POLÍTICA DE SEGURIDAD PARA LA GESTIÓN DE CREDENCIALES

CÓDIGO: A-GI-POL-001
Versión: 1
Fecha de aprobación: 22/02/2024

San José del Guaviare

Tabla de contenido

1. INTRODUCCIÓN

El tratamiento diario de la información en ENERGUAVIARE S.A.S implica el acceso a diversos servicios, dispositivos y aplicaciones por parte de los trabajadores, quienes utilizan credenciales de acceso compuestas por un nombre de usuario y una contraseña. Es fundamental garantizar la seguridad de los servicios y sistemas que requieren autenticación de usuarios, asegurando que las credenciales se generen, actualicen y revoquen de manera óptima y segura. Asimismo, es prioritario garantizar que solo las personas autorizadas accedan a los sistemas de información de la empresa.

2. OBJETIVO

Establecer, difundir y verificar el cumplimiento de buenas prácticas en el uso de las cuentas de usuario y contraseñas para los trabajadores

3. ALCANCE

El alcance de los lineamientos que se definen en esta política da cubrimiento a los accesos que involucren:

a) Acceso a alguno de los siguientes sistemas:
   - Bases de datos.
   - Aplicativos.
   - Sistemas de información.
   - Elementos de infraestructura tecnológica (Firewall, Router, Switch…).
   - Equipos de cómputo.
   - Sistemas de seguridad electrónica

Esta política se aplica a todos los trabajadores de ENERGUAVIARE S.A.S., incluidos aquellos de carrera administrativa, provisionales, de libre nombramiento y remoción, trabajadores oficiales, contratistas y cualquier otro personal que cuente con un usuario y contraseña para acceder a sistemas de información, bases de datos, equipos de cómputo o aplicaciones que requieran autenticación. Todos los usuarios deben garantizar la confidencialidad de la información de la empresa, cumpliendo con los mismos estándares de seguridad y responsabilidades para proteger los datos. Además, están obligados a mantener la confidencialidad incluso después de finalizada su relación laboral o contractual con ENERGUAVIARE S.A.S

4. DECLARACIÓN DE COMPROMISO

En este documento se encuentran los lineamientos que garantizan una actuación adecuada para alcanzar un alto nivel en cuanto a seguridad de la información en ENERGUAVIARE S.A.S. Dado que la información representa un activo crucial para la empresa y tiene un valor significativo, la empresa ha definido las directrices de seguridad para sus activos de Información. Estas directrices deben orientar todas las acciones a seguir en materia de seguridad de la información.

Estas directrices están basadas en la NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27002 (anteriormente denominada ISO 17799) es un estándar para la seguridad de la información publicado por la *International Organization for Standardization* y la Comisión Electrotécnica Internacional. La versión más reciente es la ISO/IEC 27002:2013).

Por lo anterior, se busca minimizar riesgos en la información, asegurar la continuidad de ENERGUAVIARE y ayudar en el cumplimiento de los objetivos misionales.

5. RESPONSABILIDADES

ROL	RESPONSABLE	DESCRIPCIÓN DE LA RESPONSABILIDAD
LÍDER DE PROCESO	Profesional 01 Sistemas.	- Crear y documentar políticas y procedimientos sólidos relacionados con la gestión de credenciales de acceso. - Establecer, mantener y supervisar políticas efectivas de creación de contraseñas. - Establecer requisitos claros para la longitud de las contraseñas, la complejidad, la frecuencia de cambio
LÍDER DE IMPLEMENTACIÓN	Profesional 01 Sistemas.	- Garantizar la adecuada aplicación de las políticas y fortalecer la seguridad de los sistemas y datos. - Realizar un seguimiento continuo para asegurarse de que las políticas y procedimientos de seguridad de credenciales se estén cumpliendo adecuadamente en toda la empresa. - Responder y gestionar de manera efectiva cualquier incidente de

