HACKNOID

Gobierno corporativo y Ciberseguridad sobre la mesa de los directorios

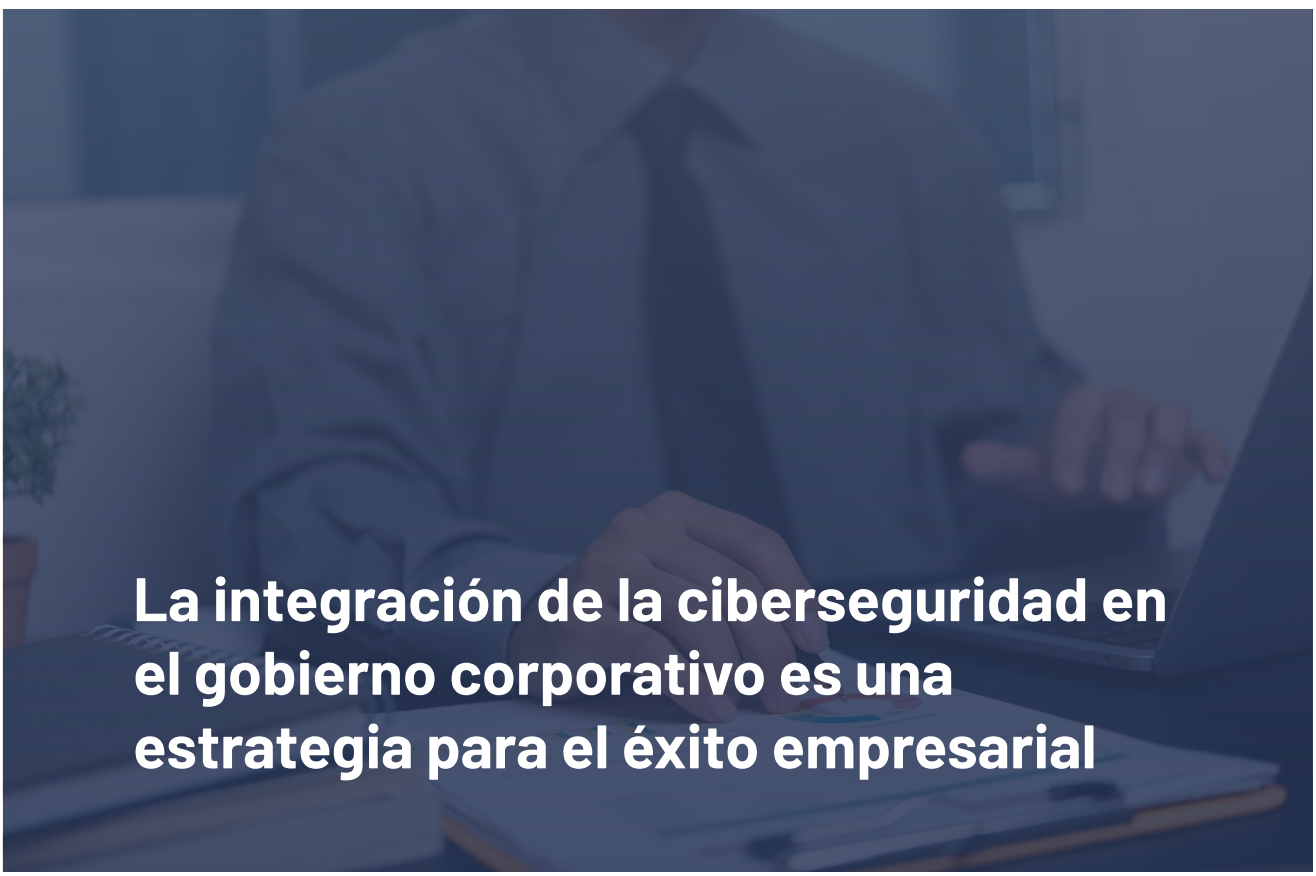
Asegurando la ciber resiliencia: Estrategias prácticas para ciberseguridad en el gobierno corporativo, en línea con marcos internacionales

www.hacknoid.com

TRANSFORMANDO LA GOBERNANZA CORPORATIVA

La alineación efectiva entre el gobierno corporativo y la ciberseguridad es crucial en el entorno empresarial actual. Frente a amenazas cibernéticas en evolución, integrar las políticas de ciberseguridad en la estructura de gobierno corporativo no solo mejora la resiliencia organizativa, sino que también asegura una gestión más efectiva de la información y los activos tecnológicos.

