tiene como finalidad de establecer los principios orientadores en seguridad que buscan garantizar la disponibilidad, integridad, confidencialidad, privacidad, continuidad, autenticidad y no repudio de la información del IPSE, así como dar lineamientos para la aplicación de mecanismos que eviten la vulneración de la seguridad y privacidad de la información, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información – SSGSI.


Por consiguiente la seguridad de la información es para el Instituto, una labor prioritaria que anima a todos a velar por el cumplimiento de las directrices establecidas en el presente documento.

1. OBJETIVO

Establecer lineamientos necesarios, con el fin de fortalecer la gestión de Seguridad y privacidad de la Información del IPSE, enmarcados en la implementación de un Sistema de Gestión de Seguridad de la Información, basado en la identificación y valoración de los riesgos asociados a ella, propendiendo por la protección de su confidencialidad, integridad, disponibilidad, privacidad, continuidad y autenticidad.

2. ALCANCE

Los lineamientos contenidos en la presente política son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los servidores públicos, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con el IPSE a través de la recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, con personal interno o externo, en el desarrollo de la misión institucional y el cumplimiento de sus objetivos estratégicos.

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Paginas
		15-09-2022	Pág. 5 de 36

3. DEFINICIONES

Activo: Se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tienen un valor para la Instituto.

Activo crítico: Instalaciones, sistemas y equipos los cuales, si son destruidos, o es degradado su funcionamiento o por cualquier otro motivo no se encuentran disponibles, afectarán el cumplimiento de los objetivos estratégicos del IPSE.

Administración de Riesgos: Se entiende por administración de riesgos, como el proceso de identificación, control, minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar la información o impactar de manera considerable la operación. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.

Análisis de Impacto al Negocio (BIA): Es una metodología que permite identificar los procesos críticos que apoyan los productos y servicios claves, las interdependencias entre procesos, los recursos requeridos para operar en un nivel mínimo aceptable y el efecto que una interrupción del negocio podría tener sobre ellos.

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Alta Dirección: Persona o grupo de personas que dirigen y controlan al más alto nivel una entidad (ministro, viceministros, secretaria general y direcciones).

Centro de cableado: El centro de cableado es el lugar donde se ubican los recursos de comunicación de tecnologías de información, como (Switch, patch, panel, UPS, Router, Cableado de voz y de datos).

Cifrado: Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

Control: Son todas aquellas políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.


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

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

Código malicioso: Es un código informático que crea brechas de seguridad para dañar un sistema informático.

Custodio: Es una parte designada de la entidad, un cargo o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación de privilegios de acceso, modificación y borrado.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o a varias personas naturales determinadas o determinables. Debe entonces entenderse el "dato personal" como una información relacionada con una persona natural (persona individualmente considerada).

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Páginas
		15-09-2022	Pág. 6 de 36

Dato personal público: Toda información personal que es de conocimiento libre y abierto para el público en general.

Dato personal privado: Toda información personal que tiene un conocimiento restringido, y en principio privado para el público en general.

Dato semiprivado: Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general.

Datos 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.

Datacenter: Se denomina también Centro de Procesamiento de Datos (CPD) a aquella ubicación o espacio donde se concentran los recursos necesarios (TI) para el procesamiento de la información de una organización.

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

Dispositivos móviles: Equipo celular Smartphone, equipos portátiles, tablets, o cualquiera cuyo concepto principal sea la movilidad, el cual permite almacenamiento limitado, acceso a internet y cuenta con capacidad de procesamiento.

Evento: Es el suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Home Office: Oficina en casa o trabajo en casa

Incidente de Seguridad: Evento o serie de eventos de seguridad de la información no deseada o inesperada, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.


Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Impacto: Resultado de un incidente de seguridad de la información.

Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la entidad

Mesa de Servicios: Constituye el único punto de contacto con los usuarios finales para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Es a través de la gestión proactiva de la Mesa de Servicios que el Proceso TIC recolecta las necesidades que tienen dependencias en cuanto a los recursos tecnológicos.

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Páginas
		15-09-2022	Pág. 7 de 36

No repudio: El emisor no puede negar que envió porque el destinatario tiene pruebas del envío. El receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor pueda negar tal envío.

Partes interesadas: Persona u organización que puede afectar o ser afectada o percibirse a sí misma como afectada por una decisión o actividad.

Plan de Continuidad de Negocio: Actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles predefinidos después de un incidente que afecte la continuidad de las operaciones.

Privacidad de la información: El derecho que tienen todos los titulares de la información, que involucre datos personales y la información clasificada que estos hayan entregado, o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de Gobierno Digital, la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Propietario de la información (titular): Es la unidad organizacional o proceso donde se crean los activos de información.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales. Conjunto de aplicaciones que interactúan entre sí para apoyar un área o proceso del IPSE.

Terceros: Personas naturales o jurídicas que tienen un contrato tercerizado y prestan un servicio a la entidad y hacen uso de la información y los medios tecnológicos dispuestos por la entidad.

Test de penetración: Es un ataque dirigido y controlado hacia componentes de infraestructura tecnológica para revelar malas configuraciones y vulnerabilidades explotables.

VPN: Red virtual privada por sus siglas en inglés Virtual Private Network.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

4. MARCO LEGAL


Constitución Política de Colombia. Artículo 15.

Ley 44 de 1993: Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).

Ley 527 de 1999: Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 594 de 2000: Por medio de la cual se expide la Ley General de Archivos.

Ley 850 de 2003: Por medio de la cual se reglamentan las veedurías ciudadanas

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Paginas
		15-09-2022	Pág. 8 de 36

Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del Habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1341 de 2009: Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones – TIC, se crea la agencia Nacional de espectro y se dictan otras disposiciones.

Resolución 500 marzo 10 2021 Política Gobierno Digital Mintic

Ley 1437 de 2011: Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.

Ley 1474 de 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.

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

Ley 1915 de 2018: Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

Ley 1952 de 2019: Por medio de la cual se expide el código general disciplinario

Decreto 2609 de 2012: Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

Decreto 0884 del 2012: Por el cual se reglamenta parcialmente la Ley 1221 del 2008. **Decreto 1377**

de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012. **Decreto 886 de 2014:** Por el

cual se reglamenta el Registro Nacional de bases de Datos.


Decreto 103 de 2015: Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

Decreto 1074 de 2015: Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

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

Decreto 1080 de 2015: Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.

Decreto 1081 de 2015: Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Paginas
		15-09-2022	Pág. 9 de 36

Resolución 512 de 2019: Por la cual se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información.

CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.

CONPES 3854 de 2016. Política Nacional de Seguridad digital.

5. POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

El IPSE, en cumplimiento de sus funciones y entendiendo la importancia de una adecuada gestión de la información, se ha comprometido a proteger, preservar y administrar la confidencialidad, integridad, disponibilidad y no repudio de la información de la Entidad, mediante una gestión integral de riesgos, implementación de controles físicos y digitales, previniendo incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua.

Para asegurar la dirección estratégica del IPSE se establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información así:

- ✓ Implementar,
- ✓ operar y mejorar de forma continua el Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.
- ✓ Minimizar el riesgo de vulnerabilidad en la seguridad de la información en la ejecución de los procesos misionales de la entidad.
- ✓ Cumplir con los principios (Disponibilidad, Integridad y Confidencialidad) de seguridad de la información.
- ✓ Mantener la confianza de los servidores públicos, colaboradores y terceros.
- ✓ Apoyar la innovación tecnológica.
- ✓ Proteger los activos de información.
- ✓ Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- ✓ Fortalecer la cultura de seguridad de la información en los servidores públicos, colaboradores y terceros, que hacen parte del IPSE.
- ✓ Verificar de manera periódica el cumplimiento de las políticas de seguridad de la información.
- ✓ Propender para que todos los servidores públicos, contratistas y terceros cumplan con las políticas, lineamientos, y buenas prácticas de seguridad de la información establecidas en la Política de Seguridad de la Información.


6. POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

6.1 POLITICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.1.1 ORGANIZACIÓN INTERNA

Lineamientos:

- a. Los activos de información deben estar custodiados por el responsable del activo, para evitar conflicto y reducir oportunidades de modificación (intencional o no), no autorizada o mal uso de los activos de información del IPSE.
- b. El proceso de gestión de TIC debe mantener y documentar los contactos con autoridades (policía, fiscalía, csirt etc.) u otros especializados, con el fin de contactar en caso de que se presente un incidente de seguridad de la información y requiera de

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Paginas
		15-09-2022	Pág. 10 de 36

asesoría externa.

- c. El IPSE a través de Proceso TIC y demás personal que se determine, debe mantener contacto con grupos de interés especializados en seguridad y privacidad de la información, con el fin de compartir e intercambiar conocimientos que permita la mejora continua del Sistema de Gestión de Seguridad de la Información del IPSE.
- d. Los proyectos que se desarrollen en el IPSE deben contemplar una gestión de los riesgos de seguridad asociados a la información del proyecto, lo cual incluye una identificación de los riesgos y la definición de la forma como serán gestionados.
- e. En cualquier caso, los proyectos desarrollados por el IPSE deben estar alineados a la directriz en seguridad contenidos en la presente política.

