Política Seguridad De La Información

Empresa De Servicios Públicos De Chía Emserchia E.S.P.

Área de Sistemas de información

emserchía a.a.a e.s.p
Empresa de Servicios Públicos de Chía

CONTENIDO

1. INTRODUCCIÓN

La Empresa de servicios Públicos de Chía Emserchia E.S.P., dando cumplimiento al decreto 1008 de 2018 *"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"* y reconociendo la necesidad de proteger los activos de información de la entidad mediante un modelo de seguridad y privacidad de la información o sistema de gestión de seguridad de la información.

Teniendo en cuenta la norma técnica NTC-ISO/IEC 27001 y el habilitador de seguridad de la información de gobierno digital del Ministerio de Tecnologías de la Información y la Comunicaciones, se debe establecer una política general de seguridad de la información, políticas y procedimientos de seguridad de la información para salvaguardar y proteger los activos en sus tres pilares: Confidencialidad, Integridad y Disponibilidad.

2. OBJETIVO

Establecer la política general de la seguridad de la información, políticas y procedimientos de la seguridad de la información de la Empresa de Servicios Públicos de Chía Emserchia E.S.P., basado en el decreto 1008 de 2018 del Ministerio de las Tecnologías de la Información y las Comunicaciones; y la norma NTC-ISO-27001.

2.1. Objetivos Específicos

- Establecer, implementar y monitorear el modelo de seguridad y privacidad de la información o sistema de gestión de seguridad de la información en la Empresa de servicios públicos de Chía Emserchia ESP.
- Dar cumplimiento a la normatividad vigente relacionada con Gobierno digital.
- Establecer las políticas necesarias para la protección de la información de la entidad.
- Establecer los procedimientos requeridos para el correcto flujo de los procesos de TI garantizando continuamente la seguridad digital.
- Garantizar el estricto cumplimiento de las políticas, normas y procedimientos acá establecidos.

3. ALCANCE

Esta política deberá ser conocida, cumplida y aplicada a todos los funcionarios de planta y contratistas que desarrollen labores administrativas en cada uno de los procesos establecidos por Emserchia E.S.P.

4. DEFINICIONES

Activo: cualquier cosa que tiene valor para la organización[1], es decir, todo elemento que contenga información (hardware, información, software, servicios y recurso humano) y cuyo valor garantice el correcto funcionamiento de la entidad o dependencia.

Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.

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

Información: información denominamos al conjunto de datos, ya procesados y ordenados para su comprensión, que aportan nuevos conocimientos a un individuo o sistema sobre un asunto, materia, fenómeno o ente determinado.

5. MARCO LEGAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data.
- Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos".
- Ley 1581 de 2012, "Protección de Datos personales".
- Decreto 1008 de 2018 ""Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".
- Decreto 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
- Artículo 61 de la Constitución Política de Colombia.
- Decisión Andina 351 de 1993. - Derechos de Autor
- Código Civil, Artículo 671. - PROPIEDAD INTELECTUAL. Las producciones del talento o del ingenio son una propiedad de sus autores.
- Ley 23 de 1982. – Derechos de Autor
- Ley 44 de 1993. – Derechos de Autor

6. CIBERSEGURIDAD

Con base en lo dispuesto en el Decreto 2573 de 2014 - Lineamientos Generales para la Estrategia de Gobierno en Línea, Guía de Ciberseguridad y con el fin de garantizar el cumplimiento de la "Política de seguridad de la información y ciberseguridad para la Empresa de Servicios Públicos de Chía EMSERCHIA E.S.P", en relación con la protección de la información, de los activos y ciberactivos críticos, la respuesta oportuna a incidentes o ataques, la resiliencia y continuidad del negocio frente a los riesgos que los pudieran afectar, se definen los lineamientos para el Sistema de gestión de seguridad de la información.

LINEAMIENTOS

6.1. PROTECCIÓN DE INFORMACIÓN, ACTIVOS CRÍTICOS Y CIBERACTIVOS

La información, los activos críticos y ciber activos objeto de protección, deben ser valorados e implementar los controles necesarios para realizar una operación segura y confiable y contar con información integra y completa, con los niveles de confidencialidad requeridos.

6.2. MANTENIMIENTO DEL INVENTARIO DE ACTIVOS CRÍTICOS Y CIBERACTIVOS

El área de sistemas de EMSERCHIA E.S.P responsables de la operación y mantenimiento de los activos como servidores y bases de datos, deben mantener actualizado el inventario de estos a través de la plataforma GLPI.