Existen diversos marcos y estándares internacionales que sirven de guía para poder iniciar una implementación que proviene de años de desarrollo y optimización, recogiendo mejores prácticas de mercado y extensivos debates e investigaciones con expertos. Cualquiera sea la opción, es importante tener en claro que hoy por hoy, la ciberseguridad es un pilar estratégico del éxito empresarial, y adaptarse a estos cambios no es solo una necesidad, sino una oportunidad para fortalecer la gobernanza empresarial.



CONTEXTO ACTUAL DE CIBERSEGURIDAD Y GOBIERNO CORPORATIVO

Las organizaciones se enfrentan a amenazas digitales en constante evolución, desde ataques de ransomware hasta ataques más sofisticados que aprovechan vulnerabilidades en la cadena de suministro. Estos desafíos demandan una gestión de ciberseguridad que va más allá de las medidas técnicas y se integra en la toma de decisiones de gobierno corporativo.

Los directivos deben abarcar la gestión de riesgos y la ciberseguridad como elementos estratégicos esenciales. Esta evolución refleja la necesidad de adaptarse a los riesgos y oportunidades que presenta la tecnología, haciendo de la ciberseguridad una piedra angular para la **sostenibilidad y el éxito empresarial en el entorno digital**.

PRINCIPIOS DEL GOBIERNO CORPORATIVO

Definición y Objetivos

El gobierno corporativo se refiere al sistema por el cual las empresas son dirigidas y controladas. Su propósito es estructurar las relaciones entre la dirección de la compañía, su consejo, sus accionistas y otras partes interesadas. Los objetivos fundamentales del gobierno corporativo incluyen aumentar la transparencia, fomentar una gestión responsable y ética, y asegurar la rendición de cuentas de los directivos hacia los stakeholders.

Esta estructura no solo busca mejorar el rendimiento empresarial, sino también asegurar el cumplimiento normativo y fomentar una cultura corporativa de integridad y responsabilidad.

¿Tu organización tiene un CISO o responsable de ciberseguridad? Si es así, asegúrate de que participe en las decisiones de cambios tecnológicos en los directorios.

Además, este rol debe ser independiente del área de TI.

Importancia en el Contexto Empresarial Actual

En el contexto empresarial actual, el gobierno corporativo juega un papel crucial. En un entorno donde las expectativas de transparencia y responsabilidad social corporativa están en aumento, una gobernanza sólida puede ser un diferenciador clave en el mercado. Además, con la rápida evolución tecnológica y la prevalencia de riesgos digitales, el gobierno corporativo debe expandir su enfoque para incluir la ciberseguridad como un aspecto crítico de su mandato.

Esta ampliación no es solo una respuesta a los riesgos, sino también una oportunidad para adoptar innovaciones y prácticas que pueden impulsar el crecimiento y la sostenibilidad a largo plazo de la organización, teniendo la ciberseguridad en el ADN de esas adopciones.

Ampliando el enfoque: ciberseguridad crítica en el mandato corporativo

DESAFÍOS Y OPORTUNIDADES EN EL GOBIERNO CORPORATIVO

Retos Comunes en la Implementación Efectiva

Uno de los principales desafíos en el gobierno corporativo es lograr un equilibrio entre la supervisión y la agilidad operativa. La implementación efectiva requiere un delicado balance entre una gobernanza robusta y la capacidad de adaptación rápida a los cambios del mercado y la tecnología. Otro desafío significativo es la integración de consideraciones de ciberseguridad y tecnología en la estrategia corporativa general. Esto a menudo implica superar brechas en la comprensión técnica entre los miembros del consejo y los equipos de TI.