6.1.2 DISPOSITIVOS MOVILES


Lineamientos:

- a. El IPSE se reserva el derecho de autorizar o denegar el acceso al servicio de acuerdo con las condiciones de seguridad que se detecten en el dispositivo.
- b. Proceso TIC, debe mantener un inventario actualizado de los dispositivos móviles autorizados.
- c. Los dispositivos móviles de propiedad de los Servidores Públicos, Contratistas, o terceros no deben estar incluidos en el dominio ipse.gov.co o cualquiera que funcione dentro del IPSE, para conectarse a los servicios de la red de datos deberán realizar solicitud a la mesa de servicios y cumplir con los lineamientos referentes a seguridad de la información.
- d. Todos los dispositivos móviles que almacenen información del IPSE deben tener instalado un software antivirus y un sistema operativo actualizado.
- e. En dispositivos móviles entregados por el IPSE, los Servidores Públicos no están autorizados a cambiar la configuración, a desinstalar software, formatear o restaurar de fábrica.
- f. En caso de pérdida o robo de un dispositivo móvil de propiedad del IPSE, los Servidores Públicos, tendrá que realizar la respectiva denuncia ante la entidad competente, luego debe dar aviso inmediato al personal de la Mesa de Servicio, quienes deben realizar las acciones necesarias para la protección de la información.

6.1.3 TRABAJO NO PRESENCIAL

Lineamientos:

- a. Proceso TIC debe establecer los requerimientos para autorizar conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las funciones de los servidores públicos, contratistas del IPSE, garantizando las herramientas y controles para proteger la confidencialidad, integridad y disponibilidad de las conexiones remotas.
- b. Toda información gestionada por el IPSE, y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo y/o de las obligaciones contractuales.

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Páginas
		15-09-2022	Pág. 11 de 36

POLITICA DE SEGURIDAD DEL TALENTO HUMANO ANTES DE ASUMIR EL EMPLEO:

Lineamientos

- a. La coordinación de Talento Humano, debe contar con procedimientos para la vinculación de personal, de acuerdo a la normatividad establecida para tal fin.
- b. Gestión Contractual, debe definir una lista de verificación que contenga los aspectos necesarios para la revisión de los antecedentes del personal a contratar por prestación de servicios de acuerdo con la normatividad vigente.
- c. Coordinación de Talento Humano y Gestión Contractual, deben establecer mecanismos o controles necesarios para proteger la confidencialidad y reserva de la información contenida en las historias laborales y expedientes contractuales.
- d. Todo Servidor Público o contratista, debe firmar un documento o cláusulas en las que se establezcan acuerdo de confidencialidad y no divulgación de la información reservada del IPSE, estos deben reposar en la historia laboral o expediente contractual según sea el caso.

6.1.4 DURANTE LA EJECUCIÓN DEL EMPLEO:


Lineamientos

- a. Los Servidores Públicos y Contratistas deben suscribir la autorización para el tratamiento de los datos personales de acuerdo con la Política de tratamiento de datos personales del IPSE y de acuerdo con lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios.
- b. Proceso TIC y el personal de apoyo que se requiera, debe diseñar y ejecutar de manera permanente, un programa de concientización en seguridad de la información, con el fin de apoyar la protección adecuada de la información.
- c. Proceso TIC en conjunto con el área de Comunicaciones deben diseñar y ejecutar un plan de Uso y apropiación de comunicaciones en apropiación del Sistema de Gestión de la Seguridad de la Información - SGSI, el cual se debe ejecutar durante la vigencia al interior del IPSE.
- d. Es responsabilidad del Servidor Público, contratista o personal provisto por terceros, informar de los incidentes de seguridad de la información a través de los medios dispuestos por Proceso TIC
- e. En lo pertinente al incumplimiento de las políticas de la seguridad de la información, se aplicará lo establecido en los procedimientos destinados para tal fin, enmarcados en la normatividad vigente.

6.1.5 TERMINACIÓN Y CAMBIO DE EMPLEO

Lineamientos

- a. Es responsabilidad del Servidor Público realizar la entrega de la información propia del IPSE, que se encuentra bajo su custodia, cuando exista una novedad de retiro, investigación, inhabilidades o cambio de funciones.
- b. El supervisor del contrato o a quien este delegue debe recoger y custodiar la información del IPSE bajo la responsabilidad

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Páginas
		15-09-2022	Pág. 12 de 36

del contratista en caso de terminación anticipada, definitiva, temporal o cesión del contrato.

- c. Proceso TIC debe parametrizar en el directorio activo, la inactivación automática de los contratistas, teniendo en cuenta la fecha de terminación del contrato; la inactivación de los usuarios de los sistemas de información que no se autentican con el directorio activo, se debe hacer de forma manual.
- d. La coordinación de Talento Humano debe informar al proceso de gestión TIC, a través de la Mesa de Servicios o canal dispuesto para tal fin, cualquier novedad de desvinculación administrativa, laboral o contractual del Servidor Público, contratista o tercero; una vez notificada la novedad el Proceso de Gestión de TIC, debe proceder a la inactivación de los y servicios accesos y servicios de red del Servidor Público, contratista o tercero
- e. Se creará una copia de respaldo del buzón de correo electrónico una vez se dé por terminada la vinculación con el IPSE.
- f. Bajo ningún parámetro se podrán restablecer los accesos a correos electrónicos; solo se podrán restablecer buzones para consulta y no se podrán emitir correos ni notificaciones desde estos buzones.
- g. Se deben inactivar todos los accesos a los sistemas de información.
- h. Se debe solicitar la devolución del carné, tarjeta de proximidad o cualquier distintivo de autenticación, que lo acredita como Servidor Público, contratista o tercero del IPSE.

6.2 POLITICA DE GESTIÓN DE ACTIVOS

- **RESPONSABILIDAD POR LOS ACTIVOS**


Lineamientos

- a. Todos los procesos del IPSE deben contar con un inventario de sus activos de información y se debe evidenciar a través de los instrumentos dispuestos.
- b. Todos los activos de información mantenidos en el inventario deben tener un responsable.
- c. Proceso de Gestión de TIC, debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información.
- d. Los servidores públicos, contratistas o terceros, no deben usar software no autorizado o de su propiedad en los activos del IPSE.
- e. Los servidores públicos, contratistas o terceros del IPSE, deben hacer entrega de los activos bajo su responsabilidad de acuerdo con el formato de paz y salvo del área respectiva.

- **CLASIFICACIÓN DE LA INFORMACIÓN**

Lineamientos

- a. Las Tablas de Retención Documental (TRD) deben indicar el tipo de clasificación de las series, subseries y documentos en ella contenidas.
- b. Los servidores públicos, contratistas o terceros del IPSE deben aplicar la clasificación de la información en, las TRD, el inventario de activos de información y lineamientos para la administración de los archivos.

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Paginas
		15-09-2022	Pág. 13 de 36

- c. Cada propietario del activo de Información debe velar por el cumplimiento de su clasificación de acuerdo con lo establecido en lineamientos para la administración de los archivos y activos de Información
- d. Para el intercambio de información se debe tener en cuenta su clasificación para su debida protección en términos de confidencialidad.

- **MANEJO DE MEDIOS**

Lineamientos


- a. Proceso de Gestión de TIC debe definir un procedimiento para el uso de medios removibles.
- b. Proceso de Gestión de TIC, debe proveer a los usuarios del IPSE los métodos de cifrado de la información, así como administrar el software o herramienta utilizada para tal fin, y generar la guía de uso para el usuario.
- c. Todo medio removible debe ser escaneado mediante las soluciones de seguridad, suministrado por Proceso TIC cada vez que se conecte a un equipo del IPSE.
- d. Es responsabilidad de cada servidor público, contratista o tercero tomar las medidas para la protección de la información contenida en medios removibles, para evitar acceso físico y lógico no autorizado, daños, pérdida de información o extravío del mismo.
- e. Se prohíbe el uso de medios removibles que contengan información reservada o clasificada del IPSE
- f. Proceso de Gestión de TIC, debe generar y aplicar lineamientos para la disposición segura de los dispositivos que almacenen información de la entidad, ya sea cuando son dados de baja o asignados a un nuevo usuario.
- g. Proceso de Gestión de TIC, debe autorizar el uso de periféricos o medios de almacenamiento externo, de acuerdo con las necesidades requeridas para el cumplimiento de las funciones y del perfil del cargo de los servidores públicos o Contratistas.
- h. Los servidores públicos, Contratistas o personal provisto por terceras partes deben acoger las condiciones de uso de periféricos y medios de almacenamiento establecidos por Proceso TIC.
- i. Se deben emplear herramientas de borrado seguro y demás mecanismos de seguridad pertinentes en los medios de propiedad del IPSE que sean reutilizados o dados de baja, con el fin de controlar que la información del IPSE contenida en estos medios no se pueda recuperar.
- j. El transporte para los medios de almacenamiento debe contar con las condiciones apropiadas para salvaguardar la integridad, confidencialidad y disponibilidad de la información del IPSE.

6.3 POLITICA CONTROL DE ACCESOS

- **REQUISITOS DE LA ENTIDAD PARA EL CONTROL DE ACCESO**

Lineamientos:

- a. Proceso de Gestión de TIC, debe suministrar y garantizar el cambio de contraseña, a los usuarios las credenciales para el

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Paginas
		15-09-2022	Pág. 14 de 36


acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, según su perfil y rol, las credenciales de acceso son de uso personal e intransferible.

