Campus Ribas Formación
20/09/2025

Crónica de la valoración en el comité de crisis de las causas de la brecha y de las medidas que debían haberse adoptado.

Brecha de seguridad en un sistema de IA

Los lamentos del día después

ribas

Noticia del día

Un volumen importante de datos personales de clientes de la empresa ha sido publicado por grupo de delincuentes especializado en ataques de ransomware que ha descubierto en los sistemas de inteligencia artificial vulnerables una gran oportunidad para obtener datos personales e información confidencial.

ribas

Cuenta personal con datos del CRM

El origen de los datos publicados se encuentra en una cuenta personal que un comercial abrió en un sistema de IA con el fin de analizar los datos del CRM de la empresa y optimizar y automatizar la gestión de su cartera de clientes.

Primeras acciones del comité de crisis

Las primeras acciones del equipo de ciberseguridad y del del comité de crisis se ha concentrado, entre otros, en los siguientes objetivos:

1. Revocar el acceso del sistema de IA al CRM.
2. Bloquear las integraciones no autorizadas mediante API keys, conectores y plugins.
3. Requerir al usuario del sistema de IA para que elimine de forma segura la información extraída o elimine la cuenta.
4. Analizar el alcance de la filtración.
5. Clasificar la información expuesta.
6. Restantes acciones habituales en el caso de brecha.

Los lamentos del día después

Una vez realizadas las acciones más críticas, llega la hora de los lamentos, el momento de analizar las medidas que podían haber evitado la brecha.

(Todos sabemos desde hace años que no hay que contestar este tipo de preguntas-trampa en el formulario de notificación de una brecha. Ni las medidas que se podían haber aplicado para prevenir la brecha, ni las acciones correctoras realizadas, ni las medidas que se aplicarán a partir de ahora para evitar que una brecha de este estilo vuelva a producirse).

Pero internamente, realizar este ejercicio es fundamental. Y es en ese instante cuando se descubren las consecuencias de haber tardado tanto en aplicar las medidas necesarias para prevenir el uso inadecuado de los sistemas de IA en la empresa.

RAT desactualizado

En el momento de valorar los riesgos de incumplimiento que la autoridad de control puede detectar en el momento de requerir más información sobre la brecha, el comité de crisis verifica que el registro de actividades de tratamiento no contempla en ninguna sección el uso de sistemas de IA.

ribas

Evaluaciones de impacto desactualizadas

El comité de crisis también comprueba que las evaluaciones de impacto están desactualizadas y que no contemplan el uso de sistemas de IA en los tratamientos evaluados.

Análisis de riesgos desactualizados

El comité de crisis también comprueba que los análisis de riesgos están desactualizados y que no contemplan el uso de sistemas de IA en los tratamientos evaluados.

El seguro de RC no lo cubre

Otro de los “descubrimientos” del comité de crisis es que, ni el seguro de responsabilidad civil ni el seguro de ciberriesgo, incluyen en su cobertura el tratamiento de datos personales en sistemas de IA, por lo que la compañía aseguradora no se va a hacer cargo de una eventual indemnización por los daños y perjuicios causados a los clientes afectados ni de las sanciones administrativas correspondientes.

