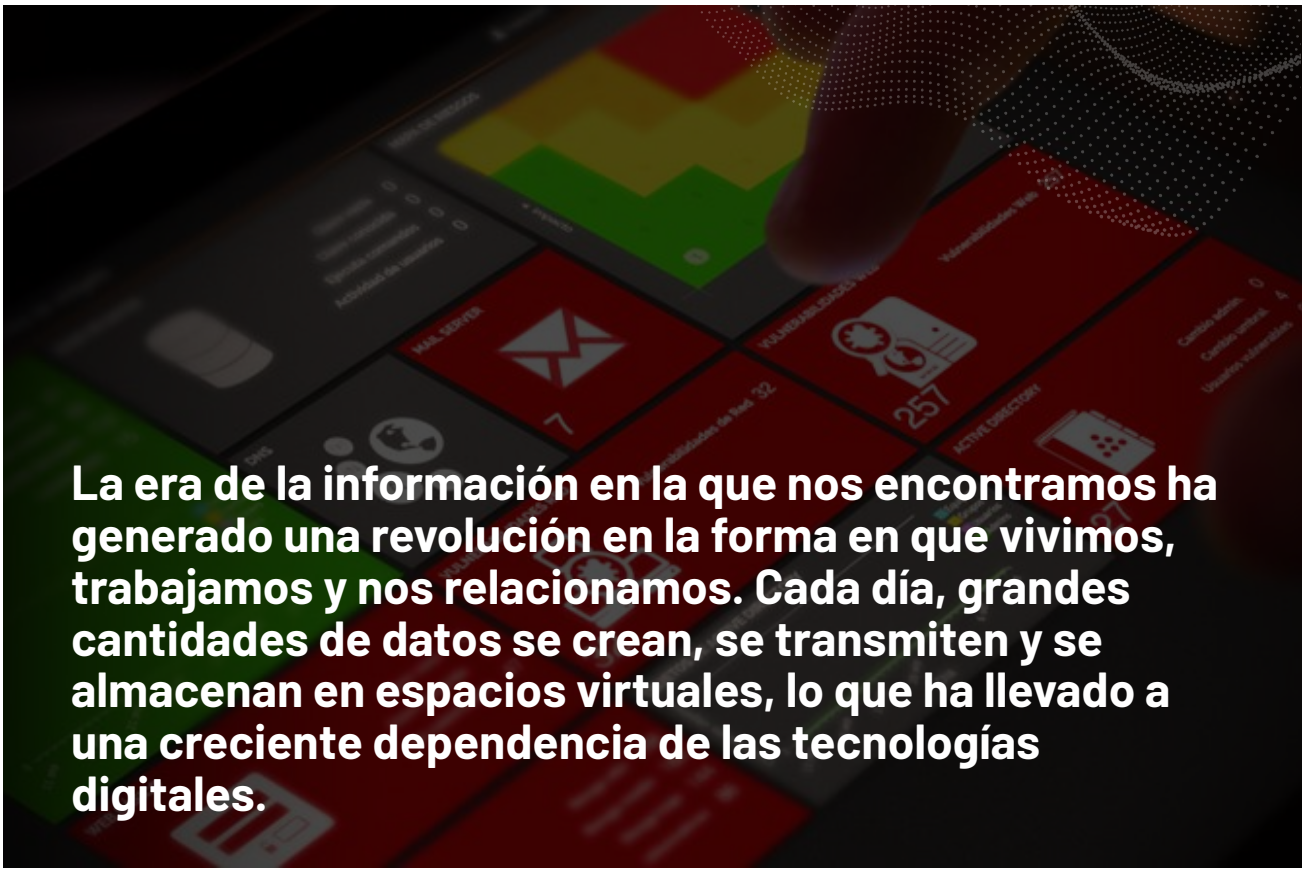
HACKNOID

Cómo Integrar una Matriz de Riesgos en tu Estrategia de Ciberseguridad

Anticipa, No Reacciones: Integra una matriz para prever y contrarrestar amenazas

www.hacknoid.com



La era de la información en la que nos encontramos ha generado una revolución en la forma en que vivimos, trabajamos y nos relacionamos. Cada día, grandes cantidades de datos se crean, se transmiten y se almacenan en espacios virtuales, lo que ha llevado a una creciente dependencia de las tecnologías digitales.

