[(2)] ANEXO 11

Incidentes de afectación en materia 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 en jefe 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

Descripción del Incidente de Seguridad de la Información		
a)	Fecha y hora en que ocurrió	
b)	Fecha y hora en que se detectó	
c)	Duración del incidente	
d)	¿La información involucrada en el incidente es administrada por terceros?	Sí ( ) No ( )
e)	En caso de ser afirmativo el inciso d), detallar datos del proveedor (nombre, dirección y datos de contacto, correo electrónico, teléfono, entre otros)	

Afectación provocada por el Incidente de Seguridad		
f)	¿El incidente puede ocasionar una pérdida monetaria para los Clientes o para la propia institución de financiamiento colectivo?	Sí ( ) No ( )
g)	¿Es viable recuperar de manera directa (gestiones propias) o indirecta (a través de seguros) la posible pérdida monetaria?	Sí ( ) No ( )
h)	¿Se han identificado otros incidentes relacionados con el que se reporta, sea por origen, modo de operación o afectación?	Sí ( ) No ( )

i) Indicar, en su caso, el tipo de información comprometida con el Incidente de Seguridad de la Información, conforme a las tablas siguientes:

Información personal del Cliente comprometida		
Nombres	Sí ( )	No ( )
Domicilios	Sí ( )	No ( )
Números de teléfono	Sí ( )	No ( )
Direcciones de correo electrónico	Sí ( )	No ( )
Datos biométricos (huellas dactilares, patrones en iris o retina o reconocimiento facial, entre otros)	Sí ( )	No ( )
Otro(s)		

Información de cuentas o saldos		
Números de tarjetas, u otros	Sí ( )	No ( )
Números de cuenta	Sí ( )	No ( )
Contraseñas o números de identificación	Sí ( )	No ( )
Identificadores de usuarios	Sí ( )	No ( )
Límites	Sí ( )	No ( )
Saldos	Sí ( )	No ( )
Otro(s)		

Información de la institución de financiamiento colectivo		
Claves de acceso	Sí ( )	No ( )
Configuraciones de seguridad	Sí ( )	No ( )
Identificación de puertos o servicios	Sí ( )	No ( )
Direcciones IP de componentes o servicios	Sí ( )	No ( )
Direcciones IP de componentes internos	Sí ( )	No ( )
Acceso a segmentos internos de red	Sí ( )	No ( )
Versiones de software, sistemas operativos o bases de datos	Sí ( )	No ( )
Identificación de vulnerabilidades	Sí ( )	No ( )
Otro(s)		

III. Clasificar el Incidente de Seguridad de la Información reportado con base en las siguientes definiciones:

a) Daño no intencional o accidental, pérdida de información o pérdida de activos		
Información compartida indebidamente	Sí ( )	No ( )
Errores u omisiones en sistemas o dispositivos	Sí ( )	No ( )
Errores en procedimientos o controles	Sí ( )	No ( )
Cambios indebidos a datos	Sí ( )	No ( )
Extravío de información o dispositivos	Sí ( )	No ( )
Otro(s):		
b) Incidentes por fallas o mal funcionamiento		
Dispositivos	Sí ( )	No ( )
Sistemas	Sí ( )	No ( )
Comunicaciones	Sí ( )	No ( )
Servicios	Sí ( )	No ( )
Equipos de terceros	Sí ( )	No ( )
Cadena de suministros	Sí ( )	No ( )
Otro(s)		

