

(2) ANEXO 12

Informe de incidentes de seguridad de la información

I. Información de la institución de financiamiento colectivo

- a) Nombre de la institución de financiamiento colectivo.
- b) Nombre completo del oficial de seguridad de la información, así como su número de teléfono y dirección de correo electrónico.

II. Información detallada del Incidente de Seguridad de la Información

Anexar, en medio digital cifrado la siguiente información:

1. Descripción del Incidente de Seguridad de la Información.
2. Números de cuenta afectadas.
3. Estado de las cuentas afectadas (bloqueada, suspendida, activa).
4. Zona de red afectada (Internet, red interna, red de administración, entre otras).
5. Tipo de sistema afectado (servidor de archivos, servidor web, servicio de correo, base de datos, estaciones de trabajo, ya sea de escritorio o móvil, entre otros).
6. Sistema operativo (especificar versión).
7. Protocolos o servicios de los componentes impactados.
8. Número de componentes de los sistemas de la institución de financiamiento colectivo afectados.
9. Aplicaciones involucradas (especificar versión).
10. Información del dispositivo comprometido, en su caso (marca, versión de software, firmware, entre otros).
11. Impacto al servicio (considerando cualquier interrupción) ocasionado por el Incidente de Seguridad de la Información.
12. Monto de la pérdida en pesos, en su caso.
13. Monto recuperado en pesos, en su caso.
14. Estado del Incidente de Seguridad de la información (Resuelto o No Resuelto).
15. Señalar si el Incidente de Seguridad de la información se ha dado a conocer a alguna autoridad. En caso afirmativo, indicar la autoridad y la fecha.
16. Direcciones IP públicas, direcciones de correo electrónico o dominios de dónde proviene el ataque.
17. El protocolo de comunicación utilizado, en su caso.
18. La URL en caso de sitios web involucrados.
19. El malware o firma detectada.
20. Detallar las acciones que se realizaron para mitigar el Incidente de Seguridad de la información, mencionando las personas responsables de implementar dichas acciones de mitigación.
21. Descripción de los resultados de las acciones de mitigación.
22. Tiempos de recuperación del incidente.
23. Acciones para minimizar el daño en situaciones similares subsecuentes.
24. Otra información que considere deba ser de conocimiento de la CNBV.
25. Acciones de comunicación con Clientes para informarles del incidente.

Nombre y firma del oficial en jefe de seguridad de la información