Oportunidades de Mejora y Optimización

Pese a estos desafíos, el gobierno corporativo moderno también ofrece numerosas oportunidades de mejora y optimización. Por ejemplo, la integración efectiva de la ciberseguridad puede convertirse en una ventaja competitiva, protegiendo los activos de la empresa y construyendo confianza con clientes y accionistas, al sostener la continuidad del negocio.

Asimismo, la adopción de tecnologías emergentes, como la inteligencia artificial y el análisis de datos, puede mejorar la toma de decisiones y la eficiencia operativa.

ENTENDIENDO LA CIBERSEGURIDAD EN LAS ORGANIZACIONES

Conceptos Clave de Ciberseguridad

La ciberseguridad se centra en proteger sistemas, redes y datos en el ciberespacio para mantener la integridad, confidencialidad y disponibilidad de la información. Implica la identificación de activos críticos, evaluación de riesgos y adopción de medidas de seguridad.

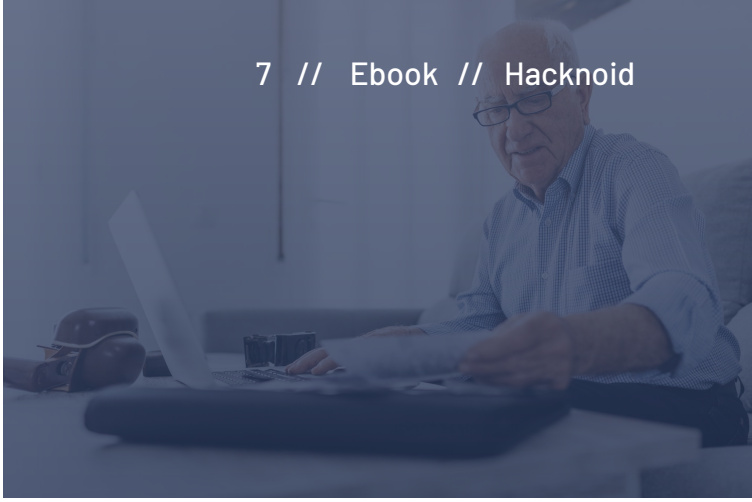
Amenazas y Vulnerabilidades

Las amenazas abarcan desde ataques externos como malware y phishing, hasta riesgos internos como errores humanos, o escalamiento de privilegios accediendo a información no autorizada. Las vulnerabilidades pueden deberse a software desactualizado, configuraciones incorrectas y prácticas deficientes en la gestión de contraseñas y vulnerabilidades.

Debemos proteger la Integridad, la Confidencialidad, y la Disponibilidad de toda nuestra operación.

Estrategias de Protección y Respuesta

Las estrategias incluyen firewalls, sistemas de detección de intrusiones, antivirus, y protocolos de autenticación robustos. La formación continua en seguridad para los empleados es crucial. Un plan de respuesta ante incidentes debe estar listo para gestionar ataques, limitar daños y recuperarse de incidentes, asegurando así una mejora continua en las prácticas de seguridad.



Responder con rapidez, el plan ante incidentes, es la clave en seguridad.

CIBERSEGURIDAD COMO PRIORIDAD ESTRATÉGICA

La ciberseguridad ha evolucionado para convertirse en una prioridad estratégica en las organizaciones, trascendiendo su papel tradicional como una preocupación meramente técnica.

Al tratar la ciberseguridad como una prioridad estratégica e integrarla en la planificación y toma de decisiones, las organizaciones pueden mejorar significativamente su capacidad para prevenir, detectar y responder a amenazas cibernéticas, asegurando así la protección de sus activos y la sostenibilidad a largo plazo de su negocio.

Ciberseguridad esencial: protegiendo activos, asegurando el futuro.