- b. La conexión remota a la red de área local del IPSE debe establecerse a través de una conexión VPN, la cual debe ser aprobada, registrada y monitoreada por Proceso TIC.
- c. Proceso de Gestión de TIC, debe establecer una segregación de las redes, separando los entornos de red de usuarios de los entornos de red de servidores y servicios publicados.
- d. Proceso de Gestión de TIC, debe asegurar que las redes inalámbricas de la Entidad cuenten con métodos de autenticación que evite accesos no autorizados.
- e. Proceso de Gestión de TIC, debe realizar el cambio de contraseña de la red inalámbrica de la Entidad mínimo tres (3) veces al año.
- f. Proceso de Gestión de TIC, para los eventos que se realicen en la Entidad debe generar usuario y clave de red Wifi, el cual debe expirar una vez finalizado el evento
- g. Proceso de Gestión de TIC, debe revisar que los equipos personales de los Servidores Públicos, contratistas o terceros del IPSE que se conecten a las redes de datos del IPSE cumplan con todos los requisitos o controles para autenticarse y únicamente podrán realizar las tareas para las que fueron autorizados.

- **GESTIÓN DE ACCESO DE USUARIOS**

Lineamientos:

- a. Proceso de Gestión de TIC, debe definir un procedimiento que contemple la creación, actualización, activación e inactivación de cuentas de usuario.
- b. Proceso de Gestión de TIC, sólo otorgará a los usuarios, los accesos solicitados y autorizados por el jefe inmediato, supervisor del contrato o un jefe de mayor jerarquía.
- c. Por defecto los usuarios creados no tienen permisos de administrador. En caso de requerirlo deben realizar la solicitud herramienta de mesa de servicios. Sólo se otorgan los privilegios para la administración de recursos tecnológicos, servicios de red, sistemas operativos y sistemas de información a aquellos usuarios que cumplan dichas actividades.
- d. El usuario y la contraseña asignados para el acceso a los diferentes servicios tecnológicos, es personal e intransferible. Cualquier actividad que se realice con el usuario y clave será responsabilidad del servidor público y contratista al cual le fue asignado.
- e. Proceso de Gestión de TIC, debe garantizar que las estaciones de trabajo con perfil de administrador local sean las que estén autorizadas, en caso contrario se debe modificar el permiso en la configuración de la estación de trabajo.
- f. Una vez finalizada la gestión de servicios prestados por terceras partes para la Entidad, el supervisor de contrato debe garantizar que los accesos queden cerrados al finalizar el proceso o contrato.
- g. Proceso de Gestión de TIC,, con el apoyo de mesa de servicios, debe garantizar que los usuarios, realicen el cambio de contraseña de acceso a los servicios del IPSE, cada vez que sea requerido.

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Páginas
		15-09-2022	Pág. 15 de 36

- h. La contraseña para la autenticación se debe suministrar a los usuarios de manera segura y el sistema debe solicitar el cambio inmediato de la misma al ingresar.
- i. Proceso de Gestión de TIC, debe establecer controles para que los usuarios finales de los servicios tecnológicos no tengan instalado en sus equipos de cómputo software o herramientas que permitan la obtención de privilegios no autorizados.

- **RESPONSABILIDADES DE LOS USUARIOS**


Lineamientos:

- a. Proceso de Gestión de TIC, debe garantizar que para el ingreso a los servicios tecnológicos de la entidad las contraseñas no sean visibles en texto claro.
- b. Las contraseñas deben poseer algún grado de complejidad y no deberán ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por tanto:
 - Debe cambiarse obligatoriamente cada 45 días de lo contrario la contraseña caducará y obligará su cambio.
 - Después de tres (3) intentos fallidos de ingreso de la contraseña el usuario se bloquea de manera inmediata y deberá esperar un tiempo determinado de dos (2) minutos para volver a intentar, o solicitar el desbloqueo a través de la Mesa de Servicios.
 - Debe cambiarse la contraseña si se ha detectado anomalía en la cuenta de usuario.
 - No ser visible en la pantalla, al momento de ser ingresada.
 - No se debe registrar en papel, correo electrónico, archivos digitales a menos que se puedan almacenar de forma segura y el método de almacenamiento debe estar aprobado por Proceso TIC.
- c. Los administradores de los servicios tecnológicos deben cumplir con los lineamientos de contraseñas seguras indicadas.
- d. Los administradores de los servicios tecnológicos o Sistema de Información deben entregar de manera adecuada las credenciales de acceso.

6.3.1 CONTROL DE ACCESOS A SISTEMAS Y APLICACIONES

Lineamientos:

- a. Proceso de Gestión de TIC, debe establecer ambientes separados a nivel físico y lógico para el desarrollo-pruebas y producción; contando con su plataforma, servidores, aplicativos, dispositivos y versiones independientes de los otros ambientes, para evitar así que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad, confidencialidad y disponibilidad de la información de los servicios en producción.
- b. , roceso de Gestión de TIC debe asegurar mediante los controles necesarios, que los usuarios utilicen diferentes cuentas de usuario para los ambientes pruebas y producción y así mismo que los menús muestren los mensajes de identificación apropiados para reducir el riesgo de error.

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Páginas
		15-09-2022	Pág. 16 de 36

- c. Los desarrolladores deben asegurar que no se desplieguen en pantalla las contraseñas ingresadas.
- d. Los desarrolladores deben, a nivel de los aplicativos, restringir el acceso a archivos u otros recursos, a direcciones URL protegidas, a funciones protegidas, a servicios, a información de las aplicaciones, a atributos y políticas utilizadas para los controles de acceso y a la información relevante de la configuración, solamente a usuarios autorizados.

6.4 POLITICA SEGURIDAD PARA EL USO DE RECURSOS CRIPTOGRÁFICOS.

CONTROLES RIPTOGRÁFICOS


Lineamientos:

- a. Proceso de Gestión de TICS, debe gestionar los controles criptográficos para protección de claves de acceso a sistemas, datos y servicios.
- b. Proceso de Gestión de TICS, debe verificar que todo sistema de información que requiera realizar transmisión de información clasificada o reservada cuente con mecanismos de cifrado de datos.
- c. Proceso de Gestión de TICS, en cabeza de los proveedores de desarrollo de software deben asegurar que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos por el IPSE.
- d. Proceso de Gestión de TICS, debe disponer de herramientas que permitan el cifrado de medios de almacenamiento de información.

POLITICA FIRMA DIGITAL

Lineamientos:

- a. Proceso de Gestión de TICS, establece los lineamientos necesarios para el control y el uso de las firmas digitales para el IPSE.
- b. Toda solicitud de asignación de firma digital se realiza a través de la mesa de servicios del IPSE, para el caso de usuarios nuevos, esta debe ser solicitada a través del formato de gestión de cuentas y servicios informáticos correspondiente.
- c. Los servidores públicos y contratistas deben firmar el documento de "Acuerdo sobre uso del mecanismo de firma digital"
- d. Los servidores públicos y contratistas, que realicen actividades para el IPSE y tengan a su cargo una firma digital, deben hacer buen uso de esta de acuerdo a lo establecido en el Instructivo de Firma Digital correspondiente.
- e. Los Servidores Públicos y contratistas que se les haya asignado firma digital, deben hacer uso de esta para el desarrollo de sus actividades, así mismo gestionar la renovación del certificado de la firma, cuando este próxima a vencer.
- f. Todos los documentos firmados digitalmente son auténticos se tomarán como originales y finales. Adicional cumplen con los criterios de seguridad de la información de integridad, confidencialidad, y disponibilidad.
- g. En caso de presentarse o identificar algún incidente de seguridad de la información relacionada con el uso de la firma digital, el usuario debe reportarlo tan pronto como sea posible, a través de la mesa de servicios del IPSE.
- h. Es responsabilidad del usuario hacer buen uso de los servicios tecnológicos donde se pretenda usar la firma digital.

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Páginas
		15-09-2022	Pág. 17 de 36


- i. En caso de que tenga dudas debe informar a la mesa de servicios del IPSE para realizar la respectiva revisión.
- j. Los servidores públicos y contratistas que realicen actividades para el IPSE y se les haya asignado un certificado de firma digital, son responsables de la seguridad de los dispositivos que utilicen para firmar los documentos.
- k. El certificado asignado es personal e intransferible, por lo cual es responsabilidad del usuario los documentos que firme.
- l. Los documentos que son firmados con la solución de firma digital del IPSE, deben ser validados digitalmente y su custodia debe estar en un repositorio institucional destinado para tal fin, de acuerdo a la ley 527 de 1999 “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones y el decreto 2364 de 2012 “Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones”.
- m. El usuario debe comprobar la información que va a firmar, es decir, antes de realizar la firma el usuario debe comprobar que está de acuerdo con el contenido que va a firmar en las condiciones o contexto en el que se realiza la firma.