6.3. RESPUESTA OPORTUNA A INCIDENTES O ATAQUES.

El área de sistemas son los responsables de gestionar los incidentes de seguridad y ciberataques monitoreando permanentemente con el fin de detectar y anticiparnos a la ocurrencia de los mismos revisando la plataforma BIT DEFENDER y los logs de reporte del FIREWALL como tráfico reenviado, trafico local, filtro web, control de aplicaciones y protección de intrusos, con el fin de hacerle frente a la ocurrencia del incidente o ataque.

6.4. COMPETENCIA Y CONCIENCIACIÓN

El área de sistemas junto con la dirección de Planeación y con la colaboración del Centro Cibernético de la Policía Nacional en el desarrollo de estrategias de sensibilización, capacitación y entrenamiento permanente para los empleados con el objetivo de crear conciencia sobre la necesidad de proteger el conocimiento y los datos de la empresa y para que en sus actuaciones no afecten el desempeño de la seguridad de la información y la ciberseguridad, ejecuta capacitaciones con personal especializado de la Policía Nacional.

7. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Empresa de Servicios Públicos de Chía Emserchia E.S.P., de acuerdo al decreto 1008 del 14 de junio de 2018 del Ministerio de Tecnologías de la Información y las Comunicaciones, establece que es necesario preservar la confidencialidad, integridad y disponibilidad de los activos de información de cada proceso de la entidad, mediante la implementación de un sistema de gestión de seguridad de la información o modelo de seguridad y privacidad de la información, mediante procesos y políticas establecidas por la norma NTC-ISO-27001.

La Empresa de Servicios Públicos de Chía Emserchia E.S.P. se compromete a proteger los activos de información de cada proceso, de acuerdo a su criticidad para minimizar los impactos financieros y legales.

La Empresa de Servicios Públicos de Chía Emserchia E.S.P., se compromete a identificar y establecer controles para mitigar los diferentes riesgos que puedan afectar los activos de información y la continuidad de algún proceso de la entidad.

8. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

8.1. Política de protección de datos y privacidad de la información

Objetivo:

Definir los lineamientos para la protección de datos y privacidad de la información de datos personales de Emserchia ESP.

Desarrollo:

La Empresa de Servicios Públicos de Chía Emserchia E.S.P. realizará procesos de recolección, almacenamiento, procesamiento, uso y transmisión (según corresponda) de datos personales, atendiendo de manera estricta los postulados de seguridad y confidencialidad postulados en la Ley 1581 de 2012 y el Decreto 1377 de 2013. Teniendo en cuenta lo postulado con anterioridad, se definieron los siguientes lineamientos:

- La Empresa de Servicios Públicos de Chía Emserchia E.S.P. reconoce que el único medio autorizado para el tratamiento de datos personales es el dueño de la información, de acuerdo a la Ley de protección de datos personales 1581 de 2012 y el decreto 1377 o la que la adicione, modifique o derogue.

- La Empresa de Servicios Públicos de Chía Emserchia E.S.P. se compromete a otorgar los recursos necesarios para garantizar los tres (3) pilares fundamentales de la seguridad como son la disponibilidad, integridad y confidencialidad de la información, con el fin de dar cumplimiento a los objetivos institucionales, la estrategia y misión de la entidad.

- La Empresa de Servicios Públicos de Chía Emserchia E.S.P. se compromete a cumplir con todos los requisitos legales, reglamentarios y contractuales que haya a lugar, con el fin de gestionar y reducir los riesgos a un nivel aceptable.

- Establecer la mejora continua del sistema de gestión de seguridad de la información, a través de un conjunto de reglas y directrices orientadas a garantizar la protección de los activos de información de La Empresa de Servicios Públicos de Chía Emserchia E.S.P., de una manera contundente, eficiente y efectiva, de la misma forma velar por tomar las acciones necesarias para la evaluación, análisis y tratamiento de los riesgos de acuerdo a la metodología adoptada por la Gerencia.

- El área de Sistemas de Información se compromete a velar por la aplicación y cumplimiento adecuado de la presente política de seguridad de la información y todas las que se deriven de ella, por parte de

todos los funcionarios, contratistas, colaboradores y terceros de la Empresa de Servicios Públicos de Chía Emserchia E.S.P..