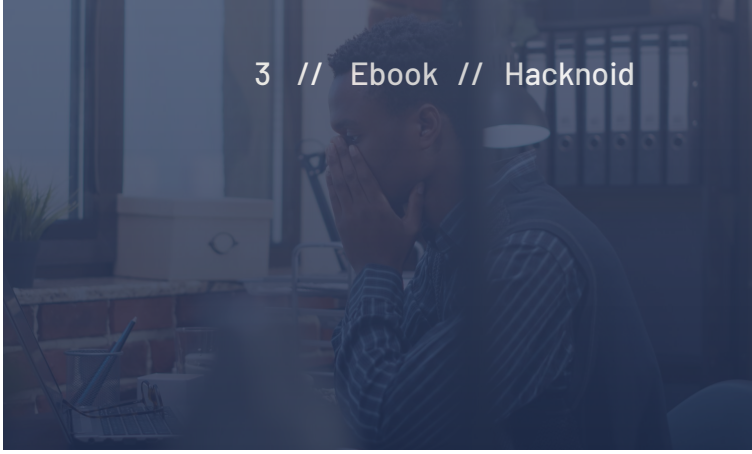
Las organizaciones, independientemente de su tamaño o sector, enfrentan desafíos constantes para proteger su información crítica. Los ciberataques no solo han aumentado en número, sino también en complejidad.

La proactividad como estándar

Adéntrate en la era donde la prevención y la preparación son más que esenciales; son vitales.

En este panorama, la **Matriz de Riesgos** emerge no solo como una herramienta, sino como un pilar esencial. Proporcionando un marco estructurado para identificar, evaluar y priorizar riesgos, esta herramienta va más allá de permitir a las organizaciones reaccionar ante amenazas.

Su verdadero poder **se centra en la anticipación**. En una era dominada por la digitalización, donde la rapidez y adaptabilidad definen el éxito, integrar una Matriz de Riesgos en la estrategia de ciberseguridad puede ser el factor determinante que te resguarde de consecuencias desastrosas.



¿Qué es una Matriz de Riesgos?

Una Matriz de Riesgos es una herramienta visual y analítica que se utiliza para identificar, evaluar y priorizar los riesgos asociados a cualquier actividad o proceso.

En el ámbito de la ciberseguridad, esta matriz se enfoca en los riesgos relacionados con la información y las infraestructuras tecnológicas.

Al evaluar tanto la probabilidad de ocurrencia de un evento adverso como el impacto que tendría en caso de materializarse, la matriz proporciona una comprensión clara de dónde deberían centrarse los esfuerzos y recursos de seguridad.

Principales dimensiones Matriz de Riesgos

Probabilidad

Refiere a la chance o frecuencia con que un determinado riesgo podría materializarse.

Se suele calificar en un rango, que puede ser numérico (por ejemplo, del 1 al 5) o descriptivo (bajo, medio, alto).

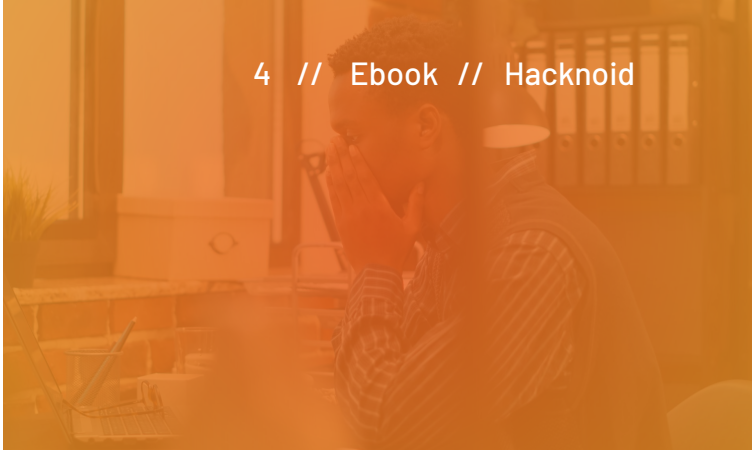
Impacto

Se refiere a las consecuencias o daños que se generarían si el riesgo se materializa. Al igual que la probabilidad, se categoriza en diferentes niveles según la severidad de sus efectos.

