# EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE PITALITO EMPITALITO E.S.P.

# POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION


**HENRY LISCANO PARRA**
**GERENTE**


**2023**

## TABLA DE CONTENIDO

## 1. INTRODUCCION

En Colombia se viene adelantando la implementación de la política de gobierno digital, tal como lo establece el decreto 1008 de 2018, cuyas disposiciones se compilan en el Decreto Único Reglamentario del Sector TIC 1078 de 2015, específicamente en el capítulo 1, titulo 9, parte 2, libro 2; como un instrumento fundamental para mejorar la gestión pública y la relación del estado con los ciudadanos, la cual, se ha articulado con el Modelo Integrado de Planeación y Gestión como una herramienta dinamizadora para cumplir las metas de las políticas de desarrollo administrativo, articulada a otras políticas esenciales para la gestión pública en Colombia.

El Manual de Política de Gobierno Digital expedido por el Ministerio de Tecnologías de información y de las Comunicaciones establece que la política tiene como propósito promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones, para consolidar un Estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital. Según el manual, la implementación de la política de Gobierno Digital se ha definido en dos componentes: TIC para el Estado y TIC para la sociedad, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales. Estos cinco elementos, se desarrollan a través de lineamientos y estándares que son requerimientos mínimos que todos los sujetos obligados deben cumplir para alcanzar los logros de la política.

El manual en mención, precisa que el habilitador de seguridad de la información busca que las empresas públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Este habilitador se soporta en el Modelo de Seguridad y Privacidad de la información –MSPI.

Como parte de los procesos tecnológicos de la empresa, entendiendo la importancia de mantener segura, integra, confiable y disponible toda la información que se maneja en EMPITALITO E.S.P, se presenta el Plan de Seguridad y privacidad de la Información. Este, busca proteger la información y los elementos clave dentro de la empresa tales como: activos, equipos y demás componentes de la infraestructura tecnológica y su información, definiendo las responsabilidades que deben asumir cada uno de los funcionarios de la empresa, durante su permanencia en la misma. Esto con el fin de desarrollar operaciones y servicios seguros, basados en normativas y estándares en seguridad de la información. Igualmente, se contempla la definición de estrategias y actividades que se deben llevar a cabo durante la implementación de este plan y su permanente control, validación y actualización.

Este plan es aplicable a todo el contexto empresarial y del negocio de la empresa de servicios públicos EMPITALITO E.S.P, incluyendo sus recursos tecnológicos y humanos, a la totalidad de los procesos internos y externos, a los proveedores, contratistas y/o terceros que de alguna forma pudieran tener alguna manera habitual u ocasional de interacción con la información o con los equipos y dispositivos propios y/o de la empresa.

Cualquier problema que sea detectado por las diferentes áreas y usuarios de la empresa que hagan uso de los recursos tecnológicos en materia de seguridad de la información, se deberá informar al área TIC de la empresa, como responsable del control y de la seguridad de la información, quien tratará de subsanar lo ocurrido.

Es importante mencionar que, la definición del plan de seguridad y privacidad de la información se realiza con base en las directrices del MINTIC y las líneas de operación relacionadas con seguridad de la información en la Empresa, que permiten generar la capacidad requerida para la ejecución de las actividades definidas en este documento.

La adopción, implementación y evaluación del modelo mencionado, es una actividad obligatoria según lo expresado en el artículo 2.2.9.1.3.2., en el numeral 2, en los literales A, B y C, el cual debe ser planificado en atención a lo establecido en el decreto 612 de 2018, que en el artículo 1 señala la importancia de la integración de los planes institucionales y estratégicos al Plan de Acción Institucional, en el ámbito de aplicación del modelo integrado de planeación y gestión.

## 2. JUSTIFICACIÓN

El Estado colombiano cuenta con normatividad vigente que obliga el adecuado tratamiento de la información manejada por la Empresa en términos de confidencialidad, integridad y disponibilidad. Entre otras se citan:

- Ley 1437 de 2011, Capítulo IV, "utilización de medios electrónicos en el procedimiento administrativo".