- En cualquier situación que se deba realizar el tratamiento de la información personal de algún ciudadano funcionario, se deberá contar con el consentimiento previo del titular de los datos para realizar el ejercicio y tener un registro del mismo teniendo en cuenta que se recolecta información por diferentes medios electrónicos.
- Se deberá conservar la información bajo condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- En caso tal que la información obtenida contenga datos erróneos, se deberá notificar de inmediato y realizar las correcciones correspondientes en el menor tiempo posible.
- Se deberá garantizar al dueño de la información, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- Se deberá informar con prontitud cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los servidores públicos.

8.2.Política de dispositivos móviles

Objetivo:

Establecer los estándares para el uso y configuración de los dispositivos móviles suministrados por Emserchia ESP.

Desarrollo:

- El área de sistemas de información es la única encargada de realizar la configuración y descarga de software de los dispositivos móviles.
- El personal de la Empresa de Servicios Públicos de Chía Emserchia E.S.P. tiene una cuenta de correo electrónico institucional y por tal motivo los dispositivos móviles deben ser configurados con esa cuenta para su uso.
- El personal que cuente con dispositivos móviles de la Empresa de Servicios Públicos de Chía Emserchia E.S.P. no deben enviar documentos, audios, videos e imágenes con información reservada o clasificada.

- Los dispositivos móviles no se podrán conectar a redes inalámbricas públicas.
- Los dispositivos móviles deben contar con mecanismos de contraseña o bloqueo de pantalla cuando no estén en uso.
- En caso que el dispositivo móvil contenga información reservada o clasificada de la entidad esta información se deberá cifrar.
- El personal de La Empresa de Servicios Públicos de Chía Emserchia E.S.P. es responsable del buen uso de los dispositivos móviles a su cargo.

8.3.Política pantalla y escritorio limpio

Objetivo:

Establecer los estándares para prevenir el riesgo de acceso no autorizado, pérdida, robo o modificación de la información durante y después de horas laborales.

8.3.1. **Pantalla limpia:**

- Las personas que trabajan o laboran en la Empresa de Servicios Públicos de Chía Emserchia E.S.P., deben bloquear, suspender o apagar los equipos tecnológicos (impresoras, equipos de cómputo, escáner y portátiles) cuando no estén en uso.
- La pantalla se debe conservar limpia, libre de información, que pueda ser utilizada por personas externas y sin autorización para su uso.
- El fondo de pantalla de los equipos de cómputo y portátiles de la Empresa de Servicios Públicos de Chía Emserchia E.S.P. es establecido por el área de Sistemas de información.
- Cada equipo de cómputo y portátil de la Empresa de Servicios Públicos de Chía Emserchia E.S.P. cuenta con un tiempo establecido para el bloqueo de la pantalla cuando no se encuentre en uso, este tiempo no deberá ser modificado por el usuario y no debe superar los 5 minutos de inactividad
- Los equipos de cómputo o portátiles se pueden bloquear o suspender utilizando las teclas Windows + L.
- Cada equipo de cómputo y portátil que se encuentre Empresa de Servicios Públicos de Chía Emserchia E.S.P. cuenta con un sistema de autenticación por usuario y contraseña establecido por la Oficina de Tecnologías de la Información y las Comunicaciones.

8.3.2. **Escritorio limpio:**

- Las personas que trabajan o laboran en la Empresa de Servicios Públicos de Chía Emserchia E.S.P., cuando se ausenten del puesto de trabajo o después del horario laboral deben guardar los documentos o medios de almacenamiento removibles (USB, CD, Discos duros o DVD) que contengan información confidencial o clasificada de la entidad en un gabinete o escritorio con llave.
- Los documentos o medios de almacenamiento removibles (USB, CD, Discos duros o DVD) que se encuentren sin uso o desatendidos se deben guardar.
- Los documentos con información confidencial o clasificada se deben retirar de la impresora, fotocopiadora, escáneres y/o fax.
- Evitar escribir o dejar a la vista las contraseñas de acceso a sistemas, aplicaciones o equipos de cómputo.

8.4.Política gestión de medios removibles

Objetivo:
Definir las directrices para la gestión de medios removibles de la Empresa de Servicios Públicos de Chía Emserchia E.S.P., cumpliendo con la preservación de la confidencialidad e integridad de la información.