La intersección de estas dos dimensiones en la matriz **permite clasificar los riesgos** en categorías como "bajo", "medio", "alto" o "crítico". Por ejemplo, un riesgo con alta probabilidad y alto impacto sería considerado crítico y requeriría atención inmediata, mientras que uno con baja probabilidad y bajo impacto podría ser monitoreado, pero no sería prioritario.

Además de **ofrecer una visión panorámica de los riesgos**, la matriz es una herramienta dinámica. Debe ser revisada y actualizada regularmente para reflejar las cambiantes condiciones del entorno, la evolución de las amenazas y las modificaciones en los activos y recursos de la organización.

La importancia de la Matriz de Riesgos en ciberseguridad radica en su capacidad para **transformar datos y análisis abstractos en información accionable.** Al visualizar y entender dónde se encuentran los mayores riesgos, las organizaciones pueden tomar decisiones informadas sobre dónde invertir, qué amenazas mitigar de forma prioritaria y cómo distribuir de manera efectiva los recursos de seguridad.



6 pasos para integrar la Matriz de Riesgos

La clave de la anticipación

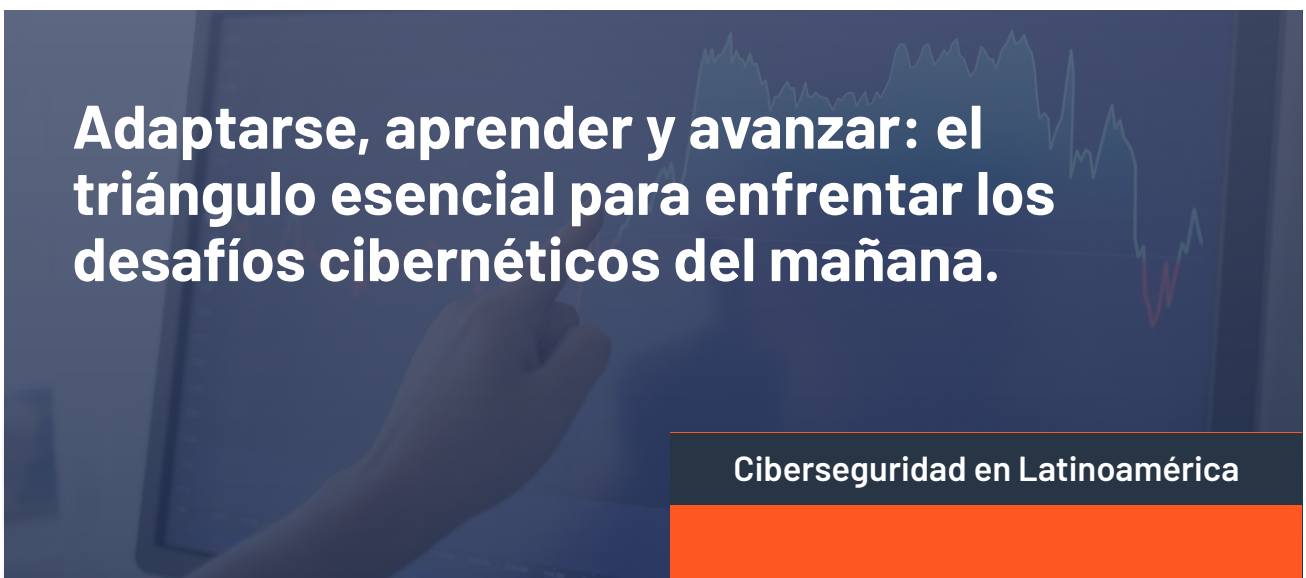
En un mundo donde la anticipación puede ser la diferencia entre la seguridad y la vulnerabilidad, es crucial contar con una estrategia estructurada.

Integrar una Matriz de Riesgos no es solo una tarea, sino una transformación hacia una seguridad más inteligente y desde una perspectiva preventiva.