"Los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos."

- Ley 1581 de 2012, g) Principio de seguridad:

"La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento."

- Ley 1581 de 2012, Artículo 17, ítem d:

"Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento".

- Ley 1712 de 2014, "principio de transparencia":

"Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta ley se presume pública, en consecuencia, de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley."

- Ley 1712 de 2014, artículo 7:

"Disponibilidad de la información" "En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten."

- Ley 1712 de 2014 -Título III:

"Excepciones acceso a la información" "Información exceptuada por daño de derechos a personas naturales o jurídicas. Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito."

- Decreto 1413 de 2017, artículo 2.2.17.6.6:

"Seguridad de la información." "Los actores que traten información, en el marco del presente título, deberán adoptar medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prácticas consignadas en el modelo de seguridad y privacidad de la información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, o un sistema de de seguridad de la información certificable. Esto con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información."

- Decreto 1413 de 2007, artículo 2.2.17.6.1:

"Responsable y encargado del tratamiento": "Los operadores de servicios ciudadanos digitales serán responsables del tratamiento de los datos personales que los ciudadanos le suministren directamente y encargados del tratamiento respecto de los datos que otras empresaes le proporcionen."

- Decreto 612 de 2018, artículo 1.

"Integración de planes institucionales y estratégico. Las empresas del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y , al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web."

- Conpes 3854 de 2016, objetivo general

"Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país".

Por lo anterior, la empresa de servicios públicos EMPITALITO E.S.P debe emprender acciones orientadas a la protección de la información que gestiona, realizando la identificación y tratamiento de riesgos de la información de los activos críticos que la soportan, de manera que se establecen y realiza el seguimiento a dichas acciones en el marco del plan de acción y del Sistema Integrado de gestión.

## 3. DEFINICIONES / GLOSARIO

- **Administrador de Base de Datos:** Un administrador de bases de datos (ODBA) tiene la responsabilidad de mantener y operar las bases de datos que conforman el sistema de información de una compañía.
- **Activo de información:** recurso del sistema de información que tiene valor para la organización.
- **Activos de información:** bases de datos, documentación física y digital, software, hardware, equipos de comunicación, servicios informáticos y de comunicaciones, infraestructura (iluminación, energía, aire acondicionado, etc.) y las personas (son quienes generan, transmiten y destruyen información)
- **Análisis del riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo [ISO 27000:2014].
- **Amenaza:** Una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización [ISO 27000:2014].

- **Centro de Comunicaciones:** Cualquier oficina dentro de la empresa de servicios de públicos EMPITALITO E.S.P que cuenten con equipamiento de cómputo, telecomunicaciones o servidores.
- **Comité:** Equipo integrado por La Gerencia, el Gestor de Seguridad y los líderes de procesos.
- **Ciberdefensa:** Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.
- **Cibernética:** Ciencia o disciplina que estudia los mecanismos automáticos de comunicación y de control o técnica de funcionamiento de las conexiones de los seres vivos y de las máquinas. (Academia de la Lengua Española)
- **Ciberdelito / Delito Cibernético:** Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito. (Ministerio de Defensa de Colombia)
- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Comunicación del riesgo:** Comunicar o intercambiar la información acerca del riesgo entre la persona que toma la decisión y otras partes interesadas.
- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. [ISO/IEC 27000: 2014] .
- **Cifrado:** Que está escrito con letras, símbolos o números que solo pueden comprenderse si se dispone de la clave (llave criptográfica) necesaria para descifrarlos.
- **Cifrar:** Es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) que transforma la información, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta.
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada [27000:2014].
- **Data Center (Centro de Datos):** Oficina con equipos de cómputo, telecomunicaciones y servidores que prestan servicios a todas las áreas de la empresa de servicios públicos EMPITALITO E.S.P con las características físicas y ambientales adecuadas para que los equipos alojados funcionen sin problema.
- **Gerencia:** Representante de nivel superior de la empresa de servicios públicos EMPITALITO E.S.P que a su vez integra el comité de seguridad. Bajo su administración están la aceptación y seguimiento de las Políticas de Seguridad.
- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una amenaza con relación a la probabilidad de ocurrencia.

