# POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y MANEJO DE DATOS PERSONALES

## COMITÉ TÉCNICO MULTIDISCIPLINARIO PARA LA PROTECCIÓN DE DATOS PERSONALES

Revisado el 31 Julio 2018

| Sobre este documento | |
|---|---|
| **Versión:** | 6.0.0 |
| **Fecha de Publicación:** | 19/09/2018 |
| **Propósito:** | Establecer las políticas, prácticas y lineamientos de seguridad para la empresa Energéticos en Red Electrónica, S.A. de C.V. |
| **Audiencia:** | Toda la empresa, así como a las personas que directa o indirectamente, prestan sus servicios profesionales dentro de la misma. |

| Control de Cambios | | |
|---|---|---|
| **Fecha** | **Autor** | **Descripción del cambio** |
| 31 de Julio del 2018 | Comité Técnico | Modificación en la sección de Sanciones puntos, 1,2,3 y 4 |
| 23 de Abril del 2018 | Comité Técnico | Revisión sin modificación |
| 27 de octubre del 2017 | Comité Técnico | Modificación en Definiciones, se agrega el Comité técnico multidisciplinario y punto 1.9 |
| 23 de octubre del 2017 | Comité Técnico | Modificación en punto 1.5.4, 1.6.4 y 6 |
| 18 de mayo del 2017 | Comité Técnico | Actualización de Sanciones |
| 7 de noviembre del 2016 | Comité Técnico | Revisión sin modificación |
| 30 de mayo del 2016 | Comité Técnico | Actualización en punto 1.9 y 2.3 |
| 10 de noviembre 2015 | Comité Técnico | Revisión sin modificación |
| 11 de mayo 2015 | Comité Técnico | Revisión sin modificación |
| 5 de Agosto 2014 | Comité Técnico | Revisión sin modificación |
| 9 de Septiembre 2013 | Comité Técnico | Revisión sin modificación |
| 8 de Agosto 2012 | Comité Técnico | Creación del documento |

**POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y MANEJO DE DATOS PERSONALES**

Proteger los recursos de información, tales como información confidencial de la empresa y datos personales de los empleados, clientes y demás titulares de los que trate datos personales **ENERGÉTICOS EN RED ELECTRÓNICA, S.A. DE C.V.** y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de los principios de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información, de acuerdo a los requerimientos de la LFPDPPP y su Reglamento, así como de la legislación aplicable en materia de seguridad y privacidad de la información.

En un esfuerzo para dar un mayor sustento y en apego a las reformas a la ya citadas leyes, la dirección general manifiesta un compromiso total para el cabal cumplimiento de la ley, normas regulatorias, así como de estas mismas políticas de seguridad de manejo de datos personales.

**Representante Legal**

**Jorge Humberto Salcido Salcido**

**DIRECTIVAS**

- Asegurar la implementación de las medidas de seguridad comprendidas para los datos personales e información confidencial, identificando los recursos y su plena realización.
- Mantener la Política General de Seguridad de la Información y Manejo de Datos Personales actualizada, a efectos de asegurar su vigencia y nivel de eficacia.
- Determinar los lineamientos de seguridad de la información de los terceros autorizados, proveedores y en general todos los autorizados que tengan acceso a información.

**OBJETIVO:**

Establecer las políticas, prácticas y lineamientos de seguridad para la empresa **Energéticos en Red Electrónica, S.A. de C.V**.

Así como hacer saber a los integrantes de la empresa, las políticas de nos rigen en el manejo de información, tales como información confidencial de la empresa y datos personales de los empleados, clientes y demás titulares de los que trate datos personales **Energéticos en Red Electrónica, S.A. de C.V.**

**ALCANCE:**

Aplica a toda la empresa, así como a las personas que directa o indirectamente, prestan sus servicios profesionales dentro de la misma, y a toda la información obtenida, creada, procesada, almacenada o intercambiada.

Las prácticas y lineamientos de seguridad de la información de esta política están orientadas a proteger en todo momento y circunstancia, los datos e información contra los riesgos de robo, divulgación, acceso no autorizado, modificación, pérdida, interrupción o mal uso, producidas en forma intencional o accidental.

