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

MANUAL DE POLITICAS 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.

Teniendo en cuenta lo anterior, el presente Manual tiene como finalidad de establecer los principios orientadores en seguridad que buscan garantizar la disponibilidad, integridad, confidencialidad, privacidad, continuidad, autenticidad y no repudio de la información del Ministerio, así como dar lineamientos para la aplicación de mecanismos que eviten la vulneración de la seguridad y privacidad de la información, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información – SGSI/ Modelo de Seguridad y Privacidad de la Información – MSPI, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital. Para que el Ministerio incorpore la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información.

Sé encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas, el MSPI pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital. Y Se desarrolla mediante el Documento Maestro del Modelo de Seguridad y Privacidad de la Información y sus guías de orientación.

2. DEFINICIONES / GLOSARIO

- **Administrador de Base de Datos:** Un administrador de bases de datos (CDBA) 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 caracteristicas fisicas 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.

3. OBJETIVO

Establecer lineamientos relacionados con la seguridad de la información abordando temáticas específicas, como complemento a lo definido en la "Política General de Seguridad de la Información de EMPITALITO ESP" con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de la empresa de servicios públicos domiciliarios de Pitalito EMPITALITO ESP

4. ALCANCE DEL MANUAL

El presente manual de políticas de seguridad 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.

5. POLITICAS

La empresa de servicios públicos domiciliarios de Pitalito EMPITALITO ESP, establece a continuación, los siguientes lineamientos de seguridad de la información, los cuales deberán ser cumplidos por todos los funcionarios, contratistas, terceros, usuarios y visitantes.

Los lineamientos de seguridad están clasificados en diferentes temáticas, teniendo en cuenta el contexto interno y externo de la entidad.

5.1. POLÍTICAS DE SEGURIDAD FÍSICA

Objetivo

Administrar el Data center, equipos, dispositivos, los medios de almacenamientos y las personas que conforman el sistema informático de la empresa y que estas cumplan con las medidas necesarias en lo relativo a la infraestructura física y al mantenimiento de la seguridad de los recursos de la organización.

❖ **Acceso Físico:**

- Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario no tenga acceso físico directo.
- Entendiendo por sistema de comunicaciones: el equipo activo y los medios de comunicación.
- El acceso de terceras personas debe ser identificado plenamente, controlado y vigilado durante el acceso portando una identificación que les será asignado por el área de seguridad de acceso al edificio y a las oficinas de la empresa.
- Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas cuando menos por un responsable del área de TIC .
- Las visitas a las instalaciones físicas al centro de Datos se harán en el horario establecido.
- El personal autorizado para mover, cambiar o extraer equipo de cómputo es el poseedor de este o el superior responsable, a través de formatos de autorización de Entrada/Salida, los cuales notificarán a las personas delegadas del Área Administrativa de la empresa EMPITALITO E.S.P y al personal de seguridad del edificio.

❖ Data Center:

- Es un área restringida, con un sistema de control de acceso que garantice la entrada solo al personal autorizado por el encargado de los procesos tecnológicos de la empresa y/o la gerencia general de la empresa de servicios públicos EMPITALITO E.S.P.
- Recibir limpieza al menos una vez por semana, que permita mantenerse libre de polvo.
- Estar libre de contactos e instalaciones eléctricas en mal estado.
- Aire acondicionado. Mantener la temperatura a 21 grados centígrados.
- Existe un control diario temperatura y aires acondicionados para llevar un registro de estos controles.
- Respaldo de energía redundante.
- Seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.
- Los sistemas de tierra física, sistemas de protección e instalaciones eléctricas están recibiendo mantenimiento anual con el fin de determinar la efectividad del sistema.
- Contar con un esquema que asegure la continuidad del servicio.
- Prevención y/o detección de incendios.
- Contar con dos extintores de incendio adecuado y cercano al Data Center.

❖ Control de acceso Infraestructura:

- EMPITALITO E.S.P cuenta con guardas de seguridad; en horarios laborales y se ubican en el interior del edifico.
- El personal que tiene acceso permitido lo realiza con sistema biométrico ubicado en el quinto piso.

❖ Instalaciones de equipos de cómputo:

La instalación del equipo de cómputo quedará sujeta a los siguientes lineamientos:

- Los equipos para uso interno se instalarán en lugares adecuados, lejos de polvo y tráfico de personas.
- El espacio de trabajo de los encargados de los procesos tecnológicos de la empresa, así como las áreas operativas deberán contar con un plano actualizado de las instalaciones eléctricas y de comunicaciones del equipo de cómputo en red.
- Las instalaciones eléctricas y de comunicaciones, estarán preferiblemente fijas o en su defecto resguardadas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.
- Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.
- En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.

❖ Control de activos:

- El área de almacén y/o el encargado de los procesos tecnológicos de la empresa deben llevar un control total y sistematizado de los recursos de cómputo y licenciamiento.
- Los encargados del área de TIC son los responsables de organizar al personal encargado del mantenimiento preventivo y correctivo de los equipos de cómputo.
- El área de Recursos Humanos deberá reportar al área de TIC cuando un usuario deje de laborar o de tener una relación con la empresa el fin de retirarle las credenciales de ingreso a los recursos y supervisar la correcta devolución de los equipos y recursos asignados al usuario.

- El usuario, en caso de retiro deberá tramitar ante la Oficina de TIC paz y salvo correspondiente, incluyendo la eliminación de los permisos, privilegios, usuario y contraseña asignados durante su labor en la empresa.
- Los encargados de los procesos tecnológicos de la empresa no podrán remover del sistema ninguna información de cuentas individuales, a menos que la información sea de carácter ilegal, o ponga en peligro el buen funcionamiento de los SISTEMAS, o se sospeche de algún intruso utilizando una cuenta ajena.

❖ **Configuración e instalación de servidores:**

El encargado de los procesos tecnológicos de la empresa tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad en los servidores conectados a la Red. Igualmente:

- La instalación y/o configuración de todo servidor conectado a la red será responsabilidad del encargado de los procesos tecnológicos de la empresa.
- Durante la configuración de los servidores, el encargado de los procesos tecnológicos de la empresa debe generar las normas para el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios.

Los servidores que proporcionen servicios a través de la red e Internet deberán:

- Funcionar 24 horas del día los 365 días del año.
- Recibir mantenimiento preventivo mínimo una vez al año
- Recibir mantenimiento semestral que incluya depuración de logs.
- Recibir mantenimiento anual que incluya la revisión de su configuración.
- Ser monitoreados por el encargado de los procesos tecnológicos de la empresa.

La información de los servidores deberá ser respaldada de acuerdo con los siguientes criterios, como mínimo:

- Diariamente, información crítica.
- Semanalmente, los documentos web.
- Mensualmente, configuración del servidor y logs.
- Los servicios hacia Internet sólo podrán proveerse a través de los servidores autorizados por el encargado de los procesos tecnológicos de la empresa.

5.2. POLÍTICAS DE SEGURIDAD LÓGICA

Objetivo

Determinar los controles de accesos de los usuarios a las plataformas de procesamiento informático y a los datos que éstas gestionan, con el fin de controlar irregularidades que obstaculicen la confidencialidad, exactitud y disponibilidad de la información, y las mejoras que fueran factibles de efectuarse.

❖ **Uso de Contraseñas de parte de los usuarios de red y aplicaciones:**

El uso de contraseñas robustas (Mínimo 8 dígitos con combinaciones alfanuméricas y símbolos , con caducidad máxima de 45 días) constituye la primera línea de defensa para el acceso a la información y a los recursos, razón por la cual el correcto uso de las contraseñas generadas para los usuarios de la red y aplicaciones, es de vital importancia en la seguridad de la información, por lo tanto deben cumplirse lineamientos básicos de seguridad que serán de acatamiento obligatorio por parte de todos los usuarios de la red y aplicaciones, dichos aspectos buscan que los usuarios utilicen contraseñas más "robustas".

Aplicación: En el directorio activo se activará para todos los usuarios las políticas de Contraseñas requeridas por EMPITALITO E.S.P. Esta política aplicara al login de inicio, de la aplicación, y demás programas que se considere necesario. Es de vital importancia que ningún usuario quede por fuera de la aplicación de la política para evitar fugas de seguridad.

❖ **Identificación de Usuarios y contraseñas:**

- Todos los usuarios con acceso a un sistema de información o a la Red, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.
- Ningún usuario recibirá un identificador de acceso a la Red, Recursos Informáticos o Aplicaciones hasta que no acepte formalmente la Política de Seguridad vigente.
- El usuario deberá definir su contraseña de acuerdo al procedimiento establecido para tal efecto y será responsable de la confidencialidad de esta.
- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recurso que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por La Gerencia y/o el encargado de los procesos tecnológicos de la empresa.
- La longitud mínima de las contraseñas será igual o superior a seis caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.
- Los identificadores para usuarios temporales se configurarán para un corto periodo de tiempo. Una vez expirado dicho periodo, se desactivarán de los SISTEMAS.

El usuario deberá renovar su contraseña y colaborar en lo que sea necesario, a solicitud del área de TIC, con el fin de contribuir a la seguridad de los servidores en los siguientes casos:

- Cuando ésta sea una contraseña débil o de fácil acceso.
- Cuando crea que ha sido violada la contraseña de alguna manera.

El usuario deberá notificar a el área de TIC en los siguientes casos:

- Si observa cualquier comportamiento anormal (mensajes extraños, lentitud en el servicio o alguna situación inusual) en el servidor.
- Si tiene problemas en el acceso a los servicios proporcionados por el servidor.
- Si un usuario viola las políticas de uso de los servidores, el encargado de los procesos tecnológicos de la empresa podrá cancelar totalmente su cuenta de acceso a los servidores, notificando a La Gerencia.

❖ **Administración De Contraseñas Por Parte De Los Administradores Del Directorio Activo (Active Directory) Y Administradores De Aplicaciones:**

La correcta administración de las contraseñas generadas para los usuarios de la red y aplicaciones de para la empresa de servicios públicos EMPITALITO E.S.P, es de vital importancia en la seguridad de toda la información institucional, por lo tanto, deben cumplirse lineamientos básicos de configuración de seguridad que deberán ser aplicados por los administradores de red, de aplicaciones, desarrolladores, personal de soporte. La administración correcta de las contraseñas incluye entre otros aspectos, velar porque los usuarios usen contraseñas seguras.

Aplicación: todas las contraseñas utilizadas en los equipos de administración tales como, router, servidores, aplicaciones y demás alas que hubiere lugar, deben ser de conocimiento al gerente encargado y reposadas en una bitácora debidamente protegidas y asignadas a los subalternos de acuerdo con su rol de responsabilidad.

❖ **De Contraseñas De Administrador De Las Estaciones De Trabajo:**

Con el fin de prevenir el acceso no autorizado a los datos de las estaciones de trabajo propiedad de la empresa de servicios públicos EMPITALITO E.S.P, la cuenta de administrador local de cada una de las estaciones de trabajo propiedad de la entidad, debe administrarse y configurarse de manera segura (Mínimo 8 dígitos con combinaciones alfanuméricas y símbolos, con caducidad máxima de 45 días), ya que de ello depende minimizar el riesgo de que terceros puedan acceder a la información almacenada en las mismas.

- La cuenta de administrador local de las estaciones de trabajo, tiene que ser creada y administrada, considerando características de seguridad y robustez iguales a las que se configuran para las cuentas de red y aplicaciones.
- Los administradores de la red, deben ser colaboradores activos con los usuarios en el cumplimiento de esta política.
- Las estaciones de trabajo que estén fuera del dominio deben contener una contraseña única y usuario de rol estándar al igual que los equipos que se encuentren dentro del dominio de la empresa de servicios públicos EMPITALITO E.S.P, local en este último se aplicará como política de grupo.

