	POLITICA	CÓDIGO:	TEC-POL-001
RED Servi	SEGURIDAD DE LA INFORMACIÓN	VERSIÓN:	02
		FECHA:	05/04/2023
		PÁGINA:	1 de 1

RED INTEGRADORA S.A.S, adquiere un compromiso total en la realización de actividades que brinden un ambiente de seguridad en el uso y protección de los sistemas de las tecnologías de la información.

Para garantizar el cumplimiento de los lineamientos establecidos por la organización con referencia al uso de las tecnologías de manera segura, nos apoyamos en los siguientes principios:

- **Confidencialidad:** Mantener la confidencialidad de la información utilizada en las actividades laborales, la cual es propiedad es la empresa. 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:** Garantizar el uso y acceso correcto y confiable, exactitud y fiabilidad de los datos compartidos o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada.

- **Disponibilidad:** Garantizar el acceso a la información y a los recursos relacionados a las tecnologías de la información de manera oportuna.

De acuerdo con lo anterior, la organización ha establecido los siguientes lineamientos de implementación a los controles operacionales:

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.

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 90 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. No deben usarse contraseñas empleadas anteriormente o similares y su uso debe ser personal.

Copias de Seguridad: Mantener copias periódicas de la información sensible de la organización, para ello deben usar la herramienta de respaldo OneDrive para tal fin, las cuales son respaldadas diariamente en la nube.

Uso Seguro Internet y Correo: Evitar el acceso a páginas de contenido peligroso, ocio, descarga de software, música o contenidos ilegales, identificar amenazas conexas al correo electrónico, mensajes que pretendan capturar contraseñas de forma fraudulenta (Phishing) y eliminar contenido publicitario no deseado (SPAM). Identificar conductas de ingeniería social o espionaje dirigido a la organización y reportar al equipo de tecnología, evitando revelar información confidencial o de reserva de los procesos de negocio de la compañía.

Esta política proporciona el marco de referencia para el establecimiento de los lineamientos y controles operacionales para el uso de las tecnologías de la información.

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

Se aprueba a los 5 días del mes de Abril de 2023

CLAUDIA PATRICIA GIL BENITEZ
Representante Legal