PUTUMAYO GOBERNACIÓN NIT. 800.094.164-4	SISTEMA INTEGRADO DE GESTIÓN	CÓDIGO: FT-SG-004
	CREACIÓN, MODIFICACIÓN Y ELIMINACIÓN DE DOCUMENTOS	VERSIÓN: 04
		FECHA: 08/10/2020

PROCESO QUE REALIZA LA SOLICITUD: GESTION DE TECNOLOGIA E INFORMACION.

TIPO DE SOLICITUD	☐ *Creación* ☒ *Modificación* ☐ *Eliminación*	**TIPO DE DOCUMENTO**	☐ *Guía*	☐ *Instructivo*	☐ *TRD*
			☐ *Manual*	☐ Reglamento	☐ *TVD*
			☐ *Procedimiento*	☐ *Protocolo*	☐ *Cuadro*
			☐ *Programa*	☒ *Política*	☐ *Sistema*
			☐ *Caracterización*	☐ *Lineamiento*	☐ *Plan*
			☐ *Diagnostico*	☐ *Anexo*	☐ *Formato*
			☐ *Otro.* _____		

NOMBRE DEL DOCUMENTO	***POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION***	**CÓDIGO**	PA-GTI-001
		VERSIÓN	02
~~**JUSTIFICACIÓN DE LA SOLICITUD**~~	En cumplimiento a la Resolución 74367 del 17 de noviembre de 2021, del Ministerio de Comercio, Industria y Turismo Superintendencia de Industria y comercio; y en atención a los preceptos de la Constitución Política de Colombia, articulo 15 que exige la recolección, tratamiento y circulación de datos personales, se respeten la libertad y demás garantías consagradas en la constitución. Ordena a la Entidad Departamento del Putumayo que documente y monitoree una política de seguridad de la Información que contenga medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los datos personales evitando su adulteración, perdida, consulta, uso o acceso no autorizado.		
CAMBIO PROPUESTD	Actualización del documento según lineamientos de la Resolución 74367 del 17 de noviembre de 2021 del Ministerio de Comercio, Industria y Turismo Superintendencia de Industria y comercio El documento fue creado el 30-04-2019 como Manual de Política de Seguridad y Privacidad de la Información código MA-GTI-001; sin embargo, su estructura obedece a una "Política", razón por la cual se realiza su modificación y denominación a Política así: Política de Seguridad y Privacidad de la Información PA-GTI-001 V 02. Asimismo, se elimina el documento MA-GTI-001 V 01		
ELABORADD POR: Favian Alejandro Moreno Calderón	**REVISÓ:** Yuley Nayibe Rodríguez Tobón. Oscar German González Cortes	**APROBÓ:** Luis Carlos Guevara Montilla	**ACEPTADO**
Cargo: Profesional Universitario Unidad de Gestión de Tecnología e Información	**Cargo:** Secretaria de Servicios Administrativos. Profesional Especializado Secretaría de Planeación Departamental	**Cargo:** Secretario de Planeación Departamental. Secretario Técnico Comité Institucional de Gestión y Desempeño.	
Firma: Favian Moreno C.	**Firma:**	**Firma:**	**FECHA**
JUSTIFICACIÓN DE LA NO APRDBACION:			

Nota: *Marcar en el campo* ☐ *con una X según el caso. Para los espacios donde no se cuente con información para diligenciar, colocar No Aplica.*
Anexo:()Folios

PUTUMAYO
GOBERNACIÓN

POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Elaborado por:	**Revisado por:**	**Aprobado por:**
FAVIAN ALEJANDRO MORENO .	Yuley Nayibe Rodríguez Tobón Oscar German González Cortes.	Luis Carlos Guevara Montilla
Cargo: Profesional Universitario Unidad de Gestión de Tecnología e Información	Cargo: Secretaria de Servicios Administrativos Profesional especializado Secretaria de Planeación Departamental .	Cargo: Secretario de Planeación Departamental. Secretaria Técnica Comité Institucional de Gestión y Desempeño.
Firma:	Firma:	Firma:

TABLA DE CONTENIDO

1. OBJETIVOS:

1.1 OBJETIVO GENERAL:

- Conservar, proteger y administrar de manera efectiva la información de la Gobernación del Putumayo y los medios utilizados para su tratamiento o procesamiento, contra amenazas internas o externas, intencionales o accidentales, para asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

1.2 OBJETIVOS ESPECÍFICOS:

- Mantener una política de seguridad de la información actualizada, vigente, operativa y controlada, enmarcada en el manejo de riesgos de la información de la Gobernación del Putumayo, para asegurar la sostenibilidad y eficacia de los resultados de la política.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad y privacidad de la información.
- Proteger los activos tecnológicos de la gobernación de Putumayo de las vulnerabilidades y amenazas internas o externas que puedan afectar la seguridad informática de sus recursos.
- Minimizar el riesgo de los servicios y sistemas más importantes de la entidad.
- Garantizar la prestación oportuna de los servicios que ofrece la Entidad enmarcados dentro de las dimensiones de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información indispensable para la gestión institucional y la toma de decisiones por parte de los cargos directivos.
- Conservar las políticas de seguridad y privacidad de la información de la Entidad actualizadas, con el fin de mantener su vigencia y nivel de validez.
- Concientizar a los servidores públicos, contratistas y terceros de la Gobernación del Putumayo sobre los temas de seguridad de la información.

2. ALCANCE

Esta Política aplica a todas las secretarías, Oficinas asesoras, oficinas y organismos dependientes que integran la Gobernación del Putumayo, sus recursos, todos los procesos internos o externos relacionados con la administración pública a través de contratos o

convenios con terceros y con todo el Estado empleados, cualquiera que sea su relación, la relación de dependencia que les une y la medida en que la función o tarea que desempeñan.