		seguridad relacionado con credenciales.
COLABORADORES	Trabajadores y contratistas	- Debe conservar su contraseña en secreto. - No debe guardar las contraseñas de forma legible en medios impresos o manuscritos expuestos a otros usuarios o terceros a la empresa. - No debe guardar las contraseñas de forma digital, bajo nombres evidentes como “Contraseñas” u otros - No debe entregar su contraseña a nadie, incluso a los administradores o personal de soporte técnico de ENERGUAVIARE S.A.S excepto en caso de que ellos lo soliciten como condición para realizar un servicio. - No se debe utilizar en sistemas externos, incluyendo bancos y redes sociales una clave que se esté usando en los sistemas de ENERGUAVIARE S.A.S. - No se debe utilizar la función “Remember password” o “Recordar contraseña” en los navegadores. - No se deben prestar las contraseñas. - No se deben utilizar las credenciales de acceso de usuarios retirados o en periodos de vacaciones. - Generar contraseñas fuertes y únicas para cada cuenta. Utilizar una combinación de letras mayúsculas y minúsculas, números y caracteres especiales. - Cuando termine de trabajar en un dispositivo, debe asegurarse de cerrar sesión en las aplicaciones y bloquear el dispositivo para evitar accesos no autorizados.

6. CONTROL Y CUMPLIMIENTO

El cumplimiento de esta Política es obligatorio. Todos los trabajadores de ENERGUAVIARE S.A.S deberán entender su rol y responsabilidad en relación con esta Política.

6.1 Incumplimiento

El incumplimiento de las políticas de seguridad de credenciales puede tener diversas consecuencias, tanto para el trabajador como para la empresa. Las posibles consecuencias incluyen:

- ***Amonestación o advertencia:*** En casos menos graves, la empresa podría emitir una amonestación o advertencias formales al trabajador que incumplió las políticas de seguridad.

- ***Formación adicional:*** Si el incumplimiento fue resultado de una falta de comprensión o conocimiento, la empresa podría proporcionar formación adicional sobre las políticas de seguridad y cómo mantener las mejores prácticas.

- ***Acciones disciplinarias:*** En casos más serios, las acciones disciplinarias podrían ser apropiadas. Esto podría incluir medidas como suspensiones temporales, retiro de privilegios de acceso o reducción de responsabilidades para el trabajador.

- ***Investigación interna:*** En situaciones en las que el incumplimiento ha resultado en una violación de seguridad o en daños significativos, la empresa podría llevar a cabo una investigación interna para determinar la causa y el alcance del incumplimiento.

- ***Responsabilidad civil y penal:*** Dependiendo de la gravedad del incumplimiento y las consecuencias resultantes, podría haber responsabilidad civil o incluso penal para el trabajador o la empresa.

6. 2 Revocación de credenciales

Revocar credenciales se refiere a la acción de invalidar o deshabilitar las credenciales de acceso de un usuario a sistemas, aplicaciones o recursos debido a diversas razones. Las razones comunes para revocar credenciales incluyen:

- ***Término de empleo o relación:*** Cuando un trabajador finaliza su relación con la empresa, es necesario revocar sus credenciales para evitar el acceso no autorizado a sistemas y datos.
- ***Cambio de roles o responsabilidades:*** Si un trabajador cambia de rol dentro de la empresa y ya no necesita el mismo nivel de acceso, es posible que se deban revocar algunas de sus credenciales anteriores y asignar nuevas.

- ***Violación de políticas de seguridad:*** Si un trabajador incumple repetidamente las políticas de seguridad de la empresa, como usar contraseñas débiles o compartir credenciales, sus credenciales podrían ser revocadas como medida disciplinaria.

- ***Detección de actividades maliciosas:*** Si se detectan actividades sospechosas o maliciosas en una cuenta de usuario, es importante revocar las credenciales para evitar más daños y proteger los sistemas y datos.

- ***Violación de privacidad o regulaciones:*** Si un trabajador maneja información sensible o personal y se descubre que ha violado la privacidad de los datos o las regulaciones aplicables, sus credenciales podrían ser revocadas.

- ***Cese de contrato con proveedores o socios:*** Si se finaliza una relación con un proveedor externo o un socio comercial, es importante revocar sus credenciales para asegurarse de que ya no tengan acceso a los sistemas internos.

- ***Expiración de contraseña o certificado:*** En algunos casos, las credenciales pueden revocarse cuando las contraseñas o certificados asociados a ellas expiran y no se renuevan a tiempo.

- ***Pérdida o robo de dispositivos:*** Si un dispositivo que contiene credenciales se pierde o es robado, es necesario revocar las credenciales para prevenir el acceso no autorizado en caso de que el dispositivo sea comprometido.

