



ENERGUAVIARE
SA ESP

**EMPRESA DE ENERGÍA ELÉCTRICA DEL
DEPARTAMENTO DEL GUAVIARE S.A. E.S.P.**

Nit. 822.004.680-9

Avanzando con Energía

POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN Y DE USUARIOS

COPIA CONTROLADA

San José del Guaviare 17 de Abril de 2018

CALLE 8 # 23-55 CENTRO
LINEA DE SERVICIO AL CLIENTE
584 04 93 - CEL.: 318 782 7947
OFICINAS 584 04 93
SAN JOSÉ DEL GUAVIARE

La Empresa de Energía Eléctrica del Departamento del Guaviare - **ENERGUAVIARE S.A. E.S.P.**, se constituye bajo la iniciativa de la Administración Departamental con la figura de sociedad anónima el 30 de agosto de 2001, mediante Escritura Pública No. 848 de la Notaría Única de San José del Guaviare, inscrita en la Cámara de Comercio el 10 de Septiembre de 2001, folio número 282 del libro respectivo.

El objeto social y Registro Único de Prestadores de Servicios públicos – **RUPS** de **ENERGUAVIARE S.A. E.S.P.**, es Comercialización y Distribución de Energía Eléctrica en el Sistema Interconectado Nacional – **SIN**, Generación, Distribución y Comercialización de Energía en Zonas No Interconectadas – **ZNI**, prestando sus servicios en la actualidad en San José del Guaviare y en las localidades de El Retorno, Calamar, La Libertad, el Capricho y Puerto Concordia – Meta.

Que La Empresa de Energía Eléctrica del Departamento del Guaviare **ENERGUAVIARE S.A. E.S.P.**, en su calidad de prestadora de un servicio público domiciliario requiere recolectar y tratar datos de carácter personal no solo de los funcionarios, terceros, proveedores, si no de la comunidad que se beneficia del servicio que presta, razón por la cual se encuentra sujeta al cumplimiento de lo dispuesto por la Ley 1581 de 2012, Decreto reglamentario 1377 de 2013 y el Decreto 886 de 2014, que regulan la recolección y tratamiento de los datos de carácter personal, establecen las garantías legales que deben cumplir todas las personas en Colombia para el debido tratamiento de dicha información, y el Registro Nacional de Base de Datos

La Empresa de Energía Eléctrica del Departamento del Guaviare **ENERGUAVIARE S.A. E.S.P.** Identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la empresa, razón por la cual se hace necesario establecer un marco en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.

Este documento describe las políticas y normas de seguridad de la información y de usuarios de datos personales, definidas por **ENERGUAVIARE S.A. E.S.P.**

Las políticas incluidas en este manual se constituyen como parte fundamental del sistema de gestión de seguridad de la información de **ENERGUAVIARE S.A. E.S.P.** y se convierten en la base para la implementación de los controles, procedimientos y estándares definidos para la protección de base de datos.

CALLE 8 # 23-55 CENTRO
LINEA DE SERVICIO AL CLIENTE

584 04 93 - CEL.: 318 782 7947

OFICINAS 584 04 93

SAN JOSÉ DEL GUAVIARE

La seguridad de la información y de los usuarios es una prioridad para ENERGUAVIARE S.A. E.S.P. y por tanto es responsabilidad de todos velar por que no se realicen actividades que contradigan la esencia de cada una de estas políticas.

2. OBJETIVO

El objetivo de este documento es establecer las políticas en seguridad de la información y de usuarios de datos personales tratados por ENERGUAVIARE S.A. E.S.P. con el fin de regular la gestión de la seguridad de la información al interior de la entidad.

3. ALCANCE

Las políticas de seguridad de la información y de usuarios de datos personales cubren todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios y terceros que laboren o tengan relación con ENERGUAVIARE S.A. E.S.P., para conseguir un adecuado nivel de protección, seguridad y calidad de la información relacionada.

4. DEFINICIONES

La Empresa de Energía Eléctrica del Departamento del Guaviare **ENERGUAVIARE S.A. ESP** pone de presente las siguientes definiciones establecidas, para facilitar la interpretación de la presente política

Activo de información: Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de ENERGUAVIARE S.A. E.S.P. y, en consecuencia, debe ser protegido.

Acuerdo de Confidencialidad: Es un documento en los que los funcionarios de ENERGUAVIARE S.A. E.S.P., usuarios, proveedores y los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la empresa comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Autenticación: Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Confidencialidad: Es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Control: Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Custodio del activo de información: Es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

Disponibilidad: Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Equipo de cómputo: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Incidente de Seguridad: es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Integridad: Es la protección de la exactitud y estado completo de los activos.

Inventario de activos de información: Es una lista ordenada y documentada de los Activos de información pertenecientes a ENERGUAVIARES S.A. E.S.P

Licencia de software: Es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Los repositorios: Proporcionan acceso a tipos específicos de fuentes de archivos. También pueden permitir, donde sea apropiado, que los usuarios suban archivos, accedan a archivos subidos previamente, y traer contenido fácilmente adentro desde fuentes externas.

Medio removible: Es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

Grupos de usuarios: Son grupos que concentran varios usuarios con similares necesidades de autorizaciones idénticas sobre los recursos tecnológicos de acuerdo con las o

los sistemas de información a los cuales se les concede acceso a funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

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

Recursos tecnológicos: Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), puestos de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior ENERGUAVIARE S.A. E.S.P.

Responsable por el activo de información: Es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

SGSI: Sistema de Gestión de Seguridad de la Información.

Sistema de información: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por ENERGUAVIARE S.A. E.S.P. o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.