- **Líder de Seguridad informática:** Persona dotada de conocimientos técnicos, encargada de velar por la seguridad de la información, realizar auditorías de seguridad, elaborar documentos de seguridad como, políticas, normas; y de llevar un estricto control de los servicios prestados y niveles de seguridad aceptados para tales servicios. Este rol es desempeñado por el encargado de los procesos tecnológicos de la empresa, con apoyo de la gerencia y los funcionarios de la misma.
- **Identificación del riesgo:** Proceso para encontrar, numerar y caracterizar los elementos del riesgo.
- **Impacto:** Cambio adverso en el nivel de los objetivos del negocio logrado.
- **Integridad:** Propiedad de la información relativa a su exactitud y completitud. [ISO/IEC 27000: 2014]
- **Probabilidad:** Frecuencia o factibilidad de ocurrencia del riesgo.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- **Red:** Equipos de cómputo, SISTEMAS de información y redes de comunicación, que hacen parte de la infraestructura del EMPITALITO E.S.P.
- **Responsable de Activos:** Personal del área administrativa de la empresa, que velará por la seguridad y correcto funcionamiento de los activos informáticos, así como de la información procesada en éstos, dentro de sus respectivas áreas. Esta persona debe mantener el inventario físico al día, velar por que todos los activos tengan sus respectivas pólizas de seguros bajo los parámetros entregados por la gerencia.
- **Seguridad:** Protección de los activos de información, contra amenazas que garanticen la continuidad del negocio, minimizando el riesgo y maximizando las oportunidades de la unidad.
- **Tratamiento del riesgo:** Selección e implementación de las opciones o acciones apropiadas para ocuparse del riesgo.
- **Usuario:** Cualquier persona (funcionario o no) que haga uso de los servicios de las tecnologías de información proporcionadas de la empresa de servicios públicos EMPITALITO E.S.P, tales como equipos de cómputo, SISTEMAS de información, redes de comunicaciones, etc.
- **Valor del Impacto:** Está determinado por el responsable del activo de información, quién provee el grado de afectación por incidentes o materialización de riesgos de los activos de información que tenga a cargo.
- **Vulnerabilidad:** La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

## 4. OBJETIVO

### Objetivo General

Establecer los lineamientos que permitan proteger, asegurar y salvaguardar confidencialidad, integridad y disponibilidad de los activos de información de la empresa de servicios públicos EMPITALITO E.S.P, teniendo en cuenta los procesos, la operación, los objetivos de negocio y los requisitos legales vigentes en la empresa.

### Objetivos Específicos

- Definir la política de seguridad y privacidad de la información la empresa de servicios públicos EMPITALITO E.S.P.
- Definir los lineamientos a ser considerados para diseñar e implementar el Sistema de Seguridad de la Información alineado con las necesidades, los procesos, los objetivos y la operación de la empresa de servicios públicos EMPITALITO E.S.P.
- Dar conformidad y cumplimiento a las leyes, regulaciones y normativas que le aplican a la empresa de servicios públicos EMPITALITO E.S.P en el desarrollo de su misión.
- Proteger los activos de información de la empresa de servicios públicos EMPITALITO E.S.P
- Mantener un sistema de políticas, manuales, procedimientos y estándares actualizados, a efectos de asegurar su vigencia y un nivel de eficacia, que permitan minimizar el nivel de riesgo de los activos de información de la empresa de servicios públicos EMPITALITO E.S.P
- Fortalecer la cultura de seguridad de la información en funcionarios, terceros y clientes de la empresa de servicios públicos EMPITALITO E.S.P, mediante la definición de una estrategia de uso y apropiación de la política.
- Garantizar la continuidad de negocio frente a la materialización de incidentes de seguridad basados en la norma ISO 27035.
- Definir una estrategia de continuidad de los procesos de la empresa frente a incidentes de seguridad de la Información.