Identificación de amenazas y vulnerabilidades

El primer paso es identificar los activos a proteger, pero que se van a desprender del proceso de negocio al cual proveen valor. Dependiendo de la criticidad PRIMERO del proceso de negocio, se asocian los activos y se pondera su criticidad posteriormente

- Esto implica no solo identificar amenazas genéricas sino también aquellas específicas para tu sector o negocio.
- Las vulnerabilidades pueden ser tanto tecnológicas (fallos en software, sistemas desactualizados) como humanas (colaboradores que desconocen protocolos de seguridad).
- Utilizar herramientas como escáneres de vulnerabilidades o auditorías de seguridad es esencial para obtener una imagen clara y actualizada de dónde se encuentran las brechas.



¿Por qué es clave identificar amenazas y vulnerabilidades dentro de tu empresa?

- Conocimiento Profundo del Entorno
- Prevención es Mejor que Restauración
- Optimización de Recursos
- Cumplimiento Regulatorio
- Confianza y Reputación
- Preparación para Respuestas de Incidentes
- Desarrollo Continuo

Ciberseguridad en Latinoamérica

+1.2 MM

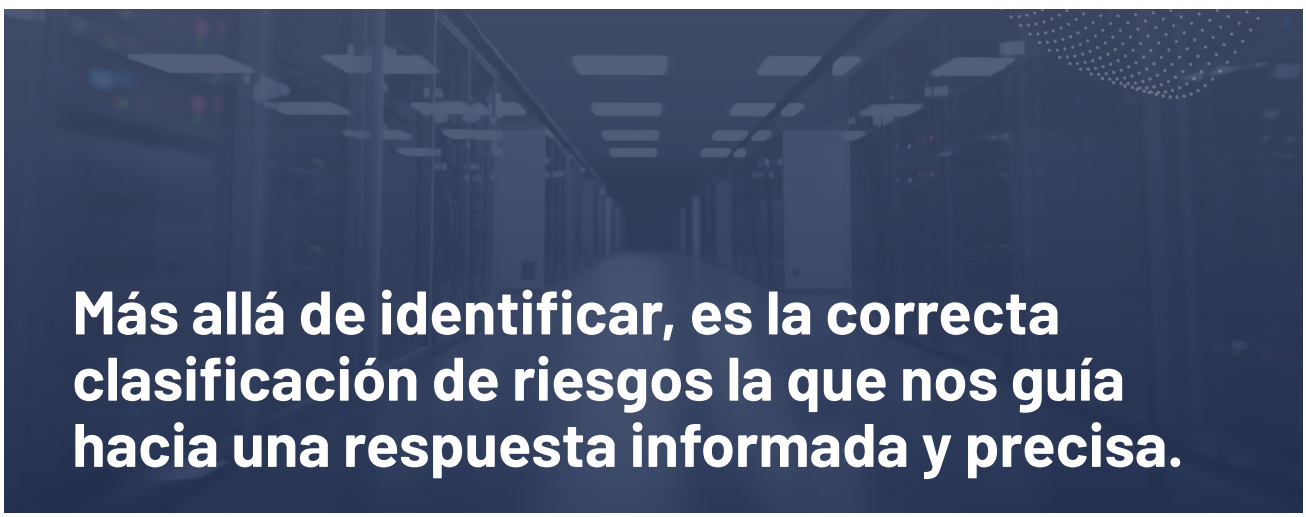
Ataques cibernéticos al día sólo en Latinoamérica

Fuente: Latin America Cybersecurity Market Report 2022-2028

Evaluación y clasificación de riesgo

Pulso de la Organización: Al evaluar y categorizar los riesgos, captamos el pulso vital de nuestra empresa. Entendemos sus fortalezas, debilidades y, más importante aún, las prioridades que deben establecerse para garantizar una operación segura y fluida.

