Oficina del Comisionado de Seguros

Lista de cotejo para cumplir con la Regla Núm. 108, "Normas de Ciberseguridad para la Industria de Seguros"

Lea más información sobre la Regla 108 y recursos para la implementación de tecnología en la industria de seguros en https://ciberseguridad.ocs.pr.gov.

Certificación Anual de Cumplimiento

No más tarde del 30 de junio de cada año, los Regulados radicarán una certificación anual de cumplimiento a través del Portal de Ciberseguridad de la OCS. Este documento es una declaración escrita en la que el Regulado certifica que ha cumplido con los requisitos dispuestos en el Artículo 8:

- ☐ **Implementación de un Programa de Ciberseguridad** – Conlleva desarrollar, implementar, mantener y documentar un programa integral para la protección los datos del Regulado y sus sistemas de información.
  - ☐ Controles administrativos de ciberseguridad (políticas, estándares, procesos y planes que se enfoquen en (a) proteger la confidencialidad, integridad y disponibilidad de los datos, (b) prevenir cualquier acceso o uso no autorizado y (c) definir períodos de retención y destrucción adecuados para la información No-Pública
  - ☐ Controles técnicos de ciberseguridad (ej. *firewalls,* antivirus, configuraciones, etc.) que se utilizarán para implementar los controles establecidos en las políticas, estándares y procesos
  - ☐ Controles de seguridad física (controles de acceso, cámaras de seguridad, etc.)

- ☐ **Evaluación de Riesgos** – Existen varios marcos, metodologías y herramientas a utilizarse para evaluar su riesgo de ciberseguridad, por ejemplo: CISA CPGs, CIS Critical Security Controls, y otras herramientas alineadas al NIST CSF
  - ☐ Designar personas responsables por el Programa de Ciberseguridad
  - ☐ Identificar amenazas internas y externas
    - ☐ Evaluar la posibilidad y daño potencial de cada una
  - ☐ Reevaluar al menos una vez al año la suficiencia del Programa de Ciberseguridad y la efectividad de los controles implementados, haciendo los ajustes necesarios

- ☐ **Manejo de Riesgos** – Conlleva la implementación de controles de ciberseguridad, a base de la Evaluación de Riesgos realizada:
  - ☐ Incluir medidas para mitigar los riesgos identificados en su Programa de Ciberseguridad (debe considerar el uso de contratistas de servicios):
    - ☐ Implementar un programa formal de adiestramientos sobre modalidades de ataques cibernéticos para el personal, llevando un récord del desempeño de cada empleado
    - ☐ Asignar y adiestrar al personal sobre sus responsabilidades de ciberseguridad
    - ☐ Establecer controles de acceso, incluyendo autenticación multifactorial en la medida que sea posible y/o adecuada para prevenir accesos no autorizados
    - ☐ Supervisar a aquellos proveedores de servicios con acceso a sus datos, mediante requisitos en acuerdos de servicio y controles de ciberseguridad
    - ☐ Identificar los activos de información de la empresa y administrarlos de forma segura
    - ☐ Restringir el acceso físico a las áreas donde se encuentre la Información No-Pública
    - ☐ Implementar encriptación u otros controles para proteger la transmisión de datos y la información almacenada en dispositivos móviles
    - ☐ Adoptar prácticas seguras de desarrollo de software y probar la seguridad de aplicaciones desarrolladas por recursos internos y externos
    - ☐ Incluir procesos de respaldo, resguardo y gestión de registros ("*audit logs*")
    - ☐ Regularmente probar y monitorear los sistemas y procedimientos para detectar ataques y actividad sospechosa, incluyendo respaldo, resguardo y gestión de registros ("*audit logs*")
    - ☐ Prevenir la destrucción, pérdida o daño por peligros ambientales, desastres naturales, fallos tecnológicos, mediante un plan de continuidad del negocio, plan de recuperación de desastres, y plan de respuesta a incidentes de ciberseguridad
    - ☐ Implementar y mantener procedimientos para la disposición segura de datos

- ☐ Mantenerse informado con respecto a las nuevas amenazas o vulnerabilidades para poder reaccionar ágilmente con las mitigaciones necesarias
- ☐ Incluir la ciberseguridad en el proceso de manejo de riesgos empresariales y en los informes de gobernanza corporativa.
- ☐ Realizar pruebas de vulnerabilidades regularmente en sus sistemas de información

Para más detalles sobre la implementación efectiva de controles de ciberseguridad, refiérase a la ***Guía de Implementación de Controles de Ciberseguridad para la Industria de Seguros***, disponible en la página de Ciberseguridad de la OCS: https://ciberseguridad.ocs.pr.gov.

