DECIDE FIRST

A DIFFERENT WAY TO DECIDE.


EDICIÓN 01 • 2026
DECIDE
FIRST
La ciberseguridad
como decisión ejecutiva
“La ciberseguridad no empieza en sistemas. Empieza en las decisiones.”
DECIDE FIRST
MAGAZINE
A DIFFERENT WAY TO DECIDE
DESCUBRE AQUÍ

Una nueva conversación ejecutiva sobre ciberseguridad

La transformación digital **ha ampliado las oportunidades** de las organizaciones, **pero también ha elevado la exposición y la complejidad del riesgo.**

Durante demasiado tiempo, la ciberseguridad fue **confinada al ámbito técnico**, confinada a la operación de TI. Eso ya no responde al contexto.

Hoy, el verdadero **desafío** no es tecnológico.

La ciberseguridad debe asumirse como lo que realmente es: una **decisión de liderazgo** que impacta la estrategia, la reputación, los clientes, la continuidad y el valor de la empresa.

DECIDE FIRST es una invitación a los líderes a asumir ese rol con claridad, tiempo y responsabilidad.

> La seguridad no se delega.
> Se decide.

ScaleUp

ISRAELI HITECH IN LATIN AMERICA


Generamos sinergias
impulsando el
progreso en
América Latina.
ScaleUp
ISRAELI HITECH IN LATIN AMERICA
Postulá para ser un
Partner ScaleUp

ÍNDICE

NUESTRA VISIÓN

La seguridad madura cuando las decisiones se conectan

En DECIDE FIRST creemos que la ciberseguridad efectiva nace cuando la estrategia, el liderazgio y la tecnologia trabajan con un mismo propósito.

No se trata de tener más herramientas. Se trata de alinear prioridades, tomar decisiones oportunas y sostener una ejecución disciplinada.

Nuestra propuesta es acompañar a los líderes e instituciones en la capacidad de anticipar con claridad, responder con determinación y fortalecer la resiliencia de su organización.

Porque cuando la información circula y las decisiones se toman a tiempo, las organizaciones crecen, se protegen y construyen confianza.

Dirección Editorial
DECIDE FIRST

ARTÍCULO

Por qué la ciberseguridad no puede seguir encerrada en TI

El liderazgo debe administrar consecuencias, no solo sistemas.

La ciberseguridad ya no se limita a evitar intrusiones. Su impacto abarca continuidad operativa, experiencia del cliente y el cumplimiento de compromisos que definen la reputación.

Cuando un riesgo se gestiona solo desde TI, las decisiones clave llegan tarde o incompletas. Y cuando eso ocurre, las consecuencias ocurren en toda la organización.

La tecnología protege sistemas. El liderazgo define prioridades, establece límites aceptables y asume el impacto de cada decisión.

Ciberseguridad no es solo un tema técnico: es parte de cómo se gobierna la empresa, cómo se asignan recursos y cómo se responde ante lo inesperado.

No se trata de transferir la propiedad a TI, sino de asumirla desde el comité de dirección.

> “TI puede administrar sistemas; el liderazgo debe administrar consecuencias.”

Lo que TI puede proteger vs. lo que la organización debe decidir

TI PUEDE PROTEGER

- Infraestructura y aplicaciones
- Redes y endpoints
- Datos y accesos
- Monitoreo y detección
- Respuesta a incidentes
- Controles técnicos

LA ORGANIZACIÓN DEBE DECIDIR

- Tolerancia al riesgo
- Prioridades del negocio
- Asignación de recursos
- Continuidad y resiliencia
- Cumplimiento y reputación
- Cultura y comportamiento

La tecnología reduce riesgo.
El **liderazgo** define el riesgo que la organización está dispuesta a asumir.

ARTÍCULO

Las personas no son el eslabón más débil

El verdadero riesgo comienza cuando una organización exige decisiones correctas sin haber desarrollado el criterio necesario para tomarlas.

ANGIE PIEDRA CEDEÑO
Directora de innovación e ingeniería estratégica en ciberseguridad, para la firma **ÓKTARITECH**

En ciberseguridad se ha repetido constantemente una afirmación que terminó instalándose como una verdad aparentemente incuestionable: las personas son el eslabón más débil.

Es una frase fácil de recordar, pero profundamente limitada.

Reducir la dimensión humana a una debilidad no solo resulta injusto; también revela una forma incompleta de comprender la seguridad. Cuando una persona abre un enlace malicioso, comparte información de manera inadecuada, utiliza una contraseña predecible o responde bajo presión a una solicitud fraudulenta, la explicación no puede limitarse a señalar el error.

La pregunta verdaderamente estratégica es otra:

> ¿Qué hizo la organización para desarrollar en esa persona la capacidad de reconocer el riesgo y decidir correctamente?

Culpar a las personas ha sido, durante demasiado tiempo, una forma cómoda de evitar una responsabilidad más profunda. Si alguien no logra identificar una amenaza, quizá el problema no esté únicamente en su conducta, sino en la manera en que le comunicamos la ciberseguridad, en los hábitos que permitimos consolidar y en la distancia que todavía existe entre el conocimiento especializado y la realidad cotidiana.

Las personas no nacen preparadas para interpretar entornos digitales complejos. Esa capacidad debe construirse.

Por ello, sostener que constituyen el eslabón más débil perpetúa un paradigma que ya no responde a las necesidades de las organizaciónes actuales. La dimensión humana no es una falla inevitable del sistema. Es una capacidad estratégica que puede fortalecerse, entrenarse y convertirse en una de las defensas más valiosas de la organización.

El cambio comienza cuando dejamos de señalar a las personas y asumimos, como especialistas, líderes y tomadores de decisión, la responsabilidad de prepararlas mejor.

1.
La autoridad también se demuestra al comunicar con claridad

Quienes ejercemos responsabilidades en ciberseguridad y seguridad de la información debemos comprender que el conocimiento técnico, por sí solo, no transforma una organización. Puede diagnosticar vulnerabilidades, diseñar controles y anticipar amenazas. Sin embargo, si no somos capaces de comunicar ese conocimiento con claridad, su capacidad para proteger se reduce.