❖ **Desarrollo, mantenimiento y actualización de aplicaciones:**

La implementación de políticas y estándares para el desarrollo y mantenimiento de sistemas, además de homologar la forma de trabajo, fomentará el avance y sobre todo la innovación tecnológica, aprovechando al máximo los recursos actuales y futuros, procurando además la integración de las tecnologías y evitando su obsolescencia prematura.

El desarrollo de aplicaciones y la de proyectos informáticos sean estos internos o externos, deberán basarse en los lineamientos de la entidad para el desarrollo y mantenimiento de sistemas de información, según lo

defina la Oficina TIC con el propósito de gestionar de forma óptima y homogénea las actividades que conlleva este proceso.

Importante: La cuentas y claves de acceso de administrador y usuarios finales, tiene que ser creada y administrada, considerando características de seguridad y robustez iguales a las que se configuran para las cuentas de red y equipos (Mínimo 8 dígitos con combinaciones alfanuméricas y símbolos, con caducidad máxima de 45 días).

❖ **Confidencialidad de la información institucional y trato con terceros:**

Cada funcionario contratado por la institución, para cumplir con las tareas propias de su cargo, tiene acceso a información de la empresa en diferentes formatos (escrita, digital o verbal). Ejemplos de este tipo de información son las notas, circulares, minutas, acuerdos, bases de datos, reportes, consultas a los sistemas de información.

Toda la información confidencial a la cual cada funcionario o contratista tiene acceso en cumplimiento de sus funciones debe ser administrada de modo que no sea divulgada a personas que podrían utilizarla en beneficio propio, en contra de terceros o de la propia institución.

- Ningún funcionario podrá modificar, borrar, esconder o divulgar información en beneficio propio o de terceros.
- En la norma asociada con esta política, se hace referencia a la normativa y base legal que sustenta el principio de confidencialidad de la información

5.3. POLÍTICA DE SEGURIDAD DE LAS COMUNICACIONES

Objetivo

Controlar la seguridad de las comunicaciones, los datos transmitidos, los dispositivos usados durante la transmisión, la documentación necesaria para la realización eficiente e ininterrumpida de esta transmisión, y los sistemas usados para la transmisión de datos de un entorno a otro, comprobando el cumplimiento de las normas de seguridad de la información.

- Las redes tienen como propósito principal servir en la transformación e intercambio de información dentro de la empresa entre usuarios, departamentos, oficinas y hacia afuera a través de conexiones con otras redes o con los Clientes y/o Convenios.
- La gerencia o el encargado de los procesos tecnológicos de la empresa no son directamente responsables por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.
- Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo y/o el encargado de los procesos tecnológicos de la empresa.
- No se permite el uso de los servicios de la red cuando no cumplan con las labores propias de la empresa
- Las cuentas de ingreso a los SISTEMAS y los recursos de cómputo son propiedad de la empresa de servicios públicos EMPITALITO E.S.P y se usarán exclusivamente para actividades relacionadas con la labor asignada.
- Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.

- El uso de analizadores de red es permitido única y exclusivamente por el encargado de los procesos tecnológicos de la empresa, con el fin de monitorear la funcionalidad de las redes, contribuyendo a la consolidación del sistema de seguridad bajo las Políticas de Seguridad.
- Cuando se detecte un uso no aceptable, se cancelará la cuenta o se desconectará temporal o permanentemente al usuario o red involucrada dependiendo de las políticas. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

❖ **Navegación En Internet:**

El uso de Internet se concede a los funcionarios como una herramienta que colabora y apoya en la realización de las tareas, por lo tanto, cada usuario debe darle un uso apropiado a este servicio estrictamente relacionado con las labores que desempeña en la institución, cualquier uso para otros propósitos no es aceptable. El usuario deberá considerar las medidas de racionalidad y seguridad que garanticen que su trabajo se llevará a cabo de una manera eficiente y productiva.

- EMPITALITO E.S.P, dependiendo del mal uso o abuso que le dé el usuario al servicio otorgado para la navegación en Internet, suspenderá o eliminará el servicio, en caso de comprobarse mal uso o abuso del mismo, según se define en la norma asociada con esta política.
- EMPITALITO E.S.P cuenta con herramientas automatizadas para monitorear y filtrar todas las actividades con respecto al uso de Internet que realicen los usuarios y los informes y reportes que se generan con dichas herramientas podrán ser utilizadas como evidencia del mal uso o abuso del servicio de navegación, según se define en la norma asociada con esta política.

❖ **Redes sociales:**

La empresa de servicios públicos EMPITALITO E.S.P. define las pautas generales para asegurar una adecuada protección de la información de la empresa, en el uso del servicio de mensajería instantánea y de las redes sociales, por parte de los usuarios autorizados.

- La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de la empresa de servicios públicos EMPITALITO E.S.P., que sea creado a nombre personal en redes sociales como: twitter®, facebook®, youtube® likedink®, blogs, instaram, etc, se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.
- Toda información distribuida en las redes sociales que sea originada por la entidad, debe ser autorizada por los jefes de área para ser socializadas y con un vocabulario institucional.
- No se debe utilizar el nombre de la entidad en las redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la filosofía de la empresa.
- Las personas designadas para el manejo operativo de las redes sociales en la Entidad (Community Manager), los funcionarios, contratistas y demás colaboradores de la empresa deben acatar las directrices dadas por el jefe inmediato.
- La dependencia que requiera la apertura de una red social bajo el dominio de empres o que tenga nombre de las dependencias adscritas empresa; debe presentar una solicitud por servicios en línea, motivada relacionando la necesidad, objeto y alcance de la cuenta institucional, enunciando los datos personales de los funcionarios administradores y dinamizadores de la red social.

- Los responsables de cada red social deberán aplicar complejidad en las contraseñas de las cuentas institucionales, acatando los protocolos de seguridad de las mismas y realizando el cambio periódicamente, de acuerdo a lo establecido en el Manual de Políticas de Seguridad de la Información.
- No se recomienda la administración de las redes sociales de la empresa en dispositivos móviles personales.

❖ **Conexiones Externas:**

La seguridad del servidor de hosting el cual es contratado y cuenta con la seguridad y estabilidad en sus sistemas ofreciendo lo siguiente:

- Protección pasando por un firewalls (firewall proveído por el centro de datos)
- Servidores DNS redundantes ubicados en dos lugares distintos en Estados Unidos. Con un servidor primario y secundario sincronizados entre sí, lo que impedirá interrupciones en la resolución de dominios si alguno llegara a presentar inconvenientes técnicos.
- Todos los servidores de hosting se encuentran monitoreados 24 horas al día 365 días al año mediante un sistema que revisa todos los servicios de cada uno de los servidores y envía notificaciones a los técnicos ante cualquier anomalía.
- Monitoreo de la red, cuenta con un sistema de monitoreo del tráfico que pasa por la red lo que permite detectar ataques y anomalías, permitiéndonos tomar acciones de inmediato.
- Cuenta con un Sistema de Detección de Intrusos que bloqueará los ataques antes de que lleguen a los servidores.
- Se Realizan copias de seguridad de la información almacenada en los servidores de hosting mediante un sistema comercial de Backus (R1Soft) que realiza copias diarias incrementales en un servidor de Backus externo.

❖ **Uso del correo electrónico:**

EMPITALITO E.S.P les proveerá cuentas de correo personales, la cuenta de correo electrónico es personal y se asignará a todos los servidores y/o contratistas de la empresa con dominio "EMPITALITO.GOV.CO", así mismo, se configurar una cuenta de correo GMAIL, la cual tendrá relación con los cargos de la entidad y esta se parametrizará con sistema de reenvió de correos con la cuenta con dominio EMPITALITO.GOV.CO.

En el caso de requerir una cuenta de correo para un grupo especial u otro correo en su área, se debe solicitar la creación de este por medio de un correo enviado al área de TIC especificando el nombre del grupo, o área a desempeñar, la persona responsable del mismo y el objetivo o función que tendrá la cuenta de correo electrónico.

- Es obligación tanto de los servidores públicos como de los contratistas, leer e interiorizar la normativa descrita en el documento de términos y condiciones de uso del correo electrónico personal Institucional de la empresa de servicios públicos EMPITALITO E.S.P.
- El encargado de los procesos tecnológicos de la empresa se encargará de asignar las cuentas a los usuarios para el uso de correo electrónico en los servidores que administra.
- La cuenta será activada en el momento en que el usuario ingrese por primera vez a su correo y será obligatorio el cambio de la contraseña de acceso inicialmente asignada.

- El correo electrónico no se deberá usar para envío masivo, materiales de uso no institucional o innecesarios (entiéndase por correo masivo todo aquel que sea ajeno a la empresa, tales como cadenas, publicidad y propaganda comercial, política, social, etcétera
- Los buzones de correo asignados a los funcionarios, contratistas o terceros pertenecen a EMPITALITO ESP, por lo tanto, su contenido también es propiedad de la Entidad.
- El correo electrónico solo deberá emplearse para uso institucional y el desempeño de las funciones correspondientes a cada cargo.
- La oficina TIC de la entidad, podrá verificar el contenido de los buzones de los correos telefónicos en los casos que se requiera acudir a información para continuar con la prestación del servicio o para investigaciones específicas.

5.4. POLÍTICA DE SEGURIDAD EN LAS APLICACIONES

Objetivo

La seguridad de la información evalúa las aplicaciones utilizadas en la empresa de servicios públicos EMPITALITO E.S.P, la consistencia de sus datos de entrada y la exactitud de sus datos de salida, la integridad de las bases de datos y la existencia y el uso de la documentación necesaria para su funcionamiento, de acuerdo a los estándares propuestos.

❖ **Software:**

El área TIC de acuerdo con las disponibilidades existentes de software ha fijado un estándar para ser utilizado por las áreas. Todo equipo de cómputo antes de ser entregados al usuario final cuenta con dicho software, que es denominado Software Institucional.

Así mismo existe software adicional utilizado para el desarrollo de soluciones automatizadas y que es de uso exclusivo del área de TIC.

La empresa cuenta con tres servidores y un sistema NAS:

- Servidor 1: Con Sistema operativo Linux (Ubuntu server 12) para la base de Datos del sistema de gestion Documental (ORFEO),
- Servidor 2: Servidor asignado para el sistema HASSQL con SQL server estándar y Windows server 2016.
- Servidor 3: Servidor con sistema operativo LINUX (Ubuntu server 22.04) para la base de datos del sistema Help Desk (GLPI).
- Servidor 4: servidor NAS synology para copias de seguridad.

- **HASSQL:** La empresa cuenta con dos aplicaciones de gran importancia que son financiera y comercial; la aplicación financiera de la empresa esta suministrada por la empresa HAS-SQL la cual trabaja bajo un motor de la base de datos es SQL Server. (NO SUMINISTRADO POR HAS SQL SAS.), un Sistema Operativo Windows Server 2012 en adelante por lo que la empresa está desarrollado con herramientas de programación SQL, Ms Vbasic, Ms Access, con estructura Cliente Servidor y Bases de Datos Relacional con integridad referencial , el cliente se ejecuta en modo RUN-TIME sin necesidad de licenciar Software

adicional para su funcionamiento. La empresa se ejecuta bajo el sistema operativo: Windows 10. Estos softwares se encuentran funcionando desde hace aproximadamente un año.

