POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

GOBERNANZA TECNOLÓGICA E INFRAESTRUCTURA DIGITAL

Entorno Corporativo:	Plataforma Web e Infraestructura de Servidores
Ámbito de Aplicación:	linkadvance.cl y Sistemas Conectados
Versión de Política:	1.4 (Abril 2026)
Estándar de Referencia:	Buenas Prácticas Basadas en la Norma ISO/IEC 27001

1. Objetivo y Alcance

La presente Política de Seguridad establece las directrices, medidas técnicas y protocolos organizacionales implementados por Link Advance para salvaguardar la confidencialidad, integridad y disponibilidad de la infraestructura digital, bases de datos y la información gestionada a través del dominio linkadvance.cl.

Esta política aplica rigurosamente a todos los componentes de hardware, capas de software, procesos automatizados, flujos de integración de datos, así como al personal técnico y consultores externos con acceso a los sistemas de administración del sitio.

2. Pilares de Seguridad Tecnológica

Nuestra estrategia de seguridad se fundamenta en mitigar los riesgos digitales de manera proactiva, estructurándose en tres pilares esenciales:

C — **Confidencialidad:** Garantizar que la información y los datos recolectados sean accesibles única y exclusivamente por el personal técnico debidamente autorizado y autenticado.

I — **Integridad:** Proteger la exactitud, consistencia y totalidad dela información frente a modificaciones noautorizadas, corrupciones dearchivos o inyecciones maliciosas de código.

D — **Disponibilidad:** Asegurar que la plataforma web linkadvance.cl y sus canales técnicos asociados permanezcan operativos, estables y accesibles ante visitas y consultas legítimas.

Definición de Información Confidencial: Se entiende como información confidencial cualquier dato, documento o conocimiento al que se tenga acceso en virtud del servicio, como por ejemplo:

- Datos personales.
- Información de equipos, flotas o especificaciones técnicas.
- Programación y registros de mantenimiento.
- Informes técnicos, operacionales, de seguridad o de procesos.
- Procedimientos internos, políticas o metodologías del cliente.
- Cualquier otra información que, por su naturaleza, o por indicación expresa, deba mantenerse en reserva.

3. Medidas Técnicas de Protección Implementadas

Para mitigar vectores de ataque y vulnerabilidades en la web, Link Advance ejecuta los siguientes controles tecnológicos:

- Cifrado de Comunicaciones (SSL/TLS): Implementación obligatoria de certificados criptográficos seguros (HTTPS) para cifrar todo el tráfico de datos entrante y saliente entre el navegador del usuario y los servidores de hosting, impidiendo la interceptación por parte de terceros (ataques Man-in-the-Middle).
- Infraestructura de Hosting de Alta Seguridad: Alojamiento en servidores optimizados ubicados físicamente en centros de datos con latencia optimizada para Chile, equipados con almacenamiento NVMe/SSD de alto rendimiento y capas de hardware protegidas por firewalls a nivel de red y de aplicación web (WAF).
- Protección contra Ataques de Denegación de Servicio (DDoS): Monitoreo activo del tráfico web y mitigación de sobrecargas de peticiones sospechosas mediante capas de filtrado perimetral.
- Hardening y Parcheo de Sistemas: Actualizaciones continuas del núcleo de la plataforma, plantillas, módulos y sistemas operativos del servidor para mitigar vulnerabilidades conocidas en el día cero.

4. Control de Acceso y Gestión de Privilegios

El acceso a los entornos de administración (Back-End), bases de datos y paneles de hosting asociados a linkadvance.cl se rige bajo estrictos protocolos:

1. **Principio de Menor Privilegio:** Los accesos administrativos se segmentan estrictamente por roles. El personal recibe los permisos mínimos necesarios para realizar tareas específicas de desarrollo o soporte.

2. **Autenticación Robusta:** Uso obligatorio de contraseñas de alta complejidad (alfanuméricas con caracteres especiales) combinadas con sistemas de Autenticación de Múltiples Factores (MFA / 2FA) para el acceso a plataformas críticas.

3. **Auditoría de Sesiones:** Registro y monitorización periódica de los inicios de sesión administrativos, IPs de origen y modificaciones realizadas en los archivos de configuración del sitio.

5. Política de Respaldos y Recuperación ante Desastres (DRP)

Para prevenir pérdidasaccidentales de información provocadas por fallas de hardware,incidentes de seguridad o errores de software, se ejecuta un plan de continuidad de negocio automatizado:

- Generación de respaldos (backups) periódicos y automatizados de la base de datos y de la totalidad de archivos que componen el sitio web.
- Almacenamiento de copiasde seguridad en entornos aisladosy servidores externosgeorredundantes, evitando puntos únicos de falla.
- Pruebas periódicas de restauración de datos para certificar la velocidad y efectividad del proceso de recuperación ante contingencias de negocio.

6. Gestión de Incidentes de Seguridad

En caso de detectarse cualquier anomalía, brecha de datos o actividad sospechosa en los sistemas de linkadvance.cl, se activará de inmediato el protocolo de respuesta ante incidentes, el cual contempla el aislamiento inmediato de la amenaza, auditoría forense de los archivos de registro (logs), corrección técnica de la vulnerabilidad y la notificación transparente a las partes afectadas y autoridades correspondientes según lo determine el marco normativo nacional.