Software malicioso: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

Usuario. Es la persona natural o jurídica a la que se le presta el servicio.

Terceros: Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

CALLE 8 # 23-55 CENTRO
LINEA DE SERVICIO AL CLIENTE
584 04 93 - CEL.: 318 782 7947
OFICINAS 584 04 93
SAN JOSÉ DEL GUAVIARE

Vulnerabilidades: Son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la empresa (amenazas), las cuales se constituyen en fuentes de riesgo.

I. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

En la Empresa de Energía Eléctrica del departamento del Guaviare ENERGUAVIARE S.A. E.S.P. la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad de la empresa, la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de las necesidades actuales, ENERGUAVIARE S.A. E.S.P. implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad que garantice el cumplimiento de los requerimientos legales, contractuales, regulatorios vigentes.

Los funcionarios, personal externo, usuarios, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes y recursos de procesamiento de la información de ENERGUAVIARE S.A. E.S.P., deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, a fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

ENERGUAVIARE S.A. E.S.P. adoptará las medidas necesarias (técnicas, humanas y administrativas) para otorgar seguridad a los registros, evitando su pérdida, adulteración, consulta, uso o acceso no autorizado o fraudulento. Lo anterior acorde con el principio de seguridad consagrado en la ley 1581 de 2012.

ENERGUAVIARE S.A. E.S.P. tendrá la potestad de modificar las Políticas Específicas de Seguridad de la Información de acuerdo con las necesidades de revisión establecidas periódicamente o a la aplicabilidad de las mismas.

1.1. IMPLEMENTACIÓN DE LAS MEDIDAS DE SEGURIDAD.

ENERGUAVIARE S.A. E.S.P. tendrá o implementará un protocolo de seguridad, el cual será de obligatorio cumplimiento para el personal con acceso a los datos y a los sistemas de información. Este protocolo tendrá como mínimo los siguientes aspectos:

- Ámbito de aplicación del procedimiento con especificación detallada de los recursos protegidos.
- Procedimientos y estándares direccionados a garantizar el nivel de seguridad exigido en la Ley 1581 de 2012.
- Funciones y obligaciones del personal a cargo del manejo de los sistemas de información.
- Estructura de las bases de datos de carácter personal y descripción de los sistemas de información que los tratan.
- Procedimiento de notificación, gestión y respuesta ante las solicitudes y/o reclamos mediante un protocolo de atención a los titulares de datos.
- Protocolos para la ejecución de back up y recuperación de los datos.
- Controles periódicos de verificación del cumplimiento del protocolo de seguridad implementado.
- Adopción de medidas para el transporte, destrucción o reutilización de los documentos soporte de los sistemas de información.
- Actualización y revisión del protocolo, por lo menos una vez al año, o cuando se produzcan cambios relevantes en el sistema de información.

PARAGRAFO: El protocolo se mantendrá actualizado a las disposiciones vigentes en materia de seguridad de los datos personales.

1.2. AVISO DE PRIVACIDAD:

El Aviso de Privacidad es el documento físico que es puesto a disposición del Titular para el tratamiento de sus datos personales. A través de dicho documento se da a conocer al Titular, la información relativa a la existencia de las políticas de seguridad de la información y de usuarios que le serán aplicables, la forma de acceder a las mismas y las características del tratamiento que se pretende dar a los datos personales.

1.2.1. CONTENIDO MÍNIMO DEL AVISO DE PRIVACIDAD.

El Aviso de Privacidad, como mínimo, deberá contener la siguiente información:

- ✓ La identidad, domicilio y datos de contacto del Responsable del Tratamiento.
- ✓ El tipo de tratamiento al cual serán sometidos los datos y la finalidad del mismo.

CALLE 8 # 23-55 CENTRO
LÍNEA DE SERVICIO AL CLIENTE
584 04 93 - CEL.: 318 782 7947
OFICINAS 584 04 93
SAN JOSÉ DEL GUAVIARE

- ✓ Los mecanismos generales dispuestos por el Responsable para que el Titular conozca la política de tratamiento de la información y los cambios sustanciales que se produzcan en ella.
- ✓ En todos los casos, debe informar al Titular cómo acceder o consultar la política de tratamiento de información y el protocolo de atención a los titulares de datos.

EL AVISO DE PRIVACIDAD Y POLÍTICAS DE TRATAMIENTO DE LA INFORMACIÓN. LA EMPRESA DE ENERGIA ELECTRICA DEL DEPARTAMENTO DEL GUAVIARE "ENERGUAVIARE S.A. ESP" conservará el modelo del aviso de privacidad que fue transmitido por el responsable del tratamiento a los Titulares, mientras se lleve a cabo el tratamiento de datos personales y perduren las obligaciones que de éste deriven. Para el almacenamiento del modelo, LA EMPRESA DE ENERGIA ELECTRICA DEL DEPARTAMENTO DEL GUAVIARE "ENERGUAVIARE S.A. ESP" empleará medios físicos, informáticos, electrónicos o cualquier otra tecnología.

1-COMPROMISO DE LA DIRECCION

La Junta Directiva de ENERGUAVIARE S.A. E.S.P aprueba esta Política de Seguridad de la Información y de usuarios como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la entidad.

La Junta Directiva y la Gerencia de ENERGUAVIARE S.A. E.S.P. demuestran su compromiso a través de:

- La revisión y aprobación de las Políticas de Seguridad de la Información y de usuarios contenidas en este documento.
- La promoción activa de una cultura de seguridad.
- Facilitando la divulgación de esta política a todos los funcionarios de la entidad.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.
- La verificación del cumplimiento de las políticas aquí mencionadas.