Hablar sin tecnicismos no significa renunciar a la profundidad profesional. Significa demostrar dominio suficiente para convertir la complejidad en comprensión y la comprensión en acción.

La verdadera autoridad no se encuentra en utilizar un lenguaje que pocos entienden, sino en lograr que una junta directiva comprenda por qué una decisión aparentemente comercial puede aumentar la exposición de la organización; que una gerencia reconozca las consecuencias de postergar una medida importante; y que una persona colaboradora sepa cómo actuar cuando algo no parece correcto.

La ciberseguridad madura cuando puede conversar con toda la organización.

Necesitamos profesionales capaces de transmitir experiencias, no únicamente conceptos. Especialistas que puedan explicar el riesgo sin generar miedo, diseñar aprendizajes conectados con el trabajo cotidiano y crear espacios en los que las personas desarrollen criterio antes de enfrentar una situación real.

La claridad no reduce la sofisticación. La convierte en valor.

> “La verdadera autoridad no está en utilizar un lenguaje que pocos entienden, sino en lograr que toda la organización comprenda el riesgo y pueda actuar con criterio.”

2.
No basta con capacitar: es necesario desarrollar destrezas

Muchas organizaciones continúan confundiendo transmisión de información con preparación.

Una charla anual, una política firmada o una presentación sobre amenazas pueden cumplir un requisito, pero no garantizan que una persona sepa actuar bajo presión. Conocer una norma no equivale a haber desarrollado la capacidad para aplicarla en un momento de incertidumbre.

La verdadera preparación surge cuando las personas practican decisiones.

Por ello, los escenarios deben responder a la cultura, los procesos y las tensiones reales de cada organización. No todas las empresas enfrentan los mismos riesgos ni toman decisiones de la misma manera. Una estrategia efectiva debe reconocer cómo se trabaja, cómo circula la información, qué presiones existen y cuáles comportamientos se han normalizado.

Los escenarios genéricos informan. Los escenarios contextualizados desarrollan destrezas.

Cuando una persona se enfrenta a una situación simulada que reproduce su realidad, aprende a reconocer señales, valorar consecuencias, formular preguntas y actuar con mayor seguridad. Deja de ser una receptora pasiva de instrucciones y se convierte en parte consciente de la protección organizacional.

Ese debe ser el objetivo: no crear obediencia automática, sino criterio.

Una organización fortalecida no es aquella en la que nadie comete errores. Es aquella en la que las personas pueden **reconocerlos, comunicarlos a tiempo y responder de manera coordinada** antes de que se conviertan en una crisis.

3.

La ciberseguridad debe salir del aislamiento tecnológico

Otro paradigma que debe cambiar es la idea de que la ciberseguridad pertenece exclusivamente al departamento de TI. TI es fundamental, pero no puede definir por sí solo cuánto riesgo está dispuesta a aceptar una organización, qué activos son esenciales para su continuidad ni cuáles consecuencias podrían comprometer su reputación, sus operaciones o la confianza de sus clientes.

Esas no son decisiones técnicas. Son decisiones de negocio.

La ciberseguridad debe ocupar un lugar permanente en las mesas de las juntas directivas y los equipos ejecutivos, porque es allí donde se define la dirección de la organización, se establecen prioridades y se decide qué nivel de exposición resulta compatible con sus objetivos.

La alta dirección no necesita convertirse en especialista para tomar decisiones informadas, pero sí necesita tener la claridad suficiente para entender el riesgo, evaluar alternativas y asumir la responsabilidad que conlleva cada decisión estratégica.

Para saber gobernar, primero hay que entender.
Esa es la base de una ciberseguridad madura.

La ciberseguridad no es un tema de TI. Es un tema de negocio, de liderazgo y de continuidad.

4.

La tecnología no transforma las malas costumbres

Las herramientas evolucionan rápidamente, pero la tecnología, por sí sola, no modifica comportamientos. Una plataforma avanzada no compensa una cultura que normaliza prácticas inseguras, procesos poco claros o decisiones tomadas sin evaluar consecuencias.

La seguridad no se rompe únicamente por un ataque complejo. Se rompe cuando alguien reutiliza credenciales porque "es más fácil", cuando se ignora un procedimiento porque "no aplica aquí", cuando se comparte información porque "no parece sensible" o cuando se silencian señales de alerta porque "no es mi responsabilidad".

La tecnología multiplica lo que una cultura permite.
Si la cultura es sólida, potencia la protección. Si la cultura es débil, amplifica el riesgo.

La transformación comienza cuando se fortalecen los comportamientos cotidianos que sostienen la seguridad: curiosidad sana, duda, comunicación temprana, respeto por los procesos y responsabilidad compartida.

Ahí es donde realmente comienza a cambiar el riesgo.

La tecnología multiplica lo que una cultura permite: puede fortalecer la seguridad o amplificar el riesgo.

> "Para saber gobernar, primero hay que entender. La ciberseguridad debe estar presente en las decisiones que definen el rumbo de la organización."

5.
El liderazgo debe construir confianza, no temor

El miedo puede generar obediencia inmediata, pero no desarrolla criterio. Y sin criterio, las personas no pueden proteger realmente a la organización. Una cultura basada en el temor oculta errores, disuade la comunicación y reduce la capacidad de reacción ante incidentes.

La confianza, en cambio, crea entornos donde es posible preguntar, reportar, aprender y mejorar. Cuando alguien se equivoca y lo comunica a tiempo, la organización puede contener el impacto. Cuando el error se oculta, se convierte en un incidente.

Los líderes deben modelar comportamientos que fortalezcan esa confianza: reconocer fallas, promover conversaciónes abiertas, escuchar sin juicio y valorar la transparencia.

La ciberseguridad no es un sistema que se impone. Es una cultura que se inspira.

6.
El cambio debe comenzar desde las nuevas generaciones

La protección de una organización no puede depender únicamente de lo que aprenden hoy sus colaboradores. Debe comenzar mucho antes, en quienes pronto participarán activamente en la vida digital, académica y profesional.