- Tras la identificación, cada amenaza y vulnerabilidad debe ser evaluada en términos de su gravedad potencial y probabilidad de ocurrencia.
- Las consultas con diversos departamentos son esenciales, ya que diferentes áreas pueden ofrecer distintas perspectivas sobre el mismo riesgo. Consensuar esa mirada nos permite alinear esfuerzos.
- Al final de esta etapa, deberías tener una lista categorizada de riesgos según su importancia y urgencia. Esto permite tener un orden de prioridad para trabajar. Ya sea desde que tipo de acción en concreto se va a tomar, que pueden ser: mitigar, aceptar (cuando las medidas de mitigación son más costosas que la eventual materialización del riesgo), o transferir (por ejemplo a través de la contratación de un seguro); como de las acciones concretas según la elección anterior(por ejemplo qué medidas de mitigación se utilizarán, dentro de las posibles).



Fomento de la Colaboración

Las consultas interdepartamentales no solo enriquecen la evaluación de riesgos sino que también promueven un sentido de propiedad colectiva del proceso de ciberseguridad, alentando a todos los involucrados a ser parte activa de la solución.

Propuesta de medidas correctivas y preventivas

Frente a un panorama de riesgos identificados, no basta con soluciones genéricas. Cada amenaza exige una respuesta a medida, moldeada por la esencia y el contexto único de cada organización.

Una estrategia personalizada

- Con una lista clara de riesgos, el siguiente paso es desarrollar acciones específicas para abordarlos.
- Algunos riesgos pueden requerir soluciones tecnológicas, como firewalls o sistemas de detección de intrusos. Otros pueden ser abordados mediante capacitaciones o cambios en las políticas internas.
- Es esencial que estas soluciones se adapten a las particularidades de cada organización y su contexto.

Conociendo los riesgos, es hora de tejer una red de defensa que se ajuste perfectamente a las características y necesidades de tu organización.

Desde las barreras digitales hasta el empoderamiento humano, la seguridad se construye con soluciones adaptadas y precisas.

Priorización de acciones

No todas llevan el mismo peso. Es esencial discernir y priorizar acciones basándonos no solo en el impacto potencial, sino también en la probabilidad de ocurrencia

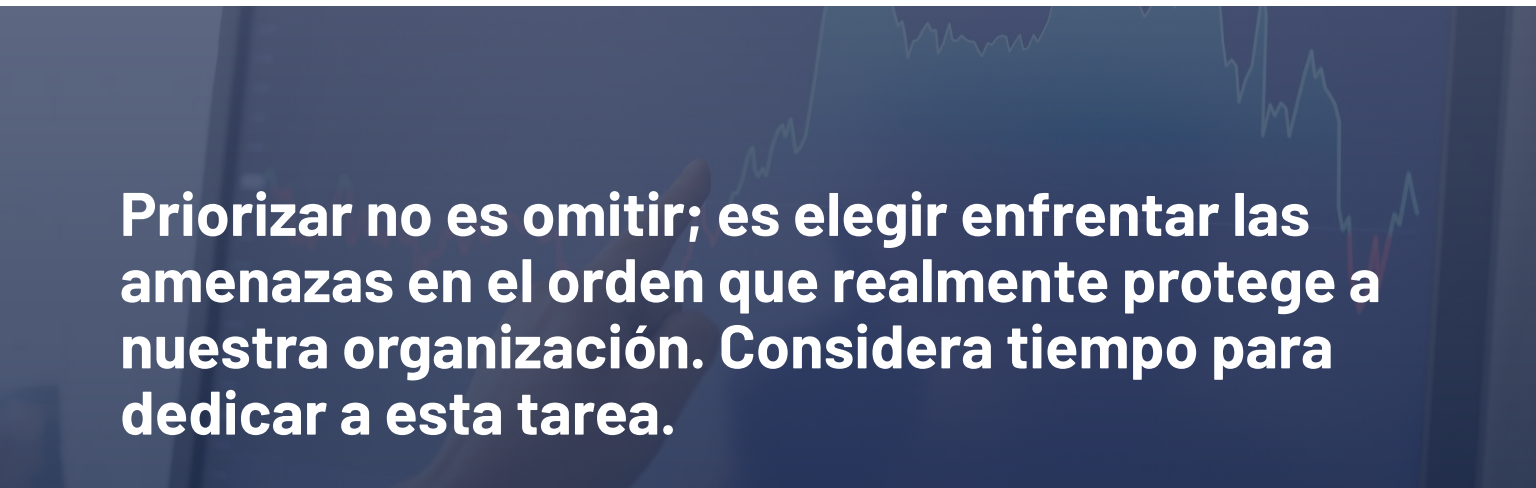
- Mientras que algunos riesgos pueden ser extremadamente dañinos, su probabilidad de ocurrencia podría ser baja. Por otro lado, riesgos menores pero más probables podrían necesitar atención inmediata debido a su frecuencia.
- La Matriz de Riesgos te permite visualizar cuáles son las amenazas más apremiantes, asegurando que los recursos se utilicen de manera efectiva.
- Debes tener en cuenta que se trata de un ciclo continuo que se retroalimenta y que es importante contar con herramientas y recursos que permitan que estés al día tanto en la identificación de nuevos activos de tu empresa como de las amenazas que los acechan.