2. MEDIDAS DE SEGURIDAD. ENERGUAVIARE S.A. E.S.P:

Adoptará las medidas necesarias (técnicas, humanas y administrativas) para otorgar seguridad a los datos personales tratados por ENERGUAVIARE S.A. E.S.P, evitando su pérdida, adulteración, consulta, uso o acceso no autorizado o fraudulento. Lo anterior acorde con el principio de seguridad consagrado en la ley 1581 de 2012

2.1 SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y DE USUARIOS

Las Políticas de Seguridad de la Información y de usuarios, pretenden instituir y afianzar la cultura de seguridad de la información entre los funcionarios, personal externo, usuarios del servicio y proveedores de ENERGUAVIARE S.A. E.S.P. por tal razón, es necesario que las violaciones a las Políticas Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

3. DE LA ESTRUCTURA ORGANIZACIONAL DE LA SEGURIDAD DE LA INFORMACIÓN

ENERGUAVIARE S.A. E.S.P. establecerá un esquema de seguridad de la información en donde existan roles y responsabilidades definidos que consideren actividades de administración, operación y gestión de la seguridad de la información de las bases de datos tratadas por ENERGUAVIARE S.A. E.S.P.

3.1. Normas que rigen para la estructura organizacional de seguridad de la información

Normas dirigidas a: COMITÉ MECI-CALIDAD

- El Comité MECI-CALIDAD debe actualizar y presentar ante la Junta Directiva y la Gerencia las Políticas de Seguridad de la Información, la metodología para el análisis de riesgos de seguridad y la metodología para la clasificación de la información, según lo considere pertinente.

- El Comité MECI-CALIDAD debe analizar los incidentes de seguridad y activar el procedimiento requerido y contacto con las autoridades, cuando lo estime necesario.
- El Comité MECI-CALIDAD debe verificar el cumplimiento de las políticas aquí mencionadas.

Normas dirigidas a: OFICINA DE CONTROL INTERNO

- La Oficina de Control Interno debe planear y ejecutar las auditorías internas a las áreas que custodian la información de las bases de datos a fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos de la ley.
- La Oficina de Control Interno debe ejecutar revisiones totales o parciales de los procesos en las áreas que custodian las bases de datos, con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas.
- La Oficina de Control Interno debe informar a los jefes de las áreas responsables de la información de la base de datos, de los hallazgos de las auditorías.

Normas dirigidas a: AREA DE SISTEMAS

- El área de Sistemas debe asignar las funciones, roles y responsabilidades, a sus funcionarios para la operación y administración de las bases de datos personales que serán tratados por ENERGUAVIARE S.A. E.S.P. dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.

Normas dirigidas a: TODOS LOS USUARIOS

- Los funcionarios y personal provisto por terceras partes que realicen labores en o para ENERGUAVIARE S.A. E.S.P, tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información y de usuarios.

4. SEGURIDAD DEL PERSONAL

4.1 RELACIONADA CON LA VINCULACIÓN DE FUNCIONARIOS

ENERGUAVIARE S.A. E.S.P reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales y con el interés de contar con el personal mejor calificado que la vinculación de nuevos funcionarios se realice siguiendo un

proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las funciones y roles que deben desempeñar los funcionarios en sus cargos.

4.2. Normas relacionadas con la vinculación de funcionarios

Normas dirigidas a: GRUPO DE TALENTO HUMANO

- El Grupo de Talento Humano debe realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo en ENERGUAVIARE S.A.E.S.P, antes de su vinculación definitiva.
- El Grupo de Talento Humano debe certificar que los funcionarios de ENERGUAVIARE S.A. E.S.P. firmen un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.

Normas dirigidas a: SUPERVISORES DE CONTRATO, Y JEFES DE AREAS

- Cada Supervisor de Contrato y Jefes de Área deben verificar la existencia de Acuerdos y/o Cláusulas de Confidencialidad y de la documentación de Aceptación de Políticas para el personal provisto por terceras partes, antes de otorgar acceso a la información de ENERGUAVIARE S.A. E.S.P.

Normas dirigidas a: PERSONAL PROVISTOS POR TERCERAS PARTES

- El personal provisto por terceras partes que realicen labores en o para ENERGUAVIARE S.A. E.S.P debe firmar un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información, antes de que se les otorgue acceso a las instalaciones y a la parte operativa.
- El personal provisto por terceras partes, deben garantizar el cumplimiento de los Acuerdos y/o Cláusulas de Confidencialidad y aceptación de las Políticas de Seguridad de la Información de la empresa.

5. POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

5.1. DE RESPONSABILIDAD POR LOS ACTIVOS DE INFORMACION

ENERGUAVIARE S.A. E.S.P como propietario de la información física, así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

La información, archivos físicos, los sistemas, los servicios y los equipos (ej. Puesto de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) propiedad de ENERGUAVIARE S.A. E.S.P, son activos de la empresa y se proporcionan a los funcionarios y terceros autorizados, para cumplir con los propósitos del objeto misional de la empresa.

Toda la información sensible de ENERGUAVIARE S.A. E.S.P, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios establecidos en las políticas de protección de la información. Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

5.2. DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

ENERGUAVIARE S.A. E.S.P definirá los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad, y generará una guía de Clasificación de la Información para que los propietarios de la misma la cataloguen y determinen los controles requeridos para su protección.

Toda la información de ENERGUAVIARE S.A. E.S.P debe ser identificada, clasificada y documentada de acuerdo con las guías de Clasificación de la Información establecidas por el Comité MESI.