## 5. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La implementación y sus lineamientos del Modelo de Seguridad y Privacidad de la Información asociados como directriz de la empresa de servicios públicos domiciliarios de Pitalito EMPITALITO E.S.P, será de aplicabilidad e implementación para todos los procesos y aspectos administrativos de la organización y de cumplimiento por parte de todos los funcionarios, servidores públicos, contratistas, subcontratistas, pasantes-practicantes y terceros que presten sus servicios o tengan algún tipo de relación con la Empresa.

El alcance del MSPI permitirá a la empresa definir los límites sobre los cuales se implementará la seguridad y privacidad de la información, por tanto, deberá tener en cuenta, los procesos que impactan directamente la consecución de los objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados e interrelaciones del MSPI con otros procesos.

## 6. TRATAMIENTO DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN

La administración y control de la seguridad de la información participan todos los funcionarios y contratistas de la empresa de servicios públicos EMPITALITO E.S.P, Como punto central en Seguridad de la Información se encuentra el área de TIC integrada por un ingeniero de sistemas y un técnico y/o a fines contratados encargados de los procesos tecnológicos de la empresa, el cual brindan apoyo a las demás áreas, ejecutando las funciones y responsabilidades propias asociadas a su cargo y dependencia dentro de la empresa.

Para garantizar una adecuada ejecución de los procesos y funciones referentes a la seguridad informática de la empresa; se adopta la siguiente estructura para el análisis, control y prevención tecnológica:

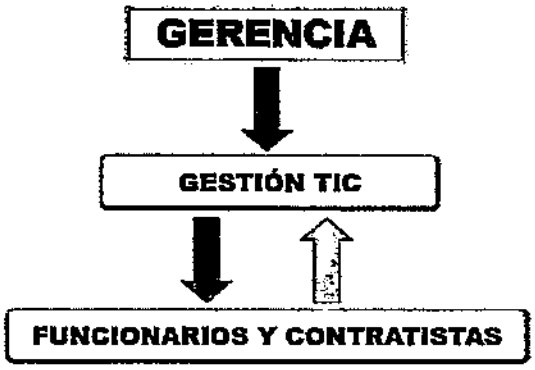


*Figura 1. Organización de la seguridad*

## 7. POLÍTICA DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN

La empresa de servicio públicos domiciliarios de Pitalito EMPITALITO ESP, entendiendo la importancia de sus activos de información para el cumplimiento de su misión institucional, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) buscando proteger la confidencialidad, integridad y disponibilidad de los activos de información y además establecer un marco de confianza en el ejercicio de su misión con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes aplicables.

EMPITALITO E.S.P pretende mediante la adopción e implementación de la Seguridad de la Información enmarcado en el Sistema de Seguridad de la información, proteger, preservar y administrar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información.

La empresa de servicio públicos domiciliarios de Pitalito EMPITALITO ESP en su propósito de dar cumplimiento con la política de seguridad y privacidad de la información, establece los siguientes compromisos:

- Fortalecer la cultura de seguridad de la información en los funcionarios, servidores públicos, contratistas, aprendices, practicantes y clientes de la empresa de servicios públicos domiciliarios de Pitalito EMPITALITO ESP.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Definir los riesgos de los activos de información teniendo en cuenta el nivel de tolerancia al riesgo de la empresa.
- Un plan integral de riesgos basada en la implementación de controles físicos y digitales orientados a la prevención de incidentes.
- La implementación de políticas de seguridad de alto nivel y de políticas complementarias por cada dominio de la norma ISO/IEC 27001 :2013, para asegurar la confidencialidad, integridad y disponibilidad de la información institucional
- Minimizar el riesgo de todos los procesos de la entidad.
- Mejorar continuamente el sistema de gestión de seguridad de la información.
- Implementar los controles tecnológicos necesarios para la protección de los activos de la entidad y para la reducción de los riesgos.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, junta directiva o terceros.
- Proteger la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej: proveedores o clientes), o como resultado de un servicio interno en Outsourcing.
- Se mitigarán los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital de forma efectiva, eficaz y eficiente, y se protegerá la información creada, procesada, transmitida o

resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- Se implementará control de acceso a la información, sistemas y recursos de red.
- Se garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- Se garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- EMPITALITO E.S.P. protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio y proyectos de inversión, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de la misma. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

