1. PROPOSITO

1.1 Esta política establece los principios, lineamientos y responsabilidades en materia de ciberseguridad con el objetivo de proteger la información, los activos digitales y los sistemas tecnológicos de la compañía. La ciberseguridad es un pilar esencial para asegurar la continuidad del negocio, prevenir incidentes y proteger a nuestros colaboradores, clientes y socios.

1.2 Esta política se fundamenta en el marco normativo y operativo de Tecnologías de la Información (TI) establecido por la compañía. Las políticas específicas de TI proporcionan lineamientos y controles detallados que refuerzan y complementan esta política de ciberseguridad. La lista de estas políticas se incluye en el apartado de Referencias

2. ALCANCE

2.1 Esta política es aplicable a todos los empleados de GCC, así como contratistas, proveedores y terceros que interactúan directa o indirectamente con los sistemas informáticos e información de la organización, en todas nuestras ubicaciones.

3. RESPONSABLE

3.1 Gerente / Supervisor: Responsable de asegurar que su equipo conozca y cumpla la política, identificar necesidades de capacitación y reporte oportuno de incidentes.

3.2 Madata / Comité de TI (responsable de Ciberseguridad): Diseñar, coordinar y supervisar la implementación de controles, programas y reportes asegurando el cumplimiento de la política, así como tomar decisiones clave ante incidentes críticos.

3.3 Todos los Usuarios Deben cumplir estrictamente esta política, asistir a capacitaciones, mantener prácticas seguras en sus actividades diarias, y reportar inmediatamente incidentes o situaciones sospechosas.

4. DEFINICIONES

4.1 Ciberseguridad: Conjunto de prácticas, tecnologías y procesos destinados a proteger sistemas, redes, programas y datos frente a ataques, daños o accesos no autorizados.

4.2 Activo de información: Todo recurso que almacene, procese o transmita información.

4.3 Incidente de seguridad: Evento que compromete la confidencialidad, integridad o disponibilidad de la información.

4.4 SIEM: Sistema de Gestión de Eventos e Información de Seguridad que permite detectar y responder a amenazas en tiempo real.

4.5 Terceros: contratistas, proveedores y terceros que tengan acceso a la información o los sistemas de la compañía.

5. CONTENIDO

5.1 En GCC estamos comprometidos con la protección integral de nuestra información y sistemas tecnológicos contra riesgos cibernéticos, los siguientes principios representan los fundamentos que guían nuestra postura organizacional frente a la ciberseguridad. Son las ideas rectoras sobre las cuales se diseñan los controles y procedimientos:

5.2 Protección Integral: Asegurar la confidencialidad, integridad y disponibilidad de la información, considerando la infraestructura de TI.

5.3 Gestión de Riesgos: Aplicar un enfoque sistemático basado en ISO/IEC 27001 y NIST para identificar, evaluar, tratar y monitorear los riesgos cibernéticos.

5.4 Gobernanza Activa: Garantizar la participación de la alta dirección mediante la aprobación formal de esta política y revisiones periódicas, asignando responsabilidades específicas.

5.5 Conciencia y Capacitación: Desarrollar competencias mediante programas de formación continua, simulacros de ataques, campañas de comunicación y refuerzo del comportamiento seguro.

5.6 Controles Técnicos y Organizacionales: Implementar medidas como cifrado, gestión de accesos, autenticación multifactorial, firewalls, antivirus, segmentación de redes y respaldo de datos.

5.7 Respuesta a Incidentes: Contar con un plan formalizado de respuesta y recuperación ante incidentes de seguridad, incluyendo notificación, contención, investigación, recuperación y lecciones aprendidas.

5.8 Auditoría y Mejora Continua: Realizar auditorías internas y externas, evaluaciones de vulnerabilidades y pruebas de penetración de manera periódica para validar la eficacia de los controles.

5.9 Cumplimiento Normativo: Asegurar el cumplimiento de las leyes locales y marcos internacionales de referencia (ej. ISO/IEC 27001, NIST CSF, IEC 62443).

5.10 Lineamientos Generales Estos lineamientos definen las acciones prácticas que deben seguirse para cumplir con los principios definidos:

1. Mantener un inventario actualizado y clasificado de activos digitales.
2. Aplicar parches y actualizaciones en tiempo y forma.
3. Controlar accesos mediante principios de mínimo privilegio.
4. Segmentar redes entre entornos TI y OT.
5. Monitorear eventos y alertas a través de herramientas SIEM.
6. Realizar simulacros de phishing y ejercicios de concientización.
7. Mantener respaldos protegidos y realizar pruebas de restauración.
8. Establecer métricas y reportes de indicadores clave.

5.11 Políticas específicas:

5.11.1 Gestión de accesos y contraseñas: Las contraseñas deben tener mínimo 12 caracteres, incluyendo letras, números y símbolos, es obligatorio cambiar contraseñas cada 90 días. Se utilizará autenticación multifactorial para accesos críticos. (Se prohíbe el compartir contraseñas).

5.11.2 Protección de información sensible: Toda información sensible deberá almacenarse y transmitirse con cifrado.

5.11.3 Control sobre software: Está prohibida la instalación de software no autorizado o ilegal.

5.11.4 Uso Adecuado de Recursos Tecnológicos - Está estrictamente prohibida la instalación de software no autorizado o ilegal. - El acceso a internet está limitado a actividades laborales. - Prohibido conectar dispositivos externos no autorizados a la red corporativa.