Una vez clasificada la información, ENERGUAVIARE S.A. E.S.P proporcionará los recursos necesarios para la aplicación de controles en busca de preservar la confidencialidad, integridad y disponibilidad de la misma, con el fin de promover el uso adecuado por parte de los funcionarios de la empresa y personal provisto por terceras partes que se encuentre involucrados en ella para la ejecución de sus actividades.

CALLE 8 # 29-55 CENTRO

LÍNEA DE SERVICIO AL CLIENTE

584 04 93 - CEL.: 318 782 7947

OFICINAS 584 04 93

SAN JOSÉ DEL GUAVIARE

6. POLÍTICAS DE CONTROL DE ACCESO

6.1. POLÍTICA DE ACCESO A REDES Y RECURSOS DE RED

El área de sistemas de ENERGUAVIARE S.A. E.S.P, como responsables de las redes de datos y los recursos de red de la empresa, debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

6.1.1. Normas de acceso a redes y recursos de red

Normas dirigidas a: AREA DE SISTEMAS

- El área de sistemas debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de ENERGUAVIARE S.A. E.S.P
- El área de sistemas debe asegurar que las redes inalámbricas de la empresa cuenten con métodos de autenticación que evite accesos no autorizados.
- El área de sistemas debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red de ENERGUAVIARE S.A. E.S.P, así como velar por la aceptación de las responsabilidades de dichos terceros. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.

7. POLÍTICA DE ADMINISTRACIÓN DE ACCESO DE USUARIOS

ENERGUAVIARE S.A. E.S. P establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la empresa. Así mismo, velará porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de

7.1. NORMAS DE ADMINISTRACIÓN DE ACCESO DE USUARIOS

Normas dirigidas a: AREA DE SISTEMAS

- El área de sistemas debe establecer un procedimiento formal para la administración de los usuarios en las redes, los recursos tecnológicos y sistemas de información de la empresa que contengan base de datos tratadas por ENERGUAVIARE S.A.E.S.P.
- El área de sistemas, previa solicitud de los jefes inmediatos de los solicitantes de las cuentas de usuario debe crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes, los recursos tecnológicos y los sistemas de información administrados, que contengan base de datos tratadas por ENERGUAVIARE S.A. E.S.P. acorde con el procedimiento establecido.
- El área de sistemas, en conjunto comité MESI, debe definir lineamientos para la configuración de contraseñas que aplicaran sobre la plataforma tecnológica, los servicios de red, los sistemas de información y las bases de datos tratadas por ENERGUAVIARE S.A. E.S.P dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.
- El área de sistemas debe establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los funcionarios se desvinculan, toman licencias, vacaciones, o sean trasladados o cambiados del cargo.

Normas dirigidas a: JEFES DE AREAS

Los Jefes de áreas deben solicitar la creación, modificación, bloqueo y eliminación de cuentas de usuario, para los funcionarios que laboran en sus áreas, acogiendo al procedimiento establecido para tal fin, en especial en aquellas áreas que custodien bases de datos tratados por ENERGUAVIARE S.A. E.S.P.

7.2. DE LA RESPONSABILIDADES DE ACCESO DE LOS USUARIOS

Los usuarios de los recursos tecnológicos y los sistemas de información de ENERGUAVIARE S.A. E.S.P. realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

7.2.1. NORMAS DE RESPONSABILIDADES DE ACCESO DE LOS USUARIOS

Normas dirigidas a: TODOS LOS USUARIOS

- Los usuarios de la plataforma tecnológica, los servicios de red y los sistemas de información y la base de datos personales de ENERGUAVIARE S.A. E.S.P. deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.
- Los funcionarios no deben compartir sus cuentas de usuario y contraseñas con otros funcionarios o con personal provisto por terceras partes.
- Los funcionarios y personal provisto por terceras partes que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información de ENERGUAVIARE S.A. E.S.P. deben acogerse a lineamientos para la configuración de contraseñas implantadas por la empresa en especial aquellos funcionarios que se encuentren custodiando las bases de datos tratadas por ENERGUAVIARE S.A. E.S.P.

7.3 CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS

La Gerencia y los Jefes de áreas como propietarias de los sistemas de información y aplicativos que apoyan los procesos en las áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

El área de sistemas, como responsable de la administración de dichos sistemas de información y aplicativos, propenderá para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, velará porque funcionarios, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los

CALLE 9 # 23-55 CENTRO

LÍNEA DE SERVICIO AL CLIENTE

584 04 93 - CEL.: 318 782 7947

OFICINAS 584 04 93

SAN JOSÉ DEL GUAVIARE

7.3.1. NORMAS DE CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS

Normas dirigidas a: JEFES DE AREAS

Los jefes de área deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiéndose los procedimientos establecidos.

Normas dirigidas a: AREA DE SISTEMAS

- El área de sistemas debe establecer un procedimiento para la asignación de accesos a los sistemas y aplicativos de ENERGUAVIARE S.A. E.S.P.
- El área de sistemas debe asegurar, mediante los controles necesarios, que los usuarios utilicen diferentes perfiles para el desarrollo de sus actividades, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.
- El área de sistemas debe establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los funcionarios internos o externos, posean acceso limitado y controlado a los datos y archivos.
- El área de sistemas debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.
- El área de sistemas debe monitorear periódicamente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos e informar cualquier irregularidad.