6.5 POLITICA SEGURIDAD FÍSICA Y DEL ENTORNO

6.5.1 ÁREAS SEGURAS

Lineamientos

- a. Gabys y el GGSST debe señalar las áreas seguras de acuerdo con el inventario de áreas seguras.
- b. Las puertas y ventanas de las áreas seguras deben permanecer cerradas y bloqueadas cuando no haya supervisión o estén desocupadas.
- c. Todos los puntos de acceso deben tener un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o instalación.
- d. Gabys y el GGSST debe establecer un sistema de control de acceso a las instalaciones del IPSE, así como a las áreas seguras.
- e. El personal de vigilancia debe establecer mecanismos para inspeccionar y examinar los morrales, bolsos, cajas, etc. que ingresen los Servidores Públicos y Contratistas o visitantes.
- f. Proceso de Gestión de TICS,, deben controlar el ingreso a los centros de datos y centros de cableado del IPSE.
- g. Proceso de Gestión de TICS,, autorizan el ingreso a personal ajeno al IPSE a los centros de datos y centros de cableado, este debe estar acompañado por quien sea autorizado, éste se hará responsable de la estadía del personal ajeno al IPSE durante el tiempo que permanezca en las instalaciones.
- h. Gabys con acompañamiento de Proceso TIC es responsable de la identificación y organización del cableado estructurado desde los puestos de trabajo hasta los paneles de conexión (patch panel) de los centros de cableado.
- i. Proceso TIC debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia, monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas deben monitorearse de manera permanente.


	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Paginas
		15-09-2022	Pág. 18 de 36

- j. Proceso de Gestión de TICS, debe velar por que los recursos de la plataforma tecnológica de la Entidad ubicado en el centro de cómputo se encuentren protegidos contra fallas o interrupciones eléctricas.
- k. Proceso de Gestión de TICS, con el apoyo de GABYS, debe certificar que el centro de cómputo y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran el riesgo de inundaciones e incendios.
- l. La Dirección de Talento Humano y Proceso TIC establecen los lineamientos para los controles contra amenazas externas y ambientales y quedarán enmarcadas en los planes de contingencia, de emergencia y de continuidad del negocio.
- m. Proceso de Gestión de TICS, debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado.
- n. Proceso TIC debe realizar mantenimientos preventivos al centro de cómputo y centros de cableado que estén bajo su custodia; así mismo, se debe llevar el control al plan de mantenimiento de servicios tecnológicos.
- o. Las puertas del centro de cómputo deben permanecer cerradas.
- p. En el centro de cómputo y centro de cableado está prohibido: (Fumar, Ingresar comidas o bebidas, el porte de armas de fuego, corto punzantes o similares, Mover, desconectar y/o conectar equipos sin autorización, Modificar la configuración del equipo o interconectarlo sin autorización, Alterar software instalado en los equipos sin autorización, Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas, Extraer información de los equipos en dispositivos externos sin previa autorización)
- q. Proceso de Gestión de TICS, debe velar por que los cables de potencia estén separados de los de comunicaciones siguiendo las normas técnicas pertinentes.
- r. Proceso TIC debe controlar el acceso de visitantes a los centros de cómputo y centros de cableado que estén bajo su custodia.

6.5.2 EQUIPO

Lineamientos

- a. Gabys y Proceso TIC velarán que los equipos de cómputo, escáneres e impresoras estén situados y protegidos en áreas para reducir el riesgo contra amenazas ambientales y de acceso no autorizado.
- b. Gabys y Proceso TIC, debe propender que los equipos de cómputo portátiles suministrados por el IPSE se protejan mediante mecanismos que no permitan su pérdida.
- c. Gabys y Proceso TIC establece los lineamientos para el uso de la red de energía regulada en los puestos de trabajo en los cuales solo se deben conectar equipos como computadores de escritorio, portátiles y pantallas; los otros elementos deben conectarse a la red eléctrica no regulada.
- d. Gabys y Proceso TIC debe proteger el cableado que transporta voz, datos y suministro de energía eléctrica contra la interceptación, interferencia o daños de cualquier tipo dentro del perímetro del IPSE.
- e. Gabys y Proceso TIC debe definir mecanismos para que los cables de energía eléctrica deben estar separados de los cables de comunicaciones para evitar interferencia y ruido.

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Páginas
		15-09-2022	Pág. 19 de 36


- f. Proceso de Gestión de TICS, debe definir mecanismos de soporte y mantenimiento a los equipos de cómputo, servidores y equipos activos de red y debe llevar registro de estos.
- g. Cuando un equipo o medio extraíble sea reasignado o retirado de servicio, Proceso TIC debe garantizar la eliminación de toda información mediante mecanismos de borrado seguro teniendo en cuenta que previo a esta actividad debe realizarse una copia de seguridad de esta.
- h. Cuando aplique, los servidores públicos, contratista o terceros que tengan asignado un equipo portátil propiedad del IPSE deben asegurarlo mediante una guaya de seguridad. El código de seguridad deberá ser entregado a la mesa de servicios una vez termine su vínculo contractual con la entidad.
- i. Es responsabilidad de los usuarios registrar el ingreso o salida de los equipos portátiles ya sean propios o de la entidad.
- j. Cuando aplique el personal de seguridad y vigilancia de cada piso de las instalaciones del IPSE tendrá la potestad de recoger y entregar a Gabys los equipos que se encuentren sin su respectiva guaya de seguridad, en el caso de que el responsable del equipo se encuentre ausente.
- k. Proceso de Gestión de TICS, debe configurar como política general que todos los equipos de cómputo que se encuentren en los dominios del IPSE bloqueen automáticamente su sesión después de (5) cinco minutos de inactividad
- l. Los servidores públicos, contratista o terceros del IPSE, durante su ausencia no deben conservar sobre el escritorio información propia del IPSE como: documentos físicos o medios de almacenamiento, por lo tanto, se requiere guardar en un lugar seguro para impedir su pérdida, daño, copia o acceso por parte terceros o personal que no tenga autorización para su uso o conocimiento.
- m. Los servidores públicos, contratista o terceros del IPSE, deben bloquear la pantalla del computador a su cargo cuando se ausenten de su puesto de trabajo, para impedir el acceso de terceros no autorizados a la información almacenada en el equipo de cómputo.
- n. Los Servidores Públicos, contratista o terceros que impriman documentos con clasificación (Clasificada – Reservada), estos deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sincustodia.
- o. No se debe reutilizar documentos impresos con clasificación (Clasificada – Reservada), estos deben ser destruidos y no deben estar como papel reciclable.

6.6 POLITICA SEGURIDAD DE LAS OPERACIONES

- **PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES**

Lineamientos

- a. Proceso de Gestión de TICS, con el apoyo de la Oficina de Planeación debe documentar y mantener actualizados todos sus procedimientos operativos paragarantizar la disponibilidad, integridad y confidencialidad de la información.
- b. Proceso de Gestión de TICS, debe documentar la gestión de capacidad de la plataforma tecnológica, definir su responsable y mantenerla actualizada
- c. Proceso de Gestión de TICS, debe velar por la capacidad de procesamiento requerida en los recursos tecnológicos de la

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Páginas
		15-09-2022	Pág. 20 de 36

información de la entidad.

- d. Proceso de Gestión de TICS, debe realizar las tareas de optimización de servicios tecnológicos y sistemas de información, al igual que la verificación de capacidad de los servicios de red de la entidad.
- e. Proceso de Gestión de TICS, debe garantizar que todo cambio que se deba realizar en los sistemas información en producción deba ser probados en un ambiente de pruebas antes de aplicarlos a los sistemas en producción, de acuerdo a la metodología de desarrollo del instituto.


- **PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS**

Lineamientos

- a. Proceso de Gestión de TICS, debe definir y documentar los controles para la detección, prevención y recuperación contra códigos maliciosos. Además, proporcionará los mecanismos para generar cultura de seguridad entre los servidores públicos, contratistas y terceros frente a los ataques de software malicioso.
- b. Proceso de Gestión de TICS, debe contar con herramientas tales como antivirus, antimalware, antispam y antispysware que reduzcan el riesgo de contagio de software malicioso
- c. Proceso de Gestión de TICS, debe asegurar que el software de antivirus, antimalware, antispysware y antispam cuente con las licencias de uso requeridas, certificando su autenticidad y la posibilidad de actualización periódica.
- d. Proceso de Gestión de TICS, debe velar por que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.
- e. Proceso de Gestión de TICS,, debe asegurar que no se pueda realizar cambios en la configuración del software de antivirus, antispysware, antispam y antimalware.
- f. Proceso de Gestión de TICS, debe velar que el software de antivirus, antispysware, antispam y antimalware posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.
- g. Los servidores públicos, contratista o terceros del IPSE, deben abstenerse de abrir o ejecutar archivos y/o documentos de fuentes desconocidas, especialmente los que se encuentran en medios de almacenamiento externo o que provienen de correos electrónicos desconocidos.
- h. Los servidores públicos, contratista o terceros del IPSE no deben descargar archivos de internet de fuentes desconocidas, en caso de requerirlo, debe generar la solicitud a Proceso TIC a través de la mesa de servicios.
- i. Los servidores públicos, contratista o terceros del IPSE que sospechen o detecten alguna infección por software malicioso deben notificar de inmediato a Proceso TIC a través de la mesa de servicios, con el fin de ejercer los controles correspondientes.

