POLITICA CORPORATIVA

CONTRASEÑAS

Documento N° Inkia Energy– T – 03

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 propósito de esta política es definir los estándares para la protección, creación, cambio y eliminación de contraseñas para 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 Colaboradores y Proveedores de la 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.

La seguridad de contraseñas es una parte fundamental de un Programa de Ciberseguridad exitoso, pues éstas son la protección de primera línea para las cuentas de usuario. Una contraseña débil puede resultar en el acceso no autorizado a información sensible o explotación de recursos de la empresa. Todos los empleados, contratistas, consultores, trabajadores temporales y otros con acceso a los sistemas de Inkia Energy, deberán cumplir con esta política.

3. DEFINICIONES

TÉRMINO	DEFINICIÓN
Ciberseguridad	La habilidad de proteger o defender el uso del ciberespacio de ciberataques.[1]
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.
Contraseña	También denominada clave, es una forma de autenticación para controlar el acceso hacia algún recurso informático, ya sea un archivo, un programa o un equipo.
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.
TI	Tecnología de la Información
VPN	Red Virtual Privada (por sus siglas en inglés)

[1] Definición basada en la NIST (National Institute of Standards and Technology)

4. DECLARACIÓN DE LA POLITICA

Todos los usuarios recibirán contraseñas iniciales de manera temporal, esta les forzará a cambiarla de manera inmediata. Las contraseñas iniciales serán establecidas por el departamento de TI y deberán ser únicas. Las contraseñas temporales solo podrán ser entregadas con identificación válida del usuario. Las contraseñas se entregarán de manera segura (ej. No como texto de un e-mail) y deberán mantenerse confidenciales.

4.1 Lineamientos para la construcción de contraseñas

- La contraseña debe tener un mínimo de 10 caracteres.
- Las contraseñas deben contener las siguientes clases de caracteres:
  - Letras minúsculas
  - Letras mayúsculas
  - Números
  - No-alfanuméricos (ej. @#$%^&*() _+|~-=\` {} []:";'<>/ etc.)
- Las contraseñas no deben ser una palabra regular, un nombre propio, cumpleaños, el número de identificación, o cualquiera de las opciones anteriores junto a un dígito.
- Las contraseñas deben cambiarse cada 100 días.
- Las contraseñas solo pueden ser reutilizadas después de ser cambiadas como mínimo 8 veces o tras 800 días.
- No deben utilizarse contraseñas similares para cada cuenta relacionada al trabajo.
- No deben utilizarse las mismas contraseñas para cuentas personales.
- Las cuentas con privilegios de administrador en los sistemas deben tener una contraseña única, distinta de todas las contraseñas del sistema.
- Las contraseñas de servicios críticos en ambientes productivos deben incluirse en una base de datos de gestión de contraseñas globales, parte de la Seguridad de la Información.

4.2 Cambio de Contraseñas

- Las contraseñas nuevas (por asignación nueva o restauración) deben enviarse a través de métodos seguros.
- En caso de sospecha que una contraseña ha sido comprometida, deberá cambiarse de inmediato.
- El descifrado de contraseñas o uso de fuerza bruta se realizará de manera periódica o aleatoria por el equipo de TI o sus delegados. Si una contraseña es descifrada durante estas pruebas, el usuario deberá cambiarla en cumplimiento con los lineamientos de construcción de contraseñas en la sección 1.1.

4.3 Estándares de Protección de Contraseñas

- Las contraseñas se deben manejar como información sensible, parte de la información confidencial de la Compañía.
- No deben compartirse con nadie, incluyendo personal de TI, supervisores u otros colaboradores, bajo ninguna comunicación electrónica o por teléfono.
- Los usuarios deberán declinar la funcionalidad “Recordar mi contraseña” en las aplicaciones.
- El formato o contenido de la contraseña no debe insinuarse a otros (ej. “el nombre de mi perro”)
- Las contraseñas no deben escribirse o guardarse en ningún lado, incluyendo archivos en la computadora sin encriptar.
- Ante la sospecha de que la contraseña ha sido comprometida, el usuario debe reportarlo a Soporte de TI Local de inmediato y cambiar todas sus contraseñas.
- Las contraseñas solo podrán guardarse en “gestores de contraseñas” autorizados por la Compañía para servicios críticos.

4.4 Borrado de Contraseñas

Las contraseñas que ya no sean necesarias deben borrarse o inhabilitarse de inmediato, incluyendo, pero no limitado a:

- Retiros, despidos, renuncias, reasignaciones, etc.
- Contraseñas temporales

- Cuentas de contratistas o terceros que ya no se requieran o vencido el contrato. Las cuentas de externos deberán crearse con un periodo de validez definido.

Cuando ya no se requiera una contraseña, deberán ejecutarse lo siguiente:

- El usuario deberá notificar a su supervisor inmediato.
- El contratista deberá notificar al administrador de contrato o nexo en la compañía.
- Los supervisores o puntos de contacto deben informar a Soporte de TI Local y RRHH.
- El equipo de Soporte de TI eliminará la contraseña y eliminará o suspenderá la cuenta.
- Deberán realizarse revisiones regulares para validar que la contraseña fue eliminada de manera satisfactoria.

4.5 Inicio de sesión fallidos

- Las cuentas de usuario deben bloquearse tras 5 intentos de inicio de sesión fallidos.
- La duración del bloqueo será ilimitada.
- Para recuperar una contraseña el usuario deberá contactar a Soporte de TI Local.

4.6 Estándares para el Desarrollo de Aplicaciones

Los desarrolladores de aplicaciones deben asegurar que los programas cumplan con las siguientes medidas de seguridad:

- Autenticación de usuarios individuales, no grupos,
- No deben guardar las contraseñas en texto simple o reversible de manera fácil.
- Incluir gestión de roles con el fin de permitir la reasignación de funciones sin necesidad de contar con la contraseña de otro usuario.

4.7 Acceso Remoto

- El acceso remoto a la red de la Compañía se controla por el uso de una Red Virtual Privada (VPN por sus siglas en inglés), para lo cual se requiere una identificación de usuario y contraseña, así como el uso de doble autenticación.

4.8 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

4.9 Referencias

- SANS – Organización de Investigación y Educación enfocada en seguridad de la información.
- ISO 27001 – Estándar internacional en Sistemas de Gestión de Seguridad de la Información
- Programa de Ciberseguridad de Inkia

5. RESPONSABILIDADES

Colaboradores

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

Gerentes y Supervisores

- Sensibilizar a los colaboradores sobre el contenido y cumplimiento de esta Política.
- Coordinar con el Área TI y solicitar su orientación para establecer procesos y prácticas que aseguren el cumplimiento de requisitos / exigencias de esta Política.

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.

Responsable de TI Local

- Actualizar la documentación local basada en la dirección corporativa.
- Asegurar la distribución adecuada de la información de ciberseguridad dentro de la compañía.

Departamento de TI Local

- Establecer los controles de acceso de usuario y requerimientos de contraseñas.
- Realizar auditorías regulares para asegurar el cumplimiento de la política.
- Brindar apoyo a los usuarios.

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