



OFICINA DEL

COMISIONADO  
DE SEGUROS

GOBIERNO DE PUERTO RICO



# PREPARACIÓN DE LAS ENTIDADES REGULADAS

## ANTE LOS RIESGOS CIBERNÉTICOS

Recomendaciones de la  
**Oficina del Comisionado  
de Seguros de Puerto Rico**



Mensaje a las  
**Entidades Reguladas**





# Mensaje a las Entidades Reguladas



Cumplan con los requisitos establecidos en la **Regla 108 del Código de Seguros** de Puerto Rico y mantengan programas de ciberseguridad acordes con su perfil de riesgo.



Realicen evaluaciones periódicas de riesgos para identificar, evaluar y mitigar amenazas a la **confidencialidad, integridad y disponibilidad** de la información.



Mantengan **inventarios actualizados** de sistemas de información, activos tecnológicos y datos sensibles.



Implementen **controles de acceso** basados en el principio de menor privilegio y revisen periódicamente los accesos de usuarios y terceros.



Utilicen **autenticación multifactor (MFA)** para el acceso remoto, cuentas privilegiadas y sistemas críticos.



# Mensaje a las Entidades Reguladas



Mantengan programas efectivos de **gestión de identidades y accesos** para empleados, contratistas y proveedores.



Implementen **controles de seguridad** para proteger la información no pública, incluyendo cifrado, segmentación de redes, monitoreo continuo y herramientas de **detección y respuesta**.



Mantengan procesos oportunos para la **instalación de parchos de seguridad, actualización de sistemas y remediación de vulnerabilidades**.



Realicen pruebas periódicas de **vulnerabilidad, evaluaciones de seguridad y ejercicios de respuesta a incidentes**.



Revisen y actualicen regularmente sus planes de respuesta a incidentes **cibernéticos, continuidad operacional y recuperación ante desastres**.



# Mensaje a las Entidades Reguladas



Capaciten periódicamente a empleados, directivos y contratistas sobre **riesgos cibernéticos, phishing, ingeniería social y protección de datos.**



Mantengan mecanismos adecuados para la **supervisión y gestión de riesgos** asociados a **proveedores y terceros** con acceso a información o sistemas críticos.



**Notifiquen oportunamente** a la Oficina del **Comisionado de Seguros** los eventos de ciberseguridad sujetos a notificación conforme a la **Regla 108.**



Promuevan una **cultura organizacional** de **protección de datos, resiliencia operacional y cumplimiento regulatorio.**



La **resiliencia digital** es un componente esencial de la **continuidad operacional**, la **confianza del consumidor** y la **estabilidad del mercado asegurador.**