PIONONIK S.A.S.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código: POL-SI-001
Versión: 01
Fecha: Septiembre de 2026
Estado: Vigente

1. IDENTIFICACIÓN

Razón social: PIONONIK S.A.S.
NIT: 900.490.861-0
Dirección: Cll 75 No. 15 - 19 Of. 102, Bogotá D.C., Colombia
Correo: info@piononik.com
Teléfono: 313 237 0556
Web: www.piononik.com

---

2. OBJETIVO

Establecer los lineamientos para proteger la información de PIONONIK, sus clientes, empleados, contratistas, proveedores y demás partes interesadas.

La política busca garantizar:

Confidencialidad + Integridad + Disponibilidad

de la información.

---

3. ALCANCE

Aplica a:

- Empleados.
- Contratistas.
- Proveedores.
- Administradores de sistemas.
- Personal técnico.

- Usuarios de sistemas.
- Equipos corporativos.
- Equipos autorizados para actividades laborales.
- Servidores.
- Bases de datos.
- Aplicaciones.
- APIs.
- Servicios cloud.
- Correo electrónico.
- Sistemas de control de acceso.
- Dispositivos móviles.
- Redes.
- Copias de seguridad.

---

4. PRINCIPIOS

PIONONIK gestionará la seguridad de la información bajo los principios de:

Confidencialidad

La información solamente deberá estar disponible para personas autorizadas.

Integridad

La información deberá mantenerse completa, correcta y protegida contra modificaciones no autorizadas.

Disponibilidad

La información y los sistemas deberán estar disponibles cuando sean necesarios para la operación.

Trazabilidad

Cuando resulte técnicamente posible, las actividades relevantes deberán poder ser identificadas y registradas.

Mínimo privilegio

Cada usuario tendrá únicamente los permisos necesarios para desarrollar sus funciones.

---

5. CLASIFICACIÓN DE LA INFORMACIÓN

PIONONIK podrá clasificar la información como:

Clasificación	Descripción
Pública	Información autorizada para divulgación
Interna	Información destinada al uso organizacional
Confidencial	Información cuya divulgación puede afectar a PIONONIK o terceros
Restringida	Información crítica, sensible o de alto impacto

Ejemplos de información restringida:

- Contraseñas.
- Credenciales.
- Llaves de acceso.
- Bases de datos.
- Información biométrica.
- Configuraciones de seguridad.
- Información crítica de clientes.
- Información financiera.
- Código fuente.
- Configuración de servidores.
- Tokens y claves API.

---

6. CONTROL DE USUARIOS

Cada usuario deberá disponer de mecanismos de identificación individual cuando el sistema lo permita.

Se prohíbe:

- Compartir cuentas.
- Compartir contraseñas.
- Utilizar cuentas de terceros.
- Mantener usuarios activos de personas retiradas.
- Otorgar privilegios superiores a los necesarios.

Los accesos deberán ser retirados o modificados cuando cambien las funciones del usuario o termine su relación con PIONONIK.

---

7. CONTRASEÑAS

Las contraseñas deberán:

- Ser individuales.
- Ser confidenciales.
- Evitar información fácilmente deducible.
- No compartirse.
- No almacenarse en lugares inseguros.

Para sistemas críticos se procurará implementar autenticación multifactor cuando técnicamente sea posible.

---

8. CORREO ELECTRÓNICO

El correo corporativo deberá utilizarse de manera responsable.

Los usuarios deberán:

- Verificar remitentes.
- Evitar abrir archivos sospechosos.
- No entregar credenciales mediante enlaces desconocidos.
- Reportar mensajes sospechosos.
- Evitar reenviar información confidencial a cuentas personales.
- Utilizar medidas de protección disponibles.

---

9. WHATSAPP Y MENSAJERÍA

WhatsApp podrá utilizarse para coordinación operativa cuando PIONONIK lo haya autorizado.

No deberá utilizarse como repositorio permanente de:

- Contraseñas.
- Bases de datos completas.

- Información biométrica.
- Información financiera sensible.
- Credenciales de sistemas.
- Información crítica de seguridad.

Los usuarios deberán verificar cuidadosamente los destinatarios antes de enviar información.

---

10. DISPOSITIVOS

Los computadores y dispositivos utilizados para actividades corporativas deberán contar, según corresponda, con:

- Bloqueo de pantalla.
- Contraseña o autenticación.
- Actualizaciones.
- Antivirus o protección equivalente.
- Copias de seguridad cuando corresponda.
- Control de acceso.

La pérdida o robo de un dispositivo deberá reportarse inmediatamente.