## 8. POLITICA GENERAL

- La información que se maneja en la empresa de servicios públicos domiciliarios de Pitalito EMPITALITO ESP, solamente podrá ser utilizada con fines de interés público de conformidad con la constitución y las leyes.
- Las herramientas y servicios informáticos asignados a cada usuario, son para uso limitado a la función institucional.
- Todos los servidores públicos, contratistas y terceros que conforman las diferentes áreas de EMPITALITO ESP deberán clasificar la información que tengan bajo su custodia en alguna de las categorías establecidas.
- La información confidencial de terceros que por cualquier circunstancia se conozca por parte de EMPITALITO ESP, debe ser tratada bajo los mismos lineamientos establecidos para el tratamiento de la información confidencial de la entidad.
- Toda la información catalogada por las áreas como critica debe contar con copias de respaldo para garantizar su seguridad.
- Los centros de cómputo y procesamiento de información son áreas de acceso restringido por tal motivo el ingreso y permanencia debe ser controlado y supervisado.
- El acceso a los diferentes equipos informáticos y sistemas de información debe hacerse a través de los mecanismos de autenticación establecidos de acuerdo con los niveles de seguridad.
- El acceso no autorizado a los sistemas de información y uso indebido de los recursos informáticos de la entidad está prohibido. Se considera que hay uso indebido de la información y de los recursos, cuando la persona incurre en cualquiera de las siguientes conductas:

  - Suministrar información confidencial o que tenga carácter reservado a quien no tenga derecho a conocerla.

- Usar la información con el fin de obtener beneficio propio o de terceros
- Ocultar la información maliciosamente causando cualquier perjuicio.
- Hacer pública la información sin la debida autorización
- Hurtar software de EMPITALITO ESP (copia o reproducción entre usuarios finales).
- Realizar copias no autorizadas de software de EMPITALITO ESP, dentro y fuera de sus instalaciones.
- Falsificar y duplicar un producto informático de EMPITALITO ESP.
- Descargar software, a través de Internet sin la debida autorización
- Intentar modificar, reubicar o sustraer equipos de cómputo, software, información o periféricos sin la debida autorización.
- Capturar sin autorización la información de los accesos de otros usuarios a los sistemas.
- Transgredir o burlar los mecanismos de autenticación u otros sistemas de seguridad.
- Utilizar la infraestructura de EMPITALITO ESP (computadores, software, información o redes) para acceder a recursos externos con propósitos ilegales o no autorizados.
- Enviar cualquier comunicación electrónica fraudulenta.
- Apropiarse los aplicativos, desarrollos o información de EMPITALITO ESP y publicarla como propio.
- Adueñarse del trabajo de otros individuos, o de alguna manera apropiarse del trabajo ajeno.
- Usar cualquier medio para dañar o perjudicar de alguna manera los recursos disponibles electrónicamente.
- Lanzar cualquier tipo de virus, gusano o programa de computador cuya intención sea hostil o destructiva.
- Descargar o publicar material ilegal, o implique la vulneración de derechos de terceros, o material nocivo usando un recurso de EMPITALITO ESP.
- Uso personal de cualquier recurso informático de EMPITALITO ESP para acceder, descargar, imprimir, almacenar, redirigir, transmitir o distribuir material prohibido.
- Acceder sin autorización a información o documentos públicos que tengan carácter reservado por disposición constitucional o legal.
- Violar cualquier Ley o Regulación Nacional respecto al uso de sistemas de información.