8. POLÍTICAS DE SEGURIDAD FISICA Y MEDIO AMBIENTAL

ENERGUAVIARE S.A. E.S.P. proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus sedes. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren en los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

8.1. NORMAS DE ÁREAS SEGURAS

Normas dirigidas a: AREA DE SISTEMAS

- El área de sistemas debe velar porque los recursos de la plataforma tecnológica de ENERGUAVIARE S.A. E.S.P. ubicados en su área se encuentran protegidos contra fallas o interrupciones eléctricas.
- El área de sistemas debe certificar que en su área y los centros de cableados que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
- El área de sistemas debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

Normas dirigidas a: GERENCIA Y JEFES DE AREAS

- Los jefes de área deben autorizar cualquier ingreso temporal a sus áreas, que conlleve la utilización de la información física o que se encuentren en los equipos bajo su custodia o responsabilidad, evaluando la pertinencia del ingreso; así mismo, deben delegar en personal del área el registro y supervisión de cada ingreso a sus áreas.

Normas dirigidas a: TODOS LOS USUARIOS

- Los ingresos y egresos de personal a las instalaciones de ENERGUAVIARE S.A. E.S.P. deben ser registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.
- Los funcionarios deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de ENERGUAVIARE S.A. E.S.P.; en caso de pérdida o daño deben reportarlo a la mayor brevedad posible y solicitar su reposición de

- Los funcionarios de ENERGUAVIARE S.A. E.S.P y el personal provisto por terceras partes no deben intentar ingresar a áreas a las cuales no tengan autorización.

8.2. NORMAS DE SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES

Normas dirigidas a: AREA DE SISTEMAS

- El área de sistemas debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de ENERGUAVIARE S.A. E.S.P
- El área de sistemas debe realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la empresa con una periodicidad mínima de dos (2) en cada una de la áreas y sedes de ENERGUAVIARE S.A. E.S.P.
- El área de sistemas debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios de la empresa
- El área de sistemas debe establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos de la empresa y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.
- El área de sistemas debe aislar los equipos de áreas sensibles, como la de Tesorería para proteger su acceso de los demás funcionarios de la red de la empresa.
- El área de sistemas debe establecer, generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios de la empresa, ya sea cuando son dados de baja o cambian de usuario.

Normas dirigidas a: OFICINA DE CONTROL INTERNO

- La Oficina de Control Interno tiene la responsabilidad de incluir dentro del plan anual de auditorías la verificación aleatoria a los equipos de cómputo de todas las dependencias y puntos de atención de ENERGUAVIARE S.A. E.S.P
- La Oficina de Control Interno debe evaluar y analizar los informes de verificación de equipos de cómputo de las diferentes áreas de la empresa, en particular de las áreas sensibles.

Normas dirigidas a: TODOS LOS USUARIOS

- El área de sistemas es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos (hardware o software); por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de la empresa.
- Cuando se presente una falla o problema de hardware o software en un puesto de trabajo u otro recurso tecnológico propiedad de ENERGUAVIARE S.A. E.S.P el funcionario responsable debe informar al área de sistemas con el fin de realizar una asistencia adecuada. El funcionario no debe intentar solucionar el problema.
- La instalación, reparación o retiro de cualquier componente de hardware o software de los equipos de cómputo y demás recursos tecnológicos de la empresa, solo puede ser realizado por los funcionarios del área de sistemas o personal de terceras partes autorizado por dicha área.
- En caso de pérdida o robo de un equipo de cómputo de ENERGUAVIARE S.A. E.S.P se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.
- Los funcionarios de la empresa y el personal provisto por terceras partes deben asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

9. POLITICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

ENERGUAVIARE S.A. E.S.P. proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso. Además, proporcionará los mecanismos para generar cultura de seguridad entre sus funcionarios y personal provisto por terceras partes frente a los ataques de software malicioso.

9.1. NORMAS DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

Normas dirigidas a: AREA DE SISTEMAS

- El área de sistemas debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de ENERGUAVIARE S.A. E.S.P y los servicios que se ejecutan en la misma.
- El área de sistemas debe asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así mismo su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.
- El área de sistemas debe certificar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.
- El área de sistemas, a través de sus funcionarios, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.
- El área de sistemas, a través de sus funcionarios, debe certificar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.

Normas dirigidas a: TODOS LOS USUARIOS

- Los usuarios de recursos tecnológicos no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por el área de sistemas; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.
- Los usuarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.
- Los usuarios deben asegurarse de que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.
- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar al área de sistemas, para que tome las medidas de control correspondientes.

10. POLITICA DE CONTROL AL SOFTWARE OPERATIVO

ENERGUAVIARE S.A. E.S.P, a través del área de sistemas, designará responsables y establecerá procedimientos para controlar la instalación de software operativo, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo es actualizado.

10.1 Normas de control al software operativo

Normas dirigidas a: AREA DE SISTEMAS

- El área de sistemas debe establecer responsabilidades y procedimientos para controlar la instalación del software operativo, que interactúen con el procedimiento de control de cambios existente en la empresa

- El área de sistemas debe asegurarse que el software operativo instalado en la plataforma tecnológica del ENERGUAVIARE S.A. E.S.P cuenta con soporte de los proveedores.
- El área de sistemas debe conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.
- El área de sistemas debe validar los riesgos que genera la migración hacia nuevas versiones del software operativo. Se debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.
- El área de sistemas debe establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo de ENERGUAVIARE S.A. E.S.P.

12. POLÍTICA DE USO DEL CORREO ELECTRONICO

ENERGUAVIARE S.A. E.S.P, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre funcionarios y terceras partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

12.1. NORMAS DE USO DEL CORREO ELECTRÓNICO

Normas dirigidas a: AREA DE SISTEMAS

- El área de sistemas debe generar y divulgar un procedimiento para la administración de cuentas de correo electrónico.
- El área de sistemas debe diseñar y divulgar las directrices técnicas para el uso de los servicios de correo electrónico.