- **Soluciones Globales S.A.S:** provee un sistema de información comercial desarrollado especificamente para atender las necesidades del sector de servicios públicos. Considera toda la reglamentación como la ley 142, 1437 de 2011 y sus decretos reglamentarios. Por lo anterior el sistema es parametrizable y "Multiservicio", es decir que soporta los procesos de cualquier Servicio público como Aseo, Acueducto y Alcantarillado. A continuación, enumeraremos algunos de los módulos y Servicios de cada una de las plataformas. Soluciones Globales es una empresa legalmente constituida desde 2000 y Certificada bajo la norma ISO 9001:2015, hace parte de Marca Colombia TI, Están valorados bajo modelo CMMI (Capability Matueity Model) Dev Nivel III, desarrollado bajo la convocatoria MinTIC – Colciencias. Esta herramienta trabja con empresas de servicios públicos y directamente en el proceso de Gestión comercial (Centros de Recaudo, Seguimiento Georreferenciado procesos Operativo, Centros de Atención al Cliente, Facturación, Gestión de Cartera, Critica de Consumos, Catastro de Usuarios, Catastro de Medidores, Procesos Técnicos Operativos Acueducto y alcantarillado); presta los servicios de lectura, impresión y distribución de facturas, así como las visitas previas de crítica, visitas de seguimiento de consumos y/o novedades, visitas de atención de reclamaciones (pqr).

- **Orfeo:** Es un sistema de Gestión Documental y de procesos desarrollado inicialmente por la Superintendencia de Servicios Públicos Domiciliarios (SSPD) en Colombia, licenciado como software libre bajo licencia GNU/GPL para compartir el conocimiento y mantener la creación colectiva. Orfeo permite incorporar la gestión de los documentos a los procesos de cualquier organización, automatizando procedimientos, con importantes ahorros en tiempo, costos y recursos tales como toners de impresora, papel, fotocopias, entre otros, así como el control sobre los documentos. Además de la SSPD, Orfeo se está utilizando y/o implementado en un sinnúmero de entidades tanto públicas como privadas que reúnen ya más de 15.000 usuarios y se estudia su uso por parte de entidades y organizaciones en otras partes del mundo, gracias a su filosofía de Software Libre. Ésta herramienta puede instalarse en cualquier sistema Operativo (GNU/Linux, Unix, Windows, ...), con diferentes bases de datos (PostgreSQL, Oracle y MS SQL Server), además maneja múltiples tipos de Formatos (ODT, XML, DOC), logrando así obtener independencia de plataforma tecnológica y reducción de costos en la implementación.

- **GLPI:** Es una herramienta web en software libre que ofrece una gestión integral del inventario informático de la empresa además de incluir un sistema de gestión de incidencias (ticketing / helpdesk). La herramienta está desarrollada para entornos LAMP (Apache-PHP-MySQL), por lo que puede ser instalada tanto en servidores Windows como Linux y su fácil instalación y manejo permite gestionar todo el soporte y mantenimiento informático de la empresa de una manera rápida y sencilla. Este doble papel de gestor de inventario (equipos, servidores, periféricos, licencias de software, topología de red, reserva de recursos compartidos, etc) y helpdesk para el seguimiento de intervenciones, permite a los administradores, y al personal de soporte, vincular las intervenciones realizadas a Usuarios y a equipos, generándose así un historial completo del mantenimiento realizado.

❖ **Bases de Datos:**

- El Administrador de la Base de Datos no deberá eliminar ninguna información del sistema, a menos que la información esté dañada o ponga en peligro el buen funcionamiento del sistema.
- El Administrador de la Base de Datos es el encargado de asignar las cuentas a los usuarios para el uso.
- Las contraseñas serán asignadas por el Administrador de la Base de Datos en el momento en que el usuario desee activar su cuenta, previa solicitud al responsable de acuerdo con el procedimiento generado.

- En caso de olvido de contraseña de un usuario, será necesario que se presente con el Administrador de la Base de Datos para reasignarle su contraseña.
- La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.
- Toda la información de la empresa de servicios públicos EMPITALITO E.S.P deberá invariablemente ser operada a través de un mismo tipo de sistema manejador de base de datos para beneficiarse de los mecanismos de integridad, seguridad y recuperación de información en caso de presentarse alguna falla.
- El acceso a los SISTEMAS de información deberá contar con los privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información de la empresa de servicios públicos EMPITALITO E.S.P. Los niveles de seguridad de acceso deberán controlarse por un administrador único y poder ser manipulado por software.
- Se deben delimitar las responsabilidades en cuanto a quién está autorizado a consultar y/o modificar en cada caso la información, tomando las medidas de seguridad pertinentes.
- Los datos de los SISTEMAS de información deben ser respaldados de acuerdo a la frecuencia de actualización de sus datos, guardando respaldos históricos periódicamente.
- Es indispensable llevar una bitácora oficial de los respaldos realizados, asimismo, discos portátiles, de respaldo deberán guardarse en un lugar de acceso restringido con condiciones ambientales suficientes para garantizar su conservación.
- En cuanto a la información de los equipos de cómputo personales, se recomienda a los usuarios que realicen sus propios respaldos en los servidores de respaldo externo (Google Drive) o en medios de almacenamiento alternos.
- Todos los SISTEMAS de información que se tengan en operación, deben contar con sus respectivos manuales actualizados. Uno técnico que describa la estructura interna del sistema, así como los programas, catálogos y archivos que lo conforman y otro que describa a los usuarios del sistema y los procedimientos para su utilización.
- Los SISTEMAS de información, deben contemplar el registro histórico de las transacciones sobre datos relevantes, así como la clave del usuario y fecha en que se realizó (Normas Básicas de Auditoría y Control).
- Se deben implantar rutinas periódicas de auditoría a la integridad de los datos y de los programas de cómputo, para garantizar su confiabilidad.

❖ **Condiciones bajo las que puede utilizarse Software adicional:**

Software proporcionado por el área TIC con el fin de:

- Realizar actualizaciones remotas
- Actualizar software preinstalado
- Sustituir software preinstalado
- Accesos o componentes de software instalados en los servidores de información.
- Software de uso emergente o temporal (previo análisis de disponibilidad de licencia).
- Software proporcionado por el área de TIC a través de medios no directos (instalaciones no asistidas).

Software que no puede ser instalado:

- Copias ilegales de cualquier programa.
- Software descargado de Internet.

- Software que no se haya identificado como institucional.
- Instalaciones no autorizadas o que no hayan sido solicitadas al área de TIC .
- Software adquirido para uso personal del usuario (sin fines institucionales).
- Software de esparcimiento.
- Software utilizado por el área TIC para el desarrollo de soluciones automatizadas.

❖ **Derechos de Autor:**

Queda estrictamente prohibido inspeccionar, copiar y almacenar programas de cómputo, software y demás fuentes que violen la ley de derechos de autor. Para tal efecto, todos los usuarios deberán firmar un documento donde se comprometan, bajo su responsabilidad, a no usar programas de software que violen la ley de derechos de autor.

Para asegurarse de no violar los derechos de autor, no está permitido a los usuarios copiar ningún programa instalado en los computadores bajo ninguna circunstancia sin la autorización escrita de la Gerencia o el encargado de TIC de la empresa.

No está permitido instalar ningún programa en su computadora sin dicha autorización o la clara verificación de que la empresa posea una licencia que cubre dicha instalación.

Se debe tener en cuenta lo siguiente:

- No está autorizada la descarga de Internet de programas informáticos no autorizados por la Gerencia o el área encargada de los procesos tecnológicos de la empresa.
- Se restringirá que el funcionario realice copias no autorizadas de programas informáticos.
- Se restringirá que un funcionario realice intercambios o descargas de archivos digitales de música (MP3, WAV, etc) de los cuales no es el autor o bien no posee los derechos de distribución de este.
- Si se descubre que un funcionario ha copiado programas informáticos o música en forma ilegal, este puede ser sancionado, suspendido o despedido.
- Si se descubre que un funcionario ha copiado programas informáticos en forma ilegal para dárselos a un tercero, también puede ser sancionado, suspendido o despedido.
- Si un usuario desea utilizar programas informáticos autorizados por el Gerente de la empresa de servicios públicos EMPITALITO E.S.P en su hogar, debe consultar con el responsable de tecnología para asegurarse de que ese uso esté permitido por la licencia del editor.
- El encargado de soporte del área de TIC revisará las computadoras constantemente para realizar un inventario de las instalaciones de programas informáticos y determinar si la empresa posee licencias para cada una de las copias de los programas informáticos instalados.
- Si se encuentran copias sin licencias, estas serán eliminadas y, de ser necesario, reemplazadas por copias con licencia.
- EMPITALITO E.S.P autorizan el uso de programas informáticos de diversas proveedoras externos. La empresa de servicios públicos EMPITALITO E.S.P no es dueño de estos programas informáticos o la documentación vinculada con ellos y, a menos que cuente con la autorización del creador de los programas informáticos, no tiene derecho a reproducirlos excepto con fines de respaldo.
- Los usuarios utilizarán los programas informáticos sólo en virtud de los acuerdos de licencia y no instalarán copias no autorizadas de los programas informáticos comerciales.

- Los usuarios que se enteren de cualquier uso inadecuado que se haga en la empresa de servicios públicos EMPITALITO E.S.P de los programas informáticos o la documentación vinculada a estos, deberán notificar al Gerente y al encargado de los procesos tecnológicos de la empresa. (ver manual de politicas).

5.5. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA.

Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los usuarios.

- Los funcionarios, contratistas, personas en comisión, pasantes y terceros que tienen algún vínculo con la empresa deben conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
- Los usuarios de los sistemas de información y comunicaciones de la empresa deben bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.
- Los usuarios de los sistemas de información y comunicaciones de la empresa deben cerrar las aplicaciones y servicios de red cuando ya no los necesite.
- Al imprimir documentos con información pública reservada y/o pública clasificada, deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.
- No se debe utilizar fotocopiadoras, escáneres, equipos de fax, cámaras digitales y en general equipos tecnológicos que se encuentren desatendidos.

5.6. POLÍTICA PARA EL USO DE LOS RECURSOS DE CÓMPUTO

Los encargados de los procesos tecnológicos de la empresa deben suministrar medidas de seguridad adecuadas contra la intrusión o daños a la información almacenada en los sistemas, así como la instalación de cualquier herramienta, dispositivo o software que refuerce la seguridad en cómputo.

El encargado de los procesos tecnológicos de la empresa deberá mantener informados a los usuarios y poner a disposición de estos, el software que refuerce la seguridad de los SISTEMAS de cómputo.

El encargado de los procesos tecnológicos de la empresa es el único autorizado para monitorear constantemente el tráfico de paquetes sobre la red, cámaras de seguridad, con el fin de detectar, reportar y solucionar anomalías, registrar usos indebidos o cualquier falla que provoque problemas en los servicios.

❖ **Uso de Servicios de Red:**

- La Gerencia definirá los servicios de Internet a ofrecer a los usuarios y se coordinará con el área de TIC para su otorgamiento y configuración.
- La Gerencia puede utilizar la infraestructura de la Red para proveer servicios a los usuarios externos y/o visitas previa autorización del encargado de los procesos tecnológicos de la empresa.

- El encargado de los procesos tecnológicos de la empresa es el responsable de la administración de contraseñas y deberán guardar su confidencialidad, siguiendo el procedimiento para manejo de contraseñas.
- No se darán equipo, contraseñas ni cuentas de correo a personas que presten servicio social o estén haciendo prácticas profesionales en la empresa de servicios públicos EMPITALITO E.S.P, excepto por orden expresa de la gerencia.
- El encargado de los procesos tecnológicos de la empresa hará respaldo de información conforme a los procedimientos establecidos.
- El encargado de los procesos tecnológicos de la empresa hará revisión de logs y reporte de cualquier eventualidad.
- Implementar de forma inmediata las recomendaciones de seguridad y reportar posibles faltas a las políticas de seguridad en cómputo.
- El encargado de los procesos tecnológicos de la empresa es el único autorizado para asignar las cuentas a los usuarios.
- El encargado de los procesos tecnológicos de la empresa podrá aislar cualquier servidor de red, notificando a las Gerencias y áreas de la empresa, en las condiciones siguientes:
- Si los servicios proporcionados por el servidor implican un tráfico adicional que impida un buen desempeño de la Red.
- Si se detecta la utilización de vulnerabilidades que puedan comprometer la seguridad en la Red.
- Si se detecta la utilización de programas que alteren la legalidad y/o consistencia de los servidores.
- Si se detectan accesos no autorizados que comprometan la integridad de la información.
- Si se viola las políticas de uso de los servidores.
- Si se reporta un tráfico adicional que comprometa a la red de la empresa de servicios públicos EMPITALITO E.S.P.

