**Universidad Nacional**

**Escuela de informática**

**Matriz de riesgos: Qué es y cómo se hace una**

En el ámbito empresarial, los riesgos, así como también las amenazas y oportunidades, deben conocerse en profundidad. Entender qué riesgos corre nuestra empresa, es vital para su evolución y crecimiento. Al comprenderlos, es más fácil sortearlos, a través de distintas actividades. Una herramienta de suma importancia para esto, es la **matriz de riesgos**.

**Contenidos**

[1 ¿Qué es una matriz de riesgos?](https://ciberseguridadtips.com/matriz-de-riesgos/#Que_es_una_matriz_de_riesgos)

[2 ¿Para qué sirve una matriz de riesgos?](https://ciberseguridadtips.com/matriz-de-riesgos/#Para_que_sirve_una_matriz_de_riesgos)

[3 Cómo realizar una matriz de riesgos](https://ciberseguridadtips.com/matriz-de-riesgos/#Como_realizar_una_matriz_de_riesgos)

[3.1 Elementos de la matriz de riesgos informáticos](https://ciberseguridadtips.com/matriz-de-riesgos/#Elementos_de_la_matriz_de_riesgos_informaticos)

[4 ¿Cómo elaborar una matriz de riesgos?](https://ciberseguridadtips.com/matriz-de-riesgos/#Como_elaborar_una_matriz_de_riesgos)

[4.1 1 | Identificar los riesgos y clasificarlos](https://ciberseguridadtips.com/matriz-de-riesgos/#1_Identificar_los_riesgos_y_clasificarlos)

[4.2 2 | Priorización de riesgos identificados](https://ciberseguridadtips.com/matriz-de-riesgos/#2_Priorizacion_de_riesgos_identificados)

[4.3 3 | Evaluar la frecuencia, probabilidad e impacto](https://ciberseguridadtips.com/matriz-de-riesgos/#3_Evaluar_la_frecuencia_probabilidad_e_impacto)

[4.4 4 | Representar gráficamente los riesgos identificados](https://ciberseguridadtips.com/matriz-de-riesgos/#4_Representar_graficamente_los_riesgos_identificados)

[5 A modo de conclusión](https://ciberseguridadtips.com/matriz-de-riesgos/#A_modo_de_conclusion)

**¿Qué es una matriz de riesgos?**

La matriz de riesgos es una herramienta del ámbito de la **gestión**que busca determinar cuáles son los riesgos más importantes para la seguridad y salud general de los trabajadores y activos de una empresa u organización. Se plantea en una clásica matriz para que su llenado sea simple, pero requiere de un arduo **análisis**de las distintas actividades que se desarrollan en la empresa.

**¿Para qué sirve una matriz de riesgos?**

La matriz de riesgos es la herramienta indicada para entender los**riesgos que corre la organización**. Permite comparar por nivel de riesgos las distintas tareas que se llevan a cabo. Una vez que se cuente con esa información, es posible poder tomar acciones concretas para la solución completa o disminución de los mismos.

Los riesgos son distintas **situaciones o tópicos que ponen en peligro** la integridad de una organización. Tanto el ámbito material, como la salud de las personas, pueden estar en riesgo.

**Cómo realizar una matriz de riesgos**

El proceso general de una matriz de riesgos cuenta con cinco pasos generales:

* Identificación de riesgos
* Cálculo de **exposición al riesgo**
* Identificación de controles
* Cálculo de riesgo residual
* Aceptación o rechazo del riesgo residual

Ahora bien, ¿qué elementos se deben tener en cuenta y cuál es la forma en la que estos ingresan en la matriz?

**Elementos de la matriz de riesgos informáticos**

**Actividad:**se explicita la actividad o tarea que realizan los trabajadores de la empresa. Siempre conviene tener un listado de todas las actividades que se llevan a cabo, sean estas rutinarias o no. Es un plus poder llenar esta sección con la participación misma de los trabajadores.

**Probabilidad**: se refiere a establecer las posibilidades de que el riesgo se convierta en una realidad, de que llegue a producir el daño potencial. Puede expresarse de manera cualitativa o cuantitativa. Es decir, con conceptos generados (poco posible, muy posible, nulo) o directamente en números, si es cuantitativo.

