SHCP
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

CNSF
COMISIÓN NACIONAL DE SEGUROS Y FIANZAS

Ciudad de México, 22 de Junio de 2018.

SHCP | CNSF COMISIÓN NACIONAL DE SEGUROS Y FIANZAS
DESPACHADO
22 JUN 2018
DIRECCIÓN DE VIGILANCIA FINANCIERA

PRESIDENCIA
VICEPRESIDENCIA DE OPERACIÓN INSTITUCIONAL
DIRECCIÓN GENERAL DE SUPERVISIÓN FINANCIERA

Expediente: C00.221.17.4.5-F0006"18"
Oficio No. 06-C00-22100/35778

ASUNTO: Bases de coordinación en materia de seguridad de la información.- Se informa sobre los términos para el envío del Reporte Inicial de Incidentes de Seguridad de la Información.

Afianzadora Sofimex, S.A. (En proceso de transformación a Sofimex, Institución de Garantías, S.A.)
Blvd. Adolfo Lopez Mateos 1941, Piso 2
Col. Los Alpes
Álvaro Obregón, C.P. 01010
Ciudad de México

At'n.: Director General

CORREO CONDUSEF 2018 JUN 27 PM

El 24 de mayo de 2018, la Secretaría de Hacienda y Crédito Público, el Banco de México, la Comisión Nacional Bancaria y de Valores, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, la Comisión Nacional del Sistema de Ahorro para el Retiro, la Comisión Nacional de Seguros y Fianzas, la Procuraduría General de la República, así como diversas Asociaciones Gremiales del Sistema Financiero Mexicano, entre las cuales se encuentran la Asociación Mexicana de Instituciones de Seguros, A.C. y la Asociación Mexicana de Instituciones de Garantías, A.C., suscribieron el documento denominado **"Bases de coordinación en materia de seguridad de la información"** (en adelante "Bases de Coordinación").

El objeto del referido documento, es establecer las bases para la colaboración que las autoridades financieras y la Procuraduría General de la República se brindarán entre ellas, en coordinación con dichas Asociaciones Gremiales y las entidades que conforman el Sistema Financiero Mexicano, en materia de seguridad de la información, en los términos descritos en las propias "Bases de Coordinación", las cuales se encuentran disponibles para su consulta en la página Web de esta Comisión en la liga electrónica: http://www.gob.mx/cnsf.

En este contexto, y a efecto de crear las condiciones propicias que permitan la adecuada instrumentación y observancia de las "Bases de Coordinación", con fundamento en el primer párrafo de su Base Quinta, esa Institución deberá crear un equipo interno de identificación y respuesta a Incidentes Sensibles de Seguridad de la Información, cuya definición se prevé en el inciso e) de la Segunda de las "Bases de Coordinación", debiendo asimismo, informar sin demora a esta Comisión sobre la ocurrencia de estos, contemplando al menos, en su caso, la información siguiente:

a) Los servicios que hayan sido interrumpidos, así como el tiempo estimado para recuperar la operación.
b) Las operaciones no reconocidas y la pérdida económica con el monto estimado.
c) El tipo de recursos o información alterada, robada o perdida.
d) Las situaciones que pongan en riesgo la seguridad de los clientes, empleados o las instalaciones.
e) La clasificación del impacto del incidente con base en la información que esa Institución tenga disponible.

Asimismo, de conformidad con el penúltimo párrafo de la citada Base Quinta de las "Bases de Coordinación", las Instituciones de Seguros e Instituciones de Fianzas, deberán informar a esta Comisión de cualquier evento que vulnere los controles o implique una violación a las políticas de seguridad, sin que represente una afectación a sus operaciones o bien, que genere afectaciones parciales a sus operaciones, que impida o dificulte la atención de sus clientes o represente accesos no autorizados a información, sin generar pérdidas económicas pero que de continuar pudiera representar un Incidente Sensible de Seguridad de la Información.

En ese sentido, esa Institución deberá cumplimentar el formato denominado "Reporte Inicial de Incidentes de Seguridad de la Información", que se anexa al presente oficio y que deberá remitirse a esta Comisión a través de la dirección de correo electrónico ciberseguridad@cnsf.gob.mx, **DENTRO DE LOS CINCO DÍAS NATURALES** siguientes a la ocurrencia del incidente de que se trate. Dicho formato también puede ser consultado a través de la página Web de esta Comisión, http://www.gob.mx/cnsf, en la sección "Acciones y Programas, Sistemas de Información, Instructivos, Catálogos y Manuales, Formato de Incidentes de Seguridad".

Lo anterior se hace de su conocimiento con fundamento en la fracción VII del artículo 10 del Reglamento Interior de la Comisión Nacional de Seguros y Fianzas.

