	POLITICA	CÓDIGO:	TEC-POL-001
SERDAN Misión Temporal	SEGURIDAD DE LA INFORMACIÓN	VERSIÓN:	07
		FECHA:	07/02/2024
		PÁGINA:	1 de 1

APLICA PARA: SERDAN S.A. ☑ **MISIÓN TEMPORAL L.T.D.A.** ☑

La información es un recurso que tiene un alto valor para la organización y por consiguiente cada trabajador debe protegerla y velar por el cumplimiento de los pilares de seguridad de la información:

- **Confidencialidad:** Los trabajadores de la organización deben guardar la confidencialidad de la información manejada, la cual es propiedad de la empresa. Debe garantizar que la información sea accesible sólo a personas autorizadas, no compartirla con personas ajenas a la organización o que no estén involucradas en el proceso.

- **Integridad:** Los trabajadores de la organización deben garantizar que la información a la que tiene acceso sea correcta y confiable, en su proceso de creación tener exactitud en los datos registrados sin alteraciones, así como en su actualización y divulgación en los procesos que se involucra. No debe ser adulterada con datos inexactos o erróneos. Debe ser guardada la exactitud y totalidad.

- **Disponibilidad:** Los trabajadores de la organización deben garantizar que las personas autorizadas tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera, permitiendo su flujo normal al interior de los procesos de la misma.

Acceso sistemas de información: La cuenta de acceso es personal e intransferible, cada usuario debe tener su cuenta y está prohibido el préstamo de contraseñas. Los usuarios activos registrados en el sistema son responsables del manejo y administración de la cuenta. El sistema maneja un detallado registro de las actividades donde se capturan todos los datos de la conexión con nuestros servidores, las cuales estarán disponibles ante las autoridades competentes para reportar cualquier comportamiento. El trabajador signatario de este documento declara conocer y entender las políticas de seguridad vigentes publicadas en la Intranet de la organización y se compromete a seguirlas cuidadosamente en sus actividades durante su permanencia en la empresa.

Contraseñas: Una vez recibida la cuenta de acceso, debe cambiar inmediatamente la clave asignada por una combinación de caracteres (letras, números y carácter especial); esta deberá ser cambiada periódicamente mínimo cada 40 días. El usuario no debe guardar su contraseña en una forma legible en archivos electrónicos, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con el perfil de acceso y será responsable el titular de la misma. Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza son detectadas por el sistema y se consideran violatorias de las políticas de la organización, estas serán notificadas a las autoridades competentes.

Copias de seguridad: Los trabajadores de la organización deben mantener copias periódicas de la información sensible de la organización, para ello deben usar las carpetas compartidas del área, las cuales son respaldadas diariamente.

Uso seguro internet y correo: Los trabajadores de la organización deben comprender los riesgos externos que representan la navegación en internet, evitando el acceso a páginas de contenido peligroso, ocio, descarga de software, música o contenidos ilegales. Así mismo identificar amenazas conexas al correo electrónico, mensajes que pretendan capturar contraseñas de forma fraudulenta (Phising) y eliminar contenido publicitario no deseado (SPAM).

Así mismo identificar conductas de ingeniería social o espionaje dirigido a la organización, evitando revelar información confidencial o de reserva de los procesos de negocio de la organización.

En concordancia con lo anterior la Alta Dirección asegura la disponibilidad de los recursos y la revisión continua de la presente política.

Para constancia se firma el 07 de febrero de 2024 en la ciudad de Bogotá

ANA ROCIO SABOGAL HENAO
Representante Legal