**El no cumplimiento de estas cláusulas será sujeto a sanción según la gravedad y características de la falta, misma que será delimitado por el Comité Técnico, Recursos Humanos y el Jefe Inmediato del involucrado.**

**DEFINICIONES**

1. **Autorización**: consentimiento que de manera previa, expresa e informada emite el titular de algún dato personal para que la compañía lleve a cabo el tratamiento de sus datos personales.
2. **Titular:** persona natural cuyos datos son objeto de tratamiento por parte de la compañía.
3. **Dato personal:** información que está vinculada a una persona. Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que Política Manejo de Información y Datos Personales puedan asociarse con una persona Física o Moral. Los datos personales pueden ser públicos, semiprivados o privados.
4. **Tratamiento:** cualquier operación o conjunto de operaciones sobre datos personales dentro de las cuales se puede incluir su recolección, almacenamiento, uso, circulación o supresión.
5. **Encargado del tratamiento:** persona Física o Moral, pública o privada, que por sí misma o en asocio con otros, realiza algún tratamiento sobre datos personales por cuenta del responsable del tratamiento.
6. **Responsable del tratamiento:** persona Física o Moral, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.
7. **Dato sensible:** aquellos relacionados con el origen racial o étnico, la pertenencia a sindicatos, organizaciones sociales o de derechos humanos, convicciones políticas, religiosas, de la vida sexual, biométricos o datos de la salud. Esta información podrá no ser otorgada por el Titular de estos datos.
8. **Aviso de privacidad:** documento físico, electrónico generado por el Responsable del tratamiento que es puesto a disposición del titular con la información relativa a la existencia de las políticas de tratamiento de información que le serán aplicables, la Política Manejo de Información y Datos Personales forma de acceder a las mismas y las características del Tratamiento que se pretende dar a los datos personales.
9. **Comité técnico multidisciplinario:** Se establece con la finalidad de guardar la confidencialidad, permitir el acceso, realizar la corrección,

implementar procesos, seguridad, custodia, cuidado, tratamiento y posterior cancelación de la información que maneja la empresa en materia de datos personales. Revisar y ajustar las políticas de seguridad de datos personales, los miembros del comité quedaran estipulados en el "Acta del comité técnico multidisciplinario para la publicación de políticas de seguridad de datos".

## 1. POLÍTICAS DE SISTEMAS

### 1.1 RECURSOS INFORMÁTICOS Y DE TELEFONÍA

1.1.1 Los recursos informáticos y de telefonía podrán ser utilizados sólo por el personal de la empresa y para los fines propios de sus actividades dentro de la empresa. Los servicios informáticos se brindarán en función de los recursos disponibles y las prioridades establecidas por Dirección General.

1.1.2 Todo proyecto u orden de servicio de cualquier índole que requiera o involucre el uso de recursos informáticos y/o telefonía, deberán ser solicitados por medio del sistema Helpdesk en tiempo y forma, y proporcionando los datos necesarios para su atención, tales como, descripción del problema, ubicación, usuario y para poder determinar la prioridad de su ejecución.

1.1.3 Nadie podrá adquirir, desarrollar, implementar o instalar sistemas de información en los equipos de cómputo, telefonía o cualquier otro dispositivo asignado por la empresa, sin la previa autorización y supervisión tanto del Jefe Inmediato y del Departamento de Sistemas. Si este caso sucediera, no es responsabilidad del departamento dar soporte, mantenimiento o legalizar las licencias, una vez que de manera arbitraria y sin autorización se esté utilizando, más se deberá de supervisar que no afecte el funcionamiento o interfiera con los programas y sistemas, a manera de garantizar que aun cuando no fue del todo autorizado, se tenga un control de sus funciones y actividades.

### 1.2 PROTECCIÓN Y SEGURIDAD DE LA INFORMACIÓN

1.2.1 El área de servidores del Departamento de Sistemas se considera área restringida dentro de la empresa y sólo el personal autorizado tiene acceso al mismo.

1.2.2 Los usuarios de los sistemas de información de la empresa serán los responsables del contenido y actualización permanente de los datos.

1.2.3 Las personas que tengan bajo su responsabilidad información confidencial de personas físicas que trate la empresa, deben seguir procedimientos adecuados para protegerla de acuerdo a la LFPDPPP y la Ley de la Propiedad Industrial, y por lo tanto serán responsables de las consecuencias por la ausencia de esta protección; esto aplicará también a la información confidencial de la empresa, a la cual deberá dársele el mismo tratamiento confidencial.

1.2.4 En caso de necesitarlo, es responsabilidad del usuario solicitar capacitación necesaria para el manejo de herramientas informáticas relacionadas con sus funciones de manera que se reduzca el riesgo de daño o un mal manejo de los equipos informáticos.