El área de sistemas debe proveer un ambiente seguro y controlado para el uso de la plataforma de correo electrónico.

CALLE 8 # 23-55 CENTRO
LÍNEA DE SERVIDOR AL CLIENTE
584 04 93 - CEL.: 318 782 7947
OFICINAS 584 04 93
SAN JOSÉ DEL GUAVIARE

- El área de sistemas debe establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.
- El área de sistemas debe generar campañas para concientizar tanto a los funcionarios internos, como al personal provisto por terceras partes, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio del correo electrónico.

Normas dirigidas a: TODOS LOS USUARIOS

- La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario de la empresa o provisto por un tercero, en ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.
- Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional de ENERGUAVIARE S.A. E.S.P.
- El correo institucional no podrá ser utilizado para actividades personales.
- Los mensajes y la información contenida en los buzones de correo son propiedad de ENERGUAVIARE S.A. E.S.P y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
- Los usuarios de correo electrónico institucional tienen prohibido el envío de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los funcionarios de la empresa, el personal provisto por terceras partes y los usuarios suscriptores del servicio.
- No es permitido el envío de archivos que contengan extensiones ejecutables, en ninguna circunstancia.
- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por ENERGUAVIARE S.A. E.S.P y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

13. POLÍTICA DE USO ADECUADO DE INTERNET

ENERGUAVIARE S.A. E.S.P. consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los funcionarios que así lo requieran para el desarrollo de sus actividades diarias en la empresa

13.1 NORMAS DE USO ADECUADO DE INTERNET

Normas dirigidas a: AREA DE SISTEMAS

- El área de sistemas debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.
- El área de sistemas debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
- El área de sistemas debe monitorear continuamente el canal o canales del servicio de Internet.
- El área de sistemas debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.
- El área de sistemas debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.

Normas dirigidas a: TODOS LOS USUARIOS

- Los usuarios del servicio de Internet de ENERGUAVIARE S.A. E.S.P. deben hacer uso de este en relación con las actividades laborales que así lo requieran.

- Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en los equipos de cómputo de trabajo o dispositivos móviles asignados para el desempeño de sus labores.
- No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.
- Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN, Yahoo, Sype, Net2phome y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del objeto misional de ENERGUAVIARE S.A. E.S.P.
- No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.
- La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el jefe respectivo y la Dirección de Tecnología, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.
- No está permitido el intercambio no autorizado de información de propiedad de ENERGUAVIARE S.A. E.S.P, de sus suscriptores usuarios y/o de sus funcionarios, con terceros.

14. POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD

14.1 EL REPORTE Y TRATAMIENTO DE INCIDENTES DE SEGURIDAD

ENERGUAVIARE S.A. E.S.P. promoverá entre los funcionarios y personal provisto por terceras partes, el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información,

como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las bases de datos tratados por ENERGUAVIARE S.A. E.S.P.

La gerencia o a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

14.2 NORMAS PARA EL REPORTE Y TRATAMIENTO DE INCIDENTES DE SEGURIDAD

Normas dirigidas a: JEFES DE AREAS

- Los Jefes de Áreas deberán informar comité MECI-CALIDAD, los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

Normas dirigidas a: COMITÉ MECI-CALIDAD

- Comité MECI-CALIDAD debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.
- Comité MECI-CALIDAD debe evaluar todos los incidentes de seguridad de acuerdo con sus circunstancias particulares
- Comité MECI-CALIDAD debe designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su reincidencia.
- Comité MECI-CALIDAD debe, con el apoyo del Área de sistemas y la Secretaría General y Jurídica crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.
- Comité MECI-CALIDAD debe analizar los incidentes y las consecuencias o perjuicios ocasionados y decidirá el procedimiento a seguir y el contacto con las autoridades, cuando lo estime necesario.

CALLE 8 # 23-55 CENTRO
LÍNEA DE SERVICIO AL CLIENTE
584 04 93 - CEL.: 318 782 7947
OFICINAS 584 04 93
SAN JOSÉ DEL GUAVIARE

Normas dirigidas a: TODOS LOS USUARIOS

- Es responsabilidad de los funcionarios de ENERGUAVIARE S.A. E.S.P y del personal provisto por terceras partes reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible.
- En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada, sensible o restringida, los funcionarios deben notificarlo a su jefe correspondiente para que este lo ponga en conocimiento del comité MECI-CALIDAD para que se registre y se le dé el trámite necesario.

15. POLÍTICAS DE CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES

ENERGUAVIARE S.A. E.S.P velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a las bases de datos tratados por ENERGUAVIARE S.A. E.S.P, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

15.1. NORMAS DE CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES

Normas dirigidas a: SECRETARIA GENERAL Y JURIDICA

- La Secretaria General y Jurídica debe identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a ENERGUAVIARE S.A. E.S.P relacionados con seguridad de la información y de usuarios.

Normas dirigidas a: AREA DE SISTEMAS

- El área de sistemas debe certificar que todo el software que se ejecuta en la empresa esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.
- El área de sistemas debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en los puestos de trabajo para el desarrollo

de las actividades laborales, así como verificar periódicamente que el software instalado en dichas puestos de trabajo corresponda únicamente al permitido.

Normas dirigidas a: TODOS LOS USUARIOS

- Los usuarios no deben instalar software o sistemas de información en sus equipos de trabajo o equipos móviles suministrados para el desarrollo de sus actividades.
- Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación sin la autorización de un propietario de los derechos de autor y, su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse número de copias bajo una licencia otorgada.

