CRAM HERRAMIENTA EXCEL

Paso a paso

La Matriz de Auditoría de Riesgos Cibernéticos (CRAM) es una herramienta analítica que ayudará a las empresas de fabricación a identificar, analizar, priorizar los riesgos y establecer medidas de protección con prontitud.

Esta breve guía tiene como objetivo apoyarle en la aplicación de la herramienta Excel CRAM. Por favor, ¡lea antes el Manual CRAM!

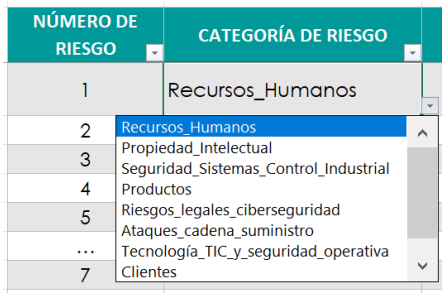
El CRAM incluye:

- **Número de riesgo** fijado automáticamente, sólo para apoyar en la identificación del riesgo.

NÚMERO DE RIESGO
1
2
3
4
5
…

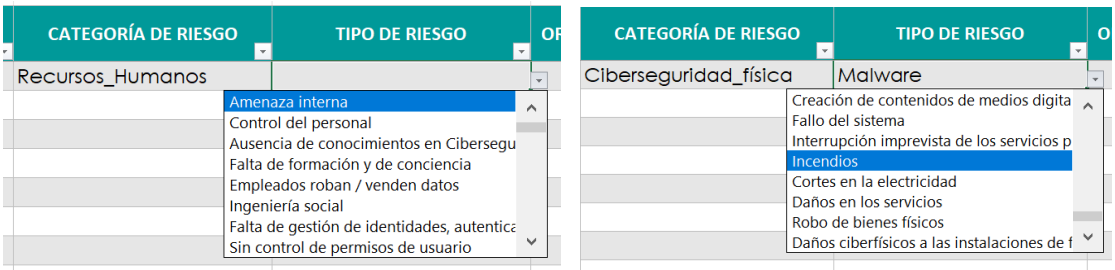
- **Categoría de riesgo**

Seleccione en la herramienta la categoría de riesgo, la descripción de las categorías se presenta en el Manual CRAM.



- **Tipo de riesgo**

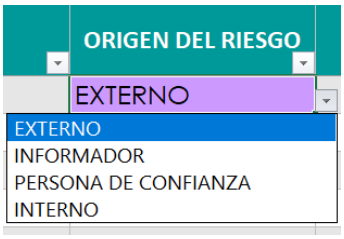
Según la categoría seleccionada, la herramienta CRAM le sugerirá el tipo de riesgo correspondiente.



En algunos tipos de riesgo, hay un menú desplegable donde se pueden encontrar algunos riesgos más que no son visibles.

- **Fuente del riesgo**

Seleccione el origen del riesgo: Externa, Insider, Insider de confianza, Interna.



Fuente del riesgo	Descripción
EXTERNA	Los ataques de fuerzas externas se originan en el entorno digital.
INFORMADOR	Una amenaza causada por un empleado que utilizará el acceso autorizado, consciente o inconscientemente, para hacer daño a la seguridad de la empresa.
PERSONA DE CONFIANZA	Es cualquier persona a la que se le ha dado acceso a los sistemas y locales físicos de una empresa. Esto incluye a antiguos empleados, proveedores, clientes, socios comerciales, visitantes u otros terceros.
INTERNA	Fuente interna (hardware, red, software, organización).

- **Descripción del riesgo**

Campo abierto para la descripción del riesgo. Esto ayudará a definir mejor el riesgo y los siguientes pasos del proceso.

* Si el tipo de riesgo es "*Problemas de integridad de datos*", incluya el tipo de datos en la "*Descripción del riesgo*".

PROBLEMAS DE INTEGRIDAD DE DATOS
Datos digitales de alto nivel
Datos digitales de bajo nivel
Datos financieros
Datos físicos
Datos de usuario

- **Costes potenciales asociados a las consecuencias del riesgo**

Campo abierto para identificar todos los costes potenciales asociados a las consecuencias de que el riesgo se produzca. Por ejemplo: el valor monetario relacionado con el robo de información propietaria o el fraude financiero; los costes relacionados con la pérdida severa de uso o productividad incluyen virus y malware, ataques de denegación de servicio a servidores web, abuso de privilegios de acceso y vandalismo o robo de equipos...