**Riesgo**: Es la situación o evento, el cual es incierto, pero se sabe que tiene un **impacto negativo**. También se puede conceptualizar como la posibilidad de sufrir un **daño**de tipo físico o material por la exposición a un peligro específico.

**Peligro**: Es de donde viene el riesgo. La situación u objeto específico.

**Magnitud del daño o Severidad**: Es el índice que indicará que **nivel de impacto**que habrá si este peligro potencial termina concretándose.

En el ambiente de la **cibernética, es particularmente importante entender estos elementos**, debido a que a los peligros normales que tiene cualquier empresa en el factor humano, se le suma todo un mundo de riesgos y amenazas cibernéticas. Peligros que se deben tener en cuenta cada vez que se realice esta matriz de riesgos.

**¿Cómo elaborar una matriz de riesgos?**

Antes de empezar a diseñar tu **matriz de riesgos**es preciso apegarte a un marco normativo. En el caso de la seguridad de la información, puedes adoptar el marco ISO 27001.

**1 | Identificar los riesgos y clasificarlos**

Identificar los riesgos que puedan atenazar a una organización es un aspecto clave para lograr una mitigación del impacto de la misma. Ya que si una amenaza no está contemplada, pasará fácilmente por nuestro radar.

Sin embargo, tampoco debemos excedernos e identificar riesgos en exceso. Esto solo complicará las tareas administrativas con el mismo resultado: pasar por alto las amenazas reales. Recomendamos ceñirse al campo de acción de nuestra industria o sector.

El paso primordial para identificar los riesgos es atenernos a una clasificación. La que podría diagramarse de la siguiente manera:

* Riesgos internos: En productos o servicios, comunicaciones, estructura organizacional y la más importante en seguridad de la información.
* Riesgos externos: Catástrofes naturales, normativa legal, alteraciones o ataques a la cadena de suministro, entre otros.

Cada riesgo identificado debe contar con una ficha exhaustiva sobre la naturaleza del mismo. Desde el nombre, la clasificación hasta las posibles causas o consecuencias de la misma.

**2 | Priorización de riesgos identificados**

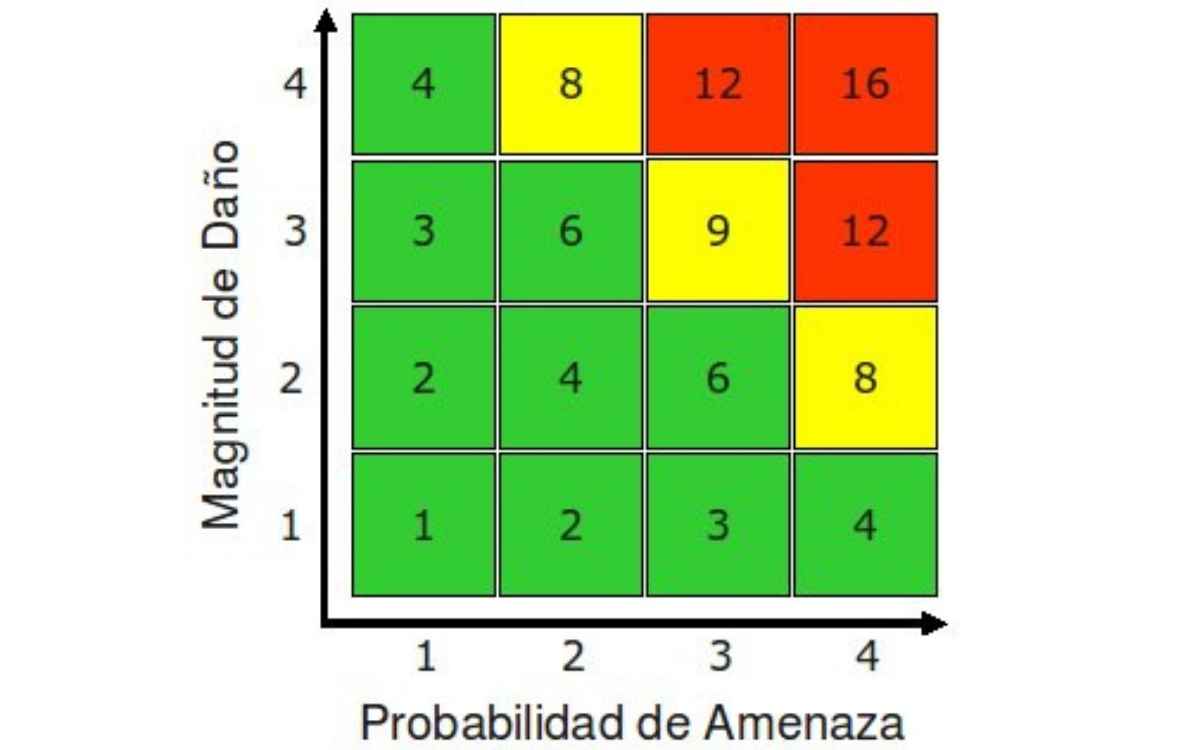
Ahora, ¿cuál es el parámetro para decidir a que amenaza en la **matriz de riesgo** se le debe dar más importancia? Esto lo fijaremos de acuerdo a la actitud que la empresa tome frente a los mismos:

* Apetito de riesgo: Hace referencia al grado de incertidumbre que la organización está dispuesta a tolerar.
* Tolerancia al riesgo: Existen organizaciones, que por su tamaño y trayectoria, pueden resistir mejor el impacto de un riesgo.
* Umbral de riesgo: El umbral de riesgo hace alusión al nivel máximo en que una empresa está dispuesta a tolerar una amenaza antes de iniciar acciones al respecto. Pero también fijará el mínimo que corresponderá a un nivel aceptable de exposición. Esto variará de acuerdo a la empresa.

**3 | Evaluar la frecuencia, probabilidad e impacto**

Ya estamos un paso más cerca de ver terminada nuestra **matriz de riesgos.** Pero todavía nos queda analizar la frecuencia e impacto de las amenazas.

* Frecuencia: La frecuencia hace alusión a la probabilidad de un riesgo se materialice. Esta se verá de la siguiente manera:
* Muy probable
* Probable
* Posible
* No muy posible
* Muy improbable
* Impacto: Luego de que se materialice el riesgo, se deberá definir el alcance de las consecuencias o del conjunto de ellas. Y cómo afecta este a la continuidad del negocio.
* Insignificante
* Menor
* Moderado
* Importante
* Catastrófico

*Poder tener una división de colores en la matriz de riesgos es vital para tener un orden visual a la hora de un análisis rápido.*

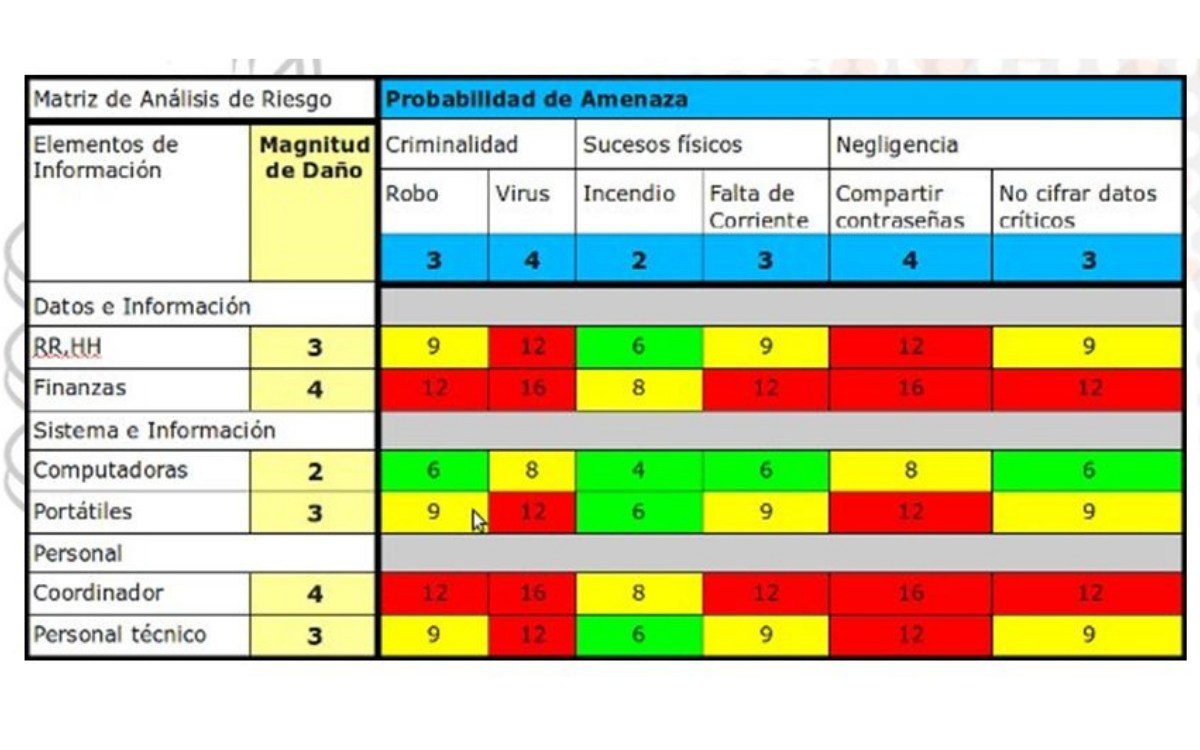
**4 | Representar gráficamente los riesgos identificados**