Resultados de Pruebas de Vulnerabilidades

Los Regulados radicarán un informe bianual de su autoevaluación de vulnerabilidades de ciberseguridad. La OCS únicamente requiere la información necesaria para determinar si el Regulado ha mitigado diligentemente sus vulnerabilidades externas. Las métricas que utiliza la OCS para analizar estas acciones son:

- **Cantidad de activos escaneados**
  Aquellos servicios y dispositivos que permiten o podrían permitir el acceso a una red a través de una interfaz, software especializado, direcciones de IP o cualquier otro medio. Algunos ejemplos incluyen computadoras, servidores, multifuncionales, etc.
- **Cantidad de servicios escaneados**
  Portales, aplicativos y protocolos ejecutados, que ofrecen capacidades de comunicación a través del Internet, de todos los activos escaneados
- **Cantidad de dispositivos escaneados**
  Aquellos dispositivos que tienen al menos un puerto o servicio abierto, de todos los activos escaneados
- **Cantidad de dispositivos vulnerables**
  Aquellos dispositivos escaneados donde se ha detectado una vulnerabilidad
- **Cantidad de vulnerabilidades**
  Debilidades en un sistema de información, proceso de seguridad, controles internos o implementación que podrían ser explotadas por un adversario o amenaza cibernética. Se analizan por severidad:
  - **Cantidad de vulnerabilidades críticas**
  - **Cantidad de vulnerabilidades de riesgo alto**
  - **Cantidad de vulnerabilidades de riesgo medio**
  - **Cantidad de vulnerabilidades de riesgo bajo**
- **Período más largo activo**
  Se refiere al período de tiempo más largo, en días, que cada vulnerabilidad ha estado activa
- **Servicios abiertos (posible riesgo)**
  Se refiere a servicios particulares, de todos los servicios escaneados, que al estar expuestos podrían aumentar el riesgo de los sistemas de información:
  - **RDP**
  - **SMB**
  - **Netbios**
  - **RPC**
  - **SQL**
  - **Telnet**
  - **LDAP**
  - **Kerberos**
  - **FTP**
  - **IRC**

Para facilitar la entrega de este requisito, se exhorta a los Regulados a suscribirse a los *Cyber Hygiene Services* que la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) ofrece **libre de costo** para todo tipo de organización. La información solicitada en su informe de vulnerabilidades aparece en la página 6 del *Cyber Hygiene Assessment*, titulada "*Cyber Hygiene Report Card*". Puede solicitar este servicio escribiendo a ngai.oliveras@cisa.dhs.gov. Para más información puede acceder a https://ciberseguridad.ocs.pr.gov/cisa.

Notificación de Incidentes de Ciberseguridad

En la medida que sea necesario notificar al Comisionado sobre un incidente de ciberseguridad, los Regulados podrán hacerlo a través del portal https://ciberseguridad.ocs.pr.gov. Al acceder al área de Regulados, encontrarán un formulario de notificación con toda la información requerida en la Regla Núm. 108, a ser radicado electrónicamente dentro de las 72 horas de haberse determinado que ocurrió un incidente de ciberseguridad.

El Regulado deberá enviar la mayor cantidad posible de información utilizando el formulario electrónico. La utilización de un formulario electrónico disminuye el riesgo de seguridad al ofrecer un mecanismo alterno al correo electrónico de un Regulado que pudiera tener un ambiente comprometido. De no ser viable la notificación a través de este formulario, y para enviar cualquier actualización o información adicional sobre el incidente, los Regulados podrán utilizar el correo electrónico ciberseguridad@ocs.pr.gov.