Brechas de seguridad: Ransomware y gestión del riesgo

El ransomware se ha consolidado como una de las amenazas más significativas en el ámbito de la ciberseguridad, especialmente en sectores críticos como el de la salud. Es fundamental comprender la seriedad de estas amenazas y adoptar medidas preventivas y reactivas adecuadas.

1. Medidas preventivas y detección temprana

Es imperativo implementar soluciones robustas de ciberseguridad para proteger los sistemas y datos. La capacitación continua del personal en ciberseguridad, incluyendo la identificación y manejo de correos electrónicos de phishing, es vital para prevenir incidentes. Además, es esencial mantener un monitoreo constante de los sistemas y redes para detectar cualquier actividad sospechosa con rapidez, permitiendo una evaluación inmediata de las posibles consecuencias.

2. Planes de continuidad y recuperación

No basta con disponer de copias de seguridad; es crucial contar con un plan integral de continuidad de negocio que asegure la restauración rápida y eficiente de la disponibilidad de los datos y servicios en caso de un ataque. Este plan debe incluir procedimientos claros y documentados para la recuperación de datos. Es fundamental recordar que no se debe considerar la opción de pagar el rescate exigido por los cibercriminales. En su lugar, se deben conservar los datos cifrados y explorar iniciativas como "No More Ransom!" para facilitar la recuperación de la información.

3. Evaluación de impacto y estrategia de respuesta

Ante una brecha de seguridad, es necesario evaluar de manera rápida y precisa el impacto del incidente. Esto incluye identificar las categorías de datos afectados, el número de registros comprometidos y el número de personas involucradas, así como la capacidad para restaurar la disponibilidad y la confidencialidad de los datos. Esta evaluación es esencial para cumplir con los requisitos del Reglamento General de Protección de Datos (RGPD), que obliga a notificar cualquier brecha a la autoridad de control correspondiente dentro de las 72 horas. También es necesario comunicar a las personas afectadas cualquier brecha que suponga un alto riesgo para sus derechos y libertades.

En ESCURA disponemos de un equipo de expertos en Protección de Datos preparados para resolver cualquier consulta.