3. DEFINICIONES

- **Base de datos:** Conjunto organizado de datos personales que sea objeto de tratamiento.
- **Clasificación de la Información:** Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la Entidad. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado
- **Confidencialidad:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.
- **Comunicación del riesgo:** Intercambiar o compartir la información acerca del riesgo entre la persona que toma la decisión y otras partes interesadas
- **Custodio:** Es una parte designada de la entidad, un cargo, proceso, 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 privilegios de acceso, modificación y borrado
- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera
- **Evitación del riesgo:** Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.
- **Identificación del riesgo:** Proceso para encontrar, enumerar y caracterizar los elementos de riesgo
- **Impacto:** Cambio adverso en el nivel de los objetivos del negocio logrados
- **Información:** Datos relacionados que tienen significado para la entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada
  La definición dada por la ley 1712 del 2014, se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.
- **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal
- **Información pública clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o sami-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 del 2014
- **Información pública reservada:** Es aquella información "que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo de esta ley
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos

- **Principio de confidencialidad:** Todas las personas que intervienen en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación laboral o contractual con la entidad.
- **Propietario de la Información:** Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.
- **Reducción del riesgo:** Acciones que se toman para disminuir la probabilidad de consecuencias negativas o su impacto o ambas.
- **Riesgo en la seguridad de la información:** Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la entidad, se mide en términos de una combinación de la probabilidad de que suceda un evento y sus consecuencias.
- **Transferencia del riesgo:** Compartir con otro actor responsable, la pérdida o la ganancia de un riesgo.
- **Usuario:** Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información.
- **Política:** proceso de tomar decisiones que se aplican a todos los miembros de un grupo.
- **Seguridad de la información:** consiste en asegurar que los recursos del sistema de información de una empresa se utilicen de la forma que ha sido decidido y el acceso de información se encuentra contenida, así como controlar que la modificación solo sea posible por parte de las personas autorizadas para tal fin y por supuesto, siempre dentro de los límites de la autorización.
- **Privacidad de la información:** es el aspecto de la tecnología de la información (ti) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros.
- **Activos (tecnológicos):** los activos son los recursos del sistema de seguridad de la información ISO 27001, necesarios para que la empresa funciones y consiga los objetivos que se ha propuesto la alta dirección.
- **Aplicaciones informáticas:** es un software diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de tareas
- **Datos:** un dato es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) De un atributo o variable cuantitativa o cualitativa
- **Cuenta de usuario:** es una colección de información que indica al sistema operativo los archivos y carpetas a los que puede tener acceso un determinado usuario del equipo, los cambios que puede realizar en él y sus preferencias personales, como el fondo de escritorio o el protector de pantalla.
- **Contraseña (clave):** es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso.

- **Copia de seguridad (backup):** se refiere a la copia y archivo de datos de la computadora de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.
- **Servidores:** es un ordenador u otro tipo de equipo informático encargado de suministrar información a una serie de clientes, que pueden ser tanto personas como otros dispositivos conectados a él. La información que puede transmitir es múltiple y variada: desde archivos de texto, imagen o vídeo y hasta programas informáticos, bases de datos, etc.
- **Estación de trabajo:** (en inglés workstation) es un computador de altas prestaciones destinado para trabajo técnico o científico, que facilita a los usuarios el acceso a los servidores y periféricos de la red.
- **Host (anfitrión):** es un ordenador que funciona como el punto de inicio y final de las transferencias de datos. Comúnmente descrito como el lugar donde reside un sitio web. Un anfitrión de internet tiene una dirección de internet única (dirección ip) y un nombre de dominio único o nombre de anfitrión (host name).
- **Dirección IP:** es un número que identifica, de manera lógica y jerárquica, a una interfaz en red de un dispositivo (computadora, tableta, portátil, smartphone) que utilice el protocolo IP o (internet protocolo).
- **Correo electrónico:** (también conocido como e-mail, un término inglés derivado de electronic mail) es un servicio que permite el intercambio de mensajes a través de sistemas de comunicación electrónicos. Los mensajes de correo electrónico posibilitan el envío, además de texto, de cualquier tipo de documento digital (imágenes, videos, audios, etc.).
- **Virus:** son programas informáticos que tienen como objetivo alterar el funcionamiento del computador, sin que el usuario se dé cuenta. Estos, por lo general, infectan otros archivos del sistema con la intención de modificarlos para destruir de manera intencionada archivos o datos almacenados en tu computador.
- **Spam:** correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales muy molestos para el usuario.
- **Antivirus:** un antivirus es un programa informático que tiene el propósito de detectar y eliminar virus y otros programas perjudiciales antes o después de que ingresen al sistema.
- **Portal web:** un portal de internet (portal web en inglés) es un sitio web que ofrece al usuario, de forma fácil e integrada, el acceso a una serie de recursos y de servicios relacionados a un mismo tema. Incluye: enlaces webs, buscadores, foros, documentos, aplicaciones, compra electrónica, etc. Principalmente un portal en internet está dirigido a resolver necesidades de información específica de un tema en particular.
- **Intranet:** red informática interna de una empresa u organismo, basada en los estándares de internet, en la que las computadoras están conectadas a uno o varios servidores web.
- **Red wifi:** wifi es una tecnología de comunicación inalámbrica que permite conectar a internet equipos electrónicos, como computadoras, tablets, smartphones o celulares, etc., mediante el uso de radiofrecuencias o infrarrojos para la trasmisión de la información.

