OFICINA DEL
COMISIONADO
DE SEGUROS

GOBIERNO DE PUERTO RICO

PREPARACIÓN DE LOS CIUDADANOS ANTE LOS RIESGOS CIBERNÉTICOS

Recomendaciones de la
Oficina del Comisionado de Seguros de Puerto Rico

Mensaje a los Ciudadanos

La información, la prevención y los hábitos seguros son su mejor protección en el entorno digital.

OFICINA DEL
COMISIONADO DE SEGUROS
GOBIERNO DE PUERTO RICO

Mensaje a los Ciudadanos

- Utilice **contraseñas robustas** y distintas para sus cuentas más importantes.
- Active la **autenticación multifactor (MFA)** siempre que esté disponible.
- Mantenga **actualizados** sus teléfonos, computadoras y aplicaciones.
- **Desconfíe** de correos electrónicos, mensajes de texto o llamadas que soliciten información personal o financiera.
- **Verifique** cuidadosamente los enlaces antes de hacer clic o descargar archivos.
- **Evite** utilizar redes públicas de internet para realizar transacciones financieras o acceder a información confidencial.
- **Proteja** la información personal y financiera que comparte en redes sociales.

Pequeñas acciones hoy pueden prevenir grandes problemas mañana. Protéjase y proteja lo que es suyo.

OFICINA DEL
COMISIONADO DE SEGUROS
GOBIERNO DE PUERTO RICO

Mensaje a los Ciudadanos

- Realice **copias de seguridad** periódicas de documentos y fotografías importantes.
- **Monitoree** regularmente sus cuentas bancarias, tarjetas de crédito y reportes de crédito.
- **Informe** inmediatamente cualquier actividad sospechosa a su institución financiera o proveedor de servicios.
- Considere alternativas de **protección financiera** y seguros especializados para riesgos cibernéticos cuando correspondan.
- La **prevención** y la **educación** son las herramientas más efectivas para reducir el riesgo de fraude y robo de identidad.
- La **ciberseguridad** comienza con decisiones informadas y hábitos seguros.

Estar informado y tomar precauciones es la **mejor defensa** contra las amenazas cibernéticas.

OFICINA DEL
COMISIONADO DE SEGUROS
GOBIERNO DE PUERTO RICO

¿Qué hacer si es víctima de un incidente cibernético?

Comuníquese de inmediato con su institución financiera, aseguradora, proveedor de servicios o plataforma afectada.

Si cuenta con una **póliza** que pudiera brindar protección o asistencia relacionada con el incidente, comuníquese con su productor de seguros o representante autorizado para orientarse sobre las cubiertas, beneficios y servicios disponibles bajo su póliza.

Cambie sus contraseñas y active la autenticación multifactor (MFA) en las cuentas afectadas.

Conserve evidencia del incidente, incluyendo correos electrónicos, mensajes, capturas de pantalla y cualquier otra información relevante.

Monitoree sus cuentas bancarias, tarjetas de crédito y reportes de crédito para detectar actividad sospechosa.

Reporte el incidente a las autoridades correspondientes, incluyendo Cybersecurity & Infrastructure Security System (CISA), Federal Bureau of Investigation (FBI) a través del Incident Crime Complaint Center (IC3) y las autoridades locales cuando corresponda.

Si entiende que su información personal, financiera o médica ha sido comprometida, **actúe con prontitud** para limitar posibles daños y proteger su identidad.

No envíe dinero, realice pagos ni comparta información adicional con personas o entidades cuya legitimidad no haya sido debidamente verificada.

La rapidez con que responda a un incidente puede ser determinante para reducir pérdidas y proteger su información personal y financiera.

https://myservices.cisa.gov/irf
https://www.ic3.gov