

Cómo cumplir con los requisitos de seguro cibernético para IBM i

Publicado el 02 de marzo de 2023

El cibercrimen es una amenaza que continúa creciendo en términos de instancias y gravedad. En 2022, la cantidad de quejas de ransomware reportadas al FBI ascendió a 150 millones, un aumento del 400 % desde 2020.

Los días en que IBM i estaba en una isla propia quedaron atrás, y las mismas amenazas crecientes que enfrentan otras organizaciones también están creciendo entre los usuarios de IBM i.

Los ataques cibernéticos pueden ser perjudiciales y, con frecuencia, provocan que las víctimas cierren su negocio. No es de extrañar que se proyecte que el seguro cibernético sea una industria de USD\$500 mil millones en los próximos 10 años.

¿Qué es el seguro cibernético?

El seguro cibernético cubre los costos asociados con las filtraciones de datos y los ataques cibernéticos a las empresas. Por lo general, estos incluyen la pérdida de ingresos debido al tiempo de inactividad, reparación de hardware/sistemas, responsabilidad y más. Tener esta cobertura es especialmente crítico en el caso de una violación de datos que involucre el compromiso de la información personal confidencial de los clientes, como números de tarjetas de crédito, números de seguro social o incluso registros de salud.

¿Qué necesito para calificar para el seguro cibernético?

Desde que sufrieron grandes pérdidas en 2020, las aseguradoras cibernéticas han descubierto la importancia de exigir a sus asegurados que mantengan una higiene básica de ciberseguridad.

Por lo tanto, para calificar para un seguro cibernético o para reducir considerablemente las primas, las organizaciones deben implementar varios controles de seguridad. En IBM i, las soluciones a considerar incluyen:

- **Multifactor Authentication (MFA):** Las credenciales de usuario robadas juegan un papel importante en la mayoría de los ciberataques exitosos. Las

soluciones MFA combaten este riesgo al requerir un paso de verificación adicional además de la entrada rutinaria de información de nombre de usuario y contraseña. Este paso de verificación adicional puede tomar la forma de una notificación automática enviada al dispositivo móvil de un usuario, un código de acceso de un solo uso o un escaneo biométrico (huellas dactilares, reconocimiento facial, etc.). La integración con otros proveedores de autenticación a través del protocolo RADIUS ayuda a ampliar la gama de dichas soluciones.




- **Security Information and Event Management:** Para las empresas con sistemas IBM i, es fundamental contar con una solución que pueda ingerir datos de eventos de seguridad sin procesar de IBM i y traducirlos a un formato significativo para el personal de operaciones de seguridad. Las soluciones avanzadas permiten el filtrado flexible de las entradas del diario de auditoría y los mensajes del sistema para que TI sepa exactamente lo que sucede en su IBM i.
- **Data Encryption:** Si un atacante obtiene acceso a sus sistemas IBM i y sus datos confidenciales no están cifrados, tendrá acceso sin obstáculos a esos datos. Cifrar sus datos hace que sean de uso limitado para los atacantes en caso de una violación de datos.
- **Antivirus and Anti-Ransomware:** Para asegurarse de que no haya malware presente en los sistemas de una organización, es fundamental que los análisis de virus se realicen con frecuencia. Las soluciones antivirus de IBM i deben poder escanear de forma nativa en IBM i y en una escala de nivel empresarial. También deberían poder detectar las amenazas más recientes. Anti-ransomware debe detectar actividad de ransomware en IBM i y evitar el cifrado malicioso de archivos en IBM i.
- **Exit Programs:** Los puntos de salida (exit points) marcan los puntos de acceso al IBM i de una organización. Las soluciones de seguridad pueden integrarse con estos puntos de salida que permiten o niegan el acceso según las reglas definidas en la solución y para registrar las solicitudes de acceso. Las soluciones que se integran con los puntos de salida son importantes para bloquear los accesos a sus sistemas y rastrear quién accedió a qué información y funcionalidad y cómo.

¿Cómo podemos ayudarle?

Es esencial contar con soluciones y procedimientos que cubran estas seis áreas de seguridad de IBM i. Hacerlo le ofrece a su organización una base sólida de ciberseguridad que reduce sustancialmente el riesgo de ser víctima de un ciberataque, lo que lo convierte en un cliente mucho más asegurable. [Louprey](#)

International ofrece productos que pueden ayudar a su organización a cumplir con los cinco fundamentos de seguridad, por lo que si desea comenzar su viaje hacia la ciberseguridad, lo alentamos a que se comunique.



 (55) 5543 6515
 marketing@louprey.com
 www.louprey.com
Kansas #7 Piso 2, Col. Nápoles, C.P. 03810,
Benito Juárez, Ciudad de Mexico