## 9. POLÍTICAS ESPECÍFICAS

Forman parte integral de la Política de Seguridad de la Información, todas aquellas directrices que, por su tema particular, requieren un mayor nivel de detalle y especialización para su definición, las cuales son elaboradas y mantenidas por las áreas de seguridad, según el dinamismo de la misión de EMPITALITO ESP

y las cuales a su vez pueden estar complementadas por estándares y guías, a continuación, se describen algunas de ellas:

- Políticas de seguridad física
- Políticas de seguridad lógica
- Política de seguridad de las comunicaciones
- Política de seguridad en las aplicaciones
- Política de escritorio y pantalla limpia.
- Política para el uso de los recursos de cómputo
- Política de administración de comunicaciones y operaciones
- Política de protección contra el código malicioso y móvil
- Políticas de almacenamiento, copias de respaldo o back-up
- Política para el manejo de información
- Políticas y procedimientos de intercambio de información
- Política de control de acceso a datos
- Política de uso de controles criptográficos
- Política para la asignación y uso de recursos tecnológicos de la entidad
- Política de trabajo en casa

## 10. COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección de la empresa de servicios públicos domiciliarios de Pitalito EMPITALITO ESP se compromete a apoyar y liderar el establecimiento, implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información (SGSI); así mismo, se compromete a revisar el avance de la implementación del SGSI de manera periódica y también garantizará los recursos suficientes (tecnológicos y talento humano calificado) para implementar y mantener el sistema, así mismo, incluirá dentro de las decisiones estratégicas, la seguridad de la información.

## 11. RESPONSABILIDADES DE LOS PROCESOS TECNOLÓGICOS

Como líder y punto de referencia de sistema de gestion de seguridad de la información, el encargado de los procesos tecnológicos de la empresa tiene la responsabilidad de:

- Identificar objetivos de seguridad, tales como prevención de virus, uso de herramientas de monitoreo etc.

- Implementar la solución de antivirus en los equipos de la empresa de servicios públicos EMPITALITO E.S.P, Solucionar contingencias presentadas ante el surgimiento de virus que la solución haya detectado automáticamente.
- Configurar y supervisar el analizador de red para la detección de virus.
- Administrar los accesos a las principales aplicaciones de la empresa de servicios públicos EMPITALITO E.S.P,
- Mantener las políticas y estándares de seguridad en la información de la empresa de servicios públicos EMPITALITO E.S.P, monitoreando su cumplimiento por parte de todos los interesados en la empresa.
- Definir metodologías y procesos relacionados con la seguridad informática.
- Comunicar aspectos básicos de seguridad de información a los funcionarios. Esto incluye programas de inducción y reinducción para comunicar aspectos básicos y las políticas, siguiendo los planes de capacitación definidos en la empresa.
- Controlar e investigar incidentes de seguridad o violaciones de seguridad, previo, durante y posterior a que suceda.
- Evaluar aspectos de seguridad de productos de tecnología, SISTEMAS o aplicaciones utilizados en la empresa, a través de evaluaciones periódicas de vulnerabilidades de los sistemas conformados por la red de datos y comunicaciones de la empresa de servicios públicos EMPITALITO E.S.P,
- Coordinar todas las funciones relacionadas a seguridad tales como: seguridad física, seguridad de personal y seguridad de información almacenada en medios no electrónicos.
- Generar reportes a la Gerencia de la empresa sobre consolidado de incidentes, informes, validación de información y/o actualización de las políticas en seguridad de la información.
- Demás responsabilidades y funciones definidas en los contratos referentes a la prestación de servicios tecnológicos, control del aplicativo y cargo desempeñado en la empresa.

## 12. RESPONSABILIDADES DE LOS USUARIOS

Las responsabilidades de los usuarios finales (funcionarios, servidores públicos, trabajadores oficiales, contratistas, subcontratistas, pasantes-practicantes, proveedores e interesados) que utilizan la información y los medios de comunicación, distribución y transporte de datos de la empresa de servicios públicos EMPITALITO E.S.P, como parte de su trabajo son:

- Mantener la confidencialidad de las contraseñas, haciendo uso adecuado de las mismas.
- Reportar supuestas violaciones de la seguridad que puedan afectar los procesos de la empresa en términos de seguridad de la información.
- Asegurarse de ingresar información adecuada a los sistemas de información de la empresa, siguiendo los procedimientos para dichas actividades correctamente y no cambiar/modificar/copiar/eliminar (integridad de la información) dichos datos, para beneficio propio y/o de terceros.