Al evaluar el riesgo de cada activo, podemos determinar qué medidas de seguridad son necesarias para protegerlo

MARCOS COBIT Y SU APLICACIÓN

Componentes Clave del Marco

COBIT (Control Objectives for Information and Related Technologies) es un marco para la gestión y gobernanza de TI, desarrollado por ISACA.

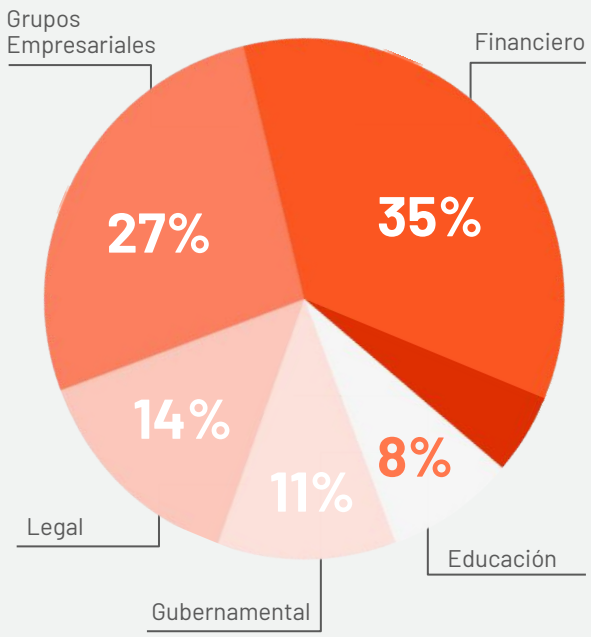
Sin embargo, también existen otros marcos relevantes en el ámbito de la ciberseguridad, como CSF, ISO 27001:2013 y NIST.

1.PRINCIPIOS DE GOBERNANZA

Orientan la optimización del valor de la TI, manteniendo un equilibrio entre la realización de beneficios, la optimización de riesgos y la optimización de recursos.

Sectores más Afectados el 2023

Financiero (35%), Grupos empresariales (27%), Legal (14%), Gubernamental (11%), Educación (8%).



2. PROCESOS:

COBIT detalla una serie de procesos gestionados para cada área de responsabilidad de TI, ofreciendo un enfoque estructurado para la administración de TI.

3.HABILITADORES DE GOBERNANZA:

Incluyen estructuras organizativas, políticas, cultura, información, servicios, infraestructura y aplicaciones que apoyan la gobernanza de TI.

COBIT brinda estructura para cada responsabilidad de TI

EN LA PRÁCTICA

La implementación de un marco en una organización se realiza a través de varios pasos:

EVALUACIÓN DE NECESIDADES:
Comprender los objetivos de negocio y las necesidades de TI para determinar cómo el marco puede apoyarlos.

ADAPTACIÓN DEL MARCO:
Personalizar los procesos y prácticas del marco para alinearlos con las necesidades y la estructura de la organización.

IMPLEMENTACIÓN:
Desarrollar e implementar políticas y procesos basados en el marco, ajustándolos a las operaciones de la organización.

MONITOREO Y MEJORA CONTINUA:
Evaluar regularmente la efectividad de las prácticas implementadas y hacer ajustes para mejorar continuamente.

Herramientas y Recursos Disponibles

COBIT proporciona una variedad de herramientas y recursos para facilitar su implementación, incluyendo guías, plantillas y casos de estudio. Estos recursos están diseñados para ayudar a las organizaciones a adaptar y aplicar el marco a sus operaciones específicas, asegurando una integración y un aprovechamiento efectivos de las mejores prácticas de gobernanza y gestión de TI.

Marcos para tener en consideración

Comparativa de definiciones y alcance

Existen varios marcos y estándares que son fundamentales para la gestión y gobernanza de TI, así como para la ciberseguridad.

