

Manual de Políticas de Ciberseguridad y Tecnologías de la Información

Directrices obligatorias para la protección de activos digitales, infraestructura de red y manejo de información confidencial.

1. POLÍTICA DE AUTENTICACIÓN, CONTRASEÑAS Y ACCESOS

El acceso a los sistemas corporativos, estaciones de trabajo, cuentas de correo y consolas en la nube está estrictamente regulado bajo el principio de menor privilegio (Least Privilege).

- Longitud y Complejidad Mínima:** Toda contraseña corporativa debe tener al menos catorce (14) caracteres alfanuméricos, incluyendo al menos una mayúscula, una minúscula, un número y un símbolo especial (@, #, \$, %).
- Autenticación Multifactor (MFA Obligatorio):** Es obligatorio activar el segundo factor de autenticación mediante aplicación autenticadora (Google Authenticator o Microsoft Authenticator) para todas las cuentas de correo institucional, accesos VPN y plataformas SaaS.
- Bloqueo Automático de Sesión:** Todo equipo de cómputo debe configurarse con bloqueo automático tras tres (3) minutos de inactividad. El usuario es responsable de cualquier actividad realizada mientras su sesión permanezca abierta.
- Prohibición de Compartir Credenciales:** Las credenciales son personales e intransferibles. Queda terminantemente prohibido anotarlas en papel, compartirlas por mensajería o guardarlas en navegadores sin cifrar.

2. CONEXIONES REMOTAS, VPN Y EQUIPOS MÓVILES (BYOD)

Para garantizar la integridad del tráfico institucional durante el trabajo remoto o híbrido, se establecen los siguientes requisitos de conexión:

- Uso Exclusivo de VPN Corporativa:** Cualquier acceso a bases de datos, repositorios de código, servidores de archivos o paneles administrativos fuera de las instalaciones físicas debe canalizarse mediante el túnel VPN cifrado con protocolo WireGuard o IPsec.
- Prohibición de Redes Wi-Fi Públicas Abiertas:** Queda prohibido conectarse a servidores de la empresa desde redes Wi-Fi públicas de cafeterías, aeropuertos u hoteles sin la protección activa de la VPN institucional.
- Dispositivos Personales (BYOD):** Los dispositivos móviles personales autorizados para consultar correo corporativo deben tener habilitado cifrado de disco completo, código de bloqueo biométrico y aceptar la administración remota de borrado selectivo de datos empresariales en caso de extravío.

3. CLASIFICACIÓN Y MANEJO DE INFORMACIÓN CONFIDENCIAL

Toda información generada o almacenada en los sistemas se categoriza en cuatro niveles de sensibilidad:

NIVEL	DESCRIPCIÓN	MEDIDAS DE SEGURIDAD OBLIGATORIAS
1. Pública	Material de marketing, comunicados de prensa, sitio web.	Divulgación libre sin restricciones.
2. Interna	Minutas de trabajo, directorios telefónicos, políticas operativas.	Acceso exclusivo para empleados activos; no compartir externamente.
3. Confidencial	Datos de clientes, contratos, estados financieros, nómina.	Cifrado en tránsito y reposo; acceso restringido por rol con registro de auditoría.
4. Restringida	Llaves criptográficas, credenciales maestras de bases de datos, código fuente clave.	Aprobación previa de Dirección; almacenamiento en bóvedas de seguridad con MFA estricto.

4. PROTOCOLO DE RESPUESTA A INCIDENTES DE SEGURIDAD (CSIRT)

Un incidente de seguridad se define como cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de los sistemas o datos corporativos. Ante cualquier anomalía, el colaborador debe activar el protocolo inmediato de 4 fases:

FASE 1: DETECCIÓN	Identificación de comportamientos inusuales: correos sospechosos con archivos adjuntos no solicitados (phishing), ventanas emergentes de extorsión (ransomware) o degradación repentina de red.
FASE 2: AISLAMIENTO	Acción inmediata del usuario: Desconectar el cable de red Ethernet y desactivar la conexión Wi-Fi de inmediato. <u>Bajo ninguna circunstancia apagar el equipo</u> , ya que la memoria RAM contiene evidencia forense volátil.
FASE 3: NOTIFICACIÓN	Reportar en un plazo máximo de quince (15) minutos al Centro de Operaciones de Seguridad (SOC / Mesa de TI) vía teléfono directo de emergencias (+52 55-6737-1417) o canal de Telegram de alertas críticas.
FASE 4: MITIGACIÓN	El equipo de TI procederá a la contención del host, revocación inmediata de tokens de sesión, análisis de bitácoras y restauración de servicios desde respaldos inmutables libres de infección.

5. POLÍTICA DE COPIAS DE SEGURIDAD (BACKUP) Y RECUPERACIÓN

Para evitar la pérdida irreversible de información ante desastres o ataques cibernéticos, la empresa implementa la estrategia de respaldo 3-2-1:

- **Estrategia 3-2-1:** Se mantienen tres (3) copias de los datos críticos, en dos (2) soportes tecnológicos distintos (almacenamiento en disco local de alta velocidad y servidores NAS dedicados), con al menos una (1) copia ubicada fuera del sitio físico en almacenamiento cloud inmutable (S3 Object Lock).
- **Frecuencia y Pruebas de Restauración:** Los respaldos incrementales de bases de datos se ejecutan cada cuatro (4) horas y los respaldos completos de servidores de forma semanal. Semestralmente se realizan simulacros de recuperación total en entornos aislados de prueba.

6. AUDITORÍAS, MONITOREO Y SANCIONES DISCIPLINARIAS

El uso de las herramientas de TI es monitoreado de forma automatizada para garantizar la seguridad perimetral y el cumplimiento normativo:

- **Monitoreo de Red:** El departamento de TI cuenta con sistemas de detección de intrusiones (IDS/IPS) y análisis de registros para detectar transferencias de datos masivas no autorizadas o conexiones a direcciones IP maliciosas.
- **Consecuencias del Incumplimiento:** La violación de las directivas de seguridad estipuladas en este manual (incluyendo la divulgación de contraseñas, instalación de software no autorizado o extracción de bases de datos confidenciales) constituirá causa de rescisión justificada de la relación laboral conforme al Artículo 47 de la Ley Federal del Trabajo, sin perjuicio de las responsabilidades civiles y penales correspondientes por revelación de secretos industriales.

COMPROMISO DE CUMPLIMIENTO DEL COLABORADOR:

He leído, comprendido y aceptado las políticas de seguridad de TI descritas en este documento. Me comprometo a observar estrictamente estas directrices en el desempeño diario de mis funciones.

Firma del Colaborador / Fecha