Atentamente.
SUFRAGIO EFECTIVO. NO REELECCIÓN.
VICEPRESIDENTE DE OPERACIÓN INSTITUCIONAL.

LIC. GERARDO LOZANO DE LEÓN

c.c.p. **Lic. Gabriel Magaña Nuñez.-** Presidente del Comité de Auditoría de Afianzadora Sofimex, S.A. (En proceso de transformación a Sofimex, Institución de Garantías, S.A.)- Insurgentes Sur Ext 3728 Depto. 204, Col. Peña Pobre, Tlalpan, C.P. 14060, Ciudad de México.- Para su conocimiento.

Anexo: El que se indica.
HRCZ

REPORTE INICIAL DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

1. Datos de quién reporta:

Nombre de la institución que reporta:	
Nombre y cargo de la persona que reporta:	
Correo electrónico:	
Teléfono:	
Áreas a quienes ha sido reportado el incidente en la institución	

2. Información General del Incidente:

Información del Incidente	
2.1. Fecha y hora del Incidente:	
2.2. Fecha y hora de detección:	
2.3. Breve descripción del incidente (¿qué pasó?, ¿dónde pasó?, ¿cuándo pasó?, ¿cómo pasó?, ¿Qué servicios y como se afectaron?)	
2.4. Componentes de la Infraestructura Tecnológica afectados en el incidente de seguridad de la información.	☐ Zona de red afectada (internet, red interna, red de administración, entre otras): _____
	☐ 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): _____
	☐ Sistema operativo (especificar versión): _____
	☐ Protocolos o servicios y aplicaciones (especificar versión): _____

Información del Incidente	
	☐ Otro: Especificar_____
2.5. Canales de atención a clientes afectados por el incidente y estimación inicial de número de puntos de atención o porcentaje de afectación:	
	☐ TPV
	☐ Sucursales
	☐ Portal Web / Móvil
	Estimación inicial: _____
2.6. Instalación afectada:	☐ Centro de Datos
	☐ Oficinas de servicio Oficina matriz
	☐ Sucursal
	☐ Proveedor Otro: _____
2.7. Nivel estimado de daño o impacto provocado por el incidente de seguridad de la información:	**Crítico; porque: _____** **Medio** **Bajo**
2.8. Detallar las acciones inmediatas que han realizado para mitigar el incidente de seguridad de la información:	

3. Clasificar el incidente de seguridad de la información reportado en el presente anexo con base en las siguientes definiciones:

Clases de Incidente	Aplica	Describir el incidente específico
3.1. Ataques físicos (deliberados o intencionales) tales como: sabotaje, vandalismo, robo de dispositivos, fuga de información en medios físicos, acceso físicos no autorizados, coerción, extorsión, ataque terrorista, entre otros.	☐	
3.2. Daño no intencional o accidental, pérdida de información o pérdida de activos, tales como: información compartida indebidamente, errores u omisiones en sistemas o dispositivos, errores en procedimientos o controles, cambios	☐	

Clases de Incidente	Aplica	Describir el incidente específico
indebidos a datos, extravío de información o dispositivos, entre otros.		
3.3. Incidentes por desastres naturales o ambientales, tales como: Terremotos, inundaciones, huracanes, incendios, radiación, corrosión, explosiones, entre otros.	☐	
3.4. Incidentes por fallas o mal funcionamiento, tales como: Falla en dispositivos o sistemas, fallas en comunicaciones, en servicios o equipos de terceros o en la cadena de suministros, entre otros.	☐	
3.5. Incidentes por la interrupción o falta de insumos, tales como: Ausencia de personal, huelgas, interrupción de servicios de energía, agua, telecomunicaciones, entre otros.	☐	
3.6. Incidentes por intercepción de datos, tales como: espionaje, intercepción de mensajes, wardriving, ataques de hombre en medio, secuestro de sesiones, programas sniffers, robo de mensajería, entre otros.	☐	
3.7. Incidentes por actividad maliciosa (ciber ataques) con el fin de tomar el control, desestabilizar o dañar un sistema informático, tales como: Robo de identidad, Phishing, Negación de servicio (DOS, DDOS), Código malicioso (malware, troyanos, gusanos, inyección de código, virus, ransomware), Ingeniería Social, Vulneración de certificados (suplantación de sitios, certificados falsos), manipulación de hardware (proxies anónimos, skimmers, sniffers), alteración de información (suplantación de direccionamiento y tablas de ruteo, DNS poisoning, alteración de configuraciones), abuso de aplicaciones de auditoría, ataques de fuerza bruta, abuso de autorizaciones, entre otros.	☐	
3.8. Originadas por aspectos legales, tales como: Violación de cláusulas y acuerdos, violación de confidencialidad, decisiones adversas (resoluciones judiciales en la misma jurisdicción o en otras), entre otras.	☐	