- **COPIAS DE RESPALDO**

Lineamientos


	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Paginas
		15-09-2022	Pág. 21 de 36

- a. Proceso de Gestión de TICS, debe definir y documentar un plan o procedimiento de copias de respaldo y restauración de la información del IPSE, donde se establezca el esquema, de qué, cómo, quién, con qué periodicidad, tipo de respaldo y nivel de criticidad.
- b. Proceso de Gestión de TICS,, velará por que los medios magnéticos que contienen lainformación sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con las seguridades físicas y medioambientales apropiadas.
- c. Proceso de Gestión de TICS, debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.
- d. Proceso de Gestión de TICS, debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.
- e. Proceso de Gestión de TICS, debe proporcionar los lineamientos para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de los activos de información de la entidad.
- f. Proceso TIC debe velar por que el software de respaldo esté instalado en las estaciones de trabajo y servidores para los cuales sea necesario la realización de Backup. Se debe contar con las licencias necesarias para garantizar continuidad en el proceso.
- g. Proceso de Gestión de TICS, debe garantizar el almacenamiento del respaldo de la información de los usuarios, por lo menos un año antes de su envío a Gestión Documental.
- h. Es responsabilidad de los procesos dueños de las aplicaciones, definir la frecuencia de la generación de copiasde respaldo adicionales a las definidas por Proceso TIC
- i. Es responsabilidad de los servidores públicos, contratistas y terceros del IPSE, guardar la información crítica de sus funciones en unidades de almacenamiento destinadas para tal fin, garantizando su respaldo.
- j. Es responsabilidad de los servidores públicos, contratistas y terceros del IPSE, guardar la información para el desarrollo de sus funciones, en la carpeta "DATOS IPSE" en sus estaciones de trabajo. La información que no se aloje en esta carpeta no se respaldará y cualquier pérdida de esta será responsabilidad del usuario.
- k. Los servidores públicos, contratistas y terceros son responsables de hacer buen uso de los servicios tecnológicos del IPSE y en ningún momento pueden ser usados para beneficio propio o para realizar prácticas ilícitas o mal intencionadas que atenten contra otros Servidores Públicos, contratistas y terceros,
- l. Por ningún motivo se permite alojar en servidores información catalogada como personal, música, videos, etc.
- m. Proceso de Gestión de TICS, garantizará el respaldo de los archivos con extensión .pdf .doc. docm, .docx, .dot, .dotm .xls, .xlsm, .xlsx, .xlt, .xltm, .xltx, .bmp, .gif, .jpg, .odp, .png, .pot, .potm, .potx, .pps, .ppt, .pptm, .jpeg.

- **REGISTRO DE EVENTOS Y SEGUIMIENTO**

Lineamientos

- a. Proceso de Gestión de TICS, debe generar registros de auditoría que permita verificar y hacer seguimiento a las

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Páginas
		15-09-2022	Pág. 22 de 36

excepciones o eventos relacionados a la seguridad en los sistemas de información que se consideren.

- b. Proceso de Gestión de TICS, debe salvaguardar los registros de auditoría que se generen de cada sistema.
- c. Proceso de Gestión de TICS, debe monitorear excepciones o los eventos de la seguridad de información.
- d. Proceso de Gestión de TICS, debe monitorear la infraestructura tecnológica para verificar que los usuarios sólo la usen para actividades propias de su labor y la Misión del IPSE.
- e. Proceso de Gestión de TICS, debe garantizar que todos los sistemas de procesamiento de información, los equipos y demás servicios tecnológicos que lo ameriten se sincronicen con una única fuente de referencia de tiempo, con el fin de garantizar la exactitud de los registros de auditoría.

- **CONTROL DE SOFTWARE OPERACIONAL**


Lineamientos

- a. Proceso de Gestión de TICS, designará responsables y establecerá instructivos y guías para controlar la instalación de software operativo, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo es actualizado.
- b. Proceso de Gestión de TICS, debe establecer responsabilidades y procedimientos para controlar la instalación del software operativo que interactúa con el procedimiento de cambios existente en el IPSE.
- c. Proceso de Gestión de TICS, debe conceder accesos temporales y controlados a los fabricantes y terceros autorizados para realizar actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.
- d. Proceso de Gestión de TICS, debe establecer las restricciones y limitaciones para la instalación del software operativo en los equipos de cómputo del IPSE.
- e. Proceso de Gestión de TICS, debe generar un plan de actualizaciones para el software, aplicaciones y librerías de programas que deberán llevar a cabo los administradores.
- f. Proceso de Gestión de TICS, debe manejar un sistema de control de configuración para mantener el control de todo el software implementado, al igual que se debe mantener la documentación del sistema.

- **GESTIÓN DE VULNERABILIDADES TÉCNICAS**

Lineamientos

- a. Proceso de Gestión de TICS, debe realizar mínimo una vez al año una revisión de vulnerabilidades técnicas a los sistemas de información críticos y misionales por medio de ethical hacking y/o pruebas de penetración.
- b. Proceso de Gestión de TICS, debe documentar, informar, gestionar y corregir las vulnerabilidades encontradas, adoptando acciones correctivas para mitigar los hallazgos, minimizar el nivel de riesgo y reducir el impacto.
- c. Proceso de Gestión de TICS, debe restringir a los usuarios finales la instalación de software en los equipos del IPSE.
- d. Proceso de Gestión de TICS, debe establecer y monitorear que la infraestructura tecnológica sea usada exclusivamente

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Páginas
		15-09-2022	Pág. 23 de 36

para el desempeño laboral, o para el desarrollo de las funciones, actividades y obligaciones acordadas o contratadas.

- e. Proceso de Gestión de TICS, debe controlar la instalación y uso de máquinas virtuales y sólo podrá realizarse siempre y cuando sea una necesidad para el uso de las funciones o labor contratada
- f. Proceso de Gestión de TICS, debe realizar de manera periódica una inspección del software instalado en los equipos del IPSE y debe desinstalar el software no autorizado.
- g. Proceso de Gestión de TICS, a través de la Mesa de Servicios es la responsable de instalar, configurar y dar soporte a los equipos del IPSE.
- h. Sólo está permitido el uso de software licenciado por el IPSE y/o aquel que sin requerir licencia de uso comercial sea expresamente autorizado Proceso TIC

CONSIDERACIONES SOBRE AUDITORIAS DE SISTEMAS DE INFORMACIÓN

Lineamientos


- a. Proceso de Gestión de TICS, debe planificar periódicamente actividades que involucren auditorias de los sistemas críticos en producción.
- b. Proceso de Gestión de TICS, debe documentar los resultados de las auditorias de los sistemas de Información del IPSE.

6.7 POLITICA SEGURIDAD DE LAS COMUNICACIONES

• GESTIÓN DE SEGURIDAD DE LAS REDES

Lineamientos

- a. Proceso de Gestión de TICS, debe disponer de controles para realizar transferencias completas, sin alteraciones y visualizaciones no autorizadas de la información entre las aplicaciones del IPSE.
- b. Proceso de Gestión de TICS, debe proporcionar recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación del servicio de internet.
- c. Proceso de Gestión de TICS, debe monitorear continuamente el canal o canales queprestan el servicio de internet, con el fin de prevenir y atender cualquier incidente que se presente tan pronto como sea posible.
- d. Proceso de Gestión de TICS, debe generar registros de navegación y los accesos de los usuarios a Internet, así como establecer e implementar procedimientos de monitoreo sobre la utilización del servicio de internet.
- e. Proceso de Gestión de TICS, debe implementar controles que eviten el ingreso a páginas con código malicioso incorporado o sitios catalogados como peligrosos
- f. Proceso de Gestión de TICS, debe proporcionar una plataforma Tecnológica que soporte los sistemas de información, esta debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a internet. La división de estos segmentos debe ser realizada por

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Paginas
		15-09-2022	Pág. 24 de 36


medio de dispositivos perimetrales e internos de enrutamiento y de seguridad.

- g. Proceso de Gestión de TICS, debe realizar segmentación de Redes para servidores públicos, contratistas y visitantes del IPSE.
- h. Proceso de Gestión de TICS, debe mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para el Instituto.
- i. Proceso de Gestión de TICS, debe instalar protección entre las redes internas y cualquier red externa, que este fuera de la capacidad de control y administración de la Instituto.
- j. Proceso de Gestión de TICS, debe permitir el acceso a redes inalámbricas mediante un portal de acceso en donde permita al usuario ingresar un usuario y contraseña.
- k. Proceso de Gestión de TICS, debe realizar de manera periódica el cambio de las claves de acceso a la red WIFI del IPSE.

- **TRANSFERENCIA DE INFORMACIÓN**

Lineamientos

- a. Proceso de Gestión de TICS,, debe establecer el procedimiento de intercambio de información con los diferentes terceros que, hacen parte de la operación del IPSE, donde se contemple la recepción o envío de la información, utilización de medios de transmisión confiables y la adopción de controles, con el fin de proteger la confidencialidad e integridad de esta.
- b. Proceso de Gestión de TICS, debe ofrecer servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información, que permitan el cumplimiento del procedimiento para el intercambio de información (digital o medio magnético), con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.
- c. Proceso de Gestión de TICS, debe establecer controles para proteger la información que se transmite como documentos adjuntos a través del correo electrónico del IPSE.
- d. Los mensajes y la información contenida en los buzones de correo son propiedad del IPSE y cada responsable, el cual debe mantener únicamente los mensajes relacionados con el desarrollo de sus actividades.
- e. El único servicio de correo electrónico controlado por el IPSE es el asignado directamente por Proceso TIC, el cual cumple con todos los requerimientos técnicos y de seguridad para evitar ataques informáticos, virus, spyware y otro tipo de software o código malicioso.
- f. Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por el IPSE y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.
- g. Los usuarios de correo electrónico tienen prohibido el envío de cadenas de mensajes de cualquier tipo, ya seacomercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los servidores públicos de la entidad y el personal provisto por terceras partes.
- h. Está prohibido el envío de o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Paginas
		15-09-2022	Pág. 25 de 36


cualquier contenido que atente con la integridad de las personas.