- **Licencia GPL:** general public license (licencia pública general). Licencia creada por la free software foundation y orientada principalmente a los términos de distribución, modificación y uso de software libre.
- **Red local:** es una red de área local (local area network, lan) los equipos informáticos están conectados a poca distancia.
- **Mensajería interna:** (también conocida en inglés como im) es una forma de comunicación en tiempo real entre dos o más personas basada en texto. El texto es enviado a través de dispositivos conectados ya sea a una red como internet, o datos móviles (3g, 4g, 4g lte, etc.) Sin importar la distancia que exista entre los dos (o más) dispositivos conectados.
- **Redes de comunicaciones:** una red de comunicaciones es un conjunto de medios técnicos que permiten la comunicación a distancia entre equipos autónomos. Normalmente se trata de transmitir datos, audio y vídeo por ondas electromagnéticas a través de diversos medios (aire, vacío, cable de cobre, fibra óptica, etc.).
- **Puerto:** en informática, un puerto es una interfaz a través de la cual se pueden enviar y recibir los diferentes tipos de datos.
- La interfaz puede ser de tipo física (hardware) o puede ser a nivel lógico o de software, en cuyo caso se usa frecuentemente el término puerto lógico.
- **Protocolo:** es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información por medio de cualquier tipo de variación de una magnitud física. Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como también los posibles métodos de recuperación de errores. Los protocolos pueden ser implementados por hardware, por software, o por una combinación de ambos.

4. RESPONSABILIDADES ASIGNADAS

La Política de Seguridad de la Información es obligatorio para todos los empleados públicos de la Gobernación del Putumayo, independientemente del tipo de relación, región o dependencia a la que estén adscritos y el nivel del cargo o función que desempeñen. El Gobernador del Departamento de Putumayo aprueba esta Política y es responsable de su aprobación y refrendar la aprobación de sus actualizaciones.

El Comité de Seguridad de la Información de la unidad es responsable de examinar, anticipar y recomendar al órgano de gobierno departamental encabezado por el gobernador para su aprobación el texto de la política de seguridad de la información, las funciones de seguridad y estructurar las funciones generales de seguridad de la información, recomendar, monitorear y mejorar continuamente el Sistema de Gestión de Seguridad de la Información de la Gobernación del Putumayo.

El mencionado comité es responsable de definir las estrategias de capacitación en seguridad de la información dentro de la Administración del Departamento.

El Coordinador del Comité de Seguridad de la Información será responsable de coordinar las actividades del comité de seguridad de la información y promover la socialización, implementación, seguimiento y control de la política.

El propietario del activo de información es responsable de clasificar, mantener, actualizar y mejorar; así como se realizan actualizaciones de perfiles y clasificaciones, definiendo perfiles de usuarios y niveles de autorización para acceder a la información de acuerdo a su ubicación, función y habilidades.
Son responsables de mantenerlo completo y confidencial. y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

Quien ejerza el cargo de secretario, o líder del área de Talento Humano, deberá notificar a todo el personal que se vincule con la Gobernación de Putumayo, el detalle de las obligaciones respecto al cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas, guías y lineamientos que surjan del Sistema de Gestión de la Seguridad de la Información.

De igual forma, será responsable de la notificación y socialización de la presente Política y de los cambios o actualizaciones que en ella se produzcan a todo el personal, a través de la suscripción de los acuerdos de Confidencialidad y de labores de capacitación continua en materia de seguridad según los lineamientos establecidos por el Comité de Seguridad de la Información de la Entidad.

Los profesionales universitarios y equipo de trabajo de la Oficina de Gestión Tecnología e Información en coordinación con la Secretaría de Servicios Administrativos, deben seguir los lineamientos de la presente política y cumplir los requerimientos que en materia de seguridad informática se establezcan para la operación, administración, comunicación y mantenimiento de los sistemas de información e infraestructura tecnológica de la Entidad.

El Archivo General del Departamento en colaboración con la Unidad de gestión de tecnología e Información determinaran el inventario de activos de información y recursos tecnológicos de los cuales son propietarios o custodios, el cual será revisado y avalado por el Almacén General del Departamento en responsabilidad de los respectivos líderes.

Quien ejerza el cargo de Jefe de Oficina Asesora de Contratación Departamental verificará que los contratos, convenios u otra documentación de la entidad con servidores públicos y con terceros incluya los lineamientos de la Política de Seguridad de la Información de la Entidad.

Es responsabilidad del usuario de la información y de los sistemas utilizados para procesarla conocer y cumplir con la política de seguridad de la información vigente.
La Oficina de Control Interno de Gestión es responsable de monitorear y controlar periódicamente la información contenida en documentos, sistemas de información y/o actividades relacionadas con la gestión de activos de información. Esta Oficina, es responsable de informar sobre el cumplimiento de los lineamientos y prácticas de seguridad de la información establecidos por esta política y la normativa adicional aplicable.

5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA GOBERNACIÓN DEL PUTUMAYO

Con la definición de las políticas de seguridad y privacidad de la información, la **GOBERNACIÓN DE PUTUMAYO** busca preservar sus activos de información (los servidores públicos, la información, los procesos, las tecnologías de información incluido el hardware y el software) y permitir un adecuado proceso de gestión de la información garantizando la integridad, confidencialidad y disponibilidad, así como también la continuidad de los servicios de la Entidad.

Con el fortalecimiento del procedimiento de la seguridad de la información de la Entidad se busca establecer al interior de la entidad cultura por parte de los servidores públicos, concientización y uso de buenas prácticas permitiendo apoyar los procesos de la Unidad Gestión Tecnología de Información de la Administración departamental.

Además de convertirse en un compromiso por parte del Mandatario(a) y los secretarios(as) de despacho de cada una de las dependencias, los cuales deben promover su difusión, consolidación y cumplimiento.

6. CONCEPTOS BÁSICOS

La seguridad de la información se define como la preservación, aseguramiento y respeto de las siguientes características de la información:

- Confidencialidad: los activos de información solo pueden ser accedidos y protegidos por usuarios autorizados.
- Integridad: El contenido del activo de información debe ser inmutable y completo. Los cambios realizados deben ser guardados, asegurando su confiabilidad.
- Disponibilidad: el contenido informativo solo puede ser recopilado durante períodos breves por usuarios con los permisos correspondientes.