❖ **Responsabilidades Personales:** .

- Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.
- Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.
- Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.
- Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar a su jefe inmediato y éste reportar al responsable de la administración de la red.
- El Usuario debe utilizar una contraseña compuesta por un mínimo de ocho caracteres constituida por una combinación de caracteres alfabéticos, numéricos y Especiales.
- La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos.
- En caso de que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.
- En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 30 días. En caso contrario, se le podrá denegar el acceso y se deberá contactar con el jefe inmediato para solicitar al administrador de la red una nueva clave.
- Proteger, en la medida de sus posibilidades, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos.
- Guardar por tiempo indefinido la máxima reserva y no se debe emitir al exterior datos de carácter personal contenidos en cualquier tipo de soporte.

- Utilizar el menor número de listados que contengan datos de carácter personal y mantener los mismos en lugar seguro y fuera del alcance de terceros.
- Cuando entre en posesión de datos de carácter personal, se entiende que dicha posesión es estrictamente temporal, y debe devolver los soportes que contienen los datos inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos.
- Los usuarios sólo podrán crear ficheros que contengan datos de carácter personal para un uso temporal y siempre necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán ubicados en unidades locales de disco del equipo de trabajo y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.

❖ **Uso Apropiado de los Recursos:**

Los Recursos Informáticos, Datos, Software, Red y SISTEMAS de Comunicación están disponibles exclusivamente para cumplir las obligaciones y propósitos de la operativa para la que fueron diseñados e implantados. Todo el personal usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso.

Como parte del servicio y labor que se realiza día a día en las instalaciones de la empresa, no está permitido:

- El uso de estos recursos para actividades no relacionadas con el propósito del negocio, o bien con la extralimitación en su uso.
- Las actividades, equipos o aplicaciones que no estén directamente especificados como parte del Software o de los Estándares de los Recursos Informáticos propios de la empresa de servicios públicos EMPITALITO E.S.P.
- Introducir en los sistemas de Información o la red corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.
- Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos Informáticos.
- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.
- Albergar datos de carácter personal en las unidades locales de disco de los computadores de trabajo.
- Cualquier fichero introducido en la Red o en el puesto de trabajo del usuario a través de soportes automatizados, internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas Políticas y, en especial, las referidas a propiedad intelectual y control de virus.

❖ **Uso del Antivirus por los usuarios:**

- El usuario no deberá desinstalar la solución antivirus de su computadora pues ocasiona un riesgo de seguridad ante el peligro de virus.
- Si el usuario hace uso de medios de almacenamiento personales, éstos serán rastreados por la Solución Antivirus en la computadora del usuario o por el equipo designado para tal efecto.
- El usuario deberá comunicarse con el encargado de los procesos tecnológicos de la empresa en caso de problemas de virus para buscar la solución.

El usuario será notificado por el encargado de los procesos tecnológicos de la empresa en los siguientes casos:

- Cuando sea desconectado de la red con el fin evitar la propagación del virus a otros usuarios de la dependencia.
- Cuando sus archivos resulten con daños irreparables por causa de virus.
- Cuando viole las políticas antivirus.

5.7. POLÍTICA DE ADMINISTRACIÓN DE COMUNICACIONES Y OPERACIONES

Objetivo

Se busca asegurar la operación correcta y segura de los medios de procesamiento de la información y que establecen las responsabilidades y procedimientos para la y operación de todos los medios de procesamiento de la información.

❖ **Procedimientos de operación documentados:**

Los procedimientos de operación se documentarán, mantendrán y pondrán a disposición de todos los usuarios que los necesiten.

Se preparan procedimientos documentados para las actividades del sistema asociadas con los medios de procesamiento de la información y comunicación; tales como procedimientos para encender y apagar computadoras, copias de seguridad, mantenimiento del equipo, manejo de medios, cuarto de cómputo, manejo del correo y seguridad. Los procedimientos de operación deberán especificar las instrucciones para la ejecución detallada de cada trabajo incluyendo:

- Procesamiento y manejo de información.
- Copia de seguridad o respaldo.
- Requerimientos de programación de horarios, incluyendo las interdependencias con otros sistemas, los tiempos de culminación y horarios de los primeros y últimos trabajos.
- Instrucciones para el manejo de errores u otras condiciones excepcionales, las cuales podrían surgir durante la ejecución del trabajo, incluyendo las restricciones sobre el uso de las utilidades del sistema.
- Contactos de soporte en el evento de dificultades operacionales o técnicas inesperadas;
- Instrucciones para el manejo de entradas/salidas especial y medios, tales como el uso de papelería especial o el manejo de entradas/salidas confidenciales incluyendo los procedimientos para la eliminación segura de las entradas/salidas de trabajo fallidos.
- Procedimientos de reinicio y recuperación del sistema para su uso en el evento de una falla en el sistema.
- Los procedimientos de operación y los procedimientos documentados para las actividades del sistema debieran ser tratados como documentos formales y cambios autorizados por la gerencia. Donde sea técnicamente factible, los SISTEMAS de información debieran ser manejados consistentemente, utilizando los mismos procedimientos, herramientas y utilidades.

❖ **Control de Cambios:**

Se deben controlar los cambios en los medios y sistemas de procesamiento de la información.

Los sistemas operacionales y el software de aplicación deben estar sujetos a un estricto control gerencial del cambio. En particular, se definen los siguientes ítems:

- Identificación y registro de cambios significativos.
- Planeación y prueba de cambios.
- Evaluación de los impactos potenciales de los cambios, incluyendo los impactos de seguridad, procedimiento de aprobación formal para los cambios propuestos.
- Comunicación de los detalles del cambio para todas las personas relevantes.
- procedimientos de emergencia y respaldo, incluyendo los procedimientos y responsabilidades para abortar y recuperarse de cambios fallidos y eventos inesperados.

Se establecen las responsabilidades y procedimientos gerenciales formales para asegurar un control satisfactorio de todos los cambios en el equipo, software o procedimientos. Cuando se realizan los cambios, se debiera mantener un registro de auditoria conteniendo toda la información relevante.

❖ **Separación de los medios de desarrollo, prueba y operación:**

Los medios de desarrollo, prueba y operación deben estar separados para reducir los riesgos de acceso no-autorizado o cambios en el sistema operacional. Se deben identificar el nivel de separación necesario entre los ambientes de desarrollo, prueba y operación para evitar los problemas operacionales y se deben implementar los controles apropiados. Donde se consideran los siguientes ítems:

- Definir y documentar las reglas para la transferencia de software del estado de desarrollo al operacional.
- El software de desarrollo y operacional deben correr en sistemas o procesadores de cómputo, y en diferentes dominios o directorios.
- Los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema no debieran ser accesibles desde los sistemas operacionales cuando no se requieran
- El ambiente del sistema de prueba debiera emular el ambiente del sistema operacional lo más estrechamente posible.
- los usuarios debieran utilizar perfiles de usuario diferentes para los SISTEMAS operacionales y de prueba, y los menús debieran mostrar los mensajes de identificación apropiados para reducir el riesgo de error.
- la data confidencial no debiera ser copiada en el ambiente del sistema de prueba.

❖ **De la entrega del servicio de terceros:**

Implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio en línea con los acuerdos de entrega de servicios de terceros. La empresa deberá chequear la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados por la tercera persona.

- Asegurar que los controles de seguridad, definiciones del servicio y niveles de entrega incluidos en el acuerdo de entrega del servicio de terceros se implementen, operen y mantengan.

- La entrega del servicio por un tercero debiera incluir los acuerdos de seguridad pactados, definiciones del servicio y aspectos de la del servicio.
- En caso de los acuerdos de abastecimiento externo, la organización debiera planear las transiciones necesarias (de información, medios de procesamiento de la información y cualquier otra cosa que necesite transferirse), y debiera asegurar que se mantenga la seguridad a través del período de transición.
- Garantizar que la tercera persona mantenga una capacidad de servicio suficiente junto con los planes de trabajo diseñados para asegurar que se mantengan los niveles de continuidad del servicio después de fallas importantes en el servicio o un desastre.

❖ **Monitoreo y revisión de los servicios de terceros:**

Los servicios, reportes y registros provistos por terceros debieran ser monitoreados y revisados regularmente, y se deben llevar a cabo auditorías regularmente. El monitoreo y revisión de los servicios de terceros debe asegurar que se cumplan los términos y condiciones de seguridad de los acuerdos, y que se manejen apropiadamente los incidentes y problemas de seguridad de la información. Esto debiera involucrar una relación y proceso de servicio entre la organización y la tercera persona para:

- Monitorear los niveles de desempeño del servicio para chequear adherencia con los acuerdos.
- Revisar de los reportes de servicio producidos por terceros y acordar reuniones de avance regulares conforme lo requieran los acuerdos.
- Proporcionar información sobre incidentes de seguridad de la información y la revisión de esta información por terceros y la organización conforme lo requieran los acuerdos y cualquier lineamiento y procedimiento de soporte.
- Revisar los rastros de auditoria de terceros y los registros de eventos de seguridad, problemas operacionales, fallas, el monitoreo de fallas e interrupciones relacionadas con el servicio entregado.

La responsabilidad de manejar la relación con terceros está a cargo del encargado de los procesos tecnológicos de la empresa. Además, la empresa, en cabeza de la gerencia, debe garantizar que los terceros asignen responsabilidad para el chequeo del cumplimiento de los requerimientos de los acuerdos. Igualmente, se debe tomar la acción apropiada cuando se observan deficiencias en la entrega del servicio.

❖ **Aceptación del sistema:**

Se deben establecer criterios de aceptación de los sistemas de información, actualizaciones o versiones nuevas, realizando la verificación y proceso de pruebas adecuada del sistema(s) durante el desarrollo y antes de su aceptación e implementación final en los procesos de la empresa. Dichos criterios deben incluir y tener en cuenta al menos, lo siguiente:

- El desempeño y los requerimientos de capacidad de las terminales de cómputo.
- Procedimientos para la recuperación tras errores y reinicio, y planes de contingencia.
- Preparación y prueba de los procedimientos de operación rutinarios para estándares definidos.
- El conjunto de controles de seguridad acordados y aceptados.

- Procedimientos manuales efectivos.
- Aseguramiento de la continuidad del negocio.
- Evidencia de que la instalación del sistema nuevo no afectará adversamente los sistemas existentes, particularmente en las horas pico del procesamiento, como fin de mes.
- Evidencia que se está tomando en consideración el efecto que tiene el sistema nuevo en la seguridad general de la organización.
- Capacitación para la operación o uso de los SISTEMAS nuevos a todos los funcionarios de la empresa, incluyendo manuales de usuario y/o videos tutoriales.
- Alta usabilidad del sistema.

Para los desarrollos nuevos, la función de las operaciones y los usuarios deben ser consultados en todas las etapas del proceso del desarrollo, especialmente en la fase de levantamiento de requerimientos. Esto, para asegurar la eficiencia operacional del diseño del sistema propuesto. La aceptación puede incluir un proceso de certificación y acreditación formal para verificar que se hayan tratado apropiadamente los requerimientos de seguridad.

5.8. POLÍTICA DE PROTECCIÓN CONTRA EL CÓDIGO MALICIOSO Y MÓVIL

- Se requiere tomar precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no-autorizados.
- El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos; como virus cómputo, virus de red, etc.
- Los usuarios deben estar al tanto de los peligros de los códigos maliciosos. Se deben aplicar los controles necesarios para el manejo de virus y amenazas, por medio de aplicaciones antivirus y/o firewall, que permitan controlar estas situaciones y utilizando adecuadamente las políticas definidas en este documento al respecto.