¿Cómo visualizar a través de una Matriz de Riesgos cuáles son las amenazas más apremiantes?

La Matriz de Riesgos es una herramienta visual que ordena las amenazas según dos dimensiones principales: su probabilidad de ocurrencia y su impacto potencial.

Al representar estos dos factores en un eje horizontal y vertical, obtenemos un cuadrante que clasifica los riesgos en distintas categorías. Amenazas que tengan alta probabilidad e impacto se sitúan en la esquina superior derecha, siendo estas las que requieren atención inmediata.

En contraste, aquellas con baja probabilidad e impacto quedan en la esquina inferior izquierda, indicando que, si bien no deben ser ignoradas, pueden no ser la principal prioridad en ese momento. Al proporcionar esta visualización clara, las organizaciones pueden distribuir sus recursos y esfuerzos de manera más efectiva, dirigiendo su atención primero a las amenazas más críticas.



Priorizar no es omitir; es elegir enfrentar las amenazas en el orden que realmente protege a nuestra organización. Considera tiempo para dedicar a esta tarea.

Implementación

Del Papel a la Práctica: No basta con proponer soluciones; es en la implementación donde enfrentamos el desafío real, ajustando y adaptándonos a las circunstancias del terreno.

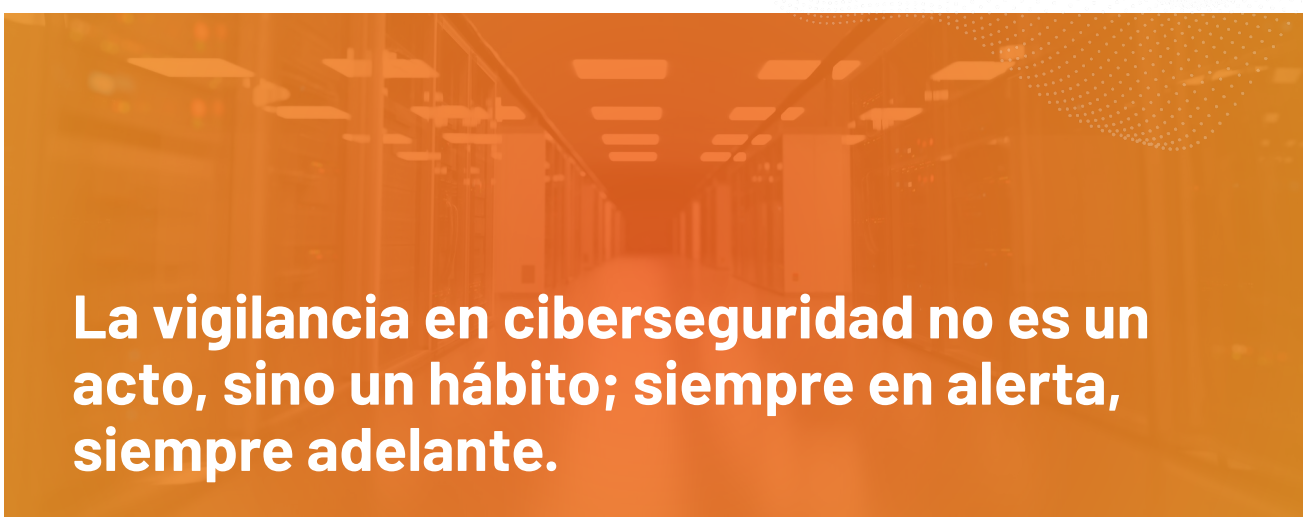
- Este paso implica poner en marcha las soluciones propuestas. Puede requerir inversiones significativas en tecnología o recursos humanos.
- Es crucial monitorear de cerca esta fase para identificar y corregir rápidamente cualquier inconveniente que pueda surgir durante la implementación.
- Una matriz de riesgos generales de una compañía puede derivar luego en diversas matrices de riesgo específicas para cada área. Idealmente éstas deberían conversar entre sí, para poder conformar un sistema eficiente y consistente.

