1. INFORMACIÓN GENERAL

ARENAS S.R.L. (en adelante "**ARENAS**") es una sociedad de responsabilidad limita dedicada a la fabricación de mallas para clasificación, módulos cerámicos antiabrasivos y a la comercialización de insumos químicos afines a la industria minera.

En apoyo a las operaciones de **ARENAS**, a través de las políticas de informática planteadas en el Plan Anual, y en busca de un ambiente confiable y resiliente, con un enfoque preventivo que se traduce en beneficios para nuestros directores y empleados, el área de sistemas ha establecido una estrategia de ciberseguridad, la cual es requerida por:

- La creciente importancia de las tecnologías de la información en la interoperación de las empresas.
- La existencia de amenazas y riesgos asociados al uso de las tecnologías e intercambio de información propiamente dicho.
- La necesidad de contar con una cultura de ciberseguridad adecuada por parte de todos los usuarios de **ARENAS**.

Es por ello que, la presente política y estrategia de ciberseguridad de **ARENAS** está alineadas con diversos marcos regulatorios que se mencionan en la Estrategia Nacional de Seguridad y Confianza Digital Peruana.

2. ALCANCE

La **POLÍTICA** se aplica para todos los usuarios y directores de **ARENAS**, sin excepción.

3. OBJETIVOS

- Crear una cultura de ciberseguridad en **ARENAS**.
- Proteger la información y la operación de **ARENAS** ante amenazas cibernéticas.
- Mantener la información institucional en un entorno seguro y protegido, asegurando su integridad y su confidencialidad.

4. USO CORRECTO DE USUARIOS Y CONTRASEÑAS

Las claves de acceso proporcionadas a un usuario deben considerarse información confidencial y personal, siendo el titular el único responsable de garantizar su buen uso, atendiendo a los siguientes principios:

- Responsabilidad: El usuario debe ejercer con responsabilidad los accesos y privilegios conferidos a su cargo por parte de **ARENAS**, como parte de su relación con la empresa.
- Respeto: Por las políticas y reglamentos de **ARENAS**, leyes de propiedad intelectual e industrial, en especial la Ley de Datos Personales.
- Confidencialidad: El acceso a la información será para quién tiene la autorización a ello.
- No Repudio: Evitar que una entidad, órgano o persona que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Asimismo, debe de cumplir con las siguientes políticas de uso:

- La responsabilidad del buen uso de usuario y contraseña será siempre del titular, por tanto, está prohibido compartir sus datos personales de acceso con un tercero.
- Está prohibido obtener y acceder a aplicaciones con las claves de acceso de otro usuario y/o tercero.
- No se permite instalar programas ajenos a los intereses de la empresa, así como emplear infraestructura o equipo de **ARENAS** para fines que no competen al que hacer de sus labores operativas, sin el conocimiento y la aprobación del área de sistemas de la empresa.
- El uso de equipos deberá alinearse en todo momento al Reglamento Interno del buen uso de la PC dispositivos y lugar de trabajo de **ARENAS**.
- Los equipos y licencias proporcionadas por **ARENAS** son de su propiedad, así como la información de la empresa a su cargo (ejemplo: información de clientes, información de proveedores, cotizaciones, productos, etc.).
- Es responsabilidad del usuario mantener a buen resguardo la información empresarial. Está prohibida la reproducción parcial y/o total de la información a la que se tenga acceso fuera del entorno de **ARENAS**.

Cualquier caso no previsto en la presente política, deberá ser canalizado por su inmediato superior e informar al área de sistemas de **ARENAS** para que sea resuelto acorde con las políticas y procedimientos internos.

5. USO CORRECTO DE LA INFORMACIÓN Y LOS EQUIPOS

Es importante respetar la infraestructura, licencias y equipos proporcionados por **ARENAS** con el fin de evitar afectaciones por malware, virus informáticos o incumplimiento de los términos de uso del software instalado.

Además, se debe de cumplir con las siguientes políticas de uso:

- Solo está permitido el uso de software institucional autorizado y debidamente licenciado.
- En caso de ocurrir una afectación derivada de una instalación prohibida de software, el usuario responsable por dicha instalación deberá asumir las consecuencias por los daños ocasionados.

6. LINEAMIENTOS PARA UNA CULTURA DE CIBERSEGURIDAD

La mayor protección ante amenazas cibernéticas radica en adoptar hábitos de seguridad que eviten que el usuario pueda verse afectado o que sufra la pérdida de información. Por tal motivo, se deben considerar los siguientes lineamientos:

- Evitar descargar material de fuentes de internet poco fiables.
- No proporcionar datos personales por medios electrónicos: **ARENAS** nunca solicitará datos por este medio.
- Evitar la instalación y uso de programas "piratas" obtenidos de manera ilegal.
- Emplear siempre el antivirus activo instalado por el área de sistemas de **ARENAS** en el equipo asignado.
- Mantener su equipo de trabajo actualizado con parches de seguridad.
  Dicha tarea es automatizada por la gestión de parches y vulnerabilidades With Secure XDR (firewall), junto con la supervisión del encargado del área de sistemas de **ARENAS**.
- En caso de pérdida de equipo, se deberá notificar a la empresa.

- La contraseña debe ser secreta, sólo el titular debe conocerla y nunca compartirla.
- La contraseña debe ser robusta: conformada por mayúsculas, minúsculas, números y caracteres especiales.
- No utilizar:
  - Patrones de teclado. Por ejemplo "qwerty".
  - Secuencias numéricas o alfabéticas. Por ejemplo, "12345678" o "abcdefg".
  - Palabras comunes o nombres propios.
  - Fechas especiales o cualquier dato que pueda asociarse con el titular. Por ejemplo: fechas de cumpleaños, aniversario, números telefónicos, entre otros.
- Cambiar la contraseña cada 90 días y no repetirla.
- Prestar especial atención cuando se accede desde lugares públicos y dentro de las instalaciones que tengan Wifi abierto.
- No utilizar la contraseña de las aplicaciones de la empresa en otros servicios o aplicaciones no relacionadas al ambiente laboral.
- Evitar almacenar contraseñas en medios impresos y digitales.
- Si accede desde algún computador no asignado, asegurarse de tener instalado un buen antivirus, recomendado por alguna institución reconocida como NSS Labs. https://www.cyberratings.org/
- Se recomienda escanear los dispositivos de almacenamiento USB Drives Discos extraíbles y mantenerlos actualizados.
- Se activará e implementará puntos de restauración de todos los equipos de la empresa.

7. MODIFICACIONES

La **POLÍTICA** ha sido actualizada el 29/01/2024 y podrá ser modificada unilateralmente por parte de **ARENAS**.

De producirse cualquier cambio o modificación de la **POLÍTICA**, el texto vigente de la misma será publicado en nuestro portal web: www.arenassrl.com.pe

ARENAS S.R.L.

MAURICIO GUSTAVO SAN MARTIN SAN MARTIN
APODERADO GENERAL

Mauricio Gustavo San Martín San Martín

Apoderado General