5.11.5 Concienciación y Capacitación
- Todo el personal debe participar obligatoriamente en capacitaciones sobre ciberseguridad.
- Se realizarán simulaciones periódicas de ataques como phishing para evaluar y mejorar la respuesta del personal.
- Habrá comunicación constante sobre nuevas amenazas y mejores prácticas mediante boletines informativos y talleres.

5.11.6 Gestión de Incidentes - Ante un incidente, se debe reportar inmediatamente al Service Desk de TI.
- Se seguirán protocolos estrictos alineados con estándares internacionales para contener y resolver el incidente rápidamente.
- Habrá comunicación clara y oportuna sobre el estado y resolución del incidente hacia todas las partes afectadas.

6. CONSECUENCIAS POR INCUMPLIMIENTO.

6.1 Cualquier incumplimiento de esta política será manejado según la Matriz de Consecuencias establecida por GCC, que contempla desde advertencias escritas y capacitaciones adicionales hasta sanciones mayores como suspensión temporal o terminación inmediata del empleo, dependiendo de la gravedad del incidente.

7. REFERENCIAS

- ISO/IEC 27001:2013
- NIST Cybersecurity Framework
- IEC 62443
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México)
- PO-DTI-TI-01 Administración de la Red Computacional
- PO-DTI-TI-03 Uso del Correo Electrónico
- PO-DTI-TI-06 Adquisición de Recursos Tecnológicos
- PO-DTI-TI-09 Instalación y Uso de Mensajería Instantánea
- PO-DTI-TI-10 Asignación de Identificación de Usuario
- PO-DTI-TI-16 Retención de la Información
- PO-DTI-TI-17 Administración de Cambios
- PO-DTI-TI-18 Coordinación de Implementación de Cambios
- PO-DTI-TI-20 Administración de Niveles de Servicio
- PO-DTI-TI-21 Administración de Problemas
- PO-DTI-TI-22 Fuente de Solicitud de Servicios a AM
- PO-DTI-TI-23 Soporte de Operación Diaria – Help Desk (Altiris)
- PO-DTI-TI-26 POLITICA GESTIÓN Y PROTECCIÓN DE LA INFORMACIÓN SENSBILE
- PO-DTI-TI-27 Aprovisionamiento y Remoción de Usuarios
- PO-DTI-TI-28 Control de Acceso a Proveedores
- PO-DTI-TI-29 Control de Acceso al Centro de Datos
- PO-DTI-TI-30 POLITICA DE USO DE INTELIGENCIA ARTIFICIAL (IA)
- PO-DTI-TI-31 Contraseñas

- PO-DTI-TI-32 Control sobre Software Licenciado Autorizado No Autorizado.
- PO-DTI-TI-34 Copias de Seguridad de Servidores
- PO-DTI-TI-35 Gestión de Equipo de Cómputo
- PO-DTI-TI-36 Encriptación de Información en Activos Usuario Final
- PO-DTI-TI-37 Control de Desarrollos o Modificaciones de Software
- PO-DTI-TI-39 Uso de los Servicios de Mensajería Instantánea
- PO-DTI-TI-40 Política para el Uso de Herramientas de Doble Autenticación
- PO-DTI-TI-41 Gestión de Incidentes de Seguridad
- PO-DTI-TI-42 Trae tu Recurso Tecnológico (BYOD)
- PO-DTI-TI-45 Administración de la Red de GCC
- PO-DTI-TI-46 Instalación y Uso de VPN
- PO-DTI-TI-49 Clasificación de la Información
- PO-DTI-TI-51 Seguridad en Dispositivos Móviles
- PO-DTI-TI-53 ADQUISICIÓN Y ASIGNACIÓN DE RECURSOS TECNOLÓGICOS

8. ANEXOS

Anexo 1. Tabla de Trazabilidad entre Política de Ciberseguridad y Políticas de TI

Sección de esta Política	Políticas de TI Relacionadas
5.1 Protección Integral	PO-DTI-TI-01, PO-DTI-TI-45, PO-DTI-TI-41, PO-DTI-TI-46
5.2 Gestión de Riesgos	PO-DTI-TI-26, PO-DTI-TI-49
5.3 Gobernanza Activa	PO-DTI-TI-20, PO-DTI-TI-30
5.4 Conciencia y Capacitación	PO-DTI-TI-03, PO-DTI-TI-09, PO-DTI-TI-39
5.5 Controles Técnicos	PO-DTI-TI-06, PO-DTI-TI-17, PO-DTI-TI-01, PO-DTI-TI-10, PO-DTI-TI-27, PO-DTI-TI-31, PO-DTI-TI-42, PO-DTI-TI-51, PO-DTI-TI-40, PO-DTI-TI-47, PO-DTI-TI-46, PO-DTI-TI-29
5.6 Respuesta a Incidentes	PO-DTI-TI-41, PO-DTI-TI-21
5.7 Auditoría y Mejora	PO-DTI-TI-17, PO-DTI-TI-18, PO-DTI-TI-37
5.8 Cumplimiento Normativo	PO-DTI-TI-32, PO-DTI-TI-07, PO-DTI-TI-35, PO-DTI-TI-26
5.9 Lineamientos Generales	PO-DTI-TI-16, PO-DTI-TI-49, PO-DTI-TI-34, PO-DTI-TI-36, PO-DTI-TI-22, PO-DTI-TI-23, PO-DTI-TI-28, PO-DTI-TI-20, PO-DTI-TI-53

9. TABLA DE REVISIONES DEL DOCUMENTO

No de Revisión	Fecha	Descripción del Cambio

0	Junio 2025	Documento Original

10. AUTORIZACIONES

Elaboró	Revisó	Autorizó
	Maria Elena Rojas/Control Interno	Ramón Velazco Unzueta/Contralor Corporativo