Desarrollo:

- Como medida preventiva el área de Sistemas de Información ha decidido restringir el uso de medios removibles en los equipos de la Empresa de Servicios Públicos de Chía Emserchia E.S.P., toda vez que realizado el análisis técnico se detectó como mayor amenaza de contagio de virus informático en los equipos de la entidad.

- Para habilitar los puertos USB en un equipo, se deberá justificar la solicitud por medio de un correo electrónico dirigido a la jefe de la Oficina Asesora de Planeación y al Profesional de Sistemas de Información, dicho correo deberá contener de manera detalla el porque se solicita dicho servicio.

- Para evitar el contagio de virus en los dispositivos de almacenamiento externos, se recomienda no hacer uso de ellos como único medio para reposar (proteger) información de la Empresa de Servicios Públicos de Chía Emserchia E.S.P.

- No es responsabilidad del área de sistemas de información salvar información en caso que los dispositivos de almacenamiento externo se hayan contagiado de virus o la información haya sido eliminada involuntariamente.

- Se recomienda no utilizar los archivos almacenados en estos dispositivos, para sobre escribir información en ellos, debido a que es un dispositivo que está expuesto a daños por su manipulación y factores externos.

- Como medio alternativo para salvaguardar información importante del funcionario, el correo institucional cuenta con Google Drive, una plataforma de almacenamiento en la nube que cuenta con una capacidad ilimitada para guardar cualquier tipo de información.

- Los funcionarios son responsables en mantener asegurada la información, libre de software malicioso y verificando el escaneo de los dispositivos para verificar que estén libres de virus cada vez que se ingresen en algún equipo.

- Se debe hacer seguimiento a los medios de almacenamiento removibles como Discos Duros, Cintas, etc., con el fin de garantizar que la información sea transferida a otro medio antes de que esta quede inaccesible por deterioro o el desgaste que sufren a causa de su vida útil.

- Al momento en que los dispositivos removibles cumplan su ciclo de vida (ya no sean funcionales), se deberá retirar de la Empresa de Servicios Públicos de Chía Emserchia E.S.P. y asegurar su des habilitación y/o destrucción pertinente.

- Como medida de seguridad se deberá promover el uso de DLP (Prevención de pérdida de datos) cuando se haga uso continuado de dispositivos removibles para el tratamiento de información de la Empresa de Servicios Públicos de Chía Emserchia E.S.P.

8.5.Política de acceso a redes y servicios en red.

Objetivo:

Definir los lineamientos clave para el acceso a redes y servicios en red de la Empresa de Servicios Públicos de Chía Emserchia E.S.P.

Desarrollo:

- El área de sistemas de información suministra a los usuarios las contraseñas de acceso a los servicios de red, servicios y sistemas de información que requiera para el desempeño de sus funciones laborales.

- El acceso a red alámbrica de la entidad se realiza con una IP única asignada al funcionario.

- Las claves para el servicio de red inalámbrico solo serán otorgadas con la previa autorización de la jefe de la oficina asesora de planeación ya sea de manera verbal o escrita.

- Las claves para los servicios en red son de uso personal e intransferible y es responsabilidad del usuario el uso de las credenciales asignadas.

- Sólo el personal designado por el área de Sistemas de Información está autorizado para configurar la red, instalar software o hardware en los equipos, servidores e infraestructura de tecnología de la Empresa de Servicios Públicos de Chía Emserchia E.S.P.

- Toda actividad que requiera acceder a los servidores, equipos o a las redes de la Empresa de Servicios Públicos de Chía Emserchia E.S.P., se debe realizar en las instalaciones y con el personal especializado. No se debe realizar ninguna actividad de tipo remoto sin la debida autorización del área de sistemas de información.

- La creación y retiro de usuarios en los sistemas de información en producción debe seguir el INSTRUCTIVO PARA LA ASIGNACION DE USUARIOS Y CONTRASEÑAS DE LA ENTIDAD publicado en el Sistema integrado de Gestión.

- Toda actividad de red se controlará mediante una UTM Fortinet donde se realizará el proceso de filtrado web, control de aplicaciones y antivirus perimetral.

- Para el acceso a los servicios de red (corrycom, SIG, Gestión de vehículos y demás aplicativos Web) el área de Sistemas de Información entrega usuario y contraseña únicos.

- Existe una red de invitados (inalámbrica) habilitada para el acceso a usuarios externos, este acceso solo podrá ser concedido por el área de sistemas de información solicitando previamente la respectiva justificación.