Finalmente, podemos diseñar nuestra **matriz de riesgos**. Esta se caracteriza por tener dos ejes, uno X y otro Y. Ambos con una representación de mayor a menor.

A partir de allí, se puede colocar cada riesgo en función del valor de la frecuencia de impacto. Si multiplicamos frecuencia e impacto, también tendremos como resultado el valor del riesgo residual. Será este número al que se le asigne un valor en colorimetría donde:

* Bajo Riesgo = 1 – 6 (verde)
* Medio Riesgo = 8 – 9 (amarillo)
* Alto Riesgo = 12 – 16 (rojo)

De esta manera, se va llenando la matriz con los riesgos y peligros específicos de cada organización, llegando a completarla con distintos colores y números según su probabilidad. Se divide según el **tipo de amenaza**, hasta lograr una matriz como esta:

*Se debe ser minucioso a la hora de elegir los peligros que se colocarán en la matriz de riesgos, buscando ser lo más conciso posible*.

**A modo de conclusión**

Generar una **matriz de riesgos** se torna cada vez más necesario para poder tener una organización con un funcionamiento correcto, con estabilidad y proyección a futuro.

Entender los peligros que corre una empresa implica poder entenderlos y actuar en consecuencia, buscandocontrarrestarlos con **acciones específicas, por ejemplo, de**[ciberdefensa](https://ciberseguridadtips.com/ciberdefensa/).

En el ámbito de la cibernética, los peligros están en aumento permanente, debido a una mayor cantidad y severidad de los [ciberataques](https://ciberseguridadtips.com/ciberataques/)**con malware**, al aumento del tráfico en las redes y a la importancia que tienen los sistemas cibernéticos en sí mismos.

De esta manera, esperamos que este artículo haya aclarado dudas sobre qué es una matriz de riesgos y sobre como esta se estructura. Así como también la **importancia vital**que esta posee en todos los ámbitos organizacionales, especialmente en el de la ciberseguridad.

Diagrama

Descripción generada automáticamente

Caso de análisis

La empresa TFG conta de 50 empleados , cada uno de ellos usa su laptop para trabajar desde la casa de habitación , para conectarse se usa un VPN que tiene solo una clave de 8 characters.

El trabajo de los empleados es trabajar en aspectos contables , pero todos tienen accesos a las BD, esto por tener que incluir modificar y borrar datos de las tablas.

La autenticación a los equipos tanto externo como interno es por medio del AD, pero si tiene un usuario admin que todos conocen.

Los expertos en computación son de bajos conocimientos por lo que implementaron un sistema de ingreso sin IPS, FW.

Los aplicativos para la gente externa son el la DMZ externa , sin embargo estos aplicativos llegan directo a las bases de datos para hacer consultas.

Sucede que uno de los empleados perdió su laptop, en este caso los de computación no sacaron del AD al empleado no tampoco se hizo estudio por medio de bitácoras de los que usan la VPN.

Que haría usted en caso de estar en esta empresa en el área de informática? Proponga soluciones

Que implementaría usted en este caso?

Complete la matriz de riesgos identificando cada uno de los riesgos.