- Utilizar la información digital y física de la empresa únicamente para los propósitos definidos en los estatutos, gobierno corporativo, código de ética y organización de la empresa.
- Adecuarse a las políticas de seguridad de la información, siguiendo los protocolos y lineamientos definidos en el presente plan y apoyados con los demás planes incluidos dentro de los requerimientos tecnológicos de la empresa.

## 13. RESPONSABILIDADES INGENIEROS Y TÉCNICOS DE SOPORTE

- Los documentos y en general la información de procedimientos, seriales, software etc. deben mantenerse custodiados en todo momento para evitar el acceso a personas no autorizadas.
- Para el cambio o retiro de equipos de funcionarios, se deben seguir políticas de saneamiento, es decir llevar a cabo mejores prácticas para la eliminación de la información de acuerdo al software disponible en la entidad. Ejemplo: Formateo seguro, destrucción total de documentos o borrado seguro de equipos electrónicos.
- Los funcionarios encargados de realizar la instalación o distribución de software, sólo instalarán productos con licencia y software autorizado.
- Los funcionarios de la oficina TIC no deben otorgar privilegios especiales a los usuarios sobre las estaciones de trabajo, sin la autorización correspondiente del Jefe del Área.

Los Ingenieros y técnicos de Soporte tendrán las siguientes atribuciones y/o responsabilidades:

- Podrán ingresar de forma remota a los computadores única y exclusivamente para la solución de problemas y bajo solicitud explícita del propietario del computador.
- Deberán utilizar los analizadores previa autorización del usuario y bajo la supervisión de éste, informando de los propósitos y los resultados obtenidos.
- Deberán realizar respaldos periódicos de la información de los recursos de cómputo que tenga a su cargo, siempre y cuando se cuente con dispositivos de respaldo.
- Deben actualizar la información de los recursos de cómputo de la empresa de servicios públicos EMPITALITO E.S.P, cada vez que adquiera e instale equipos o software.
- Deben registrar cada máquina en el inventario de control de equipos de cómputo y red de la empresa de servicios públicos EMPITALITO E.S.P,
- Deben auditar periódicamente y sin previo aviso los SISTEMAS y los servicios de red, para verificar la existencia de archivos no autorizados, música, videos, imágenes y/o configuraciones no válidas o permisos extra que pongan en riesgo la seguridad de la información.
- Realizar la instalación o adaptación de sus sistemas de cómputo de acuerdo con los requerimientos en materia de seguridad.
- Reportar a la Gerencia y al encargado de los procesos tecnológicos de la empresa los incidentes de violación de seguridad, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo.

## 14. APLICABILIDAD

La presente política, sus objetivos, además de los manuales, procedimientos o documentos derivados o complementarios aplican a toda la entidad, funcionarios, servidores públicos, contratistas, aprendices, practicantes de EMPITALITO ESP.

El incumplimiento a la Política de Seguridad y Privacidad de la Información o de sus lineamientos derivados, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad.

## 15. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ROLES Y RESPONSABILIDADES)

EMPITALITO ESP, define los roles y responsabilidades para la implementación del MSPI y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos derivados (Manuales, Procedimientos, Formatos etc....):