COBIT (Control Objectives for Information and Related Technologies)

- **Definición:** desarrollado por ISACA, COBIT es un marco para la gestión y gobernanza de TI que ayuda a las organizaciones a crear valor a través de la tecnología.
- **Alcance:** es especialmente relevante para empresas que cotizan en bolsa y deben cumplir con SOX, ya que deriva del marco COSO. COBIT abarca todos los aspectos de la gestión de TI y es útil para asegurar el cumplimiento regulatorio.

CSF (Cybersecurity Framework)

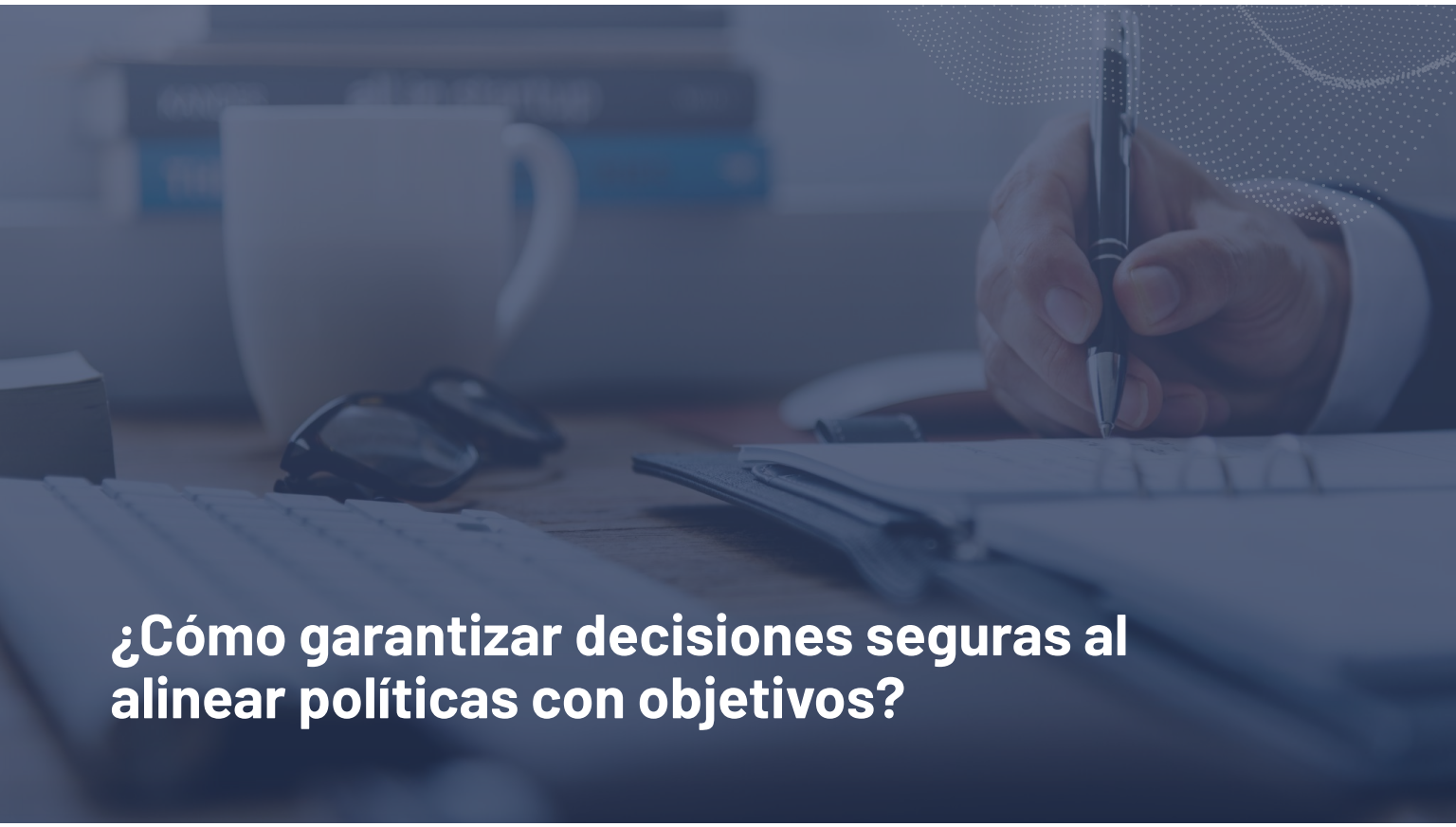
- **Definición:** desarrollado por NIST, el CSF proporciona un marco basado en estándares, directrices y mejores prácticas para gestionar y reducir los riesgos de ciberseguridad.
- **Alcance:** diseñado para ser utilizado por organizaciones de cualquier tamaño y sector, y se centra en cinco funciones principales: Identificar, Proteger, Detectar, Responder y Recuperar.