7. COMITÉ PARA LA SEGURIDAD DE LA INFORMACIÓN.

La Gobernación de Putumayo, regula la organización de la seguridad de la información, mediante la constitución de un Comité Técnico denominado Comité de Seguridad de la Información, cuya composición y funciones serán reguladas por un grupo de trabajo integrado por:

- Secretario de Gobierno o Delegado
- Secretaria de Servicios Administrativos
- Jefe de Oficina de Control Interno de Gestión
- Jefe del Área de Archivo Departamental
- Unidad de Gestión de Tecnología e Información.

Los miembros del Comité están obligados a revisar y actualizar anualmente la política de seguridad de la información, presentar proyectos o recomendaciones al Gobernador del Departamento para su aprobación mediante el acto administrativo correspondiente.

Los secretarios, jefes de Departamento o jefes de unidades u oficinas, deberán identificar y evaluar los activos de información en sus respectivas áreas, y deberán seguir los lineamientos de gestión establecidos en esta política y en las normas, reglamentos, lineamientos y procedimientos recomendados por el Comité de Seguridad y aprobado y adoptado por el Gobernador del Departamento.

8. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La política de seguridad es un documento de alto nivel que demuestra el compromiso del Gobernador con la seguridad de la información. Esta política contribuye a minimizar los riesgos relacionados con daños, mejorar la eficiencia en la gestión de proyectos y asegurar el cumplimiento de las funciones misionales de la unidad apoyadas en el uso correcto de las TIC.

9. IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN.

Cada área o dependencia de la Entidad, bajo la supervisión del Comité de Seguridad de la Información y sobre la base de un inventario de, deberá mantener un inventario de los activos de información con los que cuenta, haya sido procesada y fabricado. La forma y medios de combinar la clasificación, calificación, ubicación y acceso a la información son regulados por la Unidad de Gestión de Tecnología e Información, para brindar herramientas de gestión de inventario eficientes para cada área o dependencia, que asegura la disponibilidad, integridad y confidencialidad de los datos.

10. SEGURIDAD DE LA INFORMACIÓN EN EL TALENTO HUMANO

Los funcionarios de la Gobernación del Putumayo, independientemente del tipo de trabajo o relación contractual, la dependencia o el campo en el que se desempeñe, y el grado de función, cargo o actividad a que se desempeñe, deberá contar con un registro de perfil de la fuente de información. información del usuario, incluido el hardware y el software relacionados. La Unidad de Gestión de Tecnología e Información debe mantener un inventario completo y actualizado de las configuraciones creadas.

La Unidad de Gestión de Tecnología e Información; define los atributos que se deben definir para los diferentes perfiles.

La Unidad de Gestión de Tecnología e Información elaborará, mantendrá, actualizará, mejorará y difundirá el manual sobre "Responsabilidad Personal por la Seguridad de la Información en la Gobernación del Putumayo".

La responsabilidad de la custodia de cualquier documento o registro mantenido, utilizado o producido por un empleado jubilado o reubicado recae en el jefe de departamento, secretaría o dependientes o supervisor del contrato; En todo caso, el proceso de modificación de la cadena de custodia debe ser parte integrante del procedimiento de terminación o reposicionamiento

11. ASPECTOS GERENCIALES Y OPERACIONALES

Para que las políticas y estándares de seguridad sean efectivos, el gobierno de Putumayo debe adoptar métodos de trabajo, prácticas comerciales y procedimientos en el marco del cumplimiento de las estrategias de la organización. Por lo tanto, existen ciertos temas como el control de cambios y la documentación de los sistemas, procedimientos y estructuras organizacionales que, si bien no están directamente relacionados con la seguridad de la información, deben establecerse e implementarse para garantizar una adecuada protección de los activos de la empresa.

12. RESPONSABILIDADES DE LOS EMPLEADOS PÚBLICOS.

Todas y todos los servidores públicos de la Gobernación del Putumayo, cualquiera que sea el tipo de trabajo o relación contractual, departamento, secretaría u organismo dependiente, a que estén adscritos y la tarea o trabajo que desempeñen, deberán suscribir un convenio que contenga términos y condiciones que rigen el uso de los recursos informáticos, así como las reglas y configuraciones que permiten el uso de la información de la organización.

Los procedimientos para la obtención de las respectivas configuraciones y las características de cada una de esas configuraciones deberán ser mantenidos y actualizados por cada departamento, secretaría o filial, de acuerdo con los lineamientos que emita el documento. software del equipo.

El Líder de Talento Humano, en colaboración con la Unidad de Gestión de Tecnología e Información, será responsable de crear, actualizar, mantener e implementar un plan de capacitación en seguridad de la información basado en proyectos de socialización y mejora, concientización en temas de seguridad de la información personal y colectiva para todos los empleados.

La Unidad de Gestión de Tecnología e Información publicará en medios impresos y virtuales como intranets, correo electrónico, entre otros, información relacionada con temas de seguridad de la información como responsabilidad en el manejo de información, manejo de registros, archivos, mejores prácticas, amenazas a la seguridad, y más.

13. RESPONSABILIDADES DE LOS USUARIOS EXTERNOS

La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo; con los usuarios externos y empleados de organizaciones o empresas externas deben ser autorizados por un designado dentro de la Gobernación de Putumayo, quien será responsable de controlar y monitorear el uso racional del acceso a la información y fomentar el uso justo de las tecnologías, recursos si se proporcionan.

Los procedimientos de registro y seguimiento de dichos usuarios serán diseñados, implementados y mantenidos por La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo en colaboración con Servicios al Ciudadano.

El propietario de los activos de información será responsable de instruir a los usuarios externos autorizados para que hagan un buen uso de los componentes de información y la tecnología proporcionada.

Todos los usuarios externos, sin excepción, deben aceptar por escrito las condiciones de uso de la información organizacional y los recursos TIC.

Las cuentas de usuarios externos deben configurarse específicamente y tener una fecha de vencimiento no mayor a dos (2) meses, renovable según la naturaleza del usuario.