- i. Es responsabilidad del usuario etiquetar el mensaje de correo electrónico de acuerdo con los niveles de clasificación teniendo en cuenta el tipo de información que se pretende compartir.
- j. Es responsabilidad del usuario reportar un correo electrónico cuando crea que es de dudosa procedencia a Proceso TIC, con el fin de que el administrador tome las medidas necesarias para evitar su propagación dentro de la entidad.
- k. Es responsabilidad de cada usuario asegurar los destinatarios a los cuales va dirigida una comunicación, si estas son listas de distribución, también debe revisarlas con el fin de evitar compartir información a personas no autorizadas.
- l. El servicio de correo electrónico debe ser usado de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos, sistemas de información e imagen del instituto
- m. No es permitido el envío o recepción de archivos que contengan extensiones ejecutables, en ninguna circunstancia.
- n. Es obligación del usuario realizar la activación de las repuestas automáticas en el servicio de correo del Instituto, cuando su ausencia sea mayor a tres (3) días, igualmente, está deberá indicar quién es la persona asignada para cubrir su ausencia.
Nota: La persona encargada de cubrir la ausencia debe estar autorizada por parte del jefe inmediato o supervisor del contrato.
- o. Proceso de Gestión de TICS, define las pautas generales para asegurar un adecuado uso de Microsoft 365 (Word, Excel, Powerpoint, Outlook, Sharepoint, Stream, OneDrive, OneNote, Teams, forms) por parte de los usuarios.
- p. Está prohibida la divulgación no autorizada de información de propiedad de IPSE a través de la plataforma.
- q. Está prohibido la creación, almacenamiento o intercambio de mensajes que atenten contra las leyes de derechos de autor.
- r. Se deben establecer acuerdos de confidencialidad o de no divulgación de Información.
- s. Para el personal externo que ejecute tareas propias del IPSE y haya sido contratado en el marco de un contrato o convenio con el Instituto, debe firmar un acuerdo de confidencialidad y no divulgación de la información firmada entre el IPSE (Supervisor del Contrato) y el Representante Legal, y este debe reposar en la carpeta de ejecución del contrato.

- **ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**

Lineamientos

- a. Las áreas técnicas propietarias de sistemas de información en conjunto con Proceso TIC incluirán requisitos de desarrollo seguro en la definición de requerimientos y posteriormente se asegurarán de que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.
- b. Todos los sistemas de información y/o desarrollos de software a los que haya lugar deben tener un área técnica formalmente asignada que sea la responsable de la administración y su custodia dentro del IPSE.
- c. Proceso de Gestión de TICS, deberá establecer metodologías para el desarrollo de software seguro, que incluyan la definición de requerimientos de seguridad y las buenas prácticas, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.


	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Páginas
		15-09-2022	Pág. 26 de 36

- d. Las áreas técnicas responsables de la administración de los sistemas de información en acompañamiento con Proceso TIC deberán establecer las especificaciones de adquisición o desarrollo de sistemas de información considerando siempre los requerimientos de Seguridad de la Información.
- e. El área técnica responsable de la administración de los sistemas de información deberán definir qué perfiles pueden contener los sistemas de información a desarrollar, igualmente, deben aprobar la asignación de estos perfiles cuando sea necesario.
- f. Proceso de Gestión de TICS, deberá liderar la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, la arquitectura de aplicaciones, entre otros. Igualmente, el área técnica debe definir los controles de acceso
- g. Proceso de Gestión de TICS, debe asegurar que cada vez que se pretenda implementar un sistema de información ya sea propio o de terceros, este sea sometido a un análisis de vulnerabilidades supervisadas las cuales deberán ser remediadas antes del despliegue en producción por las áreas encargadas.
- h. Proceso de Gestión de TICS, debe establecer mecanismos que permitan deshabilitar las funcionalidades de autocompletar en formularios de solicitud que requieran información sensible.
- i. Proceso de Gestión de TICS, debe asegurar que no se permitan conexiones recurrentes con el mismo usuario a los sistemas de información construidos, garantizando la seguridad de las conexiones a los sistemas de información mediante mecanismos que aseguren una única autenticación.
- j. Proceso de Gestión de TICS, debe exigir la documentación relacionada con el código fuente para los desarrollos propios y para los casos en que el Instituto adquiriera el sistema de información a un proveedor externo
- k. Proceso de Gestión de TICS, debe exigir toda la documentación de los repositorios y bases de datos de los sistemas de información a los proveedores externos.

6.7.1 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE


Lineamientos

- a. Proceso de Gestión de TICS, debe velar por el desarrollo interno o externo de los sistemas de información, que cumplan con las buenas prácticas para el desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad del software desarrollado.
- b. Proceso de Gestión de TICS, debe establecer y mantener ambiente separados de Desarrollo/Pruebas y Producción, dentro de la infraestructura del IPSE.
 - El ambiente de desarrollo/pruebas se debe utilizar para propósitos de implementación, modificación, ajuste y/o revisión de código fuente; además se debe utilizar para realizar el conjunto de validaciones funcionales y técnicas del software, aplicación o sistema de información, teniendo como base los criterios de aceptación y los requerimientos de desarrollo.
 - El ambiente de producción debe utilizarse para la prestación de un servicio que involucra el manejo de datos reales y

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Paginas
		15-09-2022	Pág. 27 de 36

que tiene un impacto directo sobre las actividades realizadas como parte de un proceso del IPSE.

- c. Proceso de Gestión de TICS, debe restringir el acceso a compiladores, editores y otros utilitarios del sistema operativo en el ambiente de producción, sean cuando no indispensables para el funcionamiento del mismo
- d. Los administradores de los sistemas de información (Líder Funcional) con el apoyo Proceso TIC son responsables de asegurar que la calidad de los entregables cumpla con los requerimientos de seguridad y establecidos, antes del paso a producción de los sistemas utilizando metodologías para este fin, documentando las pruebas realizadas y aprobando los pasos a producción
- e. Las áreas técnicas propietarias de los sistemas de información deben probar las migraciones entre los ambientes de desarrollo, pruebas y producción que han sido aprobadas.
- f. Proceso de Gestión de TICS, debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con los últimos parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema
- g. Proceso de Gestión de TICS, debe incluir dentro del procedimiento y los controles de gestión de cambios el manejo de los cambios en el software, aplicativos y sistemas de información del IPSE
- h. Los desarrolladores internos y externos de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de estos, pasando desde el diseño hasta la puesta en marcha.
- i. Los desarrolladores internos y externos deben proporcionar un nivel adecuado de soporte para solucionar los problemas en los sistemas de información del IPSE; de acuerdo a los niveles de servicio acordados entre las partes.
- j. Los desarrolladores internos y externos deben construir los sistemas de información de tal manera que efectúen las validaciones de datos de entrada y la generación de datos de salida de manera confiable, utilizando rutinas de validación centralizada y estandarizadas.
- k. Los desarrolladores internos y externos deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.
- l. Los desarrolladores internos y externos deben suministrar opciones de desconexión o cierre de sesión de los sistemas de información (Logout) que permitan terminar completamente con la sesión o conexión asociada.
- m. Los desarrolladores internos y externos deben asegurar el manejo de operaciones sensibles o críticas de los aplicativos desarrollados permitiendo el uso de dispositivos adicionales como tokens o el ingreso de parámetros adicionales de verificación.
- n. Los desarrolladores internos y externos deben asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.
- o. Los desarrolladores internos y externos deben garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.
- p. Los desarrolladores internos y externos deben remover todas las funcionalidades y archivos que no sean necesarios

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Páginas
		15-09-2022	Pág. 28 de 36


para los aplicativos, previo a la puesta en producción.

- q. Los desarrolladores internos y externos deben prevenir la revelación estricta de directorios de los sistemas de información construidos.
- r. Los desarrolladores internos y externos deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
- s. Los desarrolladores internos y externos deben evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas independientes, los cuales se recomienda que estén cifrados.
- t. Los desarrolladores internos y externos deben certificar el cierre de la conexión con las bases de datos desde los aplicativos tan pronto como estas sean requeridas.
- u. Los desarrolladores deben implementar controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en el repositorio destinado para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.
- v. Ni los desarrolladores ni terceros deben realizar pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción. Esto puede conducir a fraude o inserción de código malicioso.
- w. Los desarrolladores deben proteger el código fuente de los aplicativos construidos, de tal forma que no pueda ser descargado ni modificado por usuarios no autorizados.
- x. Los desarrolladores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.
- y. Proceso de Gestión de TICS, en conjunto con los desarrolladores, debe crear e implementar una guía de desarrollo seguro usando metodologías apropiadas.
- z. Todo desarrollo realizado por el equipo del Proceso TIC o terceros debe estar alineado con los lineamientos de desarrollo seguro para Sistemas Información.