1.2.5 Toda la información obtenida y desarrollada en base a las funciones de los usuarios se guardará en la carpeta *Mis Documentos,* de manera que los datos puedan identificarse rápidamente y en una sola ubicación lógica para facilitar el proceso de recuperación o respaldo de archivos.

1.2.6 La ingesta de alimentos y/o bebidas mientras se operan los equipos de computación y comunicación está prohibida.

1.2.7 La colocación de cualquier objeto sobre los equipos computacionales, la adhesión de calcomanías, la ubicación de obstáculos o cosas que obstruyan los orificios de ventilación (ubicados en la fuente y parte lateral de los CPU y monitores) están prohibidas.

1.2.8 La estación de trabajo debe estar limpia de polvo y libre de humedad para disminuir daños en los equipos.

1.2.9 Los cables de conexión de los equipos computacionales a la red eléctrica, a la red de datos y el cable de conexión telefónica deben protegerse. El usuario cuidará que estos cables no sean pisados, aplastados por personas, muebles o cualquier otro objeto.

1.2.10 El Departamento de Sistemas velará porque se establezcan sistemas de protección, sistemas de detección de ataques informáticos y la creación de procedimientos de recuperación de los sistemas en caso de ocurrir incidentes.

1.2.11 La reubicación o movimiento de equipos de cómputo y telefonía deberán ser notificados con 48 horas de anticipación.

1.2.12 La instalación de dispositivos y el retiro de sellos, son atributos del personal del Departamento de Sistemas.

1.2.13 Está prohibido que los usuarios abran o desarmen los equipos de cómputo y de comunicación asignados.

1.2.14Los sistemas desarrollados por personal, interno o externo, que sea parte de la Dirección de Sistemas, o sea coordinado por ésta, son propiedad intelectual de la empresa.

1.2.15La Dirección Genera realizará acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática para usuarios.

1.2.16La Dirección de Sistemas podrá implementar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en la Política de Seguridad del Personal.

1.2.17Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por la Dirección de Sistemas.

1.2.18Está prohibido realizar pruebas de controles de los diferentes elementos de Tecnología de la Información. Ninguna persona puede probar o intentar comprometer los controles internos a menos de contar con la aprobación de la Dirección de Sistemas.

1.2.19Ningún usuario podrá probar o intentar probar fallas de la Seguridad Informática identificadas o conocidas, a menos que estas pruebas sean controladas y aprobadas por la Dirección de Sistemas.

## 1.3 MANEJO DE LA INFORMACIÓN EN USB Y MEDIOS REMOVIBLES.

1.3.1 No se admite uso de USB o cualquier otro medio de almacenamiento externo (tarjetas de memoria, discos duros externos, cámaras digitales y celulares) en los equipos de cómputo de la empresa.

- El uso es permitido solo en caso de que el usuario lo requiera y haya sido autorizado por el jefe inmediato
- Los dispositivos de almacenamiento (USB, memorias) solo podrán ser utilizados en casos necesarios y para uso interno. Se deberá evitar sacarlos fuera de las

instalaciones de la empresa salvo previa autorización del Departamento de Sistemas, así como con la autorización directa y por escrito del jefe inmediato del empleado.

- Los dispositivos entregados deberán ser registrados en el registro de medios removibles de alojamiento con fecha de entrega y deberá ser retirado a la baja del empleado.

1.3.2 El evitar fugas o pérdidas de la información almacenada dentro de los medios removibles utilizados dentro de la empresa es responsabilidad del usuario.

## 1.4 MANEJO DE 3G-USB (INTERNET MOVIL)

1.4.1 Para su uso dentro de la empresa, todos los dispositivos 3G-USB para conexión de internet móvil deberán ser registrados y el usuario deberá firmar una carta responsiva responsabilizándose de su manejo y resguardo.

1.4.2 El uso de 3G-USB personal está prohibido.

1.4.3 El acceso a internet provisto a los usuarios del es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.

1.4.4 La asignación del servicio de internet, deberá solicitarse por escrito al Departamento de Sistemas, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del titular del área correspondiente.

1.4.5 Todos los accesos a internet tienen que ser realizados a través de los canales de acceso provistos por el.

1.4.6 Los usuarios con acceso a Internet del tienen que reportar todos los incidentes de seguridad informática a la, inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

1.4.7 El acceso y uso de módem tiene que ser previamente autorizado por la Dirección de Sistemas.

1.4.7.1 Los usuarios con servicio de navegación en internet al utilizar el servicio aceptan que:

- Serán sujetos de monitoreo de las actividades que realizan en internet.
- Saben que existe la prohibición al acceso de páginas no autorizadas.
- Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
- Saben que existe la prohibición de descarga de software sin la autorización de la Dirección de Sistemas.
- La utilización de internet es para el desempeño de su función y puesto y no para propósitos personales.