c) Incidentes por la interrupción o falta de insumos		
Ausencia de personal	Sí ( )	No ( )
Huelgas	Sí ( )	No ( )
Energía	Sí ( )	No ( )
Agua	Sí ( )	No ( )
Telecomunicaciones	Sí ( )	No ( )
Otro(s)		
d) Incidentes por intercepción de datos		
Espionaje	Sí ( )	No ( )
Mensajes	Sí ( )	No ( )
Wardriving	Sí ( )	No ( )
Ataques de hombre en medio	Sí ( )	No ( )
Secuestro de sesiones	Sí ( )	No ( )
Sniffers	Sí ( )	No ( )
Robo de mensajería	Sí ( )	No ( )
Otro(s)		
e) Incidentes por actividad maliciosa con el fin de tomar el control, desestabilizar o dañar un sistema informático		
Robo de identidad	Sí ( )	No ( )
Phishing	Sí ( )	No ( )
Denegación de servicios (DOS, DDOS)	Sí ( )	No ( )
Código malicioso (*malware,* troyanos, gusanos, inyección de código, virus, *ransomware*)	Sí ( )	No ( )
Ingeniería social	Sí ( )	No ( )
Vulneración de certificados (suplantación de sitios, certificados falsos)	Sí ( )	No ( )
Manipulación de hardware (*proxies* anónimos, *skimmers, sniffers*)	Sí ( )	No ( )
Alteración de información (suplantación de direccionamiento y tablas de ruteo, DNS *poisoning,* alteración de configuraciones)	Sí ( )	No ( )
Abuso de aplicaciones de auditoría	Sí ( )	No ( )
Ataques de fuerza bruta	Sí ( )	No ( )
Abuso de autorizaciones	Sí ( )	No ( )
Crimen organizado	Sí ( )	No ( )
Hacktivistas	Sí ( )	No ( )
Gobierno o grupos afines	Sí ( )	No ( )
Terroristas	Sí ( )	No ( )
Insiders	Sí ( )	No ( )
Otro(s)		

f) Incidentes originados por aspectos legales		
Violación de cláusulas contractuales	Sí ( )	No ( )
Violación de acuerdos de confidencialidad	Sí ( )	No ( )
Decisiones adversas (resoluciones judiciales en la misma jurisdicción o en otras)	Sí ( )	No ( )
Otro(s)		
g) Otros (especificar)		

IV. Clasificación del Incidente de Seguridad de la Información.
Señalar en la tabla siguiente, la clasificación en la que se ubica el incidente mediante los conceptos del catálogo que a continuación se señalan:

Tipo	Sub Tipo	Sub Clase de Eventos	
I. Fraude Interno	1.1 Actividades no autorizadas.	1.1.1 Operaciones no reveladas (intencionalmente). 1.1.2 Operaciones no autorizadas (con pérdidas pecuniarias). 1.1.3 Valoración errónea de posiciones (intencional).	( ) ( ) ( )
	1.2 Robo y Fraude Internos.	1.2.1 Fraude / depósitos sin valor. 1.2.2 Extorsión / malversación / robo. 1.2.3 Apropiación indebida de activos. 1.2.4 Destrucción dolosa de activos. 1.2.5 Falsificación Interna. 1.2.6 Contrabando. 1.2.7 Apropiación de cuentas, de identidad, entre otros. 1.2.8 Incumplimiento / evasión de impuestos (intencional). 1.2.9 Cohecho. 1.2.10 Abuso de información privilegiada (no a favor de la empresa).	( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( )
	1.3. Seguridad de los sistemas.	1.3.1 Vulneración de sistemas de seguridad. 1.3.2 Daños por ataques informáticos. 1.3.3 Robo de información (con pérdidas pecuniarias). 1.3.4 Utilización inadecuada de claves de acceso y/o niveles de autorización.	( ) ( ) ( ) ( ) ( )
II. Fraude Externo	2.1 Hurto y Fraude Externos.	2.1.1 Robo / estafa / extorsión /cohecho. 2.1.2 Falsificación Externa / Suplantación de personalidad. 2.1.3 Uso y/o divulgación de información privilegiada. 2.1.4 Espionaje industrial. 2.1.5 Contrabando.	( ) ( ) ( ) ( ) ( )
	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad. 2.2.2 Daños por ataques informáticos. 2.2.3 Robo de información (con pérdidas pecuniarias). 2.2.4 Utilización inadecuada de claves de	( ) ( ) ( ) ( )

		acceso y/o niveles de autorización.	
III. Incidencias en el Negocio y Fallos en los Sistemas	3.1 Sistemas	3.1.1. Hardware. 3.1.2. Software. 3.1.3. Telecomunicaciones. 3.1.4. Interrupción / incidencias en el suministro.	( ) ( ) ( ) ( )

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