16.1. POLÍTICA DE PRIVACIDAD Y PROTECCION DE DATOS PERSONALES

En cumplimiento de la de Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales, ENERGUAVIARE S.A. E.S.P, propenderá por la protección de los datos personales de sus funcionarios, usuarios, proveedores y demás terceros de los cuales reciba y administre información.

Se establecerán los términos, condiciones y finalidades para las cuales el ENERGUAVIARE S.A. E.S.P, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que en algún momento, por razones del servicio que presta la empresa, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, ENERGUAVIARE S.A. E.S.P exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales.

Así mismo, buscará proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información que la empresa conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la empresa y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

16.1. NORMAS DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

ÁREAS QUE PROCESAN DATOS PERSONALES

CALLE # 23-55 CENTRO
LINEA DE SERVICIO AL CLIENTE
584 04 93 - CEL.: 318 782 7947
OFICINAS 584 04 93
SAN JOSÉ DEL GUAVIARE

- Las áreas que procesan datos personales de beneficiarios, suscriptores usuarios, funcionarios, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de ENERGUAVIARE S.A. E.S.P.
- Las áreas que procesan datos personales de beneficiarios, suscriptores, funcionarios, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.
- Las áreas que procesan datos personales de beneficiarios, funcionarios, suscriptores usuarios, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.
- Las áreas que procesan datos personales de beneficiarios, funcionarios, suscriptores usuarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos de estos para el intercambio datos con los terceros delegados para el tratamiento de dichos datos personales.
- Las áreas que procesan datos personales de beneficiarios, usuarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, usuarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.

Normas dirigidas a: COMITÉ MECI--CALIDAD

Comité MECI-CALIDAD debe establecer los controles (claves) para el tratamiento y protección de los datos personales de los beneficiarios, funcionarios, suscriptores usuarios, proveedores y demás terceros del ENERGUAVIARE S.A. E.S.P de los cuales reciban y administre información.

Normas dirigidas a: AREA DE SISTEMAS

El área de sistemas debe implantar los controles necesarios para proteger la información personal de los beneficiarios, funcionarios, suscriptores usuarios,

CALLE 8 # 23-55 CENTRO
LÍNEA DE SERVICIO AL CLIENTE
584 04 93 - CEL.: 318 782 7947
OFICINAS 584 04 93
SAN JOSÉ DEL GUAVIARE

proveedores u otras terceras partes, almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida, una vez esos controles hayan sido establecidos por el comité **MECI-CALIDAD**.

Normas dirigidas a: TODOS LOS USUARIOS

- Los usuarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la empresa o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.
- Es deber de los usuarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.

Normas dirigidas a: USUARIOS DEL PORTAL O LA PAGINA DE ENERGUAVIARE S. A. E.S.P

Los usuarios de los portales o página web de ENERGUAVIARE deben asumir la responsabilidad individual sobre la clave de acceso a dichos portales que les es suministrada; así mismo, deben cambiar de manera periódica esta clave de acceso.

Los usuarios de los portales de ENERGUAVIARE deben contar con controles de seguridad en sus equipos de cómputo o redes privadas para acceder a los portales del ENERGUAVIARE S.A. E.S.P

Los usuarios de los portales de ENERGUAVIARE S.A. E.SP. deben aceptar el suministro de datos personales que pueda hacer la empresa a los terceros delegados para el tratamiento de datos personales, a entidades judiciales y demás entes del Estado que, en ejercicio de sus funciones, solicitan esta información; de igual manera, deben aceptar que pueden ser objeto de procesos de auditoria interna o externa.

16.2 MEDIDAS DE SEGURIDAD BASES DE DATOS

ENERGUAVIARE S.A. E.S.P, con el fin de cumplir con el principio de seguridad consagrado en el artículo 4 literal g) de la LEPD, ha implementado medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

CALLE 8 # 23-55 CENTRO

LÍNEA DE SERVICIO AL CLIENTE

584 04 93 - CEL.: 318 782 7947

OFICINAS 584 04 93

SAN JOSÉ DEL GUAVIARE

Por otra parte, ENERGUAVIARE S.A. E.S.P., implementa las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de la información en el tratamiento de los datos personales.

A continuación, se exponen las medidas de seguridad implantadas por ENERGUAVIARE S.A. E.S.P.,

**MEDIDAS DE SEGURIDAD COMUNES PARA TODO TIPO DE DATOS
(Públicos, semiprivados, privados, sensibles)**

BASES DE DATOS (AUTOMATIZADAS, NO AUTOMATIZADAS)

1. Evitar el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruido.
2. Restringir la entrada al lugar donde sean almacenados los soportes de las bases de datos.
3. Tener autorización del responsable para la salida de documentos o soportes por medio físico o electrónico.
4. Realizar un Inventario de los soportes físicos del base de datos.
5. El Acceso de usuarios a los datos debe ser limitado solamente los necesarios para el desarrollo de sus funciones.
6. Realizar la lista de usuarios y accesos autorizados a las bases de datos
7. Realizar un registro de incidencias: tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras, gestionarlas y notificarlas.
8. Definir las funciones y obligaciones de los usuarios con acceso a los datos.
9. Definir de las funciones de control y autorizaciones delegadas por ENERGUAVIARE S.A. E.S.P
10. Dar a conocer las normas de protección de datos entre el personal de la empresa y las consecuencias del incumplimiento de las mismas
11. Realizar un Auditoría ordinaria cada dos meses por parte de la Oficina de Control Interno.
12. Realizar una auditoría extraordinaria por modificaciones sustanciales en los sistemas de información.
13. Realizar Informe de detección de deficiencias y propuesta de correcciones.
14. Designación de uno o varios responsables de seguridad de la información.