1.4.8 Los esquemas de permisos de acceso a internet y servicios de mensajería instantánea son:

**NIVEL 1: Sin restricciones**: Los usuarios podrán navegar en las páginas que así deseen, así como realizar descargas de información multimedia en sus diferentes presentaciones y acceso total a servicios de mensajería instantánea.

**NIVEL 2: Internet restringido y mensajería instantánea:** Los usuarios podrán hacer uso de internet y servicios de mensajería instantánea, aplicándose las políticas de seguridad y navegación.

**NIVEL 3: Internet restringido y sin mensajería instantánea:** Los usuarios sólo podrán hacer uso de internet aplicándose las políticas de seguridad y navegación

**NIVEL 4:** El usuario no tendrá acceso a Internet ni a servicios de mensajería instantánea.

## 1.5 CONFIGURACIÓN Y USO DE EQUIPOS PORTATILES

1.5.1 El equipo portátil se entrega al usuario final bajo firma de carta responsiva haciéndose responsable de su buen uso y de la información almacenada.

1.5.2 El equipo portátil debe contar con los siguientes controles de acceso:

a) Contraseña fuerte en el BIOS determinada por el Departamento de Sistemas.
b) Un perfil de cuenta estándar (Cuenta y contraseña fuerte en el sistema operativo) para el usuario y un perfil de cuenta administrador (Cuenta y

contraseña fuerte en el sistema operativo) que solo será utilizado por el departamento de sistemas

1.5.3 El Departamento de Sistemas entregará el equipo portátil con todos los programas y software necesario para las laborares del responsable. Está prohibida la instalación o descarga de software adicional en el equipo sin previa autorización del Departamento de Sistemas.

1.5.4 El equipo debe de contar con el etiquetado el cual permita su identificación en el CAF

## 1.6 PÉRDIDA Y DAÑO DEL EQUIPO

1.6.1 El usuario es responsable del equipo de cómputo portátil y de telefonía asignados. En caso de robo, extravío o pérdida responderá por el bien de acuerdo a la normatividad y sanciones aplicables de la empresa.

1.6.2 En caso de pérdida de cualquier equipo portátil o de comunicación (y accesorios relacionados) deberá informarse de inmediato al Departamento de Sistemas y jefe directo, así como estar disponible para que en su caso acuda ante la autoridad responsable.

1.6.3 El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario, deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado. Para tal caso la determinará la causa de dicha descompostura.

1.6.4 Se deberá evitar sacar los equipos portátiles fuera de las instalaciones de la empresa a excepción de puestos gerenciales y de dirección. En caso de requerir sacar el equipo fuera de las instalaciones es necesario notificar previamente al departamento de sistemas y solicitar la autorización del jefe inmediato vía correo electrónico.

## RECOMENDACIONES DEL CUIDADO DEL EQUIPO FUERA DEL ÁREA DE TRABAJO

Para los usuarios que utilizan computadoras o dispositivos portátiles fuera del área de trabajo, se recomienda que tome los siguientes pasos adicionales para proteger su equipo:

- Nunca deje su computadora portátil desatendida, particularmente en sitios públicos.
- No deje su computadora portátil a plena vista. Si debe alejarse de su área de trabajo por un tiempo extendido, considere guardarla bajo llave.
- No dejar su computadora portátil en el auto. Si la debe dejar en el auto, guárdela fuera de la vista de terceros, preferiblemente encerrándola en el baúl.
- Si va de viaje, utilice un bulto no descriptivo (e.g. una mochila), para guardar su computadora. La idea de esta recomendación es que ni la computadora ni el bulto donde la guarda llame la atención de terceros.