---

11. SERVIDORES, BASES DE DATOS Y CLOUD

Los sistemas que almacenen información de PIONONIK deberán contar, según su criticidad, con:

- Control de acceso.
- Gestión de usuarios.
- Copias de seguridad.
- Actualizaciones.
- Monitoreo.
- Protección contra accesos no autorizados.
- Gestión de privilegios.
- Registro de actividades relevantes.

Los servicios cloud deberán ser evaluados según el nivel de riesgo y la información tratada.

---

12. APIs Y AUTOMATIZACIONES

Las APIs y automatizaciones deberán gestionarse bajo controles que protejan:

- Tokens.
- Claves.
- Credenciales.
- Variables de entorno.
- Bases de datos.
- Integraciones.

Las credenciales no deberán incorporarse directamente en código público o repositorios sin protección.

---

13. COPIAS DE SEGURIDAD

PIONONIK establecerá mecanismos de respaldo para información crítica.

Las copias deberán, según el riesgo:

- Realizarse periódicamente.
- Estar protegidas.
- Tener acceso restringido.
- Verificarse periódicamente.
- Mantenerse separadas de los sistemas principales cuando resulte apropiado.

Se deberán realizar pruebas periódicas de recuperación para los sistemas críticos.

---

14. INFORMACIÓN DE CLIENTES

La información de clientes deberá utilizarse exclusivamente para las actividades autorizadas.

Los colaboradores y contratistas no podrán:

- Copiar bases de datos.
- Extraer información innecesaria.
- Compartir información con terceros.
- Publicar información de proyectos.
- Compartir credenciales.
- Utilizar información para actividades personales o comerciales no autorizadas.

---

15. PROYECTOS Y REGISTROS FOTOGRÁFICOS

Antes de compartir fotografías de proyectos deberá verificarse que:

- No aparezcan credenciales.
- No aparezcan contraseñas.
- No aparezcan datos personales innecesarios.
- No se revelen configuraciones de seguridad.
- No se exponga información confidencial del cliente.
- La publicación tenga autorización cuando sea necesaria.

---

16. SISTEMAS DE CONTROL DE ACCESO

Los sistemas de control de acceso utilizados por PIONONIK deberán administrarse bajo principios de:

- Mínimo privilegio.
- Usuarios autorizados.
- Gestión de administradores.
- Protección de credenciales.
- Registro de actividades.
- Copias de seguridad cuando corresponda.

Cuando se utilicen datos biométricos, deberán aplicarse controles reforzados por su naturaleza sensible.

---

17. CONTRATISTAS

Los contratistas deberán recibir únicamente los accesos necesarios para ejecutar sus funciones.

Al finalizar el servicio deberá verificarse:

- Retiro de usuarios.

- Devolución de información.
- Devolución de dispositivos.
- Retiro de credenciales.
- Eliminación o devolución de información cuando corresponda.

---

18. INCIDENTES

Todo incidente deberá reportarse.

Se consideran incidentes:

- Pérdida de equipos.
- Robo.
- Malware.
- Ransomware.
- Phishing.
- Acceso no autorizado.
- Fuga de información.
- Publicación indebida.
- Eliminación accidental.
- Divulgación de contraseñas.
- Compromiso de cuentas.
- Fallas críticas de respaldo.

PIONONIK mantendrá un registro de incidentes y establecerá acciones correctivas según su impacto.

---

19. CONTINUIDAD

Para los sistemas críticos se deberán identificar mecanismos de continuidad y recuperación.

Los controles podrán incluir:

- Backups.
- Redundancia.
- Procedimientos de recuperación.
- Contactos de emergencia.
- Documentación técnica.
- Pruebas de recuperación.

---

20. CAPACITACIÓN

PIONONIK realizará actividades de sensibilización sobre:

- Protección de datos.
- Seguridad informática.
- Phishing.
- Contraseñas.
- Ingeniería social.
- Uso seguro del correo.
- Uso seguro de WhatsApp.
- Manejo de información confidencial.
- Reporte de incidentes.

---

21. INCUMPLIMIENTO

El incumplimiento de esta política podrá generar medidas administrativas, contractuales o laborales según corresponda y de acuerdo con la normativa aplicable y los documentos contractuales vigentes.

---

22. REVISIÓN

Esta política será revisada como mínimo anualmente o cuando se presenten:

- Cambios tecnológicos.
- Nuevos sistemas.
- Nuevos riesgos.
- Incidentes relevantes.
- Cambios organizacionales.
- Cambios normativos.

---

23. CONTROL DOCUMENTAL

Campo	Información
Código	POL-SI-001

Versión	01
Fecha	Septiembre de 2026
Elaboró	Responsable de Seguridad / Protección de Datos
Revisó	Dirección General
Aprobó	Representante Legal
Estado	Vigente

---

24. APROBACIÓN

PIONONIK S.A.S.
NIT 900.490.861-0

Representante Legal: _____

Firma: _____

Fecha: _____