6.7.2 PROTEGER LOS DATOS USADOS PARA PRUEBAS

Lineamientos:

- a. Proceso de Gestión de TICS, protegerá los datos en ambiente de prueba que se entregarán a los desarrolladores, asegurando que no revelan información confidencial de los ambientes de producción.
- b. Proceso de Gestión de TICS, debe certificar que la información a ser entregada a los desarrolladores para sus pruebas será enmascarada y no revelará información confidencial de los ambientes de producción.
- c. Proceso de Gestión de TICS, debe eliminar la información de los ambientes de pruebas una vez estas hayan concluido.
- d. Cada vez que se realicen copias de información de producción se debe contar con un registro que permita realizar auditoría.

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Páginas
		15-09-2022	Pág. 29 de 36

6.7.3 POLITICA SEGURIDAD DE RELACIÓN CON PROVEEDORES


Lineamientos

- a. Gestión Contractual debe establecer lineamientos para el cumplimiento de las obligaciones contractuales de la dimensión de Seguridad y Privacidad de la Información con terceros o proveedores.
- b. Gestión Contractual debe establecer en el momento de suscribirse contratos de cualquier tipo los riesgos asociados a la seguridad y privacidad de la información, los compromisos establecidos de confidencialidad de la información y el cumplimiento de las políticas de seguridad de la información del IPSE.
- c. Gestión Contractual debe establecer en los contratos con terceros y proveedores los requisitos legales y regulatorios relacionados con la protección de datos personales, los derechos de propiedad intelectual y derechos de autor.
- d. Proceso de Gestión de TICS, debe documentar, establecer controles y permisos cuando un tercero o proveedor requiera tener accesos a la información por medio de la infraestructura tecnológica del IPSE.
- e. Proceso de Gestión de TICS, debe verificar mensualmente el cumplimiento de Acuerdos de Nivel de Servicio establecidos con sus proveedores de tecnología.
- f. Proceso de Gestión de TICS, debe establecer un procedimiento que permita asegurar la gestión de cambios a nivel de infraestructura, aplicativos y servicios tecnológicos que son soportados por terceros y/o proveedores, para garantizar estándares de eficiencia, seguridad, calidad y que permitan determinar los responsables y tareas a seguir para garantizar el éxito en la gestión de cambios.
- g. Cada dependencia del Instituto que establezca relación con proveedores y su cadena de suministro, debe solicitar acompañamiento periódico a la dimensión de Seguridad y Privacidad de la Información con el fin de dar a conocer las políticas que tiene el IPSE.
- h. Gestión Contractual debe incluir en las guías de contratación y supervisión obligaciones generales sobre seguridad y privacidad de la información y los formatos para su cumplimiento y verificación por parte del supervisor de contrato.

6.8 POLITICA GESTIÓN DE INCIDENTES DE SEGURIDAD

Lineamientos

- a. Proceso de Gestión de TICS, en conjunto con el Oficial de Seguridad de la Información debe definir un procedimiento para la gestión de incidentes de seguridad de la información.
- b. Proceso de Gestión de TICS, debe definir los canales para que los Servidores Públicos, contratistas y terceros de IPSE puedan reportar los incidentes de Seguridad de la Información.
- c. Proceso de Gestión de TICS, es la encargada de la evaluación de eventos de seguridad de la información y la decisión tomada sobre los mismos.
- d. Proceso de Gestión de TICS, es la encargada para la recolección de evidencias de los incidentes de seguridad de la información.

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Páginas
		15-09-2022	Pág. 30 de 36

- e. Proceso de Gestión de TICS, debe contar con los mecanismos para el cumplimiento de los tiempos en la respuesta de incidentes establecido en los lineamientos para la Gestión de Incidentes.
- f. Proceso de Gestión de TICS, debe proporcionar y mantener actualizados los medios para el aprendizaje de los incidentes de Seguridad de la Información en el Instituto.
- g. Proceso de Gestión de TICS, deberá dar a conocer a los servidores públicos, contratistas y terceros del IPSE los lineamientos establecidos para la Gestión de Incidentes de Seguridad de la Información.
- h. Proceso de Gestión de TICS, debe velar por que la recolección de evidencia tenga en cuenta la cadena de custodia, la seguridad del personal, los roles y responsabilidades del personal involucrado, la competencia del personal y la documentación.

6.9 POLÍTICA GESTIÓN CONTINUIDAD DEL NEGOCIO

6.9.1 CONTINUIDAD DE SEGURIDAD DE LA

INFORMACIÓN


Lineamientos

- a. Establecer un análisis de impacto al negocio (BIA por sus siglas en ingles), por medio del cual se identifiquen los servicios críticos del IPSE.
- b. Diseñar las estrategias y tiempos de recuperación de la operación de los servicios críticos del IPSE.
- c. Proceso de Gestión de TICS, debe disponer de planes de contingencia de los servicios Tecnológicos de Información y un plan de recuperación ante desastres, enfocados a lograr el retorno a la operación normal.

6.10 POLÍTICA DE PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES

El IPSE con el objetivo de garantizar la confidencialidad, libertad, seguridad, veracidad, transparencia, acceso y circulación restringida de datos, se reservará el derecho de modificar su Política de Tratamiento de Datos Personales en cualquier momento y se compromete a:

- Regular la recolección, almacenamiento, uso, circulación y supresión de datos personales, brindando las herramientas que garanticen la autenticidad, confidencialidad, integridad y disponibilidad de la información y datos personales almacenados en las bases de datos de la infraestructura propia y/o de un tercero.
- Velar por el cumplimiento de la ley 1581 de 2012, su decreto reglamentario 1377 de 2013 y demás normas que la adicionen, modifiquen o deroguen cuya materia se refiera a la protección y tratamiento de datos personales.
- Infundir y aplicar los principios establecidos en la ley de protección y tratamiento de datos personales
- Solicitar autorización para el tratamiento de datos personales a través de una autorización previa, expresa e informada a


	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Paginas
		15-09-2022	Pág. 31 de 36

los titulares de los datos personales, o a sus representantes. Esta autorización puede ser por escrito diligenciando un formato elaborado previamente por el IPSE o también se podrá dar de forma Biométrica (llamada telefónica, video, etc.), asegurando que el detalle de la descripción del tratamiento de los datos personales se informará mediante el mismo documento específico o adjunto, al titular de los datos, incluyendo como mínimo:

- La descripción del tratamiento al que serán sometidos sus datos sensibles y la finalidad del mismo.
 - Los derechos que le asisten como titular.
 - Los canales en los cuales podrá formular consultas y/o reclamos
- Garantizar el derecho de acceso y consulta de los datos, previa acreditación de la identidad del titular, legitimidad o personalidad de su representante, poniendo a disposición de este, sin costo o erogación alguna, de manera pormenorizada y detallada, los respectivos datos personales.
 - Llevar a cabo un adecuado tratamiento y protección de los datos personales mediante el fortalecimiento de la Seguridad y Privacidad de la Información, el desarrollo y la actualización de la política de privacidad y la normatividad relacionadas, como la clasificación de la información y gestión de activos, de conformidad a lo dispuesto en la Ley 1581 de 2012 y demás desarrollos normativos que le apliquen.
 - Comunicar la responsabilidad de los servidores públicos, contratistas y terceros del IPSE en reportar cualquier incidente de fuga de información, daño informático, violación de datos personales, comercialización de datos, uso de datos personales de niños, niñas o adolescentes, suplantación de identidad o conductas que puedan vulnerar la intimidad de una persona.
 - Divulgar, sensibilizar y capacitar a todos los servidores públicos, contratistas y terceros del IPSE en los derechos que se derivan de la protección y tratamiento de datos personales a través de las directrices que Proceso TIC, disponga para tal fin.
 - Las excepciones para la autorización del Titular lo complementan y debe entenderse como una lista no exhaustiva, de acuerdo con las normas y demás normas que los modifiquen, adicione o sustituyan:
 1. Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
 2. Datos de naturaleza pública.
 3. Casos de urgencia médica o sanitaria.
 4. Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
 5. Datos relacionados con el Registro Civil de las Personas

ALCANCE

La política de tratamiento de datos personales aplica para toda la información personal registrada en las bases de datos manuales, automatizadas o semiautomatizadas del IPSE, quien actúa en calidad de responsable del tratamiento de los datos

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Paginas
		15-09-2022	Pág. 32 de 36

personales.

Así mismo tiene el propósito de dar a conocer el compromiso del IPSE con el cumplimiento de las leyes, decretos y demás normas que tienen como objetivo la protección de los datos personales.


PRINCIPIOS RECTORES

Con el fin de garantizar la protección y tratamiento de datos personales el IPSE, aplica los principios señalados en la Ley 1581 de 2012, "Por el cual se dictan disposiciones generales para la protección de datos personales "así:

- **Principio de Legalidad en materia de Tratamiento de Datos:** El tratamiento de datos es una actividad requerida que debe estar acorde con lo establecido en la ley.
- **Principio de Finalidad:** El tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución Política y la ley, la cual debe ser informada al Titular.
- **Principio de Libertad:** El tratamiento de la información sólo podrá realizarse siempre y cuando se cuente con el consentimiento, previo, expreso e informado del Titular . Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.
- **Principio de Veracidad o Calidad:** La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
- **Principio de Transparencia:** En el tratamiento, se debe garantizar el derecho del Titular a obtener del responsable de dicho tratamiento o del Encargado y en cualquier momento y sin restricciones, a dar información acerca de la existencia de sus datos.
- **Principio de Acceso y Circulación Restringida:** El tratamiento está sujeto a los límites que se derivan de la naturaleza de los datos personales y de las disposiciones constitucionales y legales. En este sentido, el tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la Ley. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la citada ley.
- **Principio de Seguridad:** La información estará sujeta al procedimiento ejecutado por el responsable o encargado del tratamiento , el cual deberá utilizar las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad de los registros y evitar su adulteración, pérdida, consulta , uso o acceso no autorizado o fraudulento, según lo descrito en la ley

CATEGORÍAS ESPECIALES DE DATOS

Datos Personales Sensibles: Son aquellos datos que afectan la intimidad del titular o cuyo uso indebido puede generar su

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Páginas
		15-09-2022	Pág. 33 de 36

discriminación, así como los que revelan el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, 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, la vida sexual y los datos biométricos.

