

	POLITICA DE CIBERSEGURIDAD PARA SISTEMAS Y REDES INDUSTRIALES	TIT-2.0.0-PL-001	
		Página 1 de 8	Versión: 01
Proceso: TIT/OT		Sub-proceso:	

POLITICA DE CIBERSEGURIDAD PARA SISTEMAS Y REDES INDUSTRIALES

 OPERADA POR COLBUN	POLITICA DE CIBERSEGURIDAD PARA SISTEMAS Y REDES INDUSTRIALES	TIT-2.0.0-PL-001	
		Página 2 de 8	Versión: 01
Proceso: TIT./OT.		Sub-proceso:	

INDICE

1. OBJETIVO	3
2. ALCANCE.....	3
3. REFERENCIAS.....	3
4. DEFINICIONES.....	3
5. ROLES Y RESPONSABILIDADES.....	3
6. POLITICAS	4
6.1. Control de Acceso	4
6.2. Seguridad de Contraseñas.....	4
6.3. Trabajo Remoto de Terceros.....	5
6.4. Seguridad Perimetral.....	5
6.5. Protección contra Malware o Software Malicioso.....	6
6.6. Control de Cambios e Iniciativas	6
6.7. Gestión de copias de Respaldo	6
6.8. Análisis de Riesgo y Vulnerabilidades	6
6.9. Gestión de Incidentes de Seguridad.....	7
6.10. Gestión de la Continuidad del Negocio.....	7
6.11. Seguridad con Terceros.....	7
7. INCUMPLIMIENTOS	7
8. HISTORIAL DE CAMBIOS.....	8

 Fenix OPERADA POR COLBUN	POLITICA DE CIBERSEGURIDAD PARA SISTEMAS Y REDES INDUSTRIALES	TIT-2.0.0-PL-001	
		Página 3 de 8	Versión: 01
Proceso: TIT./OT.		Sub-proceso:	

1. OBJETIVO

Garantizar la seguridad de toda la infraestructura OT de Fénix a través del fortalecimiento de nuestras capacidades de prevención, defensa, detección, análisis, investigación, recuperación y respuesta a los ciberataques.

2. ALCANCE

Aplica a todas las aplicaciones y plataformas OT de Fenix.

3. REFERENCIAS

- Norma ISO/IEC 27001.
- Política de Seguridad de la Información.

4. DEFINICIONES

- **Análisis de Riesgo**
Uso sistemático de la información disponible para determinar cuán frecuentemente pueden ocurrir eventos específicos y la magnitud de sus consecuencias.
- **Ciberataque**
Explotación deliberada de sistemas informáticos, empresas y redes dependientes de la tecnología.
- **Confidencialidad**
Significa que, a los datos y a los sistemas solo accedan personas debidamente autorizadas y que la información por su sensibilidad no debe ser compartida ni divulgada a personas no autorizadas.
- **Disponibilidad**
Significa que la información y los sistemas pueden ser utilizados en la forma y tiempo requeridos por una entidad autorizada.
- **Integridad**
Significa exactitud de la información y de los sistemas contra alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.

5. ROLES Y RESPONSABILIDADES

- **PROVEEDOR**
Son responsables de la ciberseguridad de los activos de información a los cuales tienen acceso y tienen la obligación de cumplir todas las políticas,

	POLITICA DE CIBERSEGURIDAD PARA SISTEMAS Y REDES INDUSTRIALES	TIT-2.0.0-PL-001	
		Página 4 de 8	Versión: 01
Proceso: TIT./OT.		Sub-proceso:	

procedimientos y guías de Ciberseguridad implementados y publicados por el negocio, así como de asistir a los cursos de formación y actividades que se programen en materia de Ciberseguridad.

- **OFICIAL DE SEGURIDAD DE LA INFORMACION**

Esta política será revisada por lo menos una vez al año, o antes si algún evento o condición así lo amerita.

- **COLABORADOR**

Son responsables de la ciberseguridad de los activos digitales a los cuales tienen acceso y tienen la obligación de cumplir todas las políticas, procedimientos y guías de Ciberseguridad implementados y publicados por el negocio, así como de asistir a los cursos de formación y actividades que se programen en materia de Ciberseguridad.