## 1.7 ADMINISTRACIÓN Y USO DE PASSWORDS

1.7.1 Los usuarios deberán observar las siguientes guías para la construcción de su contraseña:

- La contraseña estará compuesta de caracteres alfanuméricos de mínimo 8 caracteres y máximo 12.
- No deben estar relacionados con el nombre del empleado, fecha de nacimiento, lugar o puesto dentro de la empresa, es decir, deben ser difíciles de adivinar, la cual deberá ser determinada en conjunto por el usuario y el Departamento de Sistemas.
- Las contraseñas deberán cambiarse periódicamente, pero bajo sospecha de que el password es conocido por otra persona debe cambiarse inmediatamente.
- Está prohibido que los identificadores de usuarios y contraseñas se encuentren de forma visible en cualquier medio impreso o escrito en el área de trabajo del usuario, de manera de que se permita a personas no autorizadas su conocimiento

1.7.2 El desbloqueo de password deben ser solicitados por el usuario directamente al Departamento de Sistemas.

1.7.3 Las contraseñas (claves), códigos de acceso o tokens llaves asignados a los usuarios que permiten acceder a los servicios, sistemas, redes, marcación telefónica nacional e internacional y a ubicaciones físicas de recursos informáticos, son personales e intransferibles. Su uso, administración y reserva será responsabilidad de cada usuario.

1.7.4. La asignación de la contraseña para acceso a la red y la contraseña para acceso a sistemas, debe ser realizada de forma individual, por lo que queda prohibido el uso de contraseñas compartidas.

## 1.8 BLOQUEO DE EQUIPO DE CÓMPUTO

1.8.1 El usuario que deja su lugar de trabajo por cualquier razón debe dejar bloqueado su equipo de cómputo por seguridad de la información a través de uso de nombre de usuario y contraseña.

## 1.9 USO DEL CORREO ELECTRÓNICO

1.9.1 El correo electrónico institucional es personal e intransferible, cada usuario mantiene su propia cuenta y está prohibido utilizar cuentas asignadas a otras personas para enviar o recibir mensajes de correo.

1.9.2 El uso de cuentas de correos en servidores externos (Hotmail, Gmail, etc) para comunicaciones institucionales está prohibido a menos que exista autorización previa por parte de la dirección de su departamento y de la dirección de sistemas.

1.9.3 El usuario debe utilizar el correo electrónico exclusivamente para desempeñar las funciones que le fueron asignadas para su puesto. Cualquier otro uso (anuncios personales, comerciales, reenvío de cadenas, etc.) del correo electrónico está prohibido. A su vez, en caso de requerir compartir información sensible o adjuntar archivos de tamaño mayor a 25MB, deberá solicitar apoyo al departamento de sistemas para buscar algún otro medio de envío.

1.9.4 Está estrictamente prohibido enviar por correo archivos de contenido multimedia (videos, fotos, links de videos en streaming, etc.). Cuando por la necesidad de su trabajo sea necesario, se deberá de contactar a soporte técnico del departamento de sistemas.

1.9.5 Debe evitarse el uso indiscriminado de la lista de distribución (ej. "enercardgeneral@enercard.com.mx"), y solo utilizarlas en casos justificados. De la misma manera, al responder, es necesario revisar que no estén incluidas listas de distribución si no son requeridas, por lo que deberán de mantener especial atención a estos detalles.

1.9.6 El no cumplimiento de las reglas anteriores, ocasionará la aplicación de las sanciones administrativas correspondientes y en nivel correspondiente a la gravedad de la falta.

1.9.7 Los correos electrónicos que se envíen haciendo uso de la cuenta de correo institucional deberán siempre incluir la firma asignada, así como los avisos o leyendas que expresamente indiquen las directrices o políticas generales que de a conocer la empresa mediante comunicados expresos.

El correo electrónico se ha convertido en una herramienta indispensable para las comunicaciones entre personas en el ambiente empresarial e individual. Su uso se ha generalizado por su practicidad y rapidez, lo que permite que se utilice para casi cualquier cosa, como compartir información, solicitar servicios o productos, envío de mensajes, etc. Sin embargo, esto ha provocado un aumento en la demanda de este servicio y por ende también, la necesidad de aumentar los recursos computacionales en los servidores de correo y velocidad de internet. Por lo tanto, sugerimos las siguientes recomendaciones:

a) Antes de enviar un correo, se debe preguntar si se puede tratar el asunto personalmente o mediante una llamada telefónica, es más rápido. El correo debe utilizarse sólo si se desea dejar registro o evidencia del tema con la o las personas interesadas.

b) Debemos preguntarnos, antes de enviar un correo, si las personas indicadas como destinatarios realmente necesitan esa información o si realmente tendrán injerencia en el asunto a tratar. Se debe evitar copiar a personas que no ayudarán a resolver el asunto tratado y más si va a "Responder a todos".

c) Mantenga su bandeja de entrada lo más depurada posible. Debemos eliminar todos los correos que no utilicemos y solo conservemos los que podemos utilizar como referencia en el futuro. Esto evitará que su software de correo (Outlook) se sature y trabaje demasiado lento.