CALLE 8 # 23-55 CENTRO

LÍNEA DE SERVICIO AL CLIENTE

584 04 93 - CEL.: 318 782 7947

OFICINAS 584 04 93

SAN JOSÉ DEL GUAVIARE

15. Controles periódicos de cumplimiento de las políticas de tratamiento de datos personales, de las políticas de Seguridad de la información y del Protocolo de atención a los titulares de los datos.

BASES DE DATOS NO AUTOMATIZADAS

1. El Archivo de la documentación debe ser siguiendo procedimientos que garanticen una correcta conservación, localización y consulta y permitan el ejercicio de los derechos de los Titulares.
2. El almacenamiento deber contar con mecanismos que impidan el acceso a personas no autorizadas, no todos los funcionarios pueden tener acceso a la documentación.

BASES DE DATOS AUTOMATIZADAS

1. Para acceder a la base de datos almacenada en los sistemas de información el usuario debe tener su Identificación personalizada y verificación de su autorización.
2. Se debe contar con una red segura para acceder a las bases de datos
3. Se deber crear mecanismos de identificación y autenticación; como son asignación de contraseñas, caducidad de estas y almacenamiento cifrado.

MEDIDAS DE SEGURIDAD PARA DATOS SENSIBLES SEGÚN EL TIPO DE BASES DE DATOS

BASES DE DATOS NO AUTOMATIZADAS

1. El acceso al base de datos sensibles es solo para personal autorizado.
2. Se deberá utilizar un mecanismo de identificación al momento del acceso que garantice que es autorizado.
3. Llevar el registro de accesos de los usuarios no autorizados
4. Los soportes de los datos sensibles deben ser almacenado en Archiveros, armarios u otros ubicados en áreas de acceso protegidas con llaves u otras medidas.
5. La copia o reproducción de algún soporte solo por usuarios autorizados.
6. Se debe medidas que impidan el acceso o manipulación de documentos soportes de la base de datos sensibles.

BASES DE DATOS AUTOMATIZADAS

LINEA DE SERVICIO AL CLIENTE

584 04 93 - CEL.: 318 782 7947

OFICINAS 584 04 93

SAN JOSÉ DEL GUAVIARE

1. Los documentos deben contar con un sistema de etiquetado confidencial.
2. Cifrado de dispositivos portátiles cuando se encuentren fuera.
3. Realizar el registro de accesos: usuario, hora, base de datos a la que accede, tipo de acceso, registro al que accede.
4. Realizar un control del registro de accesos por el responsable de seguridad y un Informe mensual.
5. Esta información se debe conservar como mínimo dos años.
6. Contar con la seguridad para la transmisión de datos mediante redes electrónicas cifradas.

16.3. SEGURIDAD DE NAVEGACIÓN

El sistema de navegación y el software necesario para el funcionamiento de la página Web de ENERGUAVIARE S.A. E.S.P. recoge algunos datos personales, cuya transmisión se haya implícita en el uso los protocolos de comunicación de Internet.

Por su propia naturaleza, la información recogida podría permitir la identificación de usuarios a través de su asociación con datos de terceros, aunque no se obtenga para ese fin. En esta categoría de datos se encuentran, la dirección IP o el nombre de dominio del equipo utilizado por el usuario para acceder a la página web, la dirección URL, la fecha y hora y otros parámetros relativos al sistema operativo del usuario.

Estos datos se utilizan con la finalidad exclusiva de obtener información estadística anónima sobre el uso de la página Web o controlar su correcto funcionamiento técnico, y se cancelan inmediatamente después de ser verificados.

COOKIES O WEB BUGS

Este sitio Web no utiliza cookies o Web bugs para recabar datos personales del usuario, sino que su utilización se limita a facilitar al usuario el acceso a la página Web de ENERGUAVIARE S.A. E.S.P. El uso de cookies de sesión, no memorizadas de forma permanente en el equipo del usuario y que desaparecen cuando cierra el navegador, únicamente se limitan a recoger información técnica para identificar la sesión con la finalidad de facilitar el acceso seguro y eficiente de la página Web. Si no desea permitir el uso de cookies puede rechazarlas o eliminar las ya existentes configurando su navegador, e inhabilitando el código Java Script del navegador en la configuración de seguridad.

CALLE 8 # 23-55 CENTRO

LÍNEA DE SERVICIO AL CLIENTE / O ACTUALIZACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA
INFORMACIÓN Y DE SERVIDORES
584 04 93 - CEL. 318 782 7947

OFICINAS 584 04 93

SAN JOSÉ DEL GUAVIARE

Cualquier cambio sustancial en las políticas de seguridad de la información y de usuarios, se comunicará de forma oportuna de los medios habituales de contacto y/o a través de: correo electrónico, avisos en la página web: www.energuaviere.com o en las sedes físicas de ENERGUAVIARE S.A. E.S.P.

La presente política de protección rige a partir del 17 de Abril de (2018)



MARICELA LOZANO RODRÍGUEZ
Presidenta Junta Directiva



FERNANDO SANTAMARIA LUNA
Secretario Ad hoc

COPIA CONTROLADA

CALLE 8 # 23-55 CENTRO
LINEA DE SERVICIO AL CLIENTE
584 04 93 - CEL.: 318 782 7947
OFICINAS 584 04 93
SAN JOSÉ DEL GUAVIARE