6. POLITICAS

6.1. Control de Acceso

- La persona responsable de autorizar el acceso a un sistema o red industrial es el propietario de este. Por tal motivo, se debe contar con una lista de propietarios (lista de autorizantes).
- El propietario debe autorizar y canalizar el requerimiento de alta, baja o modificación, tanto del personal interno como del de terceros.
- El Gerente / Jefe / Supervisor o encargado de cada área debe revisar, por lo menos una vez al año, los derechos de acceso tanto del personal de planilla como del personal tercero que esté a su cargo.
- El usuario debe contar con un identificador único y ser responsable del uso de su contraseña, la cual es definida por él mismo.
- Sólo en circunstancias excepcionales y cuando sea estrictamente necesario para el desarrollo del trabajo, se permitirá el uso de identificadores genéricos, los mismos que deben ser aprobados por la Gerencia y deben estar documentados.
- Los equipos informáticos que brinden acceso a la infraestructura OT deben contar con los puertos USB bloqueados.

6.2. Seguridad de Contraseñas

- La asignación de contraseñas deberá ser controlada a través de un procedimiento formal.
- Las contraseñas de usuario deberán cumplir con los siguientes requisitos:
 - Tener como mínimo una longitud de 8 caracteres
 - Cumplir por lo menos con tres (3) características de complejidad:
 - Una mayúscula
 - Una minúscula

	POLITICA DE CIBERSEGURIDAD PARA SISTEMAS Y REDES INDUSTRIALES	TIT-2.0.0-PL-001	
		Página 5 de 8	Versión: 01
Proceso: TIT./OT.		Sub-proceso:	

- Un número
 - Un carácter especial (\$, #,&,@,etc.)
 - No usar contraseñas de fácil reconocimiento tales como: \$abc1234, Inicio\$1, fechas especiales, nombres, entre otras.
 - Cumplir que se exija cambiar la contraseña al primer ingreso del usuario en el sistema.
 - Tener una vigencia máxima de 90 días.
 - A los 05 intentos fallidos de ingreso de contraseñas, la cuenta del usuario se bloqueará.
- c. Las contraseñas de usuario deberán cumplir con los siguientes requisitos:
- Tener como mínimo una longitud de 15 caracteres
 - Cumplir por lo menos con estas características de complejidad:
 - Una mayúscula
 - Una minúscula
 - Un número
 - Un carácter especial (\$, #,&,@,etc.)
 - Tener una vigencia máxima de 90 días.
 - Las cuentas de administradores de sistemas (Ejemplo: admin, root, etc.) deben guardarse en un sobre lacrado (sellado), y ser custodiadas por Seguridad de la Información.
- d. No se deben compartir las contraseñas de los recursos, servicios o sistemas de información.

6.3. Trabajo Remoto de Terceros

- a. Se debe ejecutar mecanismos de autenticación robusta, como mínimo a través de un VPN.
- b. En caso no pueda realizarse bajo esa modalidad, toda conexión remota de un proveedor a equipos OT para soporte o mantenimiento, debe ser a través de canales seguros y licenciados. Nunca debe realizarse a través de softwares gratuitos.

6.4. Seguridad Perimetral

- a. Se debe asegurar que entidades no autorizadas no tengan acceso a la red.
- b. Se debe contar con firewalls perimetrales que protejan la red industrial de otras redes.
- c. La red industrial y la red corporativa pueden coexistir en un modelo de convivencia siempre que estas redes estén debidamente segmentadas y configuradas.
- d. Se debe mantener el mínimo acceso permitido de las redes industriales hacia Internet.

	POLITICA DE CIBERSEGURIDAD PARA SISTEMAS Y REDES INDUSTRIALES	TIT-2.0.0-PL-001	
		Página 6 de 8	Versión: 01
Proceso: TIT./OT.		Sub-proceso:	

- e. Se debe realizar un monitoreo de actividades anómalas externas a través de un SIEM para coleccionar eventos.
- f. Se debe realizar un monitoreo de las actividades internas a través de plataformas de monitoreo de tráfico interno.
- g. Implementar el protocolo IEC-62443 para el diseño de zonas, conductos y canales según los estándares de ciberseguridad.
- h. Contar con certificación SIL (Safety Integrity Level) en procesos industriales.

6.5. Protección contra Malware o Software Malicioso

- a. Implementar un sistema de antivirus centralizado y que sea actualizado regularmente, el cual tenga programado rutinas de escaneo programadas en los sistemas y plataformas industriales.