14. USUARIOS INVITADOS Y SERVICIOS DE ACCESO PÚBLICO.

El acceso de los usuarios no registrados al sitio web debe estar autorizado únicamente a la información de la organización o para interactuar y realizar transacciones como ciudadano, así como los servicios de Internet a los que pueden acceder, protegidos con una contraseña pública, pero deben tener restringido el acceso no autorizado. sitio web y límite de ancho de banda. Si el usuario invitado no ha completado el proceso de registro, no se permite el acceso a cualquier otro tipo de recursos de información, aplicaciones y/o herramientas TIC.

15. SEGURIDAD FÍSICA Y DEL ENTORNO

Se debe controlar y restringir el acceso a los centros de datos y salas de comunicaciones críticas. La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo preparará y mantendrá estándares de acceso, controles y registros para esas áreas.

Seguridad del dispositivo:

Los servidores que contienen información y servicios organizacionales deben mantenerse en un entorno seguro y protegido con al menos:

- Seguridad física y control de acceso.
- Sistema de detección y extinción de incendios.
- Control de humedad y temperatura.

- Bajo riesgo de inundación.
- El sistema eléctrico está regulado y respaldado por un sistema de alimentación ininterrumpida

Toda la información corporativa en formato digital debe almacenarse en servidores aprobados por La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo. La información de la organización no podrá almacenarse en servidores ajenos, sin la respectiva aprobación por escrito del comité de seguridad de la información de la organización.

Los equipos críticos de comunicaciones deben estar alimentados por una red eléctrica regulada y protegidos por un convertidor de frecuencia.

La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo debe asegurarse de que la infraestructura de la red de datos local se mantenga y sea totalmente compatible con el hardware y el software.

Las estaciones de trabajo deben estar protegidas y ser operadas adecuadamente por el personal del establecimiento, quien debe estar capacitado en el contenido de esta política y en la responsabilidad personal por el uso y manejo de la información de la organización.

Los medios en los que se almacenen las copias de seguridad deben mantenerse adecuadamente de acuerdo con las políticas y normas que La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo desarrolle y mantenga para este fin.

Las organizaciones dependientes son responsables de adoptar y seguir estándares definidos para crear y administrar copias de seguridad.

16. AUTORIDAD DE OPERACIONES Y COMUNICACIONES

Los empleados vinculados a la Gobernación de Putumayo están obligados a reportar de manera diligente, efectiva y responsable las brechas significativas de seguridad a través de La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo. Cuando existan hechos que lo justifiquen y concurran circunstancias excepcionales, estos informes podrán ser realizados directamente por el observador del incidente o de la novedad.

La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo deberá disponer de las herramientas informáticas necesarias para la elaboración de dichos informes.

La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo diseñará, mantendrá y difundirá normas, procedimientos y lineamientos para el reporte e investigación de incidentes de seguridad.

La Gobernación del Putumayo podrá, de conformidad con la ley, interceptar o monitorear las comunicaciones a través de diversos mecanismos con la autorización previa del Comité de Seguridad de la Información y en todos los casos, previo aviso a los afectados por la decisión.

La Oficina de Gerencia de Tecnología de la Información mantendrá procedimientos escritos para la operación de los sistemas de información cuando los sistemas de información no estén disponibles que tengan un impacto significativo en el desarrollo normal del negocio o afecten la continuidad del negocio. Se deben seguir los procedimientos establecidos para garantizar la confiabilidad del servicio que brindan.

17. PROTECCIÓN CONTRA SOFTWARE MALICIOSO Y HACKING.

Se debe proteger todos los sistemas de información teniendo en cuenta un enfoque multinivel que involucre controles humanos, físicos técnicos y administrativos.

La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo elaborará y mantendrá un conjunto de políticas, normas, estándares, procedimientos y guías que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking.

Como control básico, todas las estaciones de trabajo de la Gobernación de Putumayo, edificio central y sedes externas deben estar protegidas por software antivirus con arquitectura cliente servidor, con capacidad de actualización automática en cuanto a firmas de virus. Los usuarios de la estación no están autorizados a deshabilitar este control.

La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo es responsable de monitorear el tráfico de la red local cuando hay evidencia de actividad inusual o adversa.

El área responsable está obligada a mantener una base de datos de alertas de seguridad reportadas por las autoridades competentes y actuar en consecuencia cuando una alerta pueda tener un impacto significativo en el funcionamiento del sistema, la información, las aplicaciones y el software en general.

18. COPIAS DE SEGURIDAD

Toda la información contenida en el inventario de activos de información de una organización o de interés para un proceso operativo o crítico debe protegerse mediante copias de seguridad realizadas de acuerdo con los procedimientos ordenados por Comité de Seguridad de la Información por escrito.

Este procedimiento debe incluir actividades para almacenar copias en lugares seguros.

Los registros de respaldo deben almacenarse en una base de datos creada para este propósito.

Comité de Seguridad de la Información debe definir los procedimientos de copia de seguridad, la gestión y la conservación de las copias de seguridad.

La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo debe proporcionar herramientas para que sus dependientes vean los registros de información y los registros de respaldo.

La Oficina de Control Interno está obligada a realizar auditorías aleatorias para determinar el correcto funcionamiento de los procedimientos de contingencia.

Las operaciones de respaldo de información crítica deben realizarse y mantenerse en un programa determinado y publicado.

La realización de copias de seguridad de los archivos utilizados, mantenidos o creados por usuarios individuales es responsabilidad exclusiva de dichos usuarios, es decir, la responsabilidad de realizar las copias y actualizarlas es directamente de cada usuario propietario del capital de información del Sujeto.

El usuario deberá entregar copias de seguridad al jefe de departamento respectivo para su registro y custodia. Se deben proporcionar los medios para llevar a cabo estas actividades, lo que no genera responsabilidad alguna para La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo

19. ADMINISTRACIÓN DE REDES LOCALES.

Configuración de terminales de red, enrutadores, conmutadores, cortafuegos, sistemas de detección de intrusos y otros dispositivos de seguridad de red; Debe estar documentado, acompañado de una copia de seguridad y mantenido por La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo.