8.6. Política control de acceso físico

Objetivo:

Definir los lineamientos para el control de acceso físico en áreas seguras de la Empresa de Servicios Públicos de Chía Emserchia E.S.P.

Desarrollo:

- Las áreas seguras, dentro de las cuales se encuentran el Datacenter, centros de cableado, áreas de archivo, centros de datos físicos y digitales, áreas de procesamiento de información, entre otros, deben

contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información.

- Para el acceso a áreas seguras de la Empresa de Servicios Públicos de Chía Emserchia E.S.P. se manejan accesos por medio de clave, huella, carnet institucional o permisos especiales según corresponda.
- Cada dependencia es responsable de designar a funcionarios y/o contratistas con los permisos de acceso a zonas restringidas en su área.
- Todas las entradas que utilizan sistemas de control de acceso deben permanecer cerradas y es responsabilidad de todos los funcionarios, contratistas, colaboradores y terceros autorizados, como medida de seguridad, evitar que las puertas se dejen abiertas.
- Las actividades de limpieza del Datacenter serán realizadas por solamente por el personal del área de sistemas de información, en caso que se requiera el apoyo de alguien ajeno al área se realizará el respectivo acompañamiento. La limpieza de las demás áreas seguras será coordinada y responsabilidad del encargado de dicha área.
- Se deben realizar acciones para prevenir la pérdida, daño, robo o compromiso de activos de información y la interrupción de las operaciones de la organización; los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas, peligros del entorno y las posibilidades de acceso no autorizado, protegidos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro, el cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información debe estar protegido contra interceptación, interferencia o daño.

Los lineamientos para el ingreso físico al Datacenter de la Empresa de Servicios Públicos de Chía Emserchia E.S.P. están estipulados en el procedimiento **de ingreso al Datacenter encontrado en el proceso de Gestión de las Tics.**

8.7. Política seguridad en oficinas, recintos e instalaciones

Objetivo:

Gestionar los lineamientos básicos para la seguridad en oficinas, recintos e instalaciones de la empresa de servicios Públicos de Chía Emserchia ESP.

Desarrollo:

- Se debe establecer un control de acceso al público estricto para toda oficina, recinto e instalación clave (esta característica se define por el tipo de información y equipos tecnológicos con los que cuente cada área) para la Empresa de Servicios Públicos de Chía Emserchia E.S.P.
- Se debe tener un control estricto del directorio interno de extensiones de las oficinas de la Empresa de Servicios Públicos de Chía Emserchia E.S.P., es prioridad de los servidores públicos velar por mantener seguras las extensiones de áreas sensibles (Datacenter, oficinas que generan información de alta criticidad, entre otras).
- Los perímetros de seguridad para oficinas, recintos e instalaciones de la Empresa de Servicios Públicos de Chía Emserchia E.S.P. que manejen o generen información sensible (bases de datos, archivos, almacenes, etc.) deben estar delimitados por una barrera, como una pared, puerta de acceso controlado por un dispositivo de autenticación o una oficina de recepción, atendida por personal de Emserchia E.S.P. que controle el acceso físico a estas áreas.
- Los puestos de trabajo de los funcionarios de la Empresa de Servicios Públicos de Chía Emserchia E.S.P. deberán permanecer limpios y libres de documentación sensible y/o clasificada cuando se encuentren fuera de horario laboral o en ausencia prolongada del sitio, lo anterior con el fin de evitar accesos no autorizados a la información.
- Las personas que trabajan o laboran en la Empresa de Servicios Públicos de Chía Emserchia E.S.P., son responsables de bloquear, suspender o apagar los equipos tecnológicos (impresoras, equipos de cómputo, escáner y portátiles) cuando no estén en uso. Al finalizar actividades laborales, se deberán cerrar todas las aplicaciones y dejar los equipos respectivamente apagados.
- Los documentos con información confidencial o clasificada se deben retirar de la impresora, fotocopiadora, escáneres y/o fax para evitar la pérdida o robo de información de estos documentos.

8.8.Política gestión de incidentes de seguridad de la información

Objetivo:

Gestionar de manera adecuada los eventos, incidentes y vulnerabilidades de seguridad de la información que se generen en la Empresa de Servicios Públicos de Chía Emserchia E.S.P. con el fin de prevenir y limitar el impacto de estos.