Por eso es fundamental que la formación en ciberseguridad llegue desde edades tempranas, con un enfoque pedagógico, práctico y adaptado a cada etapa del desarrollo.

No se trata solo de transmitir normas, sino de cultivar hábitos, curiosidad responsable, pensamiento crítico y comprensión de consecuencias. Cuando las nuevas generaciones comprenden cómo funciona el mundo digital y cómo sus decisiones impactan su seguridad y la de otros, se convierten en promotores naturales de una cultura más consciente.

Invertir en su formación hoy es sembrar la cultura que protegerá a la organización mañana.

La dimensión humana como diamante estratégico

La ciberseguridad no se fortalece con tecnología. Se fortalece con decisiones, hábitos, conversaciones y liderazgo.

Las personas no son el eslabón más débil. Son el diamante estratégico que, cuando está bien formado, puede transformar el riesgo en resiliencia.

Nuestro rol como profesionales, líderes y tomadores de decisión no es señalar debilidades humanas. Es preparar mejor, diseñar experiencias significativas, comunicar con claridad, tomar decisiones informadas y construir culturas que protejan lo que realmente importa.

La ciberseguridad del futuro no pertenecerá a quienes tengan la tecnología más avanzada, sino a quienes comprendan más profundamente a las personas que deben usarla y protegerla.

Ese es el cambio que debemos liderar.

> “Las personas no son el eslabón más débil. Son el diamante estratégico que, cuando está bien formado, puede transformar el riesgo en resiliencia.”

ANGIE PIEDRA CEDEÑO

Directora de innovación e ingeniería estratégica en ciberseguridad, para la firma ÓKTARITECH

CMA

Su socio en tecnología

Transformamos la tecnología en resultados para su negocio

Soluciones integrales para mejorar la gestión tecnológica de las empresas

2105-0100

7046-6273

contactenos@grupocma.com

CMA

Su socio en tecnologia

Infraestructura TI

Diseñamos, administramos y optimizamos ambientes tecnológicos seguros y escalables

Nube • Redes • Respaldo • Infraestructura Híbrida

Microsoft 365 y Automatización

Impulsa la productividad con herramientas colaborativas, automatización inteligente y agentes de IA.

Power Platform • Copilot • eForce Solutions

Usuario Final y Movilidad

Mejoramos la experiencia digital de los usuarios con dispositivos, colaboración y soporte especializado

Dispositivos • Impresión Movilidad • Gestión de activos

TalentOps

Talento tecnológico especializado para fortalecer sus proyectos y operación.

Servicios tercerizados personal Recursos especializados

INVITADO DE EDICIÓN

Matías Schvartz

CEO & Founder de ScaleUp Global

Tecnología, criterio y ejecución: una conversación sobre decisiones que sí transforman el negocio.

En un entorno donde la innovación suele confundirse con velocidad y novedad, distinguir entre tecnología útil y entusiasmo pasajero se ha vuelto una capacidad directiva. En esta conversación exclusiva para DECIDE FIRST, Matías Schvartz comparte una visión clara sobre cómo convertir la tecnología en una decisión estratégica, por qué el ecosistema israelí produce soluciones diseñadas para operar en escenarios exigentes y qué debe comprender América Latina para traducir innovación en ejecución, continuidad y negocio sostenible.

> “Comprar tecnología es reactivo, decidir es proactivo.”

ENTREVISTA EXCLUSIVA
DECIDE FIRST

¿Qué diferencia existe entre adquirir una solución innovadora y tomar una verdadera decisión estratégica de tecnología?

La diferencia es simple de decir y difícil de aplicar: comprar tecnología es reactivo, decidir es proactivo.

Vemos empresas que se suman a una tendencia tecnológica porque "hay que innovar", sin preguntarse antes qué problema puntual quieren resolver, y después de la euforia inicial la herramienta termina sin uso real. Una decisión estratégica arranca al revés: primero el problema del negocio, después la tecnología para empresas que mejor lo resuelve, y recién ahí se mira el catálogo de soluciones disponibles.

En ScaleUp trabajamos justo en ese cruce. Como brazo técnico-comercial de tecnología israelí en la región, nuestra metodología no busca entregar tecnología simplemente porque "está buena" o sea novedosa. Nos enfocamos en evaluar al partner local para validar si realmente cuenta con las capacidades operativas y comerciales para ejecutar la oportunidad que detectamos en su mercado. Si en las primeras charlas vemos que no están dadas esas condiciones, preferimos ser francos y no avanzar. Elegir al partner correcto para la oportunidad correcta es la única forma de que los proyectos tengan impacto real y duren en el tiempo.

> "Elegir al partner correcto para la oportunidad correcta es la única forma de que los proyectos tengan impacto real."

¿Cuáles son las preguntas que una alta dirección debería responder antes de incorporar una nueva tecnología dentro de su organización?

Me gusta marcar una distinción fundamental, porque las preguntas cambian drásticamente si sos una organización que va a incorporar tecnología para su propia operación, o si sos un socio comercial que busca representarla e integrarla en su territorio.

Si me pongo en el lugar de una empresa o usuario final, para mí hay tres preguntas obligadas:

- ¿Cuál es el dolor operativo o financiero concreto que necesitamos resolver hoy?
- ¿Esta nueva solución realmente resuelve ese problema mejor y más rápido que lo que ya tenemos, o solo nos añade complejidad?
- ¿Tenemos la cultura y la disciplina interna para adoptar la herramienta y medir su impacto real?

Ahora, si lo miro desde la perspectiva de un partner comercial o un integrador local que analiza sumar una nueva tecnología a su portafolio, el análisis pasa por otro lado:

- ¿Existe una demanda insatisfecha o un problema en mi mercado que esta tecnología resuelve de forma única, representando un negocio para mi empresa?
- ¿Cuento con el respaldo de un equipo especializado que entienda mi realidad local, hable mi idioma y me acompañe hombro a hombro a ejecutar la oportunidad en el terreno?
- ¿Existe la estructura, el profesionalismo y el compromiso a largo plazo para asegurar que esto no sea una venta puntual, sino una operación sostenible y escalable?