❖ **Antivirus:**

- EMPITALITO E.S.P dispondrá de una versión corporativa, de manera que en el servidor de aplicaciones se ubica la consola para en el resto de las PC hay una versión cliente /servidor de este antivirus.
- La solución corporativa de seguridad de antivirus, será una solución integra de herramientas Antivirus, antispyware, firewall y prevención contra intrusiones, además de control de dispositivos y aplicaciones usando un único agente multiplataforma para todos los clientes y gestionado mediante una consola central.
- Complementando el servicio antivirus el servicio consola Administrador, como repositorio central de actualización para toda la plataforma antivirus, facilitando la descarga y distribución actualizaciones permitiendo que todos los equipos de la empresa de servicios públicos EMPITALITO E.S.P tengan las últimas versiones y parches emitidos por el fabricante.
- Controles de detección, prevención y recuperación para proteger contra códigos maliciosos, a través de procedimientos para el apropiado conocimiento del usuario.
- La protección contra códigos maliciosos se basa en la detección de códigos maliciosos y la reparación de software y los apropiados controles de acceso al sistema y del cambio.

❖ **Se consideran los siguientes lineamientos:**

- Aplicar el manual definido sobre el uso de software no autorizado en la empresa.
- Realizar revisiones regulares del software y contenido de la data de los sistemas que sostienen los procesos comerciales críticos; se debiera investigar formalmente la presencia de cualquier activo no-aprobado o enmiendas no autorizadas.
- La instalación y actualización regular de software para la detección o reparación de códigos maliciosos para revisar las computadoras y medios como un control preventivo o una medida rutinaria.
- Escaneo antivirus de cualquier archivo en medios electrónicos u ópticos, y los archivos recibidos a través de la red para detectar códigos maliciosos antes de utilizarlo.
- Escaneo antivirus de los archivos adjuntos y descargas de los correos electrónicos para detectar códigos maliciosos antes de utilizarlos. Debe llevarse a cabo en lugares diferentes; por ejemplo, servidores de correo electrónico, computadoras desktops y cuando se ingresa a la red de la empresa.
- Definición de procedimientos y responsabilidades para lidiar con la protección de códigos maliciosos en los sistemas, capacitación en su uso, reporte y recuperación de ataques de códigos maliciosos.
- Preparar planes apropiados para la continuidad del negocio para recuperarse de ataques de códigos maliciosos, incluyendo toda la data y respaldo (backup) de software y procesos de recuperación.
- El uso de dos o más productos de software para protegerse de códigos maliciosos a través del ambiente de procesamiento de la información de diferentes vendedores puede mejorar la efectividad de la protección contra códigos maliciosos.

5.9. POLÍTICAS DE ALMACENAMIENTO, COPIAS DE RESPALDO O BACK-UP

Se busca mantener la integridad y disponibilidad de la información y los medios de procesamiento de información, por medio de procedimientos de rutina para implementar la política de respaldo acordada y la estrategia para tomar copias de respaldo de la data y practicar su restauración oportuna.

- Se deben hacer copias de respaldo de la información y software, realizando pruebas regularmente en concordancia con la política de copias de respaldo acordada.
- Los procedimientos de respaldo pueden ser automatizados para facilitar el proceso de respaldo y restauración. Estas soluciones automatizadas debieran ser probadas suficientemente antes de su implementación y también a intervalos regulares.
- Se debe contar con un sistema automático para la recolección de copias de respaldo.
- Las copias de respaldo deben tener el mismo nivel de protección de la información que poseen en su fuente original.
- Los medios magnéticos que contienen información deben ser almacenados en lugares físicamente seguros.
- Los usuarios responsables por respaldar la información, también son responsables de facilitar la oportuna restauración de la información.
- Los medios magnéticos deben tener rótulos visibles y legibles tanto internos como externos.
- Se debe mantener suficientes respaldos de la información para que en caso de contingencia se pueda recuperar la información oportunamente.
- Para responder adecuadamente a una contingencia, los respaldos de la información se deben almacenar en sitios externos.
- Cualquier medio magnético que contenga información clasificada como restringida o confidencial, debe estar claramente identificada.
- Al enviar información clasificada como restringida o confidencial a terceros se debe exigir un acuse de recibo.
- Todos los medios que contengan información clasificada como restringida o confidencial y que finalice su ciclo de vida, deben ser sobre escritos o destruidos físicamente para que la información no pueda ser recuperada.
- Es responsabilidad de los Administradores de las Plataformas, mantener respaldo de la configuración del sistema operativo y de los servicios que estas proveen.

❖ **Respaldos de Seguridad:**

- Las Bases de Datos de la empresa de servicios públicos EMPITALITO E.S.P serán respaldadas periódicamente en forma automática y manual, según los procedimientos generados para tal efecto.
- Las Bases de Datos deberán tener una réplica en uno o más equipos remotos alojados en un lugar seguro (Cloud) que permita tener contingencia y continuidad de negocio.
- Los servidores de contingencia de Bases de Datos y aplicaciones estarán alojados en Data Center de la empresa.
- Los servidores de hosting (hosting Colombia pro) deberá contar con un respaldo de seguridad para resguardar la integridad de la página web y de los correos de la empresa.
- Los demás respaldos (una copia completa) deberán ser almacenados en un lugar seguro y distante del sitio de trabajo, en bodegas con los estándares de calidad para almacenamiento de medios magnéticos.

Para reforzar la seguridad de la información, los usuarios, bajo su criterio, deberán hacer respaldos de la información en sus discos duros frecuentemente, dependiendo de la importancia y frecuencia de cambio; y en las unidades de almacenamiento asignadas por la empresa de servicios públicos EMPITALITO E.S.P (NAS), deberán realizar una sincronización continua de la información importante para la empresa. Los respaldos serán responsabilidad absoluta de los usuarios.

❖ **Backup en los equipos**

Se configura una carpeta de trabajo en el servidor para todo funcionario y contratista, estos serán los responsables de sus propias copias, proceso que se hará por cada uno, ingresando en esta carpeta la información importante para el desarrollo de sus tareas.

5.10. POLÍTICA PARA EL MANEJO DE INFORMACIÓN

Con el fin de mantener confidencialidad, integridad y disponibilidad de los datos digitales y los elementos físicos que hacen parte de la infraestructura tecnológica y están involucrados en los procesos de la empresa de servicios públicos EMPITALITO E.S.P, se define el siguiente esquema para el proceso de clasificación de la información, según su tipo, nivel de privacidad y contenido:

Restringida: Aquella información privilegiada en donde su divulgación no autorizada puede derivar en impactos financieros, legales, con la ciudadanía, con proveedores, con el propio gobierno y/o empresas externas. Ejemplos: datos de adquisiciones (antes de su anuncio), Negociaciones, Desarrollo de nuevos servicios, Juicios.

Confidencial: Aquella en donde su divulgación no autorizada puede derivar en impactos importantes para la operación de la Dependencia, perdiendo principalmente la oportunidad. Ejemplos: Información sobre operaciones y transacciones de la empresa, Resoluciones y Actas de Comités, información de clientes, nómina y compensaciones, contraseñas, entre otras.

Privada: Es aquella información ordinaria de la empresa que apoya sus procesos internos y que no ha sido clasificada como restringida ni confidencial, por lo que puede ser conocida dentro de toda la organización. No puede ser difundida a clientes ni a terceros. Su divulgación no autorizada representa un impacto menor para el Empresa. Ejemplo: Directorio Telefónico personal de los funcionarios, Comunicados Internos.

Pública: Es la información que ha sido autorizada expresamente para darse a conocer al público en general a través de canales aprobados. Ejemplo: Propaganda, Boletines de Prensa, Páginas de Internet, estados financieros, Manuales de procedimientos, presupuestos, reportes de auditoría, etc.

La clasificación asignada a la información solo puede ser cambiada por el funcionario, luego de justificar formalmente el cambio ante su jefe inmediato, el encargado de los procesos tecnológicos, la Gerencia y/o Junta Directiva, el (los) cual(es) debe(n) analizar y validar. Igualmente, debe ser examinada para determinar el impacto para la empresa EMPITALITO E.S.P, si fuera divulgada o alterada por medios no autorizados.

Frecuentemente, la información deja de ser sensible después de un cierto periodo de tiempo, este aspecto debe ser tomado en cuenta por el propietario para realizar una reclasificación. Dicho periodo debe ser de al menos 6 meses, a partir de su formalización dentro del almacenamiento de documentos de la empresa o al momento de su reclasificación.

Se debe mantener un control y adecuada de la información clasificada dentro de la empresa. Para esto, es esencial mantener el nivel de confidencialidad adecuado y garantizar un permanente nivel de seguridad óptimo en los procesos de la empresa. Las medidas de seguridad aplicadas a los activos de información clasificada incluyen, pero no se limitan, a lo siguiente:

- Manipulación y etiquetado de todos los medios en su nivel de clasificación indicado.
- Restricciones de acceso para evitar el acceso de personal no-autorizado;
- Protección de la data recolectada esperando un nivel consistente con la confidencialidad.
- Almacenaje de medios en concordancia con las especificaciones de los fabricantes.
- Marcar claramente todas las copias de los medios con atención al destinatario autorizado.
- Revisión de las listas de distribución y las listas de los destinatarios autorizados a intervalos regulares.
- La documentación del sistema se debiera almacenar de una manera segura;
- La lista de acceso para la documentación del sistema se debiera mantener en un nivel mínimo y autorizado por el propietario de la aplicación.
- La documentación del sistema mantenido en una red pública, o suministrada a través de una red pública, debiera estar adecuadamente protegida.

Toda información catalogada como digital es aquella que se encuentra almacenada o guardada en los discos duros o elementos electrónicos disponibles en la empresa (CD's, cintas magnéticas, USB's, etc.). Dicha información puede haber sido digitalizada (escaneada, fotografiada) de su archivo físico, transferida vía correo electrónico o a través de otros mecanismos de digitalización y envío de información. Estos formatos digitales

incluyen documentos realizados por medio de programas de edición de texto (Word, Excel, Bloc de Notas y similares), de edición de presentaciones (Power Point) o aplicativos de creación de documentos digitales.

Con respecto a los datos digitales, se deben seguir el siguiente tratamiento:

- La información en formato digital clasificada como PÚBLICA debe ser almacenada en cualquier sistema de la empresa y se deben tomar las medidas necesarias para no mezclarla con otra clasificación.
- Todo usuario antes de transmitir información clasificada como RESTRINGIDA O CONFIDENCIAL, debe asegurarse que el destinatario de la información este autorizado para recibir dicha información.
- Todo usuario que requiera acceso a la información clasificada como RESTINGIDA O CONFIDENCIAL, debe ser autorizado por el propietario de la misma y por tanto deben ser documentadas.
- La información en formato digital clasificada como RESTRINGIDA debe ser encriptada por un método aprobado por los administradores de la seguridad cuando es almacenada en cualquier medio.
- Toda transmisión de información clasificada como RESTRINGIDA, CONFIDENCIAL o PRIVADA realizada desde redes externas de la empresa, debe realizarse utilizando un medio de transmisión seguro o utilizando técnicas de encriptación probadas.
- Todo documento en formato digital debe presentar la clasificación correspondiente en la parte superior (encabezado) e inferior (pie de página) de cada página del documento.
- Los medios de almacenamiento, incluyendo discos duros de computadoras que albergan información clasificada como RESTRINGIDA, deben ser ubicados en ambientes cerrados diseñados para el almacenamiento de dicho tipo de información, es decir un lugar que garantice protección física y de seguridad (bajo llave).
- Todo contenedor de la información en medio digital debe presentar una etiqueta con la clasificación correspondiente

La información catalogada como no digital es aquella que se encuentra formato físico (papel u otro material similar) y es almacenada en el archivo de la empresa y/o en los archivos de los funcionarios de la empresa EMPITALITO E.S.P. Los tratamientos de seguridad referentes a la información no digital de la empresa son:

- Todo documento o contenedor de información RESTRINGIDA, CONFIDENCIAL, PRIVADA O PÚBLICA debe ser etiquetada de acuerdo a la clasificación asignada.
- Todo documento que presente información clasificada como RESTRINGIDA o CONFIDENCIAL debe ser etiquetada en la parte superior e inferior de cada página según corresponda.
- Todo documento clasificado como RESTRINGIDA o CONFIDENCIAL debe presentar una caratula que muestre la clasificación a que corresponde.
- El ambiente donde se almacena la información clasificada como RESTRINGIDA, debe contar con adecuados controles de acceso y asegurado cuando se encuentre sin vigilancia, el acceso solo será para personal formalmente autorizado.
- Solo el personal formalmente autorizado debe tener acceso a información clasificada como RESTRINGIDA o CONFIDENCIAL.