Desarrollo

- El área de sistemas de información informara oportunamente al centro de ciberseguridad de la Policía Nacional mediante el CAI Virtual disponible en la página principal de la policía.
- Informar de manera oportuna a la jefe de la oficina de planeación para coordinar las directrices dadas por gerencia.

8.9. Política instalación de software

Objetivo:

Definir las directrices para la instalación de software en los equipos de la Empresa de Servicios Públicos de Chía Emserchia E.S.P. para su correcto funcionamiento.

Desarrollo

- El área de sistemas de información deberá proporcionar el software que se requiera en los equipos de la Empresa de Servicios Públicos de Chía Emserchia E.S.P. para el respectivo cumplimiento de las actividades laborales a desarrollar.
- Sólo personal capacitado y autorizado por el área de sistemas de información se encargará de la instalación, actualización y monitoreo del software que esté instalado en los equipos de la entidad.
- Todo software que se instale en los equipos de la Empresa de Servicios Públicos de Chía Emserchia E.S.P. deberán contar con su licencia correspondiente (exceptuando casos de software libre), así como es responsabilidad del área de sistemas de información de mantener las licencias al día.
- Para el control de los programas que se instalen en los equipos de la Empresa de Servicios Públicos de Chía Emserchia E.S.P., el área de sistemas de información deberá monitorear cada equipo de cómputo con una herramienta especial para dicho proceso.
- Si alguna área de la Empresa de Servicios Públicos de Chía Emserchia E.S.P. solicita un software en específico para el funcionamiento de su área, se deberá realizar la solicitud formal a la jefe de la oficina asesora de planeación a través de un oficio, donde especifique el software requerido (el pago de la respectiva licencia de software se hace por parte del área que lo solicita).

8.10.Política de transferencia de información

Objetivo:

Garantizar que la información de la Empresa de Servicios Públicos de Chía Emserchia E.S.P. sea transferida terceros o las personas que la requieran cumpliendo una serie de acuerdos y lineamientos.

Desarrollo:

- Los funcionarios públicos de la Empresa de Servicios Públicos de Chía Emserchia E.S.P. que envíen todo tipo de documentación a entidades externas, se debe verificar previamente el envío, el nombre

de los destinatarios de la información, con el fin de reducir la posibilidad de envío de este tipo de datos, a destinatarios no deseados.

- Cuando se envía documentación con información pública reservada o clasificada, la oficina de gestión documental de la Empresa de Servicios Públicos de Chía Emserchia E.S.P. se designa un funcionario profesional y responsable para llevar directamente la correspondencia a las diferentes entidades gubernamentales como la Contraloría, Procuraduría, gobernaciones entre otras, como evidencia del documento entregado, se relaciona la información en una planilla donde el funcionario que recibe la correspondencia firma la planilla y al oficio se le coloca un stickers donde aparece el número de radicado, fecha y todos los datos para que no haya ningún tipo de pérdida o modificación del mismo.

- Existen software o aplicaciones que designan las Contralorías o Procuradurías para la transferencia de la información de diferentes áreas de la Empresa de Servicios Públicos de Chía Emserchia E.S.P., donde se asignan un usuario y contraseña permitiendo enviar todo tipo de informes y documentos de manera más eficiente y segura.

- La correspondencia que ingresa a la Empresa de Servicios Públicos de Chía Emserchia E.S.P., llega a la oficina de gestión documental y se maneja un consecutivo e informe donde se sube toda la documentación a la plataforma de Corrycom.

9. PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

9.1.Procedimiento borrado seguro

Objetivo:

Establecer los procedimientos de borrado seguro de la Empresa de Servicios Públicos de Chía Emserchia E.S.P. con el fin de garantizar que bajo los escenarios establecidos se realice una correcta eliminación de la información para evitar extracción de información confidencial.

Desarrollo

- Cualquier equipo obsoleto o dañado que se desee dar de baja y este contenga disco duro se deberá realizar un borrado seguro de la información que contenga.

- El técnico/ ingeniero realiza el formateo, eliminación de usuario y borrado seguro del medio tecnológico.

- Dependiendo del área donde se encuentra el medio tecnológico, se realiza la asignación del mismo a algún funcionario por orden del jefe del área.

- Si el jefe del área no desea realizar la asignación del medio tecnológico, este puede realizar la entrega a almacén en caso de ser equipo propio o al área de sistemas de información si es alquilado.