6.6. Control de Cambios e Iniciativas

- a. Mantener constantemente actualizado, el software y hardware de las plataformas que forman parte del ambiente industrial
- b. Se debe contar con un proceso de control de cambios en los sistemas, infraestructura y equipos de OT, el cual incluya mínimo un Comité de Cambios que realice un análisis de impacto y riesgo del cambio, y una especificación de los controles de seguridad necesarios.
- c. Toda iniciativa o proyecto que contemple la implementación o adquisición de un servicio, sistema o software OT, debe contar con la participación de Seguridad de la Información desde la concepción del requerimiento hasta su despliegue a fin de cumplir con los requisitos mínimos de seguridad de la información.

6.7. Gestión de copias de Respaldo

- a. Se debe realizar copias de respaldo de los sistemas y redes industriales de forma periódica en concordancia con las políticas establecidas por el propietario de la información, a fin de minimizar la pérdida de información crítica ante interrupciones o incidencias en los sistemas. Asimismo, se deberán realizar pruebas de restauración al menos una vez al año.
- b. Los medios de respaldo deben almacenarse en una locación geográficamente segura aislada de riesgos ambientales, y distante del servidor principal del cual se respaldó la información.

6.8. Análisis de Riesgo y Vulnerabilidades

- a. Se deben identificar y evaluar los riesgos a los cuales están expuestos los sistemas y redes industriales por lo menos una (01) vez al año o ante un cambio significativo en tecnología o arquitectura.

 Fenix OPERADA POR COLBUN	POLITICA DE CIBERSEGURIDAD PARA SISTEMAS Y REDES INDUSTRIALES	TIT-2.0.0-PL-001	
		Página 7 de 8	Versión: 01
Proceso: TIT./OT.		Sub-proceso:	

- b. Se debe realizar, por lo menos una (01) vez al año, un análisis de vulnerabilidades y ethical hacking sobre los sistemas y redes de industriales, que permitan identificar vulnerabilidades que expongan al negocio a ataques externos o internos.

6.9. Gestión de Incidentes de Seguridad

- a. Se debe contar con un proceso de gestión de incidentes de seguridad documentado, en el cual se establezcan los pasos a seguir para reportar, escalar, investigar la causa y definir las acciones correctivas del incidente de seguridad (eventos y vulnerabilidades de la seguridad de la información).
- b. Promover las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación contra incidentes y actividades del cibercrimen.

6.10. Gestión de la Continuidad del Negocio

- a. Se debe contar con un Plan de Continuidad del Negocio y un Plan de Recuperación ante Desastres aprobados por la Alta Gerencia, los cuales deberán ser revisados y actualizados periódicamente según lo definido por el negocio.
- b. Se debe contar con ambientes de contingencia y desarrollo.

6.11. Seguridad con Terceros

- a. Los contratos con terceros deberán contemplar cláusulas de confidencialidad, protección de datos personales y antifraude con las empresas contratadas y sus funcionarios, para el manejo de los sistemas y redes industriales del negocio y/o uso de su propiedad intelectual.
- b. Deben ser consideradas penalidades y cláusulas de rescisión del contrato por incumplimiento a alguno de los lineamientos establecidos en el presente documento y en la Política de Seguridad de la Información.

7. INCUMPLIMIENTOS

En caso de incumplimiento de esta Política se podrán aplicar sancione estipuladas en el Reglamento Interno de Trabajo de la compañía.

 OPERADA POR COLBUN	POLITICA DE CIBERSEGURIDAD PARA SISTEMAS Y REDES INDUSTRIALES	TIT-2.0.0-PL-001	
		Página 8 de 8	Versión: 01
Proceso: TIT./OT.		Sub-proceso:	

8. HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	NUMERAL MODIFICADO	DESCRIPCIÓN DEL CAMBIO
01	13/04/2020	NA	Documento Nuevo

Elaborado por:	Revisado por:	Aprobado por:	Fecha de Vigencia:
Angel Aldave Coordinador de TI	Sebastian Celis Oficial de Seguridad de la Información Angel Aldave Coordinador de TI Oscar Rivera Supervisor de Mantenimiento I&C	Juan Miguel Cayo Gerente General Dante Olcese Gerente de Administración y Finanzas Alejandro Galarza Gerente de Planta	13/04/2021