Los usuarios que utilizan documentos con información RESTRINGIDA o CONFIDENCIAL deben asegurarse de:

- Almacenarlos en lugares adecuados.
- Evitar que usuarios no autorizados accedan a dichos documentos.
- Destruir los documentos si luego de su utilización dejan de ser necesarios

5.11. POLÍTICAS Y PROCEDIMIENTOS DE INTERCAMBIO DE INFORMACIÓN

Se establecen políticas, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación. Los lineamientos de implementación, procedimientos y controles a seguirse cuando se utilizan medios de comunicación electrónicos para el intercambio de información debieran considerar los siguientes ítems:

- Los procedimientos diseñados para proteger el intercambio de información de la intercepción, copiado, modificación, routing equivocado y destrucción.
- Los procedimientos para la detección y protección de contra códigos maliciosos que pueden ser transmitidos a través del uso de comunicaciones electrónicas.
- Los procedimientos para proteger la información electrónica confidencial comunicada que está en la forma de un adjunto.
- Política o lineamientos delineando el uso aceptable de los medios de comunicación electrónicos.
- Los procedimientos para el uso de comunicación inalámbrica, tomando en cuenta los riesgos particulares involucrados.
- Las responsabilidades del usuario funcionario, contratista y cualquier otro para que no comprometan a la organización; por ejemplo, a través de la difamación, hostigamiento, suplantación, reenvío de cadenas de cartas, compras no autorizadas, etc.
- Uso de técnicas de codificación, para proteger la confidencialidad, integridad y autenticidad de la información.
- Lineamientos de retención y eliminación de toda la correspondencia del negocio, incluyendo mensajes, en concordancia con la legislación y regulaciones nacionales y locales relevantes.
- No dejar la información confidencial o crítica en medios impresos; por ejemplo, copiadoras, impresoras y máquinas de fax; ya que personal no-autorizado puede tener acceso a ellas.
- Los controles y restricciones asociados con el reenvío de los medios de comunicación; por ejemplo, reenvío automático de correo electrónico a direcciones externas.
- Recordar al personal que debiera tomar las precauciones apropiadas; por ejemplo, no revelar información confidencial cuando realiza una llamada telefónica, manejar adecuadamente los documentos físicos y digitales, etc.
- No dejar mensajes con información confidencial en máquinas contestadoras u otros mecanismos, dado que estos pueden ser escuchados por personas no autorizadas, ni almacenados en sistemas comunitarios o almacenados incorrectamente como resultado de un equívoco al marcar.
- Recordar al personal no registrar data demográfica, como la dirección de correo electrónico u otra información personal, en ningún software para evitar que sea utilizada sin autorización, esta debe ser de la empresa EMPITALITO E.S.P.
- Recordar al personal que no debieran mantener conversaciones confidenciales en lugares públicos, u oficinas o salas de reuniones abiertas, sin paredes a prueba de ruidos.
- Los medios de intercambio de información debieran cumplir con cualquier requerimiento legal relevante.

❖ Acuerdos de intercambio de información

El acuerdo de intercambio considera las siguientes condiciones de seguridad:

- Manejo de las responsabilidades para el control y notificación de la transmisión.
- despacho y recepción.
- Procedimientos para notificar al remitente de la transmisión, despacho y recepción.
- Procedimientos para asegurar el rastreo y no-repudio.
- Estándares técnicos mínimos para el empaque y la transmisión.
- Acuerdos de depósitos.

- Estándares de identificación del mensajero.
- Responsabilidades y obligaciones en el evento de incidentes de seguridad de la información, como la pérdida de data.
- Uso de un sistema de etiquetado acordado para la información confidencial o crítica, asegurando que el significado de las etiquetas sea entendido inmediatamente y que la información sea adecuadamente protegida.
- Propiedad y responsabilidades de la protección de data, derechos de autor, licencias de software y consideraciones similares.
- Estándares técnicos para grabar y leer la información y software.
- Cualquier control especial que se pueda requerir para proteger los ítems confidenciales, como claves criptográficas.
- Se debieran establecer y mantener las políticas, procedimientos y estándares para proteger la información y medios físicos en tránsito, y se debiera hacer referencia en los acuerdos de intercambio.
- El contenido de seguridad de cualquier acuerdo debiera reflejar la sensibilidad de la información comercial involucrada.

❖ **Sincronización de relojes**

Los relojes de todos los sistemas de la empresa EMPITALITO E.S.P de procesamiento de información relevantes dentro de una organización o dominio de seguridad deben ser sincronizados a la hora oficial colombiana o de sistema de la región de ubicación.

5.12. POLÍTICA DE CONTROL DE ACCESO A DATOS

❖ **Seguridad Perimetral**

La seguridad perimetral es uno de los métodos posibles de protección de la Red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles. Esto permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios y denegando cualquier tipo de acceso a otros.

El área TIC implementará soluciones lógicas y físicas que garanticen la protección de la información de posibles ataques internos o externos.

- Rechazar conexiones a servicios comprometidos
- Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico, http, https).
- Proporcionar un único punto de interconexión con el exterior.
- Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet (Red interna).
- Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet
- Auditar el tráfico entre el exterior y el interior.
- Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red cuentas de usuarios internos.

❖ **Firewall**

La solución de seguridad perimetral debe ser controlada con un Firewall por Hardware (físico) que se encarga de controlar puertos y conexiones, es decir, de permitir el paso y el flujo de datos entre los puertos, ya sean clientes o servidores.

Se debe tener en cuenta lo siguiente:

- Este equipo deberá estar cubierto con un sistema de alta disponibilidad que permita la continuidad de los servicios en caso de fallo.
- El encargado de los procesos tecnológicos de la empresa establecerá las reglas en el Firewall necesarias bloquear, permitir o ignorar el flujo de datos entrante y saliente de la Red.
- El firewall debe bloquear las "conexiones extrañas" y no dejarlas pasar para que no causen problemas.
- El firewall debe controlar los ataques de "Denegación de Servicio" y controlar también el número de conexiones que se están produciendo, y en cuanto detectan que se establecen más de las normales desde un mismo punto bloquearlas y mantener el servicio a salvo.
- Controlar las aplicaciones que acceden a Internet para impedir que programas a los que no hemos permitido explícitamente acceso a Internet, puedan enviar información interna al exterior (tipo troyanos).

❖ **De seguridad de la red**

La seguridad de la red, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de data, implicancias legales, monitoreo y protección. También se pueden requerir controles adicionales para proteger la información confidencial que pasa a través de redes públicas. Los sistemas de red son vulnerables y presentan riesgos inherentes a su naturaleza y complejidad. Los accesos remotos (dial-in) y conexiones con redes externas, exponen a los sistemas de información de la empresa EMPITALITO E.S.P a niveles mayores de riesgo. Asegurando que todos los enlaces de una red cuenten con adecuados niveles de seguridad, se logra que los activos más valiosos de las unidades de negocio estén protegidos de un ataque directo o indirecto, manteniendo la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.

Garantizando un control de acceso a las redes de la empresa, se deberá proceder de la siguiente manera:

- La responsabilidad operacional para las redes se debiera separar de las operaciones de cómputo.
- Aplicar las responsabilidades y procedimientos para los equipo que se han remoto, incluyendo el equipo en las áreas del usuario.
- Establecer y aplicar controles especiales para salvaguardar la confidencialidad y la integridad de los datos que pasan a través de las redes públicas o a través de las redes inalámbricas.
- Se deben llevar registros de ingreso y monitoreo apropiados para permitir el registro de las acciones de seguridad relevantes.
- Todas las conexiones realizadas entre la red interna de la empresa EMPITALITO E.S.P e Internet, deben ser controladas por un firewall para prevenir accesos no autorizados. El encargado de los procesos tecnológicos de la empresa debe aprobar todas las conexiones con redes o dispositivos externos.
- El acceso desde Internet hacia la red interna no debe ser permitido sin un dispositivo con autenticación fuerte o certificado basado en utilización de contraseñas dinámicas. Igualmente, debe estar autorizado y verificado por el encargado de los procesos tecnológicos de la empresa.
- El esquema de direccionamiento interno de la red no debe ser visible desde redes o equipos externos. Esto evita que "hackers" u otras personas pueden obtener fácilmente información sobre la estructura de red de la empresa EMPITALITO E.S.P y acceder a los datos de los computadores de la empresa.
- Para eliminar las vulnerabilidades inherentes, enrutadores y firewalls deben rechazar conexiones externas que parecieran originarias de direcciones internas.
- Para poder hacer uso de la conexión inalámbrica de la empresa, se debe tener autorización por parte del encargado de los procesos tecnológicos, la cual verificará el dispositivo a conectar e ingresará la contraseña de red, sin divulgarla al funcionario

o persona autorizada a conectar. Para esto, se debe diligenciar el formato para la conexión a la red inalámbrica o solicitar la autorización correspondiente ante el encargado de los procesos tecnológicos y/o la gerencia.

❖ **Conectividad a Internet**

- La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo.
- Todos los colaboradores del Área de TIC tienen las mismas responsabilidades en cuanto al uso de Internet.
- El acceso a Internet se restringe exclusivamente a través de la red establecida para ello, es decir, por medio del sistema de seguridad con Firewall incorporado en la misma.
- No está permitido acceder a Internet llamando directamente a un proveedor de servicio de acceso y usando un navegador, o con otras herramientas de Internet conectándose con un módem.
- Internet es una herramienta de trabajo. Todas las actividades en Internet deben estar en relación con tareas y actividades del trabajo desempeñado.
- Sólo puede haber transferencia de datos de o a Internet en conexión con actividades propias del trabajo desempeñado.

❖ **Red Inalámbrica (WIFI)**

Acceso a funcionarios de la empresa:

- La red inalámbrica es un servicio que permite conectarse a la red de la empresa EMPITALITO E.S.P e Internet sin la necesidad de algún tipo de cableado. La Red inalámbrica le permitirá utilizar los servicios de Red, en las zonas de cobertura de la empresa.
- Además de hacer uso del servicio de acceso a los sistemas, podrán acceder al servicio de Internet de manera controlada.
- Las condiciones de uso presentadas definen los aspectos más importantes que deben tenerse en cuenta para la utilización del servicio de red inalámbrica, estas condiciones abarcan todos los dispositivos de comunicación inalámbrica (computadoras portátiles, Ipod, celulares, etc.) con capacidad de conexión Wireless.
- El encargado de los procesos tecnológicos debe gestionarla administración, habilitación y/o bajas de usuarios en la red inalámbrica de la empresa de servicios públicos EMPITALITO E.S.P.

❖ **Identificación y activación**

Para hacer uso de la red inalámbrica, el solicitante necesariamente deberá seguir el siguiente procedimiento:

- Como primer paso para hacer uso de este servicio, se deben de registrar los usuarios que deseen la prestación del servicio mediante un formulario y presentando el dispositivo que se conectará a la red inalámbrica.
- Se debe registrar la dirección MAC de las tarjetas inalámbricas de todos y cada uno de los dispositivos de comunicación.
- La activación de la cuenta se realizará por un periodo semestral como máximo; salvo casos de fuerza mayor o anormalidades en el registro (Usuarios inexistentes, apagones, fallas, etc.).