9.2. Procedimiento para el uso de programas utilitarios privilegiados

Objetivo:
Establecer los procedimientos para el uso de programas utilitarios privilegiados de la Empresa de Servicios Públicos de Chía Emserchia E.S.P., con la capacidad de anular los controles de sistemas y de aplicaciones.

Desarrollo:

- El área de sistemas de información realiza la instalación de los programas utilitarios necesarios para el funcionamiento del equipo de cómputo al momento de entregar un equipo de cómputo.

- El área de sistemas de información debe revisar mensualmente las directrices para el uso de programas utilitarios con la capacidad de anular los controles de sistemas y de aplicaciones.

- El área de sistemas de información debe utilizar procedimientos de identificación, autenticación y autorización para los programas utilitarios que requieran los funcionarios para realizar trabajos específicos.

- El área de sistemas de información es la única autorizada para instalar, eliminar o modificar los programas utilitarios, si el funcionario instala algún programa de este tipo será eliminado.

9.3.Procedimiento propiedad intelectual, uso legal de software y productos informáticos.

Objetivo:
Dar cumplimiento a los requisitos contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. Con fin de tener un mayor control y seguimiento de los programas y/o aplicaciones que reposan en cada equipo o servidor de la Empresa de Servicios Públicos de Chía Emserchia E.S.P.

Desarrollo:

- Si se encuentra software ilegal o no cuenta con una licencia válida, se procede a la desinstalación de este mediante los procedimientos que realiza el área de Sistemas de información.

- La Empresa de Servicios Públicos de Chía Emserchia E.S.P. posee el inventario correspondiente y el software de verificación y control.

9.4.Procedimiento para la transferencia de medios físicos

Objetivos:
Definir acciones que prevengan y eviten la divulgación, modificación, retiro o la destrucción no autorizada de la información almacenada en los medios suministrados por la Empresa de Servicios Públicos de Chía Emserchia E.S.P., cuidando por la disponibilidad y confidencialidad de la información.

Desarrollo:

- Mantener con las medidas de protección físicas y lógicas de los medios y equipos que permitan su monitoreo y correcto estado de funcionamiento, realizando los mantenimientos preventivos y correctivos que se requieran.

- Los sistemas de información, aplicaciones (software), el servicio de acceso a Internet, Intranet, medios de almacenamiento, cuentas de red, navegadores y equipos de cómputo que son propiedad de la entidad, deberán ser usados únicamente para el cumplimiento misional de la entidad.

- Realizar el procedimiento de borrado seguro en los equipos de cómputo y demás dispositivos, una vez el funcionario haya sido retirado de Emserchia E.S.P.

- Restringir el uso de medios de almacenamiento extraíble tanto para lectura como escritura. La autorización de uso de los medios removibles debe ser gestionada a través de la jefe de la oficina asesora de planeación y será objeto de auditorías de seguridad, apoyado en la prevención de pérdida de información de la Empresa de Servicios Públicos de Chía Emserchia E.S.P.

- El intercambio de información de la entidad con otras organizaciones o terceros debe estar controlado y se debe cumplir la legislación y normas vigentes que correspondan para mantener una adecuada protección de la información de Emserchia E.S.P., estableciendo acciones, procedimientos y controles de intercambio de información a través de medios físicos disponibles.

9.5.Lineamiento de seguridad de la información en el ciclo de vida de proyectos

Integrar diferentes métodos de gestión de proyectos en la Empresa de Servicios Públicos de Chía Emserchia E.S.P., para asegurar que los riesgos de seguridad de la información que se identifican y se tratan como parte de los diferentes proyectos desarrollados.

- Alinear los objetivos de los proyectos con los de seguridad y privacidad de la información de la entidad.
- Establecer y fijar responsabilidades en roles específicos para gestionar la seguridad de información en los proyectos, de acuerdo con los métodos definidos en la gestión de proyectos.
- Realizar la valoración de riesgos de seguridad en etapas iniciales de los proyectos desarrollados en los diferentes procesos de la entidad, con el propósito de identificar los controles necesarios para mitigar los riesgos.

9.6.Procedimiento para el acceso de áreas de despacho y carga

Objetivo:
Describir los accesos de áreas de despacho y de carga donde los funcionarios, contratistas y visitantes deben ingresar a las instalaciones de la Empresa de Servicios Públicos de Chía Emserchia E.S.P. y asegurar solamente el ingreso de personal o visitantes autorizados a las diferentes dependencias al igual que en las áreas catalogadas como seguras.