Te aseguro que cuando una alta dirección responde estas preguntas con honestidad en cualquiera de los dos escenarios, sabe inmediatamente si está ante un activo estratégico o ante un intento fallido.

En un mercado donde innovación suele confundirse con novedad, ¿cómo puede una organización distinguir entre una tecnología verdaderamente relevante y una propuesta atractiva que aún no responde a una necesidad prioritaria?

Yo lo pienso así: si una empresa no puede nombrar con claridad cuál es su dolor, cualquier tendencia tecnológica le va a parecer buena, porque no tiene con qué compararla.

Ahora, hay que entender que una tecnología relevante opera de dos maneras: o te resuelve un problema crítico y costoso que tenés hoy, o te resuelve un problema pequeño que sabés que mañana va a ser gigante. Y en este último caso, no solo estás innovando, estás siendo un pionero en el mercado.

Te doy un ejemplo concreto con la agricultura. Hoy el cultivo protegido y la automatización de invernaderos son una tendencia fuertemente marcada a nivel global. Un productor o un integrador puede mirar la tecnología de automatización de GrowDirector y ver que le resuelve un problema actual de eficiencia y control técnico. Pero lo más valioso es que, si hoy incorpora GrowDirector a su portafolio o a su operación, no solo está solucionando lo cotidiano; se está anticipando a una demanda que va a explotar en los próximos años.

Entonces, para distinguir el humo de una oportunidad real hay que preguntarse: ¿Esto me resuelve un costo/riesgo directo hoy, o me posiciona como pionero para liderar la demanda que se viene? Si cumple cualquiera de las dos con datos reales y no con palabras de moda, estás ante una tecnología relevante.

> “La innovación no es un lujo ni un elemento de marketing; es una necesidad directa de supervivencia.”

Israel es reconocido internacionalmente por su capacidad de innovación tecnológica. ¿Qué condiciones de su ecosistema han favorecido el desarrollo de soluciones orientadas a resolver problemas complejos, críticos o de alta urgencia?

En Israel la innovación no es un lujo ni un elemento de marketing; es una necesidad directa de supervivencia. Hablamos de un país chico, con recursos naturales muy limitados y una situación geopolítica que te exige resolver problemas urgentes todo el tiempo: escasez de agua, seguridad, soberanía alimentaria, energía.

En el corazón de ese ecosistema está el paso por el ejército, que funciona como el gran catalizador del talento. Ahí es donde verdaderamente se entrena la capacidad de resolver bajo presión y de iterar constantemente.

En Israel se valora profundamente esa resiliencia: si algo falla en un primer intento, no hay espacio para la frustración; el error se toma como un dato real que da impulso para ajustar, aprender y seguir buscando la solución correcta.

Cuando combinás esa cultura de prueba y error con el paso por centros de investigación y una densidad altísima de startups, el resultado son soluciones hiperprobadas. No nacen para ser experimentos cosméticos ni para llenar pantallas de datos, sino para operar en escenarios complejos y resolver problemas críticos con pragmatismo absoluto.

ENTREVISTA EXCLUSIVA

Tecnología, criterio y ejecución: una conversación sobre decisiones que sí transforman el negocio.

ScaleUp
ISRAELI HITECH IN LATIN AMERICA

> “No se puede hacer un copy-paste.”

Más allá de su procedencia, ¿qué características distinguen a muchas tecnologías israelíes en áreas como ciberseguridad, inteligencia, protección de infraestructuras, automatización e industria 4.0?

Mirá, la gran diferencia es que estas soluciones no nacen en un laboratorio teórico ni en una oficina cómoda para ver qué pasa. Nacen por pura necesidad operativa y se prueban en los escenarios más exigentes del mundo.

Cuando desarrollás tecnología en un entorno de estrés constante o con recursos escasos, simplemente no tenés margen para hacer cosas que “más o menos” funcionen.

En ciberseguridad e inteligencia, por ejemplo, te das cuenta rápido de que no te están vendiendo un software defensivo o pasivo de los que se quedan esperando a que pase algo. Te encontrás con herramientas diseñadas para ir un paso adelante, anticiparse al riesgo y neutralizar amenazas antes de que te frenen la operación.

Si mirás la parte de industria 4.0 y automatización, pasa lo mismo: se acaba esa historia de llenar una planta de sensores solo para tener un tablero con gráficos lindos que nadie mira. La tecnología acá está pensada para tomar decisiones automáticas en tiempo real, recortar costos operativos y cuidar que la línea de producción no pare jamás.

Y cuando pasás a AgTech o la gestión del agua, el origen te lo dice todo. Hablamos de desarrollos que nacieron literalmente en el desierto, donde cada gota de agua y cada hectárea cuentan porque no hay margen de error. Ahí no hay espacio para la especulación; o rinde y da retorno de inversión, o no sirve.

¿Qué debería comprender una organización latinoamericana antes de asumir que una tecnología exitosa en Israel puede implementarse de la misma forma en su propio mercado?

Lo primero es entender que no se puede hacer un “copy-paste”. Así como una persona no puede bañarse dos veces en el mismo río, una misma tecnología jamás se instala de forma idéntica en dos mercados diferentes. Que una solución sea un éxito rotundo en Israel, en Europa o en Estados Unidos te garantiza que el producto funciona y es robusto, pero el despliegue en Latinoamérica es otra historia.

Una empresa acá tiene que tener clarísimas tres cosas:

- La infraestructura, la normativa y la forma de operar en nuestra región cambian muchísimo. Por eso es clave trabajar con gente que entienda tu realidad local y tus dolores diarios, no con alguien que te quiere vender una solución empaquetada a la distancia.
- Una tecnología de vanguardia no te sirve de nada si te la tiran por la cabeza. Necesitás la tranquilidad de que vas a recibir la capacitación, el conocimiento y el soporte constante para aprovecharla al 100%.
- Hay que saber que el equipo detrás está dispuesto a adaptar lo que sea necesario para la cancha local. Y si algo en la práctica no sale perfecto a la primera, tener el respaldo técnico directo para resolverlo con agilidad sin dar mil vueltas.