- ***Sospecha de compromiso:*** Si hay sospechas creíbles de que las credenciales de un trabajador han sido comprometidas, es necesario revocarlas para evitar el acceso no autorizado por parte de un atacante.

- ***No cumplir con requisitos de auditoría o cumplimiento:*** Si una auditoría interna o externa revela que un usuario no cumple con los requisitos de seguridad y cumplimiento, sus credenciales podrían ser revocadas.

- ***Falta de uso:*** Si una cuenta de usuario ha estado inactiva durante un período prolongado y no se espera que vuelva a usarse, sus credenciales podrían ser revocadas para reducir la superficie de ataque.

6.3 Casos de reincidencia en incumplimiento

En caso de reincidencia al incumplir las políticas de seguridad de contraseñas, un trabajador podría enfrentar una serie de consecuencias, que podrían variar según la gravedad del incumplimiento y las políticas específicas de la empresa. Las posibles consecuencias podrían incluir:

- ***Reeducación y capacitación:*** Se brindará formación adicional sobre las políticas de seguridad de contraseñas y la importancia de seguir las mejores prácticas. A veces, la reincidencia puede ser el resultado de una falta de comprensión o de no estar al tanto de las políticas.

- ***Advertencia formal:*** Se emitirá una advertencia formal al trabajador, indicando claramente la importancia del cumplimiento de las políticas de seguridad de contraseñas y las consecuencias de la reincidencia.

- ***Entrevista con el usuario:*** Se sostendrá una conversación individual con el trabajador para comprender por qué se está produciendo la reincidencia y discutir los riesgos asociados con el incumplimiento de las políticas.

- ***Análisis de riesgos:*** Evaluar si la reincidencia ha expuesto sistemas o datos sensibles y determinar si es necesario tomar medidas correctivas adicionales.

- ***Suspensión temporal:*** En casos más graves, se considerará la suspensión temporal del acceso a sistemas y recursos hasta que el trabajador demuestre un compromiso más sólido con la seguridad.

- ***Restricción de acceso:*** Se podrá limitar temporalmente el acceso del trabajador a ciertos sistemas o datos sensibles para reducir el riesgo mientras se aborda la reincidencia.

- ***Cambiar las credenciales:*** Se requerirá al trabajador para que cambie su contraseña inmediatamente y utilice una nueva que cumpla con las políticas de seguridad.

- ***Notificación a la gerencia:*** Informar a la gerencia o a los superiores del trabajador sobre la reincidencia y las acciones tomadas para abordarla.

- ***Registro de incidente:*** Se documentará formalmente el incidente de reincidencia y las medidas tomadas para abordarlo. Esto con el fin de tener en cuenta en caso de futuras referencias y realizar un seguimiento al trabajador en cuanto al buen uso y aplicación de las políticas de seguridad de credenciales.

- ***Supervisión adicional:*** Se realizará un seguimiento más cercano de las actividades del trabajador en relación con las políticas de seguridad de contraseñas y brindar asistencia adicional si es necesario.

- ***Considerar acciones disciplinarias:*** Si la reincidencia continúa y representa un riesgo significativo para la seguridad, podrían ser necesarias medidas disciplinarias más serias, que podrían incluir sanciones, dependiendo de la gravedad y de las políticas de la empresa.

7. DESARROLLO DE LA POLÍTICA

1. Para mantener uniformidad en la asignación de credenciales, cada usuario será creado de la siguiente manera:
    a. Persona natural: El usuario estará compuesto por la inicial de su primer nombre, seguido de su apellido. Ejemplo: José Monserrate Feliciano García -> JFELICIANO
    b. Persona Jurídica: Nombre de la empresa
2. El administrador de cada sistema de información es responsable de asegurar que se solicite las credenciales de acceso (usuario y contraseña) para permitir el acceso.
3. El trabajador es responsable de asegurar la privacidad de las contraseñas asignadas para acceder a los sistemas de información.
4. Las credenciales de acceso para los diferentes sistemas de información son personal e intransferible.
5. El usuario de los sistemas de información es responsable de establecer una contraseña segura, que cumpla con las siguientes características:
    a. La longitud de la contraseña debe ser mínimo de 8 caracteres, entre más caracteres tenga la contraseña es más difícil de descifrar por algún delincuente informático (hacker.)
    b. Las aplicaciones en las cuales la tecnología utilizada no contemple una longitud mínima de ocho caracteres, la longitud mínima deberá ser la máxima contemplado por el sistema.
    c. La contraseña debe estar compuesta por una combinación de letras Mayúsculas, minúsculas, caracteres numéricos y símbolos especiales como los siguientes: ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /.

