CASO PRÁCTICO · SERGIO CARRETERO

Para abordar el riesgo crítico identificado en la empresa del cliente, es fundamental desarrollar un enfoque estructurado que permita priorizar, revisar y evaluar las medidas de tratamiento implementadas. En este sentido, la gestión del riesgo debe alinearse con estándares reconocidos, como ISO/IEC 27005, que proporciona directrices específicas para el análisis y la gestión de riesgos en seguridad de la información.

En primer lugar, la priorización de las medidas de tratamiento debe basarse en una combinación de factores clave, como la criticidad del riesgo, el impacto potencial en el negocio y la factibilidad de implementación de los controles. Para lograrlo, es recomendable utilizar metodologías como el análisis costo-beneficio y la matriz de riesgo, donde se evalúa la probabilidad de ocurrencia del evento adverso y su impacto en la organización. Aquellas medidas que reduzcan significativamente el riesgo con un costo y esfuerzo razonables deben considerarse prioritarias. Por ejemplo, en el caso de la pérdida de integridad de los datos en el sistema de gestión de clientes, se puede priorizar la implementación de controles de acceso basados en roles (RBAC), la validación de datos en múltiples capas y la auditoría continua de cambios en la base de datos.

El proceso de revisión y actualización periódica de los planes de tratamiento es esencial para asegurar que estos sigan siendo efectivos en un entorno empresarial en constante cambio. Para ello, se recomienda establecer revisiones programadas basadas en la frecuencia de evolución del riesgo y la aparición de nuevas amenazas. Este proceso puede incluir auditorías internas y externas, pruebas de penetración periódicas y la actualización de los controles en función de cambios normativos o tecnológicos. Además, la empresa debe fomentar una cultura de seguridad que permita a los empleados reportar incidentes o vulnerabilidades detectadas en los sistemas.

Para monitorizar la efectividad de los planes de tratamiento implementados, es crucial definir indicadores clave de rendimiento (KPI) que proporcionen información cuantificable sobre el desempeño de los controles de seguridad. Algunos KPI relevantes en este contexto pueden incluir:

1. Tasa de errores o inconsistencias detectadas en la base de datos: Indicador que mide la cantidad de registros alterados indebidamente o con errores, reflejando la efectividad de los mecanismos de integridad de datos.

2. Número de intentos de acceso no autorizado bloqueados: Permite evaluar la eficacia de los controles de autenticación y autorización.
3. Tiempo promedio de detección y respuesta ante incidentes de integridad de datos: Refleja la capacidad de la empresa para reaccionar y mitigar el impacto de eventos adversos.
4. Cumplimiento de auditorías y revisiones de integridad: Indica el grado de adherencia a las políticas internas y normativas externas sobre protección de datos.

En cuanto a las opciones ante un riesgo, las organizaciones pueden elegir entre cuatro estrategias principales:

1. Evitar el riesgo, eliminando la actividad o proceso que lo genera.
2. Mitigar el riesgo, reduciendo su impacto o probabilidad mediante la implementación de controles.
3. Transferir el riesgo, delegándolo a un tercero, como una aseguradora o un proveedor de servicios especializado.
4. Aceptar el riesgo, asumiendo las consecuencias cuando el costo de mitigación es mayor que el impacto esperado.

La efectividad del tratamiento del riesgo se puede determinar a través de la implantación de controles y la medición de su impacto en la reducción del riesgo residual. Para ello, es recomendable realizar pruebas de efectividad, como auditorías de seguridad, simulaciones de ataques y análisis forense en caso de incidentes. Adicionalmente, se pueden emplear modelos de madurez que permitan evaluar la evolución de la seguridad de la información en la empresa.

BIBLIOGRAFÍA

Guide for conducting risk assessments. (2012). https://doi.org/10.6028/nist.sp.800-30r1

Pincho, P., Messias, I., & Alturas, B. (2023). User perceptions about online personal data transmissibility. En *Advances in marketing, customer relationship management, and e-services book series* (pp. 140-158). https://doi.org/10.4018/978-1-6684-8958-1.ch007

Putra, A. P., & Soewito, B. (2023). Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector. *International Journal Of Advanced Computer Science And Applications*, *14*(4). https://doi.org/10.14569/ijacsa.2023.0140468