Al final, se trata de no dejar la tecnología sola. Se trata de ejecutar con método, en el terreno y hablando tu mismo idioma.

América Latina no es un mercado homogéneo. ¿Cuáles son las principales diferencias que una empresa tecnológica debe comprender antes de ingresar a la región?

Si entendés que cada país de la región es un mundo distinto, e incluso que hay diferencias enormes dentro de un mismo país, ya tenés el 50% del trabajo hecho. El error clásico de muchas empresas es asumir que Latinoamérica es un bloque uniforme, y no hay nada más alejado de la realidad.

Una solución tecnológica que representa una tremenda oportunidad de negocio en el mercado colombiano puede no ser relevante en el panameño. Por eso, el enfoque no puede ser salir a "vender tecnología" de forma genérica.

Lo que hacemos en ScaleUp es invertir el proceso: primero analizamos y definimos exactamente en qué mercados esa tecnología representa una oportunidad comercial real y concreta. Y una vez identificado ese potencial, salimos a buscar y seleccionar al partner local indicado, que es quien verdaderamente conoce la cancha, maneja las relaciones en el terreno y tiene la capacidad para ejecutar y aprovechar esa oportunidad en su mercado.

Nosotros no traemos una "caja" con tecnología para colocar; traemos un negocio estructurado con potencial claro. Y la ejecución de ese negocio siempre está en manos de un partner local sólido que cuenta con todo nuestro respaldo.

¿Por qué la presencia de socios locales resulta determinante para que una tecnología internacional alcance adopción, continuidad y confianza?

El socio local es determinante porque es quien conoce el mercado a fondo: domina las reglas de juego escritas y no escritas, vive el día a día con el cliente final y entiende sus necesidades, a veces incluso mejor que el propio cliente. Es una pieza fundamental para que la tecnología pueda llegar a destino y generar todo su verdadero impacto en la operación.

En definitiva, las relaciones comerciales no son entre oferta y demanda, ni simplemente entre un problema y una solución; son siempre entre personas. La tecnología por sí sola no genera confianza; la confianza la construyen los equipos en el terreno.

Por eso en ScaleUp entendemos que la clave está en jugar en equipo. Traemos la solución tecnológica de Israel y el respaldo operativo oficial; el partner aporta todo su expertise y conocimiento del mercado local; y el cliente suma su necesidad real. Cuando esos tres actores jugamos alineados como un solo equipo, el resultado no es solo la adopción de una tecnología, sino un negocio sostenible y de alto impacto a largo plazo.

> “La tecnología por sí sola no genera confianza; la confianza la construyen los equipos en el terreno.”

ENTREVISTA EXCLUSIVA

Matías Schvartz

CEO & Founder de ScaleUp Global

En ciberseguridad, las organizaciones suelen concentrarse en productos, controles y plataformas. ¿Cómo debería cambiar la conversación para vincular la tecnología con continuidad, riesgo, reputación y objetivos empresariales?

Siguiendo con la idea de jugar en equipo, dentro de una organización pasa exactamente lo mismo. El experto en ciberseguridad no tiene por qué ser especialista en los procesos de operación de la planta, ni el Director de Operaciones tiene por qué saber de protocolos de red. Pero están obligados a jugar en el mismo equipo. El gran problema histórico es que no hablan el mismo idioma.

Afortunadamente, esa conversación ya está cambiando. La ciberseguridad dejó de ser un tema meramente informático para convertirse en una discusión de continuidad del negocio.

Una de las soluciones en nuestro portafolio de ciberseguridad identificó justamente este dolor y aborda el problema desde otra perspectiva: permite traducir cada riesgo cibernético en función de su impacto real en la operación. No es lo mismo tener una vulnerabilidad alta en un PLC que controla las luces del estacionamiento, que tener una vulnerabilidad baja en el controlador de la cinta transportadora principal que, si se frena, te paraliza la planta entera.

Cuando lográs ese nivel de claridad, la tecnología se transforma en un facilitador. Ya no se trata de comprar herramientas para "cumplir un checklist", sino de alinear a los departamentos para proteger la caja, la producción y la reputación de la empresa.

Entonces, la inversión en ciberseguridad deja de ser un gasto y pasa a ser una decisión estratégica más, al mismo nivel que abrir un mercado nuevo o lanzar un producto, no algo que se resuelve solo con más herramientas o más presupuesto en licencias.

> "La ciberseguridad dejó de ser un tema meramente informático para convertirse en una discusión de continuidad del negocio."

Algunas tecnologías incorporan inteligencia, monitoreo, automatización y análisis en tiempo real. ¿Qué nuevas capacidades generan para quienes deben tomar decisiones bajo presión?

La capacidad fundamental que generan es la de operar en un entorno de mucha mayor claridad y control, reduciendo al mínimo el margen de error en momentos críticos.

Quien debe tomar decisiones directivas bajo alta presión no necesita un volumen masivo de datos crudos; lo que necesita es previsibilidad y visibilidad en tiempo real. Cuando implementas inteligencia, monitoreo y automatización, lo que haces en la práctica es eliminar la "niebla" de la operación. Dejas de reaccionar a incidentes o amenazas cuando ya causaron un impacto financiero o reputacional, y pasas a anticiparte a ellos con datos precisos.

Estas tecnologías no reemplazan el criterio humano, sino que lo potencian. Le entregan al tomador de decisión un escenario controlado donde puede evaluar variables en segundos, prever consecuencias y ejecutar con la certeza de que tiene el dominio de la situación, incluso en medio de una crisis de ciberseguridad o resiliencia operativa. En industrias críticas, esa diferencia entre reaccionar a ciegas o decidir con claridad es la que define la continuidad del negocio. Y ahí es donde aparece el verdadero desafío: asegurarnos de que esa visibilidad se traduzca en un control real y no en una falsa sensación de seguridad.

ScaleUp
ISRAELI HITECH IN LATIN AMERICA

INVITADO DE EDICIÓN

> “Comprar tecnología es reactivo, decidir es proactivo.”