La integración exitosa de una Matriz de Riesgos no es un destino, sino un viaje continuo. Requiere un compromiso a largo plazo y la colaboración de todos los niveles de la organización para garantizar una gestión efectiva del riesgo en el mundo digital actual.

Monitoreo y actualización constante

El paisaje de las amenazas cibernéticas nunca duerme; tampoco debería hacerlo nuestra vigilancia.

- La naturaleza dinámica de la ciberseguridad implica que lo que es seguro hoy, podría no serlo mañana. Las nuevas amenazas surgen constantemente.
- Revisar y actualizar la Matriz de Riesgos debería ser un proceso continuo, idealmente, con revisiones periódicas que reflejen el entorno cambiante de la ciberseguridad.



¿Por qué el monitoreo continuo en ciberseguridad es vital?

Amenazas en evolución: Los ciberdelincuentes innovan constantemente. Sin actualización constante, las organizaciones se vuelven vulnerables.

Tecnologías emergentes: La tecnología evoluciona rápidamente, trayendo consigo nuevas vulnerabilidades. Es crucial mantener sistemas y software al día.

Reputación y confianza: Un incidente puede manchar la reputación de una empresa por años. El monitoreo permite detectar y atender amenazas tempranamente.

Cumplimiento normativo: Las estrictas regulaciones de datos exigen un monitoreo constante para evitar sanciones y asegurar la protección de información.

Eficiencia financiera: Aunque el monitoreo tiene un costo, prevenir una brecha de seguridad resulta más económico a largo plazo.

Herramientas y Recursos

Para una implementación exitosa

La implementación exitosa de una Matriz de Riesgos y una estrategia de ciberseguridad global requiere del uso adecuado de herramientas y recursos.

Estos instrumentos no sólo facilitan el proceso, sino que permiten una evaluación más precisa y acciones correctivas más eficientes.

Hacknoid

Hacknoid emerge como una herramienta indispensable en el panorama actual.

Esta plataforma de análisis de vulnerabilidades brinda una visión panorámica y detallada de la infraestructura tecnológica de cualquier organización.

El software detecta cifrados de baja calidad, configuraciones defectuosas, y vulnerabilidades de sistemas, tanto a nivel local como remoto, alertando de manera eficaz tanto endpoints, servidores, diferentes dispositivos IP, aplicativos y servicios asociados, entre otras funciones de auditoría.

Además, su enfoque proactivo y simplificado para identificar amenazas, antes de que los ciberdelincuentes las detecten, le otorga una ventaja única en el mercado.

Plataforma integral

Solución completa que engloba todos los elementos de tu entorno TI.

Sin puntos ciegos

Saber que cada eslabón de tu cadena está seguro es crucial. No importa cuán insignificante pueda parecer un dispositivo, Hacknoid asegura que esté monitoreado y que se alerta a tiempo para poder resolverlo antes de que pueda materializarse una explotación de la vulnerabilidad.

Protección sin excepciones

Ignorar ciertos dispositivos puede tener consecuencias graves. Hacknoid se encarga de que cada eslabón de tu red esté monitoreado continuamente.

HACKNOID

Solicita una Demo de Hacknoid

www.hacknoid.com

URUGUAY
Durazno 1504 Oficina 1 esq. Martínez Trueba
Palermo, Montevideo

CHILE
Av. Nueva Tajamar 481 Torre Norte, Of 1403,
Las Condes, Santiago