Todos los dispositivos tecnológicos deben ser revisados, registrados y aprobados por La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo, antes de conectarse a cualquier nodo de la red de datos y comunicaciones de la organización. Indicar una dependencia desconecta los dispositivos que no son de confianza y reporta esta conexión como un incidente de seguridad para ser analizado e investigado.

20. INTERCAMBIAR INFORMACIÓN CON ENTIDADES EXTERNAS.

Las solicitudes de información de terceros deben ser aprobadas por la Oficina de Control Interno de Gestión y remitidas a los responsables de la gestión y custodia.
Las solicitudes de información a entidades externas deberán realizarse por un medio válido que permita dejar constancia de la solicitud, en donde deberá identificarse el remitente, asunto y fecha.

Toda la información organizacional debe ser manejada de conformidad con las leyes colombianas y la normativa aplicable.

21. INTERNET Y CORREO ELECTRÓNICO Y SISTEMAS DE INFORMACIÓN AUTOMATIZADOS

Reglas para el uso de intranet, Internet, software antivirus, sistemas operativos, sistemas de información automatizados, paquetes y servicios de software de oficina La reglas serán desarrollada, mantenida y actualizada por La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo y El Comité de Seguridad de la Información; en todos los casos este comité debe velar por el cumplimiento del código de Integridad de la organización y la gestión responsable de sus recursos en tecnologías de la información y las comunicaciones.

22. INSTALACIÓN DE SOFTWARE

Toda instalación de software que se realice sobre sistemas operativos previamente instalados en la Gobernación del Putumayo, deberá ser aprobada por La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo de acuerdo a un proceso desarrollado para tal efecto.

No está permitido instalar software que viole las leyes de propiedad intelectual y derechos de autor, especialmente la Ley 23 de 1982 y leyes relacionadas. La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo debe desinstalar cualquier software ilegal y registrarlo como un incidente de seguridad que debe ser investigado.

La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo es responsable de mantener una base de datos que contenga un repositorio de software autorizado para ser utilizado e instalado en los sistemas informáticos de la organización.

23. CONTROL DE ACCESO

23.1 TIPOS DE ACCESO

El acceso a los recursos informáticos de una organización debe estar restringido a una configuración de usuario definida por el Comité de Seguridad de la Información.

23.2 CONTROLES DE NOMBRE DE USUARIO Y CONTRASEÑA

Se debe controlar el acceso a la información restringida. Se deben utilizar sistemas de autenticación que gestionen automáticamente los inicios de sesión o las firmas digitales.

La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo es responsable de la preparación, mantenimiento y publicación de los documentos de servicio de red proporcionados por la organización a sus funcionarios, ciudadanos y terceros.

Además, debe desarrollar, mantener y publicar procedimientos de administración de cuentas de usuario para el uso de servicios de red.

El acceso a los sistemas informáticos, y a los datos que los contienen; es de exclusiva responsabilidad del personal responsable de dichas aplicaciones o sistemas de información.

La Gobernación de Putumayo debe esforzarse por mantener al mínimo la cantidad de cuentas de usuario requeridas por los funcionarios y terceros para acceder a los servicios de red.

El control de acceso a los dispositivos intermedios de la red es responsabilidad de La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo. Estas contraseñas deben cifrarse o cifrarse y almacenarse de forma segura.

Las contraseñas de los administradores de los diversos sistemas deberán mantenerse bajo La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo y deberán ser cambiadas periódicamente y en todos los casos cuando cambie el personal asignado al cargo.

Además, La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo debe desarrollar, mantener y actualizar procedimientos y lineamientos para la correcta definición, uso y complejidad de las contraseñas de los usuarios.

Al terminar la relación contractual o laboral de un empleado con la Gobernación del Putumayo, La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo emitirá un certificado de suspensión y/o cancelación de cuentas creadas a los respectivos usuarios, dentro de cada sistema de gestión de información en el que haya operado (intranet , correo electrónico, sistemas de información automatizados, entre otros) por un período de tiempo razonable debido a la posible renovación de la relación, contrato o régimen laboral, vencido el plazo, la cuenta será cancelada si no hay renovación.

24. COMPUTADORA MÓVIL

La Gobernación del Putumayo, que lidera La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo, debe reconocer el alto nivel de exposición que genera la información y datos almacenados en dispositivos móviles (laptops, notebooks, PDA, celulares, etc.). Con base en lo anterior, el Encargado de Talento Humano es el responsable de coordinar con La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo la elaboración, mantenimiento e implementación de planes de capacitación para promover la formación y sensibilización en materia de seguridad.

Las redes inalámbricas presentan nuevos riesgos de seguridad que deben ser identificados, evaluados y abordados de acuerdo con los lineamientos de la Política de Seguridad de Redes Inalámbricas elaborada por el Comité de Seguridad de la Información.

25. AUDITORÍA Y SEGUIMIENTO

Todo uso de los recursos informáticos de la Gobernación de Putumayo debe ser monitoreado y auditado de acuerdo con los lineamientos establecidos por la Oficina de Gestión TIC

26. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.

Software

Para apoyar los procesos misionales y estratégicos la Gobernación de Putumayo debe hacer uso intensivo de las Tecnologías de la Información y las Comunicaciones.

Los sistemas de software utilizados pueden ser adquiridos a través de terceras partes o desarrollados por personal vinculado a la Gobernación de Putumayo.

La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo debe, elaborar, mantener y difundir el "La Metodología de Desarrollo de Sistemas Software en la Gobernación de Putumayo" que incluya lineamientos, procesos, buenas prácticas, plantillas y demás artefactos que sirvan para regular los desarrollos de software internos en un ambiente de mitigación del riesgo y aseguramiento de la calidad.

Todo proyecto de desarrollo de software interno debe contar con un documento de Identificación y Valoración de Riesgos del proyecto.

