ETERNA DIGITALCOM MÉXICO, S.A. DE C.V.

POLÍTICA DE SEGURIDAD DE LA PLATAFORMA

Controles generales para la operación segura y continua de servicios digitales

Código documental	EDM-CMP-002
Versión	1.0
Fecha de emisión	Julio de 2026
Última revisión	Julio de 2026
Próxima revisión	Julio de 2027
Clasificación	Documento corporativo de consulta pública

Este documento establece lineamientos generales aplicables a los servicios digitales de Eterna Digitalcom México. No constituye certificación técnica ni sustituye obligaciones contractuales o legales específicas de proveedores externos.

Índice

1. Objeto

Definir lineamientos generales para proteger la confidencialidad, integridad, disponibilidad y trazabilidad de la plataforma, sitios, cuentas, paneles, automatizaciones y herramientas digitales operadas o administradas por Eterna.

2. Alcance

Aplica a infraestructura, aplicaciones, sitios, bases de datos, cuentas administrativas, dispositivos, servicios en nube, integraciones y proveedores tecnológicos utilizados para prestar servicios digitales.

3. Principios de seguridad

- Defensa proporcional al riesgo.
- Acceso mínimo necesario.
- Separación razonable de funciones.
- Actualización y mejora continua.
- Registro de eventos relevantes.
- Recuperación ante fallas.
- No afirmar certificaciones que no se hayan obtenido.

4. Gobierno y responsabilidades

La Dirección General aprueba lineamientos y prioridades. Las personas con acceso administrativo deben usar las credenciales exclusivamente para fines autorizados y reportar anomalías. Los proveedores se sujetarán a sus contratos y a sus propios controles de seguridad.

5. Control de acceso

5.1 Altas y bajas

- Los accesos se habilitan según función.
- Los permisos deben revocarse o ajustarse cuando cambie la relación o responsabilidad.

5.2 Credenciales

- Contraseñas robustas y únicas.
- Autenticación multifactor cuando esté disponible y resulte adecuada.
- Prohibición de compartir credenciales.
- Revisión de accesos privilegiados.

6. Infraestructura y comunicaciones

- Uso de HTTPS/TLS en sitios y transmisiones compatibles.
- Servicios de alojamiento y nube con controles acordes a su función.
- Configuraciones restrictivas por defecto cuando sea viable.

- Segmentación lógica o separación de entornos cuando la arquitectura lo permita.
- Protección de secretos, llaves y credenciales de integración.

7. Desarrollo, configuración y cambios

Los cambios relevantes deben evaluarse, documentarse y, cuando sea viable, probarse antes de su liberación. Las integraciones de terceros se limitarán a permisos necesarios. Las configuraciones temporales deberán revisarse para evitar que permanezcan abiertas de forma innecesaria.

8. Respaldo y recuperación

La frecuencia y alcance de respaldos dependerán de la criticidad, volumen y naturaleza de cada servicio. Los respaldos no garantizan recuperación absoluta; se procurará verificar periódicamente su disponibilidad y conservar copias por plazos razonables.

9. Monitoreo y registros

Eterna podrá registrar accesos, errores, eventos administrativos y transacciones para diagnóstico, prevención de fraude, soporte y seguridad. El acceso a registros se limita a personal o proveedores autorizados y su conservación se ajusta a necesidades operativas y legales.

10. Gestión de vulnerabilidades

Se procurará mantener software y dependencias actualizados, priorizar vulnerabilidades relevantes y aplicar correcciones conforme al riesgo y disponibilidad. Los reportes de vulnerabilidades deberán enviarse de buena fe a seguridad@eternadigitalcom.mx, sin explotación, alteración o acceso no autorizado.

11. Gestión de incidentes

- Detección y registro.
- Contención inicial.
- Análisis de alcance e impacto.
- Preservación de evidencia.
- Recuperación y corrección.
- Comunicación a usuarios o autoridades cuando resulte legalmente exigible.
- Revisión posterior y acciones preventivas.

12. Continuidad y disponibilidad

Eterna procura mantener la disponibilidad, pero no garantiza operación ininterrumpida. Podrán existir mantenimientos, fallas, ataques, errores, interrupciones de proveedores o eventos de fuerza mayor. Cuando sea posible, se comunicarán mantenimientos relevantes y se priorizará la restauración de servicios críticos.

13. Proveedores tecnológicos

Los servicios pueden depender de proveedores de nube, dominios, correo, analítica, telecomunicaciones, autenticación, pagos y software. Eterna evaluará de manera razonable su idoneidad, sin asumir control sobre sus redes, políticas o disponibilidad.

14. Responsabilidades del usuario

- Mantener actualizados sus datos y dispositivos.
- No compartir contraseñas ni códigos.
- Cerrar sesión en equipos compartidos.
- No intentar vulnerar, escanear, saturar o eludir controles.
- Reportar accesos o actividades no reconocidas.

15. Limitaciones y contacto

Esta política describe controles generales y no constituye garantía absoluta, certificación ISO, SOC, PCI u otra acreditación. Contacto de seguridad: seguridad@eternadigitalcom.mx. Soporte: soporte@eternadigitalcom.mx. Vigente desde julio de 2026.

Control de cambios

Versión	Fecha	Descripción	Responsable
1.0	Julio 2026	Emisión inicial	Dirección General