| ROL / INSTANCIA / DEPENDENCIA | RESPONSABILIDADES (Definir los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN) |
|---|---|
| **Gerencia / Alta Dirección** | • Proporcionar los recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la información (Recursos económicos, formación y recursos tecnológicos). |
| **Comité de Gestión y Desempeño** | • Aprobar los recursos correspondientes para la implementación y el mantenimiento del sistema de gestión de seguridad de la información. |
| **Gestion TIC** | • Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información. |
| **Funcionario en Seguridad Digital** | • Analizar, definir, documentar y gestionar el plan estratégico de seguridad de la información y proponer las decisiones que permitan gestionar la seguridad de la información en el marco del cumplimiento de la política y los lineamientos definidas y aprobados por la entidad.<br>• Apoyar en la generación de los lineamientos (Manuales, procedimientos y formatos) que permitan el establecimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información en la Entidad. |

| ROL / INSTANCIA / DEPENDENCIA | RESPONSABILIDADES (Definir los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN) |
|---|---|
| **Talento Humano** | • Asegurar que los funcionarios, servidores públicos, contratistas, subcontratistas, pasantes-practicantes tomen conciencia de sus responsabilidades en seguridad de la información y las cumplan, además de dar aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos. |
| **Control Interno** | • Incluir la seguridad de la información, dentro de los planes de auditoría institucionales.<br>• Apoyar en situaciones de posibles violaciones a las políticas de seguridad de la información. |
| **Prensa / Comunicación Interna** | • Apoyar en las labores de comunicación y sensibilización en seguridad de la información, para difundir la información en todos los niveles de la entidad. |
| **Oficina de Contratación** | • Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores y contratistas de la entidad.<br>• Procurar la protección de la seguridad de la información de todos los activos de la información que puedan verse involucrados en procesos o contratos. |
| **Líderes de Proceso** | • Implementar las políticas y procedimientos de seguridad de la información que se definan como parte del SGSI (Por ejemplo: gestión de activos, gestión de riesgos, entre otros). |
| **Todos los funcionarios y contratistas** | • Apoyar a los líderes de proceso en el desarrollo de tareas como gestión de activos y gestión de riesgos.<br>• Cumplir a cabalidad con las políticas y procedimientos de seguridad de la información definidos y aprobados. |

## 16. SANCIONES

a. Cualquier violación a las políticas de seguridad de la información de la empresa de servicios públicos domiciliarios de Pitalito EMPITALITO ESP debe ser sancionada de acuerdo con el Reglamento Interno de Trabajo, a las normas, leyes y estatutos de la ley colombiana, así como la normativa atinente y supletoria, y apoyados en las leyes regulatorias de delitos informáticos de Colombia.

b. Las sanciones podrán variar dependiendo de la gravedad y consecuencias generadas de la falta cometida o de la intencionalidad de la misma.

## 17. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI

EMPITALITO ESP indica que realizará revisiones periódicas al SGSI. Dichas revisiones estarán enfocadas en los siguientes aspectos:

- Revisión de indicadores definidos para el Sistema de Gestión de Seguridad de la Información.
- Revisión de avance en la implementación del Modelo de Seguridad y Privacidad de la Información del Ministerio TIC.
- Revisión de avance de la Política de Seguridad Digital de acuerdo con lo solicitado por FURAG o la herramienta definida para tal fin.

## 18. APROBACIÓN Y REVISIONES A LA POLÍTICA

Esta política será efectiva desde su aprobación por la Gerencia. La revisión de esta política se hará en las siguientes condiciones:

1. De forma anual, donde se deberá revisar la efectividad de la política y sus objetivos.
2. Si se dan cambios estructurales en la entidad (restructuración de áreas o procesos).
3. Incidentes de seguridad de la información que requieran que la política requiera cambios.

## 19. CONTROL DE CAMBIOS

| VERSIÓN N°. | FECHA DE APROBACIÓN. | DESCRIPCIÓN DEL CAMBIO. |
|---|---|---|
| 1 | 27/11/2023 | Se crea la política general de seguridad de la información |

## 20. APROBACIÓN

| | Elaboró | Revisó | Aprobó |
|---|---|---|---|
| Nombre | Jefersson Silva Losada | Mónica Alexandra Lagos | Henry Liscano Parra |
| Cargo | Profesional de Sistemas | Jefe Oficina de Planeación y Proyectos | Gerente |

HENRY LISCANO PARRA
GERENTE