La Gobernación de Putumayo no debe emprender ningún desarrollo, ni mantenimiento, de sistemas de software de alto riesgo que no puedan remediarse.

Los sistemas de software adquiridos a través de terceros deberán acreditar el cumplimiento de estándares de calidad durante su desarrollo e integración con las plataformas tecnológicas existentes en la entidad.

27. CUMPLIMIENTO

Todo uso justo y monitorear el uso de los recursos TI Información y comunicaciones dentro de la entidad, deben cumplir con las normas internas y reglamentos, así como las leyes y reglamentos nacionales vigentes, incluyendo la Resolución 266 del 30 de mayo de 2013, por la cual se regula el soporte tecnológico, la compra y/o desarrollo de hardware y software dentro del gobierno de Putumayo.

28. RESTAURACIÓN DE LA INFORMACIÓN

Activos relacionados: Datos

Todos los sistemas de información que componen la plataforma de la entidad incluirán la documentación necesaria para garantizar la ejecución de tareas de recuperación de la información.

Cada procedimiento de restauración de información incluirá las funciones y responsabilidades del personal participante en la restauración de esta.

29. SOFTWARE DE LOS EQUIPOS DE CÓMPUTO.

Activos relacionados:
Aplicaciones informáticas

Todos los computadores de la entidad estarán configurados y vinculados al dominio y con su respectivo antivirus licenciado.

La información se almacenará únicamente en la partición del disco duro, destinada para tal fin.

El personal encargado de La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo realizará el seguimiento de los equipos de cómputo conectados a la red de la entidad.

El personal encargado de La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo programará y ejecutará mantenimiento preventivo al software de los equipos de cómputo conectados a la red de la entidad.

30. SERVIDORES

Activos relacionados:
Equipos informáticos.
Talento Humano.

Los servidores que proporcionan los servicios a la entidad deberán:

- Funcionar todos los días (7 X 24) con el fin de garantizar la disponibilidad del servicio (A excepciones programadas).
- Ser monitoreados por el personal asignado en el Unidad Gestión Tecnología de Información.
- Recibir mantenimiento preventivo mínimo dos veces al año y recibir mantenimiento semestral (de acuerdo con el plan de mantenimiento).
- Recibir mantenimiento anual que incluya la revisión de su configuración.

Los Servidores de la entidad no deben ser empleados como estaciones de trabajo, ni tener instaladas aplicaciones de usuario final, tales como navegadores y clientes de correo electrónico, así como tampoco software de escritorio.

Las excepciones a esta recomendación deben estar documentadas y aprobadas por el profesional universitario de La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo, en el caso de que algunos servidores requieran la instalación de software de usuario final para el funcionamiento de aplicaciones.

Los usuarios con derechos de administrador deben tener dos cuentas distintas, una de uso administrativo y otra para tareas generales. Se debe usar la cuenta con privilegios de administrador sólo cuando se tenga que realizar en el servidor trabajos que requieran de estos privilegios.

31. MANTENIMIENTO Y SEGURIDAD FÍSICA.

Activos relacionados:

Equipos informáticos
Instalaciones
Redes de comunicaciones

Se debe mantener actualizado el inventario de todos los equipos y dispositivos que formen parte de la infraestructura tecnológica de la Entidad, debe incluir características como: fecha de adquisición, proveedor, modelo, responsable, garantía, y demás aspectos que la oficina responsable estime conveniente, además de contener la hoja de vida del estado actual del equipo y las configuraciones o mantenimientos realizados. Es necesario que la Unidad de Gestión de Recursos Físicos reporte a La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo los nuevos ingresos de elementos de tecnología y comunicaciones para ser ingresados al sistema de seguimiento que se maneja en el área.

La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo realizará el mantenimiento periódico preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física en informática, y su acondicionamiento específico, de acuerdo con el procedimiento establecido.

La Unidad de Gestión de Tecnología e Información de la Gobernación de Putumayo formulará y ejecutará el plan de mantenimiento preventivo de los equipos.

El cambio de lugar al interior del área de un equipo de cómputo se debe coordinar con La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo, los cuales dispondrán de las condiciones adecuadas para su traslado tales como: puntos de red, eléctrico y demás aspectos; así como también se debe actualizar en el inventario las razones de cambio, y el nombre del nuevo responsable si lo hay.

Los equipos de cómputo, cables, UPS, planta eléctrica, aires acondicionados, dispositivos de almacenamiento y de comunicación inalámbrica, deben estar amparados en pólizas contra todo riesgo.

No está permitido el consumo de líquidos, alimentos, ni humo dentro de los centros de datos o lugares donde se encuentren los equipos de cómputo.

32. DOTACIÓN Y PROTECCIÓN DE LOS CENTROS DE DATOS

Activos relacionados:
Equipamiento auxiliar
Instalaciones

Se deben implementar mecanismos de seguridad física como detectores de humo, medidores de temperatura, humedad, sensores de movimiento, aire acondicionado, cableado debidamente instalado, puertas seguras y demás elementos en las áreas donde se encuentran los equipos de comunicación y servidores propiedad de la entidad con el fin de protegerlos.

Las instalaciones de comunicaciones y eléctricas deben estar protegidas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.

La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo debe contar con un plano actualizado de las instalaciones de red de comunicaciones y eléctricas de la Entidad.

33. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Activos relacionados:

Inventario de activos

La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo con el apoyo de la alta dirección (Gobernador y Secretarías) deben crear un plan de contingencias informáticas que contenga al menos los siguientes puntos:

- Identificar los sucesos que pueden ocasionar interrupciones en los procesos de la entidad, así como también identificar los riesgos, y las consecuencias para la seguridad de la información.
- Contar con procedimientos informáticos alternos que permitan continuar con la operación de la Entidad.
- Tener los respaldos de información en un lugar seguro, fuera del perímetro físico donde se encuentran los equipos.

- Tener el apoyo de medios magnéticos o en forma física (documentos), de los procesos necesarios para reconstruir los archivos dañados.