d) Se debe utilizar la herramienta de "Autoarchivar elementos de correo" para disminuir el tamaño de su bandeja de entrada. Puede preguntar al departamento de soporte técnico para realizar esta tarea.

e) Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información que es propiedad de la empresa. Los mensajes de correo

electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

f) Los usuarios podrán enviar información reservada y/o confidencial exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones, a través del correo institucional que le proporcionó la empresa.

g) La empresa, se reserva el derecho de acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico de personal que ha comprometido la seguridad violando políticas de Seguridad Informática o realizado acciones no autorizadas. Como la información del correo electrónico institucional es privada, la única forma en la que puede ser revelada es mediante una orden judicial.

h) El usuario debe de utilizar el correo electrónico, única y exclusivamente para los recursos que tenga asignados y las facultades que les hayan sido atribuidas para el desempeño de su empleo, cargo o comisión, quedando prohibido cualquier otro uso distinto.

i) La asignación de una cuenta de correo electrónico externo, deberá solicitarse por escrito a la Dirección de Sistemas o al representante de ésta en su zona , señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del titular del área que corresponda.

j) Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

## 1.10 CONTROL DE INGRESO DE EQUIPOS

1.10.1 Cualquier persona externa que acceda a las instalaciones de la empresa deberá notificar al guardia de seguridad en caseta el ingreso de equipos de cómputo personales, dispositivos de almacenamiento (USB, discos duros externos, tarjetas de memoria, etc.), equipo de comunicaciones (excepto por teléfonos móviles o celulares) y herramientas que no sean propiedad de Energéticos en Red Electrónica, S.A. de C.V., de manera que se mantenga control sobre el tráfico de los equipos computacionales que entran y salen de la empresa.

1.10.2 La información que estas personas externas graben en sus dispositivos o equipos estará bajo la responsabilidad compartida tanto del externo como del personal que lo atendió.

1.10.3 Queda prohibido para el personal, ingresar y utilizar sus equipos personales para realizar sus actividades laborales salvo previa solicitud y autorización de parte del Departamento de Sistemas.

## 2. POLITICA DE SEGURIDAD DE OFICINA Y ESCRITORIO LIMPIO

### 2.1 SEGURIDAD DE OFICINAS

2.1.1 Todas las oficinas e instalaciones de la empresa deben cumplir con los siguientes controles:

- Oficinas sensibles deben evitar el acceso al público, solamente con la previa autorización del encargado.
- Áreas críticas deberán manejar acceso restringido, tendrán acceso solo personal autorizado. Las puertas o accesos a oficinas deben permanecer cerradas en ausencia del personal que labora en las mismas.
- El uso de equipo fotográfico, de video o de audio grabación no está permitido a menos de que exista una autorización expresa de la Dirección correspondiente, exceptuando el caso que sus funciones así lo requieran.

### 2.2 EQUIPO DE OFICINA:

2.2.1 Los equipos departamentales de fotocopiado, impresión o fax que se encuentran en áreas comunes deberán utilizarse de manera correcta, evitando dejar documentos procesados o información impresa al alcance de personal no autorizado.

### 2.3 ESCRITORIO LIMPIO:

Todo el personal que labora en la empresa está obligado a cumplir con las siguientes normas de seguridad al ausentarse de su lugar de trabajo o al finalizar su jornada laboral.

- Se resguardará la información sensible que se encuentre en papel, USB, discos, medios magnéticos, etc., dentro de gabinetes apropiados, cajones con llave o cualquier otro mueble con acceso controlado.
- Apagar o bloquear el equipo de cómputo con usuario y contraseña.

- Toda documentación de importancia media o baja que ya no sea requerida deberá ser destruida (a excepción de información contable que requiera un tiempo de almacenamiento).
- No utilizar la información impresa que sea confidencial o de uso restringido para reciclaje.

**SANCIONES**

**SANCIONES GENERALES POR INCUMPLIMIENTO A LAS POLÍTICAS DE SEGURIDAD.**

**1. GENERALIDADES.**

1.1 El incumplimiento a las Políticas de Seguridad, tendrá como consecuencia la aplicación de las sanciones previstas en la política de sanciones disciplinarias y/o Reglamento Interior de Trabajo

**2. ACTOS.**

Los siguientes actos estarán sujetos a sanción según la gravedad de la falta:

2.1 Adquirir, desarrollar, implementar o instalar sistemas de información sin autorización según los daños causados al equipo(s).