- Para conectarse a la red inalámbrica se deberá emplear autenticación tipo WPA2- AUTO-PSK para lo cual los nombres de usuarios y contraseñas cambiarán periódicamente (de 6 a 12 meses) con la finalidad de proporcionarles seguridad en el acceso a los usuarios.

❖ **Seguridad en la red.**

- El encargado de los procesos tecnológicos determinará las medidas pertinentes de seguridad para usar las redes inalámbricas.
- El encargado de los procesos tecnológicos se reserva el derecho de llevar un registro de los eventos asociados a la conexión de los diferentes usuarios para asegurar el uso apropiado de los recursos de red.
- No se deben realizar intentos de ingreso no autorizado a cualquier dispositivo o sistema de la red inalámbrica. Cualquier tipo de ingreso no autorizado es una práctica ilegal y será detectada para los respectivos controles de seguridad.
- No se debe hacer uso de programas que recolectan paquetes de datos de la red inalámbrica. Esta práctica es una violación a la privacidad y constituye un robo de los datos de usuario, y puede ser sancionado.
- Con la finalidad de evitar responsabilidades, en caso de que algún usuario haga cambio de cualquiera de los equipos previamente dado de alta, este necesariamente deberá comunicar al encargado de los procesos tecnológicos para su respectiva baja del equipo de la red inalámbrica.

❖ **Restricciones/prohibiciones de acceso a Internet**

Con la finalidad de hacer un buen uso de la red inalámbrica, se aplicarán las siguientes prohibiciones:

- El uso de programas para compartir archivos (Peer to Peer).
- El acceso a páginas con cualquier tipo de contenido explícito de pornografía.
- El uso de sitios de videos en línea o en tiempo real.
- Redes sociales (Twitter, Facebook, instagran etc.)
- Uso de JUEGOS "online" en la red.

❖ **Excepciones**

Entre las medidas de seguridad se encuentra configurado para restringir algunas palabras y sitios de Internet; por lo que pueden existir palabras o sitios que a pesar de ser inofensivos tendrán negado el acceso; en este caso, los usuarios podrán notificar esta eventualidad para que sea resuelta a la brevedad posible.

En caso de eventos, cursos, talleres, conferencias, etc, se podrán habilitar equipos con acceso a la red inalámbrica de manera temporal por el tiempo necesario previa solicitud de los interesados con una anticipación de por lo menos un día hábil.

En el caso de estos eventos las restricciones para acceder podrán ser "anuladas" temporalmente previa solicitud expresa por parte de la parte interesada y con anticipación de por lo menos un día hábil.

5.13. POLÍTICA DE SEGURIDAD DEL PERSONAL.

Objetivo.

Garantizar la protección de la disponibilidad, integridad y confidencialidad de la información del personal que trabaja para la empresa EMPITALITO E.S.P, a través de mecanismos de validación y concientización del recurso humano que hará uso de esta.

- **Incorporación de la Seguridad en la matriz de Cargos de la empresa**

Deben ser incorporadas los roles y responsabilidades en seguridad de la información dentro de las funciones y obligaciones contractuales de los Colaboradores y Terceros.

- **Control y Política del Personal**

Se deben definir controles de verificación del personal en el momento en que se postula al cargo. Estos controles incluirán todos los aspectos legales y de procedimiento que dicta el proceso de contratación de personal de la empresa EMPITALITO E.S.P.

- **Acuerdo de Confidencialidad**

Todos los funcionarios, contratistas y terceros que ingresen a trabajar para la empresa EMPITALITO E.S.P, deben firmar como parte de sus términos y condiciones iniciales de trabajo, un Acuerdo de Confidencialidad o no divulgación, en caso de que no estuviere incluido como una cláusula dentro del contrato de prestación de servicios o en el Acta de Posesión del funcionario. Este acuerdo debe incluir la aceptación de las políticas y lineamientos en Seguridad y Privacidad de la Información, el tratamiento de la información de la empresa, en los términos de la Ley 1581 de 2012 y las demás normas que la adicionen, modifiquen, reglamenten o complementen, así como el Decreto 1377 de 2013. Este documento debe ser archivado de forma segura por el área de Talento Humano y Contractual, según sea el caso.

Dentro del mismo acuerdo el Colaborador o Tercero declaran conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad ni los derechos del contratista o tercero.

- **Selección de personal**

Dentro de los procesos de contratación de personal o de prestación de servicios, debe realizarse la verificación de antecedentes, de acuerdo con la reglamentación.

Se deben aplicar los controles establecidos por empresa de servicios públicos EMPITALITO E.S.P para otorgar el acceso a la información CONFIDENCIAL o RESERVADA por parte del personal que resulte vinculado a la Empresa.

El área de Talento humano y Contratación son los responsables de realizar la verificación de antecedentes disciplinarios, fiscales y judiciales y que se anexe la documentación requerida para la contratación.

❖ **Términos y condiciones Laborales**

Todos los Colaboradores y Terceros para la empresa EMPITALITO E.SP. deben dar cumplimiento a las políticas y normatividad establecida en seguridad y privacidad de la información y debe ser parte integral de los contratos o documentos de vinculación a que haya lugar.

Todos los Colaboradores y Terceros, durante el proceso de vinculación a la empresa EMPITALITO E.S.P, deberán recibir una inducción sobre las Políticas y Lineamientos de Seguridad y Privacidad de la Información.

❖ **Entrenamiento, concientización y capacitación**

Todos los contratistas y terceros de la empresa EMPITALITO E.S.P deben ser entrenados y capacitados para las funciones, actividades y cargos que van a desempeñar, esto con el fin de sensibilizar a los usuarios sobre la protección adecuada de los recursos y la información de la Empresa. Así mismo, se debe garantizar la comprensión del alcance y contenido de las políticas y directrices de Seguridad de la información y la necesidad de respaldarlas y aplicarlas de manera permanente e integral desde su función.

❖ **Formación y Capacitación en Materia de Seguridad de la Información**

Todos los colaboradores y terceros cuando sea el caso, que trabajan para la empresa EMPITALITO E.S.P deben recibir una adecuada capacitación y actualización periódica en materia de las políticas, normas y procedimientos de Seguridad y privacidad de la Información.

Dentro del contenido se deben contemplar los requerimientos de seguridad y las responsabilidades legales, así como la capacitación sobre el uso adecuado de las instalaciones de procesamientos de información y los recursos tecnológicos informáticos que les provee la Empresa para el desempeño de sus funciones laborales y contractuales.

❖ **Procesos disciplinarios**

Todos los incidentes de seguridad de la información presentados en la empresa EMPITALITO E.S.P deben tener el tratamiento adecuado y establecido en el procedimiento de atención de incidentes de seguridad de la información, con el fin de determinar sus causas y responsables.

Del resultado de los procesos derivados de los reportes y del análisis de los Incidentes de Seguridad y teniendo en cuenta el impacto y las responsabilidades identificadas, se tomarán acciones y se realizará el respectivo traslado ante las instancias correspondientes.

En lo pertinente a la violación de las políticas de seguridad de la información de la Empresa, a los contratistas y terceros, se les aplicará lo establecido en la ley, particularmente en el Código Único Disciplinario (Ley 734 de

2002), el Estatuto Anticorrupción (Ley 1474 de 2011) y demás normas que las adicionen, modifiquen, reglamenten o complementen.

5.14. POLÍTICA DE USO DE CONTROLES CRIPTOGRÁFICOS

Objetivo.

Propender porque la información de mayor nivel de sensibilidad de la empresa EMPITALITO E.S.P se cifre en el almacenamiento y la transmisión.

Esta política aplica para todas las áreas de la empresa EMPITALITO E.S.P que tratan información pública reservada y pública clasificada, para el personal encargado de implantar los controles de cifrado en los servicios de red, en la plataforma informática y en los sistemas de información de la empresa EMPITALITO E.S.P en el momento de almacenarse o transmitirse por cualquier medio.

Con el fin de garantizar la confidencialidad e integridad de algunos documentos designados como sensibles, la empresa debe utilizar sistemas y técnicas criptográficas para la protección de la información.

El sistema de información debe implementar mecanismos de protección de información que cumplan con la reglamentación, políticas, estándares, guías aplicables, así como:

- Proporcionar una protección adecuada a los equipos utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.
- Proteger las claves secretas y privadas evitando sean copiadas o modificadas sin autorización.
- La empresa EMPITALITO E.S.P deberá velar porque la información de su custodia o propiedad que es catalogada como publica reservada o pública clasificada se cifre al momento de almacenarse o transmitirse por cualquier medio.

Para dar cumplimiento al tratamiento definido para los activos de información, todos los involucrados en el alcance deben cumplir, las siguientes directrices:

❖ **Directrices de seguridad para todo el personal**

- La información que contenga contraseñas de usuario o claves para el control de acceso a los sistemas de información no podrá ser almacenada en texto plano y deberá hacer uso de mecanismos criptográficos.
- Todos los documentos que se han cifrado y descifrado, en caso que se requiera, deberán ser almacenados y tratados con las medidas de seguridad requeridas conforme al grado de clasificación de la información.
- Se deberá identificar todo sistema de información que requiera realizar transmisión de información pública reservada y pública clasificada, para así garantizar que cuente con mecanismos de cifrado de datos.
- Se deberán cifrar los discos duros de los equipos de cómputo que contengan información pública reservada o pública clasificada.
- El manejo de llaves criptográficas se debe realizar de acuerdo con los lineamientos establecidos en la Política de Llaves Criptográficas.

❖ **Directrices de seguridad para el personal que trata información**

- Se deberán cifrar los documentos lógicos, cuando contengan información pública reservada y pública clasificada, en particular los documentos importantes para la misión de la Superintendencia de Subsidio Familiar.
- Se deberán cifrar o aplicar claves a los documentos (pdf, Excel, Word, bd, csv, etc.) que contengan datos personales o datos sensibles.
- La entrega de la clave del documento debe realizarse a través de un medio diferente al del envío del archivo.
- Deberá configurar y administrar el sistema de cifrado, así como velar por el cumplimiento de la presente política y generar los reportes que se requieran.