- Se debe disponer de los planes necesarios para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempos requeridos, después de la interrupción o la falla de los procesos críticos para la entidad; para que toda acción correctiva se efectúe con la mínima degradación posible de los datos.

- Es importante tener un directorio actualizado del personal interno o externo de soporte, a los cuales se pueda llamar en el momento que se presente las fallas.

- Ejecutar pruebas de la funcionalidad y revisiones periódicas del plan de acuerdo con la identificación de prioridades para asegurar su actualización y su eficacia.

34. RESTRICCIONES

Las políticas definidas anteriormente se establecen como un firme compromiso por parte de todos los servidores públicos de la GOBERNACIÓN DE PUTUMAYO y así mismo deben ser divulgadas a través de toda la organización siendo implementados de forma que genere confianza y garantice la funcionalidad de los sistemas de la Entidad:

- Se prohíbe intentar, evadir o violar la seguridad o autentificación de usuario de cualquier host, red o cuenta.

- Se prohíbe a cualquier usuario acceder a servicios informáticos utilizando cuentas o medios de autenticación de otros usuarios. Aún con la autorización expresa del usuario propietario de la misma.

- Se prohíbe el almacenamiento, instalación, configuración o uso de software no licenciado o no autorizado o de datos no autorizados en los equipos informáticos de la Gobernación de Putumayo.

- Se prohíbe el uso, distribución y ejecución de software o código malicioso que cause daño, hostigamiento, molestias a personas, daño o alteración de información o traumatismos en la continuidad de los servicios informáticos o vulnere la seguridad de los sistemas.

- Se prohíbe el hurto, robo, sustracción o uso no autorizado de: datos, información, materiales, equipos y otros elementos pertenecientes a los activos informáticos de la Gobernación de Putumayo.

- Se prohíbe el acceso, modificación o alteración no autorizada de componentes, datos o información de los activos informáticos de la Gobernación de Putumayo.

- Se prohíbe el uso de medios electrónicos, medios de almacenamiento, software, hardware, datos o información en medios digitales provenientes de fuentes no certificadas o de terceros, sin la previa revisión y autorización de la Unidad Gestión Tecnología de Información.

- Se prohíbe el almacenamiento y reproducción de aplicaciones, programas o archivos de audio o video que no están relacionados con las actividades propias de las funciones que cumple la dependencia o el usuario.

- El software y hardware, se debe verificar para asegurar que son compatibles con otros componentes del sistema.

- Sé prohíbe la instalación en los equipos de la entidad de juegos y/o software diferente al instalado y autorizado por el profesional responsable de la Unidad Gestión Tecnología de Información de la Gobernación de Putumayo.

35. EXCEPCIONES

- Cuando se realicen eventos, capacitaciones, talleres, conferencias o visitas de personal externo que requieran hacer uso de los servicios de la red de datos de la Gobernación, se podrán habilitar equipos de manera temporal por el tiempo necesario, previa solicitud del profesional de la unidad interesado.

- En el caso de ser necesario habilitar servicios restringidos (redes sociales, YouTube u otros portales), también se deberá realizar la solicitud justificada por parte del profesional de la unidad responsable del proceso. (Si aplica)

- Entre las directivas de seguridad dispuestas por la entidad se encuentra configurado el firewall para restringir algunas categorías y sitios de Internet; por lo tanto, pueden existir portales que a pesar de ser inofensivos están restringidos su acceso, en este caso, los servidores públicos pueden notificar a La Unidad de Gestión de Tecnología e Información de la Gobernación del Putumayo para habilitarlos siempre y cuando cumplan con las políticas establecidas por la entidad.

36. GESTIÓN Y CLASIFICACIÓN DE ACTIVOS

La Gobernación del Putumayo, posibilitando así, la gestión y clasificación de los Activos, con el propósito de inventariarlos por usos, roles y responsabilidades que tienen los funcionarios sobre los mismos y, reconociendo adicionalmente el nivel de clasificación de la información que a cada activo debe dársele.

Se debe considerar que con la Gobernación un inventario de Activos de Información se cumple con lo que a nivel estratégico se ha definido en el Modelo de Seguridad y Privacidad

de la Información, con respecto a la seguridad de los activos de información de los procesos de la Entidad, y cuyo objetivo es dar cumplimiento a los puntos principales descritos en el Ítem 8 de la Tabla 2 - Guía 8 - Controles de Seguridad y Privacidad de la Información

Tabla 02: Controles de Seguridad y Privacidad de la Información, MINTIC
https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf
Tomada de la Guía 8 - Controles de Seguridad y Privacidad de la Información comprenden que la información es parte fundamental de los servicios que presta la Gobernación, y para garantizar su confidencialidad, integridad y disponibilidad, consideran necesario adoptar estrategias que permitan establecer niveles adecuados de protección, asegurando la continuidad en la prestación de servicios a sus diferentes usuarios.

Por tal razón, el presente lineamiento se articula con los principios generados por el Ministerio de las TICS (Guía No. 05 Guía para la Gestión y Clasificación de Activos de Información) y con los parámetros establecidos por el estándar internacional ISO/IEC 27001.

Enlace:
https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

37. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN	FECHA
01	Creación del documento: El documento fue creado con el nombre: "Manual de política de seguridad y privacidad de la información". Código MA-GTI-001	30/04/2019
02	Actualización del documento según lineamientos de la Resolución 74367 del 17 de noviembre de 2021 del Ministerio de Comercio, Industria y Turismo Superintendencia de Industria y comercio El documento fue creado el 30-04-2019 como Manual de Política de Seguridad y Privacidad de la Información código MA-GTI-001; sin embargo, su estructura obedece a una "Política", razón por la cual se realiza su modificación y denominación a Política así: Política de Seguridad y Privacidad de la Información PA-GTI-001 V 02. Asimismo, se elimina el documento MA-GTI-001 V 01	27/04/2022