ISO 27001:2013

- **Definición:** es un estándar internacional que proporciona los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI).
- **Alcance:** ISO 27001:2013 es aplicable a cualquier tipo de organización y se enfoca en la protección de la información mediante la implementación de controles de seguridad basados en el riesgo.

NIST (National Institute of Standards and Technology)

- **Definición:** NIST publica una serie de estándares y directrices para mejorar la seguridad de la información y la ciberseguridad en las organizaciones.
- **Alcance:** sus publicaciones incluyen el NIST SP 800-53, que proporciona un catálogo de controles de seguridad y privacidad, y el NIST SP 800-171, que se centra en proteger la información no clasificada controlada (CUI) en sistemas y organizaciones.



¿Cómo garantizar decisiones seguras al alinear políticas con objetivos?

ALINEACIÓN ESTRATÉGICA ENTRE GOBIERNO CORPORATIVO Y CIBERSEGURIDAD

La sinergia entre el gobierno corporativo y la ciberseguridad es vital para asegurar la eficacia y la sostenibilidad de las estrategias empresariales en la era digital.

Estrategias de Alineación

Integración de Políticas y Procesos: Esto incluye el desarrollo de políticas de seguridad de la información que estén alineadas con los objetivos de negocio y la incorporación de prácticas de ciberseguridad en los procesos de toma de decisiones y gestión de riesgos a nivel corporativo.

Comunicación y Colaboración entre Departamentos: Establecer canales de comunicación claros y promover una cultura de colaboración interdepartamental son fundamentales para asegurar que las decisiones de seguridad de la información estén en sintonía con los objetivos y estrategias corporativas.

Beneficios y Resultados

Mejora en la Gestión de Riesgos: Al integrar la ciberseguridad en el núcleo del gobierno corporativo, las organizaciones pueden anticipar mejor y responder a los riesgos cibernéticos, protegiendo así los activos críticos y manteniendo la continuidad del negocio.

DESAFÍOS Y SOLUCIONES EN LA ALINEACIÓN ENTRE CORPORATIVO Y CIBERSEGURIDAD

Desafíos Comunes

RESISTENCIA AL CAMBIO: La integración de la ciberseguridad en el gobierno corporativo a menudo requiere un cambio cultural significativo, que puede ser difícil de aceptar y adoptar para algunos empleados y directivos.

