23 de junio de 2016

CARTA CIRCULAR NÚM.: CC-2016-1889-AF

A TODA PERSONA QUE OSTENTE UNA LICENCIA O CERTIFICADO EMITIDO POR LA OFICINA DEL COMISIONADO DE SEGUROS QUE MANTENGA UN SISTEMA DE INFORMACIÓN ELECTRÓNICO

RE: RIESGO DE SEGURIDAD CIBERNÉTICA (CYBERSECURITY RISK)

Estimados señores y señoras:

La Seguridad Cibernética debe ser un tema de prioridad para toda aquella entidad que maneje un sistema de información, en particular aquellos con información sensitiva de asegurados, proveedores y/o acreedores. Debido al alto volumen de información manejada por estos, los Aseguradores, Organizaciones de Servicios de Salud y sus Intermediarios son especialmente sensibles a sufrir daños por el riesgo de seguridad cibernética.

La exposición al daño que este riesgo plantea son, entre otros, la pérdida de información privilegiada, extorsión, la adquisición no autorizada de información personal (data breach), robo o corrupción de información e interrupción de operaciones.

Por otra parte, los Sistemas de Seguridad Cibernética son aquellos procesos, procedimientos, tecnologías y medidas preventivas usadas para proteger la información electrónicamente almacenada del riesgo de ser utilizada o divulgada sin autorización.

Es el deber de toda entidad que ostente una licencia o certificado de autoridad emitido por esta Oficina el controlar, fiscalizar y minimizar todos los riesgos inherentes a su operación, incluido el riesgo de seguridad cibernética. A los efectos de contribuir al esfuerzo de nuestros regulados de atender su riesgo particular, se emite esta circular con guías y recomendaciones generales al efecto. Compartimos las medidas preventivas en la forma de directrices en la gobernanza corporativa, medidas administrativas y medidas técnicas en el manejo de sistemas de información, a

continuación. Las mismas deben ser consideradas e implementadas a tono con la complejidad de las operaciones de cada regulado, luego de un avalúo cuidadoso del correspondiente riesgo cibernético.

1. Gobernanza Corporativa:

    a. Promover cultura de protección de información entre directores, oficiales, administradores y empleados.
    b. Implementar Programa de Seguridad de Información.
    c. Establecer políticas y estándares.
    d. Avalúo anual de sus riesgos de negocio, incluyendo sus exposiciones por riesgo cibernético.
    e. Facilitar acceso a tecnologías adecuadas, proporcionales a las necesidades y los recursos corporativos.
    f. Formalizar y apoderamiento de un Comité de Supervisión de Programa de Seguridad de Información.

2. Medidas Administrativas:

    a. Mantener un programa formal de entrenamiento y acceso de información a sus empleados.
    b. Asignar responsabilidades de monitoreo del Programa de Seguridad de Información.
    c. Mantener un programa de supervisión a proveedores de servicios con acceso a información corporativa.
    d. Mantener programas alternativos de continuidad de operaciones en caso de daños cibernéticos.
    e. Identificar preventivamente medidas alternativas de notificación a afectados por la adquisición no autorizada de información personal (data breach).
    f. Identificar proactivamente medidas de mitigación de daños cibernéticos.
    g. Mantener entre sus pólizas seguro de responsabilidad contra riesgos cibernéticos y protección contra la pérdida de privacidad, incluyendo la cubierta de interrupción de negocios por causa de dichos riesgos.

3. Toda entidad, como mínimo, deberá contar con lo siguiente, con respecto a su red de sistemas de información:

    a. Firewall
    b. Antivirus
    c. Control de acceso y uso de credenciales alfanuméricos (EJ: AD)
    d. Programa de monitoreo del tráfico en internet
    e. Inventario de sus equipos electrónicos
    f. Licenciamiento legítimo de todas sus aplicaciones

g. Soporte técnico/Administrador de red
h. Un plan de contingencias
i. Políticas de seguridad internas para el uso de la red
j. Sistema de resguardos
k. Sistema de monitoreo/auditoría de su red
l. Control de las conexiones remotas a sus sistemas
m. Realizar al menos una vez al año un "penetration test"
n. Conexión alterna de internet (redundancia)

4. Equipos portátiles encriptados

5. El área de servidores o cuarto de comunicaciones deberá tener:

    a. Un acceso físico restringido.
    b. Control de temperatura y humedad adecuado para los equipos
    c. Sistema de control de incendios
    d. Un registro de acceso al área controlada (fecha, nombre, propósito de la visita)
    e. Deberá ser un área libre de inundaciones

6. Con respecto a los servidores:

    a. Deberán estar parchados con la última versión requerida del sistema operativo que contenga
    b. Las actualizaciones deben ser filtradas y monitoreadas
    c. Deberán tener instalado un programa antivirus
    d. Deberán estar detrás del firewall de la red
    e. Deberán estar configurados dentro de un rango de IP estáticos

7. Con respecto a la información confidencial:

    a. Deberán realizar resguardos de manera consecuente, diariamente
    b. Deberán garantizar la seguridad del flujo y almacenamiento de la data
    c. Restringirán el acceso a la red
    d. Encriptarán los archivos que contengan información privilegiada

A modo de guía adicional para el avalúo del riesgo cibernético en general, y la implementación de medidas gerenciales específicas, esta Oficina recomienda la lectura de los siguientes documentos:

- Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology (NIST), http://www.nist.gov/cyberframework

- Draft Insurance Data Security Model Law, NAIC Cybersecurity (EX) Task Force; NAIC Model Law #672 "Privacy of Consumer Financial Health and Information Regulation"; NAIC Roadmap for Cybersecurity Consumer Protections; http://naic.org/index_security_breach.htm

Cordialmente,

Ángela Weyne Roig
Comisionada de Seguros