¿Cómo puede una organización evitar que la automatización y la inteligencia artificial creen una falsa sensación de control?

Justamente evitando el error de asumir que porque una pantalla muestra métricas perfectas, la realidad en la planta o en el campo está resuelta. Esa sensación de control absoluto es peligrosa porque distorsiona la realidad operativa. La automatización y la IA son herramientas extraordinarias para procesar datos, pero el control verdadero solo existe cuando hay un equilibrio entre la tecnologia, los procesos y el factor humano.

Es por eso que en ScaleUp hacemos tanto hincapié con nuestros partners en el seguimiento continuo con el cliente después de la instalación de una solución. La tecnología sola te da un tablero, pero la clave está en tener a alguien ahí para validar, supervisar y hasta desafiar la información que viene dada en el dashboard.

Estar en el terreno para contrastar lo que dice la pantalla contra lo que pasa en la operación real es lo único que te permite corregir a tiempo si hace falta. Y recién ahí, cuando tenés ese acompañamiento y esa validación constante, es cuando podés llegar al punto de descansar con total tranquilidad en la tecnología implementada.

¿Cómo evaluar si una solución de ciberseguridad realmente mejora la capacidad de decisión y no únicamente aumenta el volumen de alertas, datos o herramientas disponibles?

El indicador real para evaluar una solución no es cuántas alertas genera ni qué tan sofisticado se ve su tablero, sino qué tan rápido le permite al equipo priorizar y tomar una decisión efectiva ante un incidente real.

En definitiva, la pregunta clave es: ¿cuánto tarda la organización en *pasar de “detectamos algo raro” a “sabemos qué es, qué tan grave es, qué parte de la operación está en riesgo y qué hacer”?*

Una herramienta que solo suma ruido, falsos positivos o métricas infinitas no está ayudando a nadie; lo único que hace es saturar al equipo y alargar los tiempos de respuesta. En ciberseguridad, sumar más herramientas no significa estar más seguro.

Por eso, cuando elegimos qué tecnologías incorporar a nuestro portafolio en ScaleUp, buscamos exactamente lo contrario: herramientas *que limpien toda esa complejidad, eliminen la fatiga de alertas y le den tanto al partner como al cliente la claridad para actuar con precisión en el momento en que la operación más lo necesita.*

> “En ciberseguridad, sumar más herramientas no significa estar más seguro.”

INVITADO DE EDICIÓN

> Una nueva tecnología puede resolver un problema, pero también introducir integraciones, dependencias y riesgos adicionales. ¿Cómo debería analizarse este equilibrio antes de su implementación?

Ese equilibrio se analiza poniendo sobre la mesa el impacto real en el negocio frente a la complejidad que le vas a sumar a la operación. Hay una tendencia muy común a querer adoptar tecnología por el solo hecho de ser innovadores o porque está de moda decir que usás inteligencia artificial, y ahí es donde se comete el primer error.

Antes de evaluar cualquier integración, tenés que determinar el ROI esperado. Si la solución no resuelve un dolor operativo concreto o no impacta directamente en el número final, el riesgo de sumar dependencias y complejidad sencillamente no se justifica. No tiene sentido meterle fricción a la empresa si el beneficio no está claro desde el día uno.

Y el segundo criterio en ese análisis es la factibilidad de mitigar el riesgo. Si para adoptar una tecnología tenés que cambiar toda la operación de golpe, el riesgo es gigante. Por eso, el equilibrio correcto exige analizar si la solución permite una adopción escalonada. Poder validar el impacto en un proceso acotado, medir cómo interactúa con lo que ya existe y comprobar en la cancha que no genera cuellos de botella antes de llevarla al resto de la organización.

Analizar este equilibrio no es ponerse a hacer teorías complejas; es garantizar que la tecnología sirva al negocio y no al revés, asegurando que cada paso que se da esté justificado en rentabilidad y bajo control operativo.

> ¿Qué condiciones debería cumplir un piloto tecnológico para producir evidencia útil y no convertirres solamente en una demostración comercial?

Para que un piloto no sea un simple show comercial, lo primero es poner las reglas claras sobre la mesa antes de tocar un solo equipo: definís qué KPI querés mover y cuál es el criterio de éxito. Si no sabés qué variable estás buscando validar, el piloto no sirve para nada.

Lo segundo es que no podés probar tecnología en un "laboratorio ideal". El piloto tiene que hacerse en la cancha real, con los volúmenes de datos reales del cliente y con la gente que opera todos los días. Ahí es donde saltan las verdaderas fricciones de integración.

Además, tiene que ser una prueba con principio y fin claro, no un experimento infinito que se arrastra meses. La clave está en el seguimiento que hace el partner en el terreno: estar ahí para supervisar, validar si la tecnología responde y hasta desafiar los datos del tablero contra la realidad operativa.

> "La tecnología debe servir al negocio y no al revés."

INVITADO DE EDICIÓN

¿Qué debería exigir una organización a sus proveedores respecto de soporte, transparencia, seguridad, actualización, transferencia de conocimiento y continuidad?

Cuando adoptás tecnología de punta, no estás comprando solo un producto; estás integrando un componente clave para la continuidad de tu negocio.

La mayor tranquilidad para un cliente final es saber que cuenta con un partner local en el terreno. La innovación más avanzada del mundo necesita ser ejecutada y respaldada por expertos locales que entiendan la realidad de la operación, hablen su mismo idioma y brinden una respuesta presencial e inmediata cuando el negocio lo requiera.

Y para que esa ecuación sea perfecta, nuestros partners locales deben tener la total garantía de que cuentan con todo el respaldo directo de la marca. Por eso, nosotros aseguramos que cada partner reciba una transferencia continua de conocimiento, entrenamiento técnico, actualizaciones y el acompañamiento constante del equipo de desarrollo comercial.

De esta forma se logra el equilibrio ideal: el cliente final opera con la tranquilidad de estar respaldado localmente por expertos de primer nivel, y el partner compite en el mercado con la seguridad de tener el soporte directo, la predictibilidad y el poder de una tecnología israelí líder.