Desarrollo:

- El acceso de personal a las zonas de despacho y carga de la Empresa de Servicios Públicos de Chía Emserchia E.S.P. debe ser autorizado por el encargado del área que solicita el servicio y en permanente compañía.
- Establecer que el material que ingresa se registra de acuerdo con los procedimientos de gestión de activos al entrar al sitio.
- Definir que los despachos entrantes y salientes están separados físicamente, en donde sea posible.
- Todo vehículo que ingrese a dejar o retirar elementos de la Entidad debe ser autorizado por el Director Administrativo y Financiero realizando la solicitud previa el funcionario encargado del área que solicita el servicio.
- Definir que el material que ingresa se inspecciona y examina para determinar la presencia de explosivos, químicos u otros materiales peligrosos.
- La salida de bienes que sean propiedad de la Empresa de Servicios Públicos de Chía Emserchia E.S.P deben ser previamente autorizados, por el jefe del Área a través de correo electrónico enviado por el nivel directivo del área donde pertenecen.

9.7.Procedimiento para la restricción de instalación de software

Objetivo:
Definir las directrices para las restricciones sobre la instalación se software de la Empresa de Servicios Públicos de Chía Emserchia E.S.P

Desarrollo:

- Cuando algún funcionario de la entidad realice un requerimiento para la instalación de un Software, el área de sistemas de información está en la obligación de evaluar la necesidad de adquisición de dicho software.
- Todo software que sea instalado en algún equipo de algún funcionario de la Empresa de Servicios Públicos de Chía Emserchia E.S.P, debe ser licenciado y aprobado por el área de sistemas de información.
- Cuando se realice la instalación de un software se deben tener en cuenta las características y/o capacidades de los equipos de cómputo.
- Ningún software licenciado de la Empresa de Servicios Públicos de Chía Emserchia E.S.P, en ninguna circunstancia debe proporcionarse a personas u organizaciones externas o usarse con fines de lucro.

9.8.Procedimiento para trabajo en áreas seguras

Objetivo:
Definir los lineamientos para el trabajo en áreas seguras en las instalaciones y sedes de la Empresa de Servicios Públicos de Chía Emserchia E.S.P.

La Empresa de Servicios Públicos de Chía Emserchia E.S.P debe mantener áreas seguras de trabajo para la gestión, almacenamiento y procesamiento de la información en la Entidad. Teniendo en cuenta lo postulado con anterioridad, se definieron los siguientes lineamientos:

Desarrollo:

- Se deben definir perímetros de seguridad según las necesidades del área de trabajo y perfiles de los empleados que estén involucrados.
- Para áreas en donde se tenga custodia servidores, centros de cómputo y/o centros de cableado, se deberá realizar un monitoreo constante de variables como temperatura y humedad de las áreas de procesamiento de datos.
- La entidad debe designar y aplicar protección física para la prevención de desastres como: incendios, inundaciones, terremotos, explosiones, manifestaciones y otras formas de desastre natural o humano.

- Para áreas con centros de cómputo y/o cableado se debe velar por el ambiente adecuado para los activos informáticos, controlando temas de ventilación, iluminación, regulación de corriente, entre otros.

- Se debe tener un control de acceso físico a zonas que lo requieran, como pueden ser centros de bodegaje de archivos, activos físicos de sistemas de información, centros de datos, entre otros.

- Cuando un área que maneje información crítica de la Entidad esté vacía o no se encuentre personal trabajando en estas áreas, se deberá mantener la zona con los recursos de seguridad correspondientes, como pueden ser cámaras activas según se requiera.

- El uso de dispositivos de grabación y/o registro fotográfico tales como cámaras en dispositivos móviles están restringido en las áreas seguras de trabajo de la Empresa de Servicios Públicos de Chía Emserchia E.S.P, a menos que se cuente con una autorización para ello.

- Se debe evitar el trabajo no supervisado en las áreas seguras de la Empresa de Servicios Públicos de Chía Emserchia E.S.P, con el fin de proteger la integridad y seguridad de la información que se maneje en dicha área.

- La responsabilidad del ingreso a áreas denominadas como seguras será exclusiva del responsable de dicha área.

- Se deben usar los elementos de protección personal que el área segura requiera.

10. **CUMPLIMIENTO**

Todos los directores, subdirectores, funcionarios y contratistas de la Empresa de Servicios Públicos de Chía Emserchia E.S.P, debe cumplir con el 100% de la política.