El IPSE, limita el tratamiento de datos personales sensibles de acuerdo con la Ley 1581 de 2014 y solicitará autorización previa e informada al titular.

Datos Personales de Niños, Niñas y Adolescentes: Los menores de edad son titulares de sus datos personales y por lo tanto portadores de los derechos correspondientes. De acuerdo a lo establecido en la Constitución Política y en concordancia con el Código de la Infancia y la Adolescencia, los derechos de los menores deben ser interpretados y aplicados de manera prevalente y por lo tanto, deben ser observados con especial cuidado y deben ser tenidas en cuenta las opiniones de los menores al momento de realizar algún tratamiento de sus datos.

El IPSE se compromete a respetar los derechos prevalentes de los menores.

PRERROGATIVAS Y DERECHOS DE LOS TITULARES


Los Titulares de los datos personales tienen los siguientes derechos:

- Acceder, conocer, actualizar y rectificar sus datos personales frente al IPSE en su condición de responsable del tratamiento.
- Solicitar prueba de la existencia de la autorización otorgada al IPSE salvo los casos en los que la Ley exceptúa la autorización.
- Recibir información por parte del IPSE, previa solicitud, respecto del uso que les ha dado a sus datos personales.
- Acudir ante las autoridades legalmente constituidas, en especial ante la Superintendencia de Industria y Comercio -SIC y presentar quejas por infracciones a lo dispuesto en la normatividad vigente, previo trámite de consulta o requerimiento ante el responsable del tratamiento.
- Modificar y revocar la autorización y/o solicitar la supresión de los datos personales cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales vigentes.
- Tener conocimiento y acceder en forma gratuita a sus datos personales, que hayan sido objeto de tratamiento.

Deberes del IPSE en relación con el Tratamiento de los Datos Personales

El IPSE, se compromete a tener presente que los datos personales, son propiedad de las personas a las que se refieren y que solamente ellas tienen toma decisión sobre los mismos.

El IPSE, se compromete hacer uso adecuado de los datos solamente y a dar cumplimiento para los fines propios de los mismos.

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Paginas
		15-09-2022	Pág. 34 de 36

CONSULTA Y RECLAMOS

Los Titulares de los datos personales o sus causahabientes, podrán consultar sus datos personales que reposan en la base de datos. En consecuencia, el IPSE garantizará el derecho de consulta, suministrando a los titulares de datos personales, toda la información contenida en el registro individual o que esté vinculada con la identificación del titular.

El titular o sus causahabientes en la medida en que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la normativa sobre Protección de Datos Personales, podrán presentar un reclamo ante el responsable del tratamiento.

Independientemente del mecanismo que se implemente para la atención de solicitudes de consulta, estas serán atendidas en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recibo. En el evento en el que una solicitud de consulta no pueda ser atendida dentro del término señalado, se informará al interesado antes del vencimiento del plazo las razones por las cuales no se ha dado respuesta a su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

Las consultas que se efectúen respecto a datos personales deberán ser remitidas mediante un correo electrónico a la siguiente dirección sistemas@ipse.gov.co. En esa consulta, el titular deberá indicar si desea que sus datos sean actualizados, rectificadas o suprimidos o bien si desea revocar la autorización que se había otorgado para el tratamiento de los datos personales, conforme lo previsto en el artículo 15 de la Ley 1581 de 2012.

SUPRESIÓN (ELIMINACIÓN) DE DATOS


La supresión de los datos, implica la eliminación total o parcial de la información personal de acuerdo a lo solicitado por el titular en los registros, archivos, bases de datos o tratamientos realizados por el IPSE.

El titular de los datos personales tiene el derecho, en todo momento, a solicitar al IPSE la supresión (eliminación) de sus datos personales en los siguientes casos:

- Cuando considere que los mismos no están siendo tratados conforme a los principios, deberes y obligaciones previstas en la normatividad vigente.
- Cuando no sean necesarios por ejercicio de la actividad.
- Cuando se haya superado el periodo establecido para el cumplimiento de los fines para los que fueron recaudados.

El derecho de supresión no es un derecho absoluto, por lo que el responsable del tratamiento de datos personales por el IPSE, puede negar el ejercicio del mismo cuando:

- El titular de los datos tenga un deber legal o contractual de permanecer en la base de datos.
- La eliminación de datos obstaculece actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, investigación y persecución de delitos o la actualización de

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Paginas
		15-09-2022	Pág. 35 de 36

sanciones administrativas.

- Los datos sean necesarios para proteger los intereses jurídicamente tutelados del titular para realizar una acción en función del interés público o para cumplir con una obligación legalmente adquirida por el Titular.

REVOCATORIA DE LA AUTORIZACIÓN

Todo Titular de datos personales puede solicitar la revocación en cualquier momento, consentimiento otorgado al tratamiento de estos, siempre y cuando no lo impida una disposición legal o contractual. Para ello, el IPSE establecerá mecanismos que le permitan al Titular revocar su consentimiento.

FUNCIÓN DE PROTECCIÓN DE DATOS PERSONALES AL INTERIOR DEL IPSE

A partir de la adopción de la presente Política, IPSE establece:

Términos y Condiciones de Uso de Herramientas Informáticas Externas

Autorregulación de los principios y las reglas consagradas en la Ley 1581 de 2012 y demás normas vigentes que la modifiquen o deroguen, dirigidos específicamente a proteger el derecho del hábeas data de clientes, usuarios y en general, de toda persona natural que interactúe con un sistema de información que gestione datos bien sea física o electrónica.

Oficina de Tecnologías y Sistemas de Información en adelante Proceso TIC

En cumplimiento del deber legal consagrado en el artículo 17 de la Ley 1581 de 2012, relativo a la necesidad de otorgar responsabilidades directas, se designa al coordinador del área TIC para que articule todas las acciones para el efectivo cumplimiento de la Política de Protección de Datos Personales en el IPSE

EL REGISTRO NACIONAL DE BASES DE DATOS


El IPSE inscribirá de manera independiente en el Registro Nacional de Base de Datos cada una de las bases de datos que contengan datos personales cuyo tratamiento se realice por parte del IPSE, identificando cada una de ellas de acuerdo con la finalidad para la cual fueron creadas. En ese sentido, actualizará la información inscrita cuando se presenten cambios sustanciales a la misma.

6.11 POLITICA DE CUMPLIMIENTO

6.11.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

Lineamientos

El IPSE gestiona la seguridad y privacidad de la información dando cumplimiento adecuado a la legislación vigente. Analizando los requisitos legales aplicables a la información de derechos de autor y propiedad intelectual, protección de datos

	MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código	Versión
		IPSE-TIC-M04	1
		Fecha:	Páginas
		15-09-2022	Pág. 36 de 36

personales, ley de transparencia y del derecho de acceso a la información pública nacional. Igualmente, velara por la protección de los registros ante cualquier pérdida, destrucción, falsificación acceso o liberación no autorizada de acuerdo con los requisitos legislativos, de reglamentación y contractuales del IPSE.

6.11.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

Lineamientos

- a. La Oficina de Control Interno, debe realizar de manera periódica auditorías internas para comprobar el correcto funcionamiento del Sistema de Gestión de Seguridad de la Información en cuanto a los objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información.
- b. Los líderes de los procesos deben asegurar, que todos los procedimientos de seguridad dentro de su área de responsabilidad se realicen correctamente, con el fin de cumplir las políticas y normas de seguridad; en caso de incumplimiento se evaluarán y propondrán acciones correctivas
- c. Proceso de Gestión de TICS, debe realizar revisiones mínimo una vez al año del cumplimiento de las políticas de Seguridad y Privacidad de la Información
- d. Es un deber de los servidores públicos contratistas y terceros del IPSE, conocer esta Política y realizar todos los actos conducentes para su cumplimiento, implementación y mantenimiento.

BIBLIOGRAFÍA

Norma Técnica Colombiana NTC-ISO-IEC-27001 (2013). Tecnología de información. Técnicas de Seguridad. Sistema de Gestión de la seguridad de la información. Requisitos.

Actualización general del documento según requerimiento NTC-ISO-IEC 27001:3013 ANEXO A 26/12/2018 GROW DATA

https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

<https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi>

<https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/>

CONTROL DE CAMBIOS

VERSIÓN	FECHA	RESPONSABLE	DESCRIPCIÓN
1.0	15-09-2022	PROCESO GESTIÓN DE TICS	Creación del manual

Elaboró	Revisó	Aprobó
Nombre: Anyela Luceidy Galindo - Contratista Simón Sarmiento - Contratista	Nombre: Jhon Ricardo Morales – Asesor TIC	Nombre: Comité Institucional de Gestión y Desempeño del mes de Septiembre del 2022