> “Producir más optimizando recursos no es una opción, **es una urgencia.**

¿Qué oportunidades observa ScaleUp para América Latina en materia de ciberseguridad, inteligencia, industria 4.0, agricultura tecnológica y protección de infraestructura?

América Latina tiene un potencial enorme porque la necesidad es real y operativa en el día a día.

Si miras ciberseguridad e infraestructura, la región se digitalizó más rápido de lo que se protegió. Sobre todo en infraestructura crítica con sistemas OT que antes estaban aislados y hoy están conectados, lo que abre vulnerabilidades muy concretas.

En Industria 4.0, el potencial de automatización e IoT industrial es altísimo en sectores manufactureros que todavía operan de forma bastante manual. Ahí el impacto de reducir fallas o paradas no planificadas se mide muy rápido en dinero.

Y en AgTech e infraestructura hídrica, la región es el motor productivo, pero el desafío del agua y la eficiencia del suelo es cada vez más crítico. Producir más optimizando recursos no es una opción, es una urgencia.

Ahí es donde entra la oportunidad para los partners locales. Esta demanda no la va a resolver una solución empaquetada que se manda por mail desde la otra punta del mundo; se resuelve en el terreno, con empresas locales que entiendan la cancha y conozcan al cliente. Para cualquier integrador o partner de la región que quiera liderar su mercado, el momento es ahora. Nosotros les acercamos la tecnología israelí más avanzada y los acompañamos con la metodología para garantizar que cada proyecto sea un negocio rentable, predecible y con impacto real.

¿Qué papel pueden desempeñar países como Costa Rica, por su talento especializado, estabilidad y capacidad de innovación, en la conexión entre tecnología israelí y mercados latinoamericanos?

Costa Rica tiene un perfil espectacular y reúne todas las condiciones para ser un referente de innovación en la región. Tienen profesionales con una formación técnica de primer nivel, estabilidad institucional y una visión muy clara hacia la tecnología, la ciberseguridad y la sostenibilidad.

Precisamente por eso, Costa Rica está en nuestro radar prioritario para abrir operaciones y sumar partners locales. Queremos armar equipo con integradores y empresas de tecnología ticas que conozcan la cancha, entiendan las necesidades de su mercado y quieran marcar la diferencia.

La oportunidad para un partner local en Costa Rica se resume en dos frentes muy claros:

- Ser los primeros en resolver dolores reales de sus clientes con tecnología israelí de vanguardia que hoy no está disponible en la zona.
- Usar esa capacidad técnica para desarrollar proyectos de alto impacto que sirvan de modelo para todo Centroamérica y el Caribe.

¿Hacia dónde va el modelo de adopción tecnológica en la región y qué van a necesitar los integradores locales para no quedar desplazados?

El modelo tradicional donde un integrador solo revendía licencias o cajas se terminó. Hoy en Latinoamérica, las empresas buscan socios estratégicos que les resuelvan problemas operativos concretos y les den garantías de ejecución.

El mayor riesgo para los integradores y empresas de tecnología locales es quedarse vendiendo lo mismo de siempre mientras las necesidades de ciberseguridad, automatización y eficiencia agrícola avanzan a otra velocidad. Para no quedar desplasados, van a necesitar incorporar innovación disruptiva de nivel mundial, pero sobre todo, metodologías de trabajo que les permitan dar previsibilidad a sus proyectos.

Hacia ahí va el mercado. A armar alianzas entre el desarrollo tecnológico más avanzado y los mejores ejecutores en el terreno. Quienes entiendan esta dinámica y se profesionalicen bajo esquemas de trabajo bien estructurados, van a ser los que lideren la región en los próximos años.

> “Las empresas buscan **socios estratégicos** que les resuelvan **problemas operativos concretos** y les den **garantías de ejecución.**”

Ciberseguridad estratégica para organizaciones que deciden con visión.

Soluciones de ciberseguridad estratégica empresarial

ESTRATEGIA Y GOBIERNO

RIESGO HUMANO Y CULTURA

RESILIENCIA ORGANIZACIONAL

DECISIONES CON VISIÓN EJECUTIVA

Decide First. Protect Better.

oktaritech.com

UNA PERSPECTIVA DIFERENTE PARA DECIDIR MEJOR.

Por qué las decisiones pesan más que los sistemas

La tecnología detecta.
Las personas interpretan.
Los líderes deciden.

Los sistemas no reaccionan, pero nos alertan. El valor real no está en la detección o el monitoreo, sino en el juicio que evalúa información, en la oportunidad de la decisión y en el liderazgo que asume las consecuencias.

La ciberseguridad no es solo un firewall. Empieza cuando alguien asume la responsabilidad de decidir.

> “Un sistema puede alertar. Solo una persona puede decidir actuar.”

Decisiones críticas

Antes, durante y después de un incidente

Antes

PREPARAR Y PREVENIR

- Asignar responsabilidades claras
- Entender y priorizar los riesgos
- Asegurar presupuesto y capacidades
- Validar planes y escenarios

Durante

RESPONDER CON CLARIDAD

- Acelerar el plan y los roles definidos
- Tomar decisiones rápidas con información confiable
- Comunicar con transparencia y control
- Proteger a las personas y al negocio

Después de un incidente

APRENDER Y FORTALECER

- Contener y recuperar con prioridad
- Analizar causas y decisiones tomadas
- Documentar lecciones y mejoras
- Fortalecer capacidades y cultura

Las decisiones no eliminan el riesgo, pero sí pueden reducir su impacto.

> “La demora también es una decisión.”

> “No decidir es dejar que el riesgo decida por la organización.”

> “Las mejores defensas fallan sin liderazgo.”

> “La cultura transforma tecnología en resiliencia.”

La cultura es el sistema operativo invisible de la seguridad

La seguridad no se instala con herramientas. Se construye con hábitos, decisiones y conversaciones cotidianas.

Lo que hacemos cada día —cómo reportamos, cómo colaboramos, cómo respondemos— puede abrir o cerrar la puerta al riesgo.

Una cultura que castiga el error termina ocultando lo que más necesitamos ver.