d. Hay que evitar utilizar secuencias básicas de teclado (por ejemplo: ”qwerty”, “asdf” o las típicas en numeración: “1234” ó “98765”)
e. No repetir los mismos caracteres en la misma contraseña. (ej.: “111222”).
f. No enviar nunca la contraseña por correo electrónico o en un sms. Tampoco se debe facilitar ni mencionar en una conversación o comunicación de cualquier tipo.
g. No deben usarse palabras o nombres comunes que aparezcan en los diccionarios.
h. No debe haber una relación obvia con el usuario, sus familiares, nombre de la entidad, abreviaciones relacionadas a la entidad, ciudad, país, año, fecha de nacimiento, el grupo de trabajo u otras asociaciones parecidas, ya que pueden ser identificadas de manera fácil a través de un ataque de ingeniería social.
i. Debe ser cambiada con una periodicidad de mínima de 90 días.
j. El administrador del sistema debe utilizar contraseñas diferentes como usuario y como administrador.
k. Si hay indicios para creer que una contraseña ha sido comprometida, debe cambiarse inmediatamente.
l. No deben usarse contraseñas que sean idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que sea posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores, esto se debe gestionar desde el sistema que asigne las credenciales.
m. Es responsabilidad del administrador de cada sistema establecer los mecanismos para que la contraseña asignada al usuario le sea transmitida de la manera más confidencial posible.
n. No se debe escribir la contraseña en papeles y dejarla en sitios donde pueda ser encontrada por terceros.
o. No se debe almacenar la contraseña en la computadora. Algunos cuadros de diálogo o ventanas emergentes de los navegadores presentan una opción para guardar o recordar la contraseña; no debe seleccionarse esa opción.
p. Las aplicaciones deben almacenar las contraseñas en forma cifrada.
q. Las contraseñas predefinidas que traen los equipos y aplicaciones, deben cambiarse inmediatamente al ponerse en operación.
r. Las contraseñas deben cambiarse cuando una persona que tiene acceso a cuentas privilegiadas compartidas, ya no hace parte de la entidad como colaborador.
s. Las credenciales asociadas a un usuario que se encuentre en vacaciones deberán ser inactivadas durante el periodo de vacaciones del colaborador.

6. Para los administradores de los sistemas de información, aplicaciones, equipos de infraestructura tecnológica, bases de datos se recomienda la creación de un usuario alterno o de contingencia con los privilegios mínimos de administración.

7. El usuario es responsable de bloquear su equipo en el momento en que se retire de su puesto de trabajo a una zona donde pierda visibilidad de este.
8. En el momento en que un usuario termina su vinculación laboral, contractual o convenio con ENERGUAVIARE S.A.S, se deben remover todos sus permisos en los sistemas de información y se debe desactivar el acceso del usuario a los mismos

8. CONTROL DE CAMBIOS

VERSIÓN N°	FECHA DE APROBACIÓN	DESCRIPCIÓN DEL CAMBIO	CONTROL OPERACIONAL
1	22/02/2024	CREACIÓN DEL DOCUMENTO	Acta N°03 del comité de CGC del 22/02/2024

	ELABORÓ	REVISÓ	APROBÓ
FIRMA	ORIGINAL FIRMADO	ORIGINAL FIRMADO	ORIGINAL FIRMADO
	ORIGINAL FIRMADO	ORIGINAL FIRMADO	
NOMBRE	JOSE LUIS ROJAS BOHÓRQUEZ	MARLON YOHAN LOPEZ SANCHEZ	Ing. CRISTIAN ANDREY PINTO LOZANO
	CAROLL JOHANA MUÑOZ CORTES	INGRID NATALI NOVOA PESCADOR	
CARGO	Profesional 01 sistemas	Director de Planeación	Gerente
	Técnico 04 sistemas	Profesional 01 Gestión de calidad	