- **Departamento de la organización que podría verse afectado**

Campo abierto para identificar el (o los) departamento(s) de la organización que podría(n) verse afectados.

- **Medidas/acciones preventivas aplicadas anteriormente**

Campo abierto para identificar y describir las medidas/acciones preventivas aplicadas anteriormente (si procede).

- **Evaluación y cálculo de los elementos de riesgo** (impacto del riesgo, probabilidad del riesgo, nivel de riesgo global)

IMPACTO	PROBABILIDAD	NIVEL DE RIESGO
ACEPTABLE	INCIERTO	BAJO
TOLERABLE	POSIBLE	
INDESEABLE	PROBABLE	
INADMISIBLE		

BAJO
MEDIO
ALTO
EXTREMO

Datos relativos a la probabilidad (es decir, la posibilidad de que se produzca un riesgo) y al impacto (es decir, la gravedad del riesgo en caso de producirse) de los riesgos identificados. Se califican tanto la probabilidad como el impacto utilizando una escala de Bajo (0), Medio (1), Alto (2) y Extremo (3).

BAJO	MEDIO	ALTO	EXTREMO
0 - Aceptable	1 - Moderado	2- En general, no es aceptable	3 - Intolerable
OK PARA CONTINUAR	TOMAR MEDIDAS DE ATENUACIÓN/MITIGACIÓN	BUSCAR APOYO - acciones a realizar en 6 meses	PONER EL EVENTO EN ESPERA

IMPACT			
ACEPTABLE	TOLERABLE	INDESEABLE	INADMISIBLE
Poco o ningún efecto	Los efectos se perciben pero sin resultado crítico	Grave impacto en el curso de la acción y el resultado	Podría resultar en un desastre
BAJO 1	MEDIO 4	MEDIO 6	ALTO 10
BAJO 2	MEDIO 5	ALTO 8	EXTREMO 11
MEDIO 3	ALTO 7	ALTO 9	EXTREMO 12

- **“Gatillos”**

Campo abierto para describir los “gatillos” o acciones que hacen que el sistema inicie una respuesta. Los gatillos producen una alerta cuando se produce un incidente o comportamiento anómalo.

- **Mitigación/acciones que deben aplicarse**

Campo abierto para la identificación de acciones de mitigación para los riesgos calificados como Medio a Alto. Se trata de intentar eliminar o reducir la frecuencia, la magnitud o la gravedad de la exposición a los riesgos, o de minimizar el impacto potencial de una amenaza.

En el Manual CRAM se identifican dos tipos de controles de acción: preventivos y correctivos en cada una de las nueve categorías de riesgo.

- **Costes potenciales de la mitigación**

Campo abierto para la identificación de los costes potenciales de la mitigación.

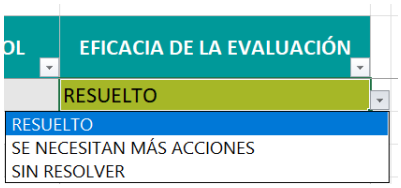
- **“Deadline” o fecha límite**

Plazo de ejecución de las acciones.

- **Responsabilidad**

Campo abierto para la identificación clara de la persona responsable de la gestión de riesgos y de el/la supervisor/a responsable del control.

- **Eficacia de la evaluación**



El CRAM de Encrypt 4.0 es un proceso sistemático y continuo. Es un proceso cíclico que una vez que ha identificado, analizado, valorado, evaluado, tratado y aceptado los riesgos, debe realizar un proceso de seguimiento y revisión de los mismos. En caso de que el problema persista, tendrá que aplicar más acciones complementarias para resolverlo, y para ello tendrá que volver al paso anterior de tratamiento de riesgos. Y si el problema sigue sin resolverse, tendrá que volver a evaluar el riesgo.

- **Informe**

Tras rellenar todos los campos necesarios, ya tiene su informe de riesgos completado.

El proyecto ENCRYPT4.0 (2020-1-RO01-KA202-079983) ha sido financiado con el apoyo de la Comisión Europea. Esta publicación refleja únicamente la opinión del autor, y la Comisión no se hace responsable del uso que pueda hacerse de la información contenida en ella.