2.2 Ingesta de alimentos y bebidas en lugares prohibidos y que derivado de este acto, pueda causar un daño a los equipos de cómputo, telefonía móvil y fija.

2.3 Obstrucción de equipos de cómputo mediante objetos no autorizados.

2.4 Abrir o desarmar los equipos de cómputo.

2.5 Uso de dispositivos de almacenamiento externo no autorizados, cualquiera que sea su naturaleza.

2.6 Robo, pérdida total o parcial de equipos de cómputo y de información clasificada y/o confidencial de la empresa.

2.7 Ingreso a la empresa de equipos electrónicos o medios de almacenamiento no autorizados cualquiera que sea su naturaleza.

2.8 Resguardo y/o extracción de información clasificada y/o confidencial de la empresa en medios de comunicación personales como teléfono, radio, etc.

## 3. APLICACIÓN DE LAS SANCIONES.

3.1 Dependiendo de la Gravedad de la falta, se podrán aplicar las siguientes sanciones

| Sanción | Responsable de Aplicar la sanción |
|---|---|
| Llama de atención verbal | Comité, Jefe Inmediato |
| Llama de atención por escrito | Comité, Jefe Inmediato |
| Acta Administrativa<br>Formato de aceptación de descuento | Comité, Jefe Inmediato, RH |
| Suspensión<br>Formato de aceptación de descuento | Comité, Jefe Inmediato, RH, Jurídico |
| Rescisión de relación laboral<br>Formato de aceptación de descuento | Comité, Jefe Inmediato, RH, Jurídico |

## 4. CASOS FORTUITOS

4.1 Así mismo se deberá de tomar en cuenta que todos los actos que se encuentren fuera de los actos previstos en el apartado #2 , deberán de ser evaluados por el Comité Técnico y/o Jefe Inmediato, quienes determinaran en conjunto, la gravedad del acto, la posible reparación, el posible monto de los daños ocasionados y en su caso la sanción aplicable.

## 5. LINEAMIENTOS PARA EL MANEJO DE INFORMACIÓN PARA PROVEEDORES, CLIENTES Y PERSONAS AJENAS AL TERCERO AUTORIZADO.

5.1 Las personas que bajo su responsabilidad se encuentre el resguardo de información confidencial de personas físicas o morales (PROVEEDORES) diferentes al Tercero Autorizado, deberán de seguir los mismo procedimientos de manejo y resguardo de la información de acuerdo a la LFPDPPP y la Ley de la Propiedad Industrial, y por lo tanto serán responsables de las consecuencias por la ausencia de esta protección.

5.2 En todo momento se deberá de mantener un resguardo total todos los datos que se consideren sensibles

5.3 Los usuarios deberán utilizar los mecanismos institucionales para proteger la información que reside y utiliza la infraestructura del tercero De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna o hacia redes externas como internet.

## 6. DISPOSICIONES ESPECIALES EN MATERIA DE DATOS PERSONALES.

Específicamente en cuanto a lo relacionado a datos personales y en todo lo no especificado en las presentes políticas respecto a su tratamiento, la empresa hace del conocimiento de los empleados los siguientes conceptos básicos:

**Datos personales.-** Cualquier información concerniente a una persona física identificada o identificable

**Titular de los datos.-** La persona física a quien corresponden los datos personales.

**Tratamiento.-** La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

**Responsable del tratamiento**.- Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.

En el caso en particular, la empresa, como persona moral de carácter privado, es Responsable del tratamiento de los datos personales de titulares, entre ellos sus empleados, clientes y socios comerciales, lo cual es necesario para el desarrollo de sus actividades comerciales, por lo que dicho tratamiento se encuentra sujeto a la legislación aplicable en materia de datos personales.

Para conocer más sobre el procedimiento adecuado a seguir para dar cumplimiento a las obligaciones de la empresa como responsable del tratamiento de datos personales y las actividades permitidas y limitadas dentro de este rubro, los empleados podrán consultar La Política de Seguridad de la Información y Manejo de datos personales que la empresa ponga a su disposición o, en caso de cualquier duda u observación al respecto, ponerse en contacto con un representante del Comité Técnico Multidisciplinario para la Protección de Datos Personales.

## 7. DIFUSIÓN DE LAS POLÍTICAS DE SEGURIDAD A LOS EMPLEADOS.

Con el objetivo de que las políticas de seguridad y de datos personales estén al alcance

A todos los miembros de la empresa:

Deberá ser de fácil acceso para todos los trabajadores.

Se debe revisar periódicamente para que no pierda adecuación a la organización.

Deberá estar disponible y actualizada para todas las partes interesadas.

Por lo tanto se difundirán de la siguiente manera:

1. Publicación en el sistema de documentos de la organización.

   La política de seguridad se encuentra disponible en el sistema de calidad

   Adhocsystem (http://serverdoc/adhocsystem/) la cual se ingresa con una cuenta de Acceso y contraseña en la opción Documentos bajo la categoría SEGURIDADEN LA INFORMACIÓN

2. Publicación en el portal de intranet de la organización.

   La política de seguridad se encuentra disponible en la página http://intranet.grupoeco.com.mxsección LFPDPPP, opción Políticas de Seguridad. Este enlace se difunde por medio de un correo electrónico a todos los empleados para su conocimiento.

3. Revisión de las políticas de seguridad por el comité interdisciplinario.

   Dependiendo de los cambios internos y externos a la organización, se realizan reuniones de parte del comité interdisciplinario para realizar ajustes a las políticas de seguridad y nombrar nuevos integrantes del comité dependiendo de la rotación de personal. Estas revisiones deberán de ser obligatorias cada 6 (seis) meses, esto con la intención de mantener vigentes nuestros procesos, y en su caso corregir errores que puedan ir surgiendo durante el día a día.

Como resultado de esta reuniones de realizan actualizaciones a la políticas y se envía a los involucrados del comité para aprobar dichos cambios.

Una vez que se aprueban se firma nueva versión por el representante legal. Después de esta aprobación se divulgan al personal con las adecuaciones realizadas así como con la fecha en que se realizó los ajustes y los participantes y monitoreado por medio de la opción de control de cambios.

4. Capacitación periódica a los empleados.

Para mantener la vigencia en el conocimiento de las políticas de seguridad de datos un miembro del comité interdisciplinario realiza la capacitación y actualización de los empleados.

## 8. FORMA DE PROCEDER RESPECTO A LAS CONSULTAS Y SOLICITUDES HECHAS POR LOS TITULARES DE LOS DATOS

Todo titular de datos personales tiene derecho a realizar consultas y elevar solicitudes a la compañía respecto al manejo y tratamiento dado a su información.

### 8.1 **PROCEDIMIENTO PARA EL TRÁMITE DE RECLAMOS O SOLICITUDES**:

Toda solicitud, petición, queja o reclamo que sea presentada a ENERGÉTICOS EN RED ELECTRÓNICA, S.A. DE C.V. Por parte de cualquier titular o sus causahabientes respecto al manejo y tratamiento dado Política Manejo de Información y Datos Personales a su información será resuelta de conformidad con la ley regulatoria al derecho al habeas data y será tramitado bajo las siguientes reglas:

1. La petición o reclamo se formulará mediante escrito o cualquier otro de los medios definidos en la presente política para tal fin, dirigido a ENERGÉTICOS EN RED ELECTRÓNICA, S.A. DE C.V. con la identificación del titular, la descripción

de los hechos que dan lugar al reclamo, la dirección o medio a través del cual desea obtener su respuesta, y si fuere el caso, acompañando los documentos de soporte que se quieran hacer valer. En caso de que el escrito resulte incompleto, la compañía solicitará al interesado para que subsane las fallas dentro de los cinco (5) días siguientes a la recepción del reclamo. Transcurridos dos meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido de la reclamación o petición.

2. Una vez recibida la petición o reclamo completo, la compañía incluirá en el registro individual en un término no mayor a dos (2) días hábiles una leyenda que diga "reclamo en trámite" y la naturaleza del mismo. Dicha información deberá mantenerse hasta que el reclamo sea decidido.

3. El solicitante recibirá una respuesta por parte de ENERGÉTICOS EN RED ELECTRÓNICA, S.A. DE C.V. Dentro de los diez (10) días hábiles siguientes contados a partir de la fecha en la cual ha tenido conocimiento efectivo de la solicitud.

4. Cuando no fuere posible atender la petición dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su petición, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

8.2 **CONSULTAS:**

Política Manejo de Información y Datos Personales Cualquier consulta que tenga un titular sobre su información o datos personales o cuando considere necesario instaurar una solicitud de información o considere que sus derechos han sido vulnerados en relación con el uso y el manejo de su información.

Si dentro de los diez (10) días señalados, no fuere posible para la compañía atender la consulta, el área correspondiente deberá informar al interesado, los motivos de la demora e indicarle la fecha en que se atenderá la misma, la cual

en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.