Algunas de las medidas que podían haber evitado la brecha

Políticas y procedimientos
Política de uso de la inteligencia artificial con una sección específica para el Shadow AI.
Prohibición expresa del shadow AI y de la integración de cuentas personales con sistemas corporativos.
Procedimiento de homologación de sistemas de IA.
Procedimiento de aprobación de casos de uso rápido.
Alternativas seguras y supervisadas
Suministro de sistemas de IA homologados a los usuarios.
Registro de sistemas de IA homologados por la empresa.
Registro de casos de uso aprobados.
Revisión periódica de casos de uso de IA en todos los departamentos.
Sandbox interno o externo para probar casos de uso sin datos.
Controles técnicos
Sistemas DLP (Data Loss Prevention) para detectar envíos de datos sensibles a dominios no autorizados.
Monitorización de accesos a sistemas de IA y de logs.
Bloqueo del acceso a sistemas de IA no homologados mediante los firewall y servidores proxy corporativos.
Gestión centralizada de identidades, que impida el uso de credenciales externas en sistemas corporativos.
Restricción de integraciones externas en el CRM - Bloqueo de APIs no aprobadas.
Monitorización de logs y anomalías en el CRM y otras aplicaciones corporativas.
Formación y concienciación
Formación obligatoria continuada para todos los usuarios en materia de IA.
Cumplimiento de los requisitos del RIA en la formación obligatoria.
Formación avanzada para usuarios con funciones de supervisión de los resultados.
Formación avanzada para departamentos críticos.
Campañas continuadas de concienciación.
Visualización de casos reales que provocaron perjuicios.

El 13% de las organizaciones ha sufrido brechas en modelos o aplicaciones de IA, y el 97% no contaba con controles de acceso adecuados, según el último informe de IBM

El coste medio de una brecha de datos en EE. UU. alcanza los 10,22 millones de dólares, mientras que la media global se reduce a 4,44 millones. Solo el 49% de las organizaciones afectadas planea invertir en seguridad.

Sep 4, 2025

Este documento forma parte del nivel avanzado de la formación obligatoria en materia de IA prevista en el artículo 4 del Reglamento de IA.

ribas

Características de nuestro curso

#	Pregunta	☑
1	¿El curso está adaptado a los conocimientos técnicos, experiencia, educación y formación del usuario de los sistemas de IA que se van a utilizar? Por ejemplo, el curso tiene un nivel básico y un nivel avanzado.	☑
2	¿El curso está adaptado al contexto previsto para el uso de los sistemas de IA?	☑
3	¿El curso tiene en cuenta el rol de la empresa o la posición que ocupa en la cadena de valor de la IA?	☑
4	¿El curso tiene en cuenta los casos de uso y los riesgos específicos del sector al que pertenece la empresa?	☑
5	¿El curso tiene en cuenta los casos de uso y los riesgos específicos del departamento que va a utilizar el sistema de IA en la empresa?	☑
6	¿El curso tiene en cuenta los casos de uso y los riesgos específicos del sistema de IA que se va a utilizar?	☑
7	¿El curso tiene en cuenta el perfil de las personas o los colectivos de personas afectadas por el uso del sistema de IA? Por ejemplo, clientes, candidatos a un puesto de trabajo, trabajadores, pacientes, etc.	☑
8	¿El curso permite mejorar las capacidades, los conocimientos y la mejora del nivel de comprensión de la IA de los usuarios de los sistemas de IA?	☑
9	¿El curso permite preparar al usuario para realizar un uso informado y responsable de los sistemas de IA?	☑
10	¿El curso permite que el usuario tome conciencia de las oportunidades y de los riesgos que plantea la IA?	☑
11	¿El curso permite que el usuario tome conciencia de los perjuicios que la IA puede causar?	☑
12	¿El curso se centra en los aspectos éticos y jurídicos del uso de sistemas de IA?	☑
13	¿El curso es auditable y ofrece trazabilidad sobre la actividad del alumno?	☑
14	¿El curso emite de forma automática un certificado de finalización de la formación para cada alumno?	☑
15	¿El curso permite crear una evidencia indubitada con sello de tiempo y sello notarial que acredita la fecha en la que la empresa ha impartido la formación?	☑

ribas

Si deseas más información sobre este curso, que puede ser adaptado a la medida de tu empresa, puedes enviar un mensaje a xavier.ribas@ribastic.com

ribas

Datos de contacto

Nombre del despacho	Ribas
Domicilio	Diagonal 640 1C - 08017 Barcelona
Persona de contacto	Xavier Ribas
Correo electrónico	xavier.ribas@ribastic.com
Teléfono fijo	934940748
Teléfono móvil	639108413
LinkedIn	https://www.linkedin.com/in/javierribas/
Web	http://ribas.legal
Blog	http://xribas.com