Una cultura basada en la confianza convierte las alertas en acción oportuna y protege lo que realmente importa.

- Liderazgo visible.
- Equipos comprometidos.
- Decisiones consistentes.

> La seguridad no es un sistema. Es una consecuencia de cómo actuamos cuando **nadie está mirando.**

La dimensión humana como infraestructura crítica

Las personas son el primer vector de riesgo y la primera línea de defensa.

Invertir en las personas —su conocimiento, criterio y capacidad de actuar— es tan estratégico como invertir en tecnología.

> La tecnología nos protege.
> Las personas nos hacen imparables.

COMPARATIVA

Cultura vulnerable vs. cultura sana

CULTURA VULNERABLE	CULTURA SANA
Oculta errores.	Reporta temprano.
Culpa antes de entender.	Aprende rápido.
Delega todo en TI.	Decide con claridad.
Cumple solo para auditoría.	Integra seguridad al negocio.
Reacciona tarde.	Comunica sin miedo.
Bloquea información.	Actúa con criterio.

La seguridad madura cuando la cultura permite actuar.

PRÁCTICAS DIARIAS

Microhábitos ejecutivos

Pequeñas acciones que generan decisiones seguras y consistentes.

VERIFICAR
antes de decidir, valida los hechos y las fuentes.

CONFIRMAR:
asegura roles, responsabilidades y próximos pasos.

REPORTAR:
comparte señales de riesgo sin demora.

DOCUMENTAR:
deja registro claro de decisiones y justificaciones.

ESCALAR:
lleva lo importante al nivel correcto, a tiempo.

PRACTICAR:
entrena escenarios y aprende continuamente.

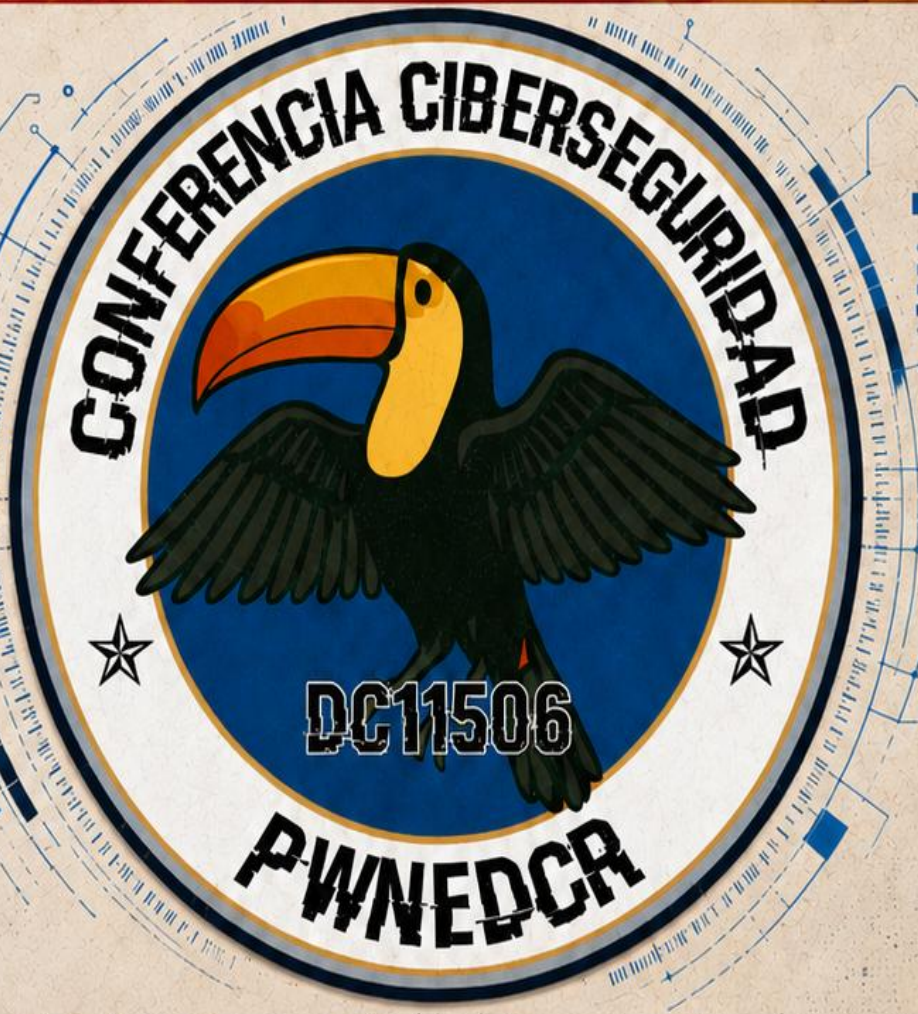
PREGUNTAR:
cuestiona supuestos y busca perspectivas diversas.

CUIDAR:
protege a las personas y promueve el bienestar.

> La madurez no nace de grandes discursos, sino de pequeños hábitos repetidos con disciplina.

PWNEDCR 0X9

LA CONFERENCIA DE HACKING Y CIBERSEGURIDAD MÁS GRANDE DE COSTA RICA



- CHARLAS DE EXPERTOS
- TALLERES PRÁCTICOS
- CAPTURE THE FLAG (CTF)
- RIFAS Y PREMIOS
- NETWORKING Y MUCHO MÁS

PWNEDCR es el evento de hacking y ciberseguridad más grande de Costa Rica, una conferencia referente donde profesionales, entusiastas y estudiantes se reúnen para compartir conocimiento a través de **charlas**, **talleres**, un **Capture The Flag (CTF)** competitivo, **rifas, premios** y mucho más.

12 Y 13 DE SEPTIEMBRE DE 2026

AUDITORIO NACIONAL DE COSTA RICA

ENTRADA VÁLIDA PARA AMBOS DÍAS DEL EVENTO

ESCANÉAME · VER VIDEO

MÁS INFORMACIÓN Y ENTRADAS EN:

>>> PWNEDCR.COM <<<

Ataques que la alta dirección debe entender

No necesita volverse técnico. Necesita entender el impacto.

La alta dirección no necesita conocