POLITICA CORPORATIVA

USO DE MEDIOS REMOVIBLES

Documento N° Inkia Energy– T – 02

Versión	Fecha de Vigencia	Preparada por:	Revisada por:	Aprobada por:
1	08/09/20	Anamaría Chalco	María Vera y Mario Lopez	Roberto Cornejo

1. PROPÓSITO

El objetivo de esta política es delinear las responsabilidades y controles de la organización sobre el uso de medios removibles, incluyendo USB flash drives, discos duros externos, dispositivos móviles usados como almacenamiento externo, medio ópticos (CD, DVD, etc.) y cualquier otro dispositivo computacional que no esté físicamente fijo dentro de una computadora. Apunta a minimizar el riesgo de pérdida o exposición de información sensible y reducir el riesgo de ser infectado con malware en los sistemas de información de Inkia Energy y sus Empresas Operativas (en adelante "la Compañía).

Esta política gobierna la interacción entre todos los activos y recursos, tanto para Tecnología de la Información como para Tecnología de Operaciones, incluye sistemas operativos, software de aplicaciones, hardware de cómputo, redes y servicios en nube, para todo equipo manejado por la Compañía (de propiedad, bajo arrendamiento o personal) o donde residan datos de la Compañía.

2. AMBITO Y APLICACIÓN

Las empresas del grupo Inkia Energy están obligadas a implementar y cumplir todas las políticas y directrices vigentes.

Asimismo, se requiere que los contratistas de las empresas del grupo mantengan el mismo espíritu e intención de dichas políticas y directrices, homologando las disposiciones que les correspondan de acuerdo con la naturaleza de su contrato.

Esta política aplica a los Colaboradores y Proveedores de Compañía, incluyendo personal afiliado a terceros, siempre que se maneje información de la Compañía y use infraestructura y/o servicios de tecnología de la Compañía.

3. DEFINICIONES

TÉRMINO	DEFINICIÓN
Colaborador (es)	Se refiere a directores, gerentes, funcionarios o empleados permanentes o temporales y practicantes o pasantes que forman parte de Inkia Energy o cualquiera de sus subsidiarias.
Encriptación de datos	El acto o proceso de convertir la información en cifrado (escrito secreto), también conocido como codificación. Esto asegura que contenido inteligible solo pueda ser accedido por usuarios autorizados y previene que externos intercepten y accedan a la información.
Encriptación de Hardware	Proceso de encriptación de datos realizado usualmente a nivel de instrucción de procesador. Encripta toda la información contenida en un dispositivo de almacenamiento removible.
Encriptación de software	Proceso de encriptación de datos realizado a nivel de software que resulta en un archivo encriptado. A diferencia de la encriptación de hardware, este puede usarse para encriptar una selección de archivos y no necesariamente un dispositivo completo.
Medios removibles	Medio portátil de almacenamiento de datos que puede introducirse o removerse de un equipo de cómputo o red. Entre estos están, pero no se limita a: • Discos ópticos (CD, DVD, Blu-ray) • Discos duros externos

TÉRMINO	DEFINICIÓN
	• Discos de estado sólido externos (SSD drives) • Cintas magnéticas y ópticas • Tarjetas de memoria externas (Secure Digital, CompactFlash, Memory Stick, MMC, xD) • Flash memory devices (USB, eSATA, Flash drive, Thumb Drive) • Microchips embebidos (Smart cards, Mobile phone memory cards, SIM cards) • Otros discos duros externos (Floppy, Zip, Jaz, Bernoulli, UMD) Otros dispositivos de almacenamiento comunes (Cámaras digitales, mp3 players, impresoras, Webcams, entre otros).
Proveedor (es)	Personas e instituciones con las cuales la empresa mantiene vínculos comerciales, contractuales o empresariales e incluye en sentido amplio a los proveedores, contratistas, prestadores de servicios, consultores, subcontratistas, asesores, agentes, distribuidores, socios comerciales, etc.

4. DECLARACIÓN DE LA POLITICA

Los medios removibles son una fuente común de infecciones de malware y fuga accidental o deliberada de información confidencial. Hoy en día existen variedad de acceso a tecnologías más seguras para la transferencia de datos, como son archivos compartidos y servicios en nube, por lo que el rol de los medios removibles debe limitarse operaciones muy específicas.

Una política de uso de medios removibles establece los lineamientos para usar, transferir y guardar información en medios removibles de manera segura.

4.1 Medios Removibles Permitidos

- El uso de medios removibles en activos de la Compañía debe responder a una necesidad de negocio, cuando no exista una alternativa adecuada y los beneficios de usar estas tecnologías superen los riesgos asociados a su uso.
- La solicitud para el uso de un medio removible deberá comunicarse al gerente de línea para aprobación y luego al departamento de TI para evaluación previo a su aprobación final. Una mayor evaluación podría ser requerida para asegurar que es la solución adecuada.

4.2 Uso de Medios Removibles

- Ningún medio removible aprobado podrá ser conectado a un equipo externo a la Compañía o fuera de la red. Toda excepción deberá ser aprobada por el departamento de TI.
- No deben usarse dispositivos de almacenamiento externos dañados y/o que presenten fallas.
- Mantener actualizados el antivirus y antimalware en los dispositivos a los que se conecte un medio removible.

