Protocolo de Notificación a Partes Interesadas ante Incidentes de Seguridad

de F-BridgeDigital

F-BridgeDigital se compromete a mantener una política de transparencia y responsabilidad ante cualquier incidente de ciberseguridad o violación de seguridad de la información, independientemente de su impacto confirmado en los servicios o activos de información.

1. Alcance del Protocolo

Este protocolo aplica a:

- Cualquier incidente de ciberseguridad detectado en los sistemas, aplicaciones, redes o dispositivos administrados por F-BridgeDigital.
- Toda violación o intento de violación de los mecanismos de seguridad.
- Eventos en los que **no se haya confirmado un impacto directo** en clientes o servicios, pero que potencialmente puedan representar un riesgo.

2. Obligación de Notificación

F-BridgeDigital notificará de forma oportuna y documentada a:

- **Clientes** cuyos servicios o datos pudieran estar potencialmente involucrados.
- **Autoridades regulatorias**, cuando así lo exijan normativas locales o internacionales.
- **Otras partes interesadas relevantes**, definidas según el tipo de servicio y la criticidad del incidente.

3. Contenido Mínimo de la Notificación

Toda notificación incluirá como mínimo:

- Fecha y hora de detección del incidente.
- Naturaleza del incidente (técnica y operativa).
- Activos o procesos posiblemente afectados.
- Acciones inmediatas adoptadas para contener y mitigar.
- Medidas de recuperación en curso.
- Evaluación preliminar del riesgo (aunque no haya evidencia de impacto).
- Próximos pasos y medidas preventivas futuras.

4. Tiempos de Notificación

- **Notificación preliminar dentro de las primeras 24 horas** desde la detección.
- **Actualizaciones periódicas** conforme avanza la investigación interna.
- **Informe final** en un plazo no mayor a 5 días hábiles posteriores al cierre del incidente.

5. Canales y Responsables

- Las comunicaciones serán realizadas por el **Gerente General** o su delegado, con apoyo del área de Seguridad de la Información y Comunicaciones.
- Se utilizarán canales oficiales: correo electrónico seguro, llamadas directas y otros medios establecidos contractualmente.

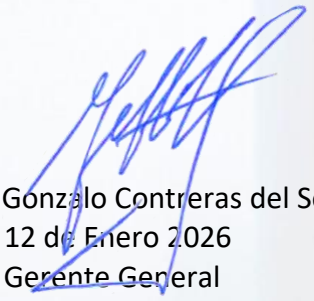
6. Registro y Seguimiento

Todas las notificaciones y comunicaciones serán:

- Registradas en el sistema de gestión de incidentes.
- Auditables para fines internos y regulatorios.
- Revisadas en comités de seguridad y continuidad para lecciones aprendidas.

Aprobación del Protocolo

El presente protocolo será aprobado por la alta dirección de la empresa y se difundirá de manera clara a todos los empleados y colaboradores para asegurar su cumplimiento efectivo.



Firma: Gonzalo Contreras del Solar
Fecha: 12 de Enero 2026
Cargo: Gerente General