5.15. POLÍTICA PARA LA ASIGNACIÓN Y USO DE RECURSOS TECNOLÓGICOS DE LA ENTIDAD

- EMPITALITO E.S.P mantendrá actualizados el sistema operativo, navegador de internet o su software de seguridad, porque si no se hace los delincuentes podrían infiltrar silenciosamente sus programas maliciosos en su computadora y usarla secretamente para irrumpir en otras computadoras, enviar correo spam o espiar sus actividades en internet.
- Cualquier elemento tecnológico o electrónico entregado al funcionario tales como: portátil, computador de escritorio, tablets, memorias USB, llaves digitales), software, datos, documentación, manuales, etc., deben ser entregados a su jefe inmediato, al área de TIC.
- Debe quedar registro de los elementos entregados, fecha y firma de recibido.
- La seguridad es responsabilidad de todos los funcionarios, contratistas, proveedores y demás personas involucradas en el día a día de la empresa. Por tanto, todas las personas deben acatar las políticas y normas de seguridad física, de infraestructura y de la información definidas para la empresa, priorizando la seguridad en sus labores corporativas, extendiéndolas a su vida personal y profesional.
- Los funcionarios deben seguir las políticas, normas de seguridad y lineamientos del área respectiva, conscientes de todas sus responsabilidades y acciones apropiadas en el reporte de incidentes y manejo de la información de la empresa.
- Referente a los equipos de cómputo, portátiles, tabletas y/u otros dispositivos que sean de propiedad de los funcionarios y sean utilizados para el manejo de información de la empresa (creación, edición, eliminación de datos), para las labores diarias en sus áreas y/o utilización de los aplicativos financieros y demás disponibles en la empresa, se establece lo siguiente:
- La utilización de estos equipos por parte de los funcionarios y contratistas como herramienta de trabajo, hace que estos equipos sean adoptados por la empresa. Por tanto, el encargado de los procesos tecnológicos debe hacer el seguimiento, mantenimiento y soporte técnico aplicado a los equipos propios de la empresa. Igualmente, se deben instalar los programas y aplicativos utilizados tanto para la de información, como aquellos de seguimiento y auditoría, además de la integración a la red de la empresa.
- Dada la adopción del equipo por parte de la empresa, éste debe permanecer dentro de las instalaciones de la empresa. Si requiere ser retirado, se debe presentar la solicitud al encargado de los procesos tecnológicos y la gerencia, detallando el tiempo que durará el equipo fuera de las instalaciones, el nombre del funcionario/contratista que se lo lleva, fecha de salida y la descripción u objetivo de la necesidad de utilizar el equipo externamente. El funcionario debe reportar el retorno del equipo a las instalaciones directamente al encargado de los procesos tecnológicos.
- Dada la adopción del equipo por parte de la empresa, dichos equipos deben contener únicamente y sin excepción información corporativa. Está prohibido el manejo de la información personal del funcionario, contratista u otra persona en dichos equipos.
- Aquellos equipos adoptados e identificados por el encargado de los procesos tecnológicos como tal por la empresa, que presenten algún tipo de información personal de funcionarios, contratistas y/o archivos o datos que no sean parte de la empresa y sus procesos, se definirán como de propiedad del funcionario. Por tanto, no se podrá manejar información de la empresa ni utilizar los aplicativos dispuestos por la empresa EMPITALITO E.S.P para la labor diaria de sus funcionarios.
- En caso de que alguno de estos equipos adoptados identificados por el área de TIC como tal contenga información tanto de la empresa, como personal del funcionario/contratista o externa a los datos y procesos de la empresa, se definirán como de propiedad

del funcionario. Por tanto, no serán sujetos a mantenimiento, soporte o asistencia técnica por parte de la empresa. Estos servicios serán asumidos por el funcionario/contratista, dueño del equipo.

- El encargado de los procesos tecnológicos no está en la obligación de realizar algún procedimiento sobre dichos equipos adoptados, si se comprueba que contiene información externa a la empresa.
- El encargado de los procesos tecnológicos está en la obligación de reportar a la gerencia cualquier irregularidad con dichos equipos y de llevar registro, seguimiento y control de los mismos.

En caso de que el funcionario/contratista se desvincule de la empresa por cualquier motivo y haya dado uno o varios equipos en adopción por la empresa EMPITALITO E.S.P, el encargado de los procesos tecnológicos debe:

- Realizar copia de seguridad de la información de la empresa contenida en el(los) equipos adoptados.
- Eliminar tanto la información ya copiada y almacenada, tanto como los aplicativos y demás programas de la empresa instalados en el mismo.
- Desvincular el(los) equipo(s) de la red de datos, asegurando que cualquier dato y/o conexión sea eliminada adecuadamente.
- Entregar el(los) equipo(s) adoptado(s) al funcionario, guardando registro del número de serie y demás datos de identificación el(los) equipo(s).

❖ **Adquisición De Bienes Informáticos**

Toda adquisición de tecnología informática se efectuará a través de la gerencia y el encargado de los procesos tecnológicos de la empresa, donde planean las operaciones relativas a la adquisición de bienes informáticos, establecerán prioridades y en su selección deberá tomar en cuenta:

- Precio: Costo inicial, costo de mantenimiento y consumibles por el periodo estimado de uso de los equipos.
- Calidad: Parámetro cualitativo que especifica las características técnicas de los recursos informáticos.
- Experiencia: Presencia en el mercado, estructura de servicio, la confiabilidad de los bienes y certificados de calidad con los que se cuente.
- Desarrollo Tecnológico: Se deberá analizar su grado de obsolescencia, su nivel tecnológico con respecto a la oferta existente y su permanencia en el mercado.
- Estándares: Toda adquisición se basa en los estándares, es decir la arquitectura de grupo empresarial establecida por el Comité.
- Capacidades: Se deberá analizar si satisface la demanda actual con un margen de holgura y capacidad de crecimiento para soportar la carga de trabajo del área.

❖ **Para la adquisición de Hardware se tendrá en cuenta lo siguiente:**

- El equipo que se desee adquirir deberá estar dentro de las listas de ventas vigentes de los fabricantes y/o distribuidores del mismo y dentro de los estándares de Las Empresa.
- Los equipos complementarios deberán tener una garantía mínima de un año y deberán contar con el servicio técnico correspondiente en el país.
- Deberán ser equipos integrados de fábrica o ensamblados con componentes previamente evaluados por el Comité.
- La marca de los equipos o componentes deberá contar con presencia y permanencia demostrada en el mercado nacional, así como con asistencia técnica y de repuestos local. Tratándose de microcomputadores, a fin de mantener actualizada la arquitectura informática de la empresa, el Comité emitirá periódicamente las especificaciones técnicas mínimas para su adquisición.

- Los dispositivos de almacenamiento, así como las interfaces de entrada / salida, deberán estar acordes con la tecnología de punta vigente, tanto en velocidad de transferencia de datos, como en procesamiento.
- Las impresoras deberán apegarse a los estándares de Hardware y Software vigentes en el mercado, corroborando que los suministros (cintas, papel, etc.) se consigan fácilmente en el mercado y no estén sujetas a un solo proveedor.
- Juntamente con los equipos, se deberá adquirir el equipo complementario adecuado para su correcto funcionamiento de acuerdo con las especificaciones de los fabricantes, y que esta adquisición se manifieste en el costo de la partida inicial.
- Los equipos adquiridos deben contar con asistencia técnica durante la instalación de estos.
- En lo que se refiere a los servidores, equipos de comunicaciones, concentradores, switches y otros equipos que se justifiquen por ser de operación crítica y/o de alto costo, deben de contar con un programa de mantenimiento preventivo y correctivo el cual se realiza trimestralmente, los cinco (5) últimos días, que incluye el suministro de repuestos al vencer su periodo de garantía.
- En lo que se refiere a los computadores personales, al vencer su garantía por adquisición, deberán de contar por lo menos con un programa de servicio de mantenimiento correctivo que incluya el suministro de repuestos.
- Todo proyecto de adquisición de bienes de tecnología, debe sujetarse al análisis, aprobación y autorización del Comité.
- Software: En la adquisición de Equipo de cómputo se deberá incluir el Software vigente precargado con su licencia correspondiente.

La empresa debiera mantener el control y la auditoría en todos los aspectos de seguridad, con relación a la información confidencial o crítica o los medios de procesamiento de la información y los datos ingresan, procesan o manejan. Finalmente, la empresa debe realizar un monitoreo constante en las actividades de seguridad como la del cambio, identificación de vulnerabilidades y reporte de un incidente de seguridad a través de un proceso, formato y estructura de reporte definidos.

5.16. POLÍTICA DE TRABAJO EN CASA

Mediante Directiva Presidencial N° 2 de 12 de marzo de 2020: Medidas para atender la contingencia generada por el COVID-19, a partir del uso de tecnologías de la información y las telecomunicaciones – TIC. Se define, que como medida preventiva se pueda realizar trabajo en casa por medio del uso de las TIC, sin que constituya como modalidad de teletrabajo, descrito en el numeral 4 del artículo 6 de la Ley 1221 de 2008 "por el cual se establecen normas para promover y regular el teletrabajo" Por **lo tanto, para el caso de la empresa de servicios públicos EMPITALITO E.S.P.** se denomina: trabajo en casa. Esta actividad se realiza mediante conexión remota a los equipos de la Entidad, ya que el DAPRE no cuenta con la implementación de teletrabajo en términos definidos por la Ley 1221 de 2008.

- La conexión remota a la red de área local de la empresa debe realizarse a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada, por la oficina TIC.

- Al usar la tecnológica VPN - Virtual Private Network (Red privada virtual), se busca prevenir la interceptación de posibles atacantes en la conexión (este tipo de ataques son denominados "hombre en el medio"). Este tipo de conexión es segura por la aplicación de una capa de cifrado y autenticación en la ruta de la comunicación (denominado túnel de comunicación).

- Las actividades de acceso remoto (uso de VPN - Virtual Private Network) a los sistemas informáticos y activos de información de la Entidad, se autorizan de acuerdo a las necesidades específicas del área solicitante. Se recomienda que mientras se haga uso

de VPN desde un equipo personal, éste tenga instalado y actualizado el antivirus y que el sistema operativo cuente con las actualizaciones de seguridad.

6. SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN

SENSIBILIZACIÓN Y COMUNICACIÓN

EMPITALITO ESP, definirá un "Plan de Comunicación en Seguridad de la Información" a través de su oficina de comunicación interna y externa y la Oficina TIC, donde se planificará ANUALMENTE la manera en que se comunicarán recomendaciones o tips de seguridad de la información por diferentes medios a todos sus funcionarios y contratistas, con el fin de socializar las políticas institucionales en seguridad de la información o las buenas prácticas en seguridad que se desean socializar para aumentar las capacidades de todas las áreas y procesos de la entidad. La creación de los contenidos se hará con apoyo de la oficina TIC y el área de comunicaciones.

CAPACITACIONES EN SEGURIDAD

EMPITALITO ESP, a través de sus áreas/procesos de Talento Humano y Contratos, incluirá dentro de sus capacitaciones e inducciones las temáticas de seguridad de la información, con el objetivo de que cualquier funcionario y/o contratista que se vincule a la entidad tenga pleno conocimiento de las políticas de seguridad de seguridad de la información, la oficina TIC de la entidad apoyará en dichas inducciones.

7. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

Las políticas aquí definidas se harán efectivas a partir de su aprobación por la Gerencia y serán revisadas por lo menos anualmente, cuando existan incidentes de seguridad de la información o cuando se produzcan cambios estructurales considerables, esto con el fin de asegurar su vigencia y aplicabilidad dentro de la empresa de servicios públicos domiciliarios de Pitalito EMPITALTIO ESP.

8. SANCIONES

La falta de conocimiento de los presentes lineamientos no libera al personal de la empresa de servicios públicos domiciliarios de Pitalito EMPITALITO ESP de las responsabilidades establecidas en ellos por el mal uso que hagan de los recursos de TIC o por el incumplimiento de los lineamientos aquí descritos.

a) Se aplicarán sanciones de acuerdo con el Código Único Disciplinario.

b) Pueden aplicarse sanciones de tipo penal según sea el caso y la gravedad de este, si así lo consideran los entes investigativos y judiciales correspondientes.

c) La oficina TIC será la encargada de recopilar y entregar a la dirección administrativa y financiera de la entidad, las evidencias de incumplimiento de los lineamientos, informes de impactos y consecuencias y cualquier otro insumo requerido para formalmente

manejar la investigación inicialmente a nivel interno, así mismo, la oficina TIC será la encargada de registrar y gestionar el Incidente de seguridad derivado con el incumplimiento de las políticas.

9. CONTROL DE CAMBIOS

VERSIÓN N°.	FECHA DE APROBACIÓN.	DESCRIPCIÓN DEL CAMBIO.
1	27/11/2023	Se crea el manual de políticas de seguridad de la información

10. 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

Elaboró: Jefferson Silva Losada	**Revisó:** Mónica Alexandra Lagos	**Vo. Bo. Jurídico:** Juanita Gaitán T.
Cargo: Profesional de Sistemas	**Cargo:** Jefe Oficina de Planeación y Proyectos (E)	**Cargo:** Asesora Jurídica (E)
Firma:	**Firma:**	**Firma:**
Aprobado mediante Estudio de novedad Interno N° 055 de 2023		