4.3 Seguridad de Datos y Reporte de Incidentes

- Todo dispositivo de almacenamiento removible en uso (que contenga información de la Compañía) deberá ser encriptado. Excepciones por motivos de negocio podrán darse previa comunicación y aprobación del departamento de TI.
- El departamento de TI debe proveer el software de encriptación, así como la guía para dicho proceso.
- Cualquier contraseña usada en un dispositivo removible debe cumplir con la Política de Contraseñas de la Compañía.
- Debido al alto riesgo de corrupción, mal funcionamiento o pérdida, los medios removibles no deben ser usados como almacenamiento primario. Se debe mantener en los sistemas e la Compañía una copia de toda la información almacenada en medios removibles.
- Todo dispositivo de almacenamiento removible en uso debe guardarse en un ambiente Seguro acorde al tipo y sensibilidad de la información contenida.

- Ante la sospecha de un dispositivo removible comprometido o si se confirma una infracción de seguridad (lo que incluye el mal funcionamiento, pérdida o robo) debe reportarse de inmediato a Soporte de TI local.
- Dicho reporte activa el Plan de Respuesta ante Incidentes.

4.4 Uso de Medios Removibles por Terceros

- Ningún tercero (esto incluye, contratistas, socios o agentes gubernamentales) puede acceder o extraer información de la Compañía con un medio removible sin el acuerdo explícito del departamento de TI y el dueño de la información.
- El uso de medios removibles por un tercero en cualquier activo de la Compañía debe pasar por una evaluación de riesgo y ser autorizado por el departamento de TI.
- De otorgar autorización a un tercero para el uso de un medio removible, deberá cumplir con todas las consideraciones de esta política sobre el almacenamiento y transferencia de información.
- Los practicantes y recepcionistas tendrán los puertos USB deshabilitados.

4.5 Desecho de Medios Removibles

- Los dispositivos removibles que no sean requeridos o que estén dañados deben retornarse a TI para un desecho seguro.
- Para evitar la fuga de información, los dispositivos removibles que funcionen deben limpiarse completamente con software y herramientas especializadas, eliminando toda la información antes de ser reutilizado. Los dispositivos que presenten fallas deben deshabilitarse físicamente, previo a desecharse, para asegurar que la información no pueda rescatarse.

4.6 Información de Contacto

PAIS	E-MAIL
Argentina	AR_JT@orazul.com
Bolivia	Helpdesk.cobee@cobee.com
Chile	Helpdesk.cl@lnkiaenergy.com
El Salvador	HelpDesk.SVGT@inkiaenergy.com
Guatemala	HelpDesk.SVGT@inkiaenergy.com
Nicaragua	Helpdesk.CAC@inkiaenergy.com
Panamá	Helpdesk.CAC@inkiaenergy.com
Perú	PE.HelpDesk@kg.com.pe
República Dominicana	Helpdesk.CAC@inkiaenergy.com
ENERGUATE	soporte_tecnico@energuate.com

5. RESPONSABILIDADES

Colaboradores

- Conocer y cumplir las disposiciones de esta Política
- Solicitar orientación al Área de TI cuando sea requerido.
- Conocer Reportar inquietudes y preocupaciones con respecto a esta Política.

Gerentes de Línea y Departamento

- Responsable de aprobar el caso de negocio de sus colaboradores a presentar al departamento de TI.
- Sensibilizar a los colaboradores sobre el contenido y cumplimiento de esta Política.
- Coordinar con el Área de TI para solicitar su orientación para establecer procesos y prácticas que aseguren el cumplimiento de requisitos / exigencias de esta Política.

Área TI Corporativo

Es la administradora de la presente política y responsable de:

- Asegurar la vigencia y revisión de esta política.
- Asegurar la distribución adecuada de las políticas a la compañía y sus socios.
- Actualizar su contenido cuando se requiera.
- Comunicar y difundir las actualizaciones, cambios, excepciones y cualquier otro asunto relacionado con la misma
- Canalizar y aclarar cualquier duda o comentario de la Política.
- Brindar orientación específica sobre cada situación o caso que se presente en aplicación a la Política.

Área TI Local

- Procesar y aprobar los casos de negocio para el uso de medios removibles.
- Proveer y aprobar las solicitudes para el uso de medios removibles.
- Proveer los dispositivos de almacenamiento removibles para los casos aprobados.
- Realizar el proceso de encriptación en los dispositivos removibles previo a su asignación.
- Mantener el registro de dispositivos de almacenamiento externo asignados.

6. CONTROL Y CUMPLIMIENTO

El cumplimiento de esta Política es obligatorio. Todo personal de Inkia Energy deberá entender su rol y responsabilidad en relación con esta Política.

7. CONSECUENCIAS DE INCUMPLIMIENTO

Desvíos e incumplimiento de la presente política puede acarrear la imposición de medidas disciplinarias, que, de aplicarse, servirán como elemento correctivo y formador de nuestra cultura organizacional.

Las medidas disciplinarias deben ser justas, razonables y proporcionales a la falta cometida, respetando el marco legal correspondiente y las normas internas de la empresa.

8. EXCEPCIONES

Cualquier excepción a esta política deberá tratarse de manera particular y deberá estar debidamente sustentada por el CEO de la OpCo, y aprobada por TI Corporativo y el Deputy CEO.

CONTROL DE CAMBIOS

Edición	Fecha	Descripción	Actualizada por:
1	08/09/20	Documento inicial	Anamaría Chalco