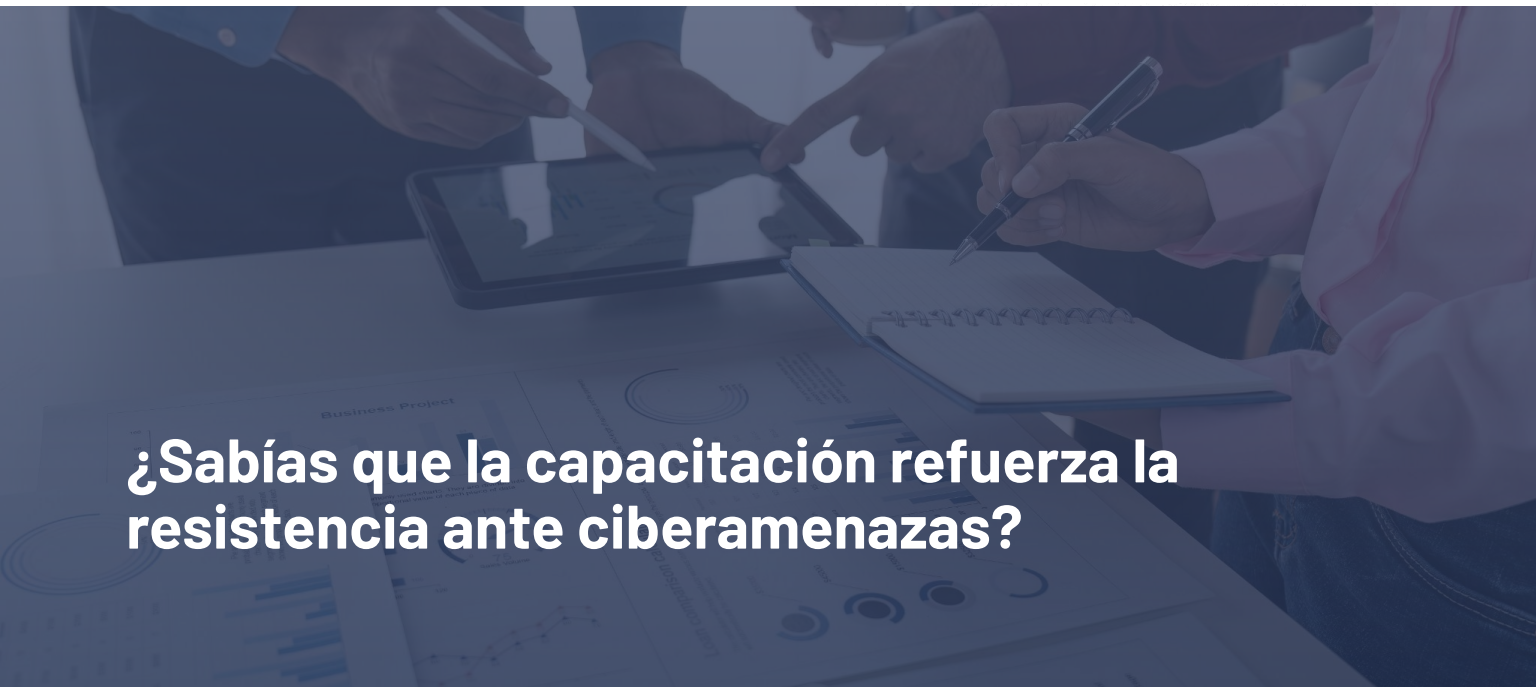
LIMITACIONES DE RECURSOS: La asignación adecuada de recursos es crucial, pero a menudo se ve desafiada por otras prioridades empresariales.

SOLUCIONES Y MEJORES PRÁCTICAS

Estrategias para Superar Obstáculos:

GESTIÓN DEL CAMBIO: Implementar una gestión del cambio efectiva, incluyendo la comunicación transparente de los beneficios de la alineación y la formación y capacitación de los empleados, puede ayudar a superar la resistencia.

LIDERAZGO INVOLUCRADO: El compromiso y la participación activa del liderazgo son esenciales para impulsar el cambio. Los líderes deben ser defensores de la integración de la ciberseguridad en el gobierno corporativo.



¿Sabías que la capacitación refuerza la resistencia ante ciberamenazas?

Evalúa y ajusta estrategias para una ciberdefensa efectiva

Recomendaciones para una Implementación Efectiva:

PRIORIZACIÓN DE RECURSOS: Esto puede implicar una reevaluación y redistribución del presupuesto y el personal.

COLABORACIÓN Y ASOCIACIONES: Establecer colaboraciones con terceros, como proveedores de servicios de seguridad cibernética y consultores, puede proporcionar acceso a experiencia y recursos adicionales.

MEDICIÓN Y REEVALUACIÓN CONSTANTE: Implementar métricas para medir la efectividad de las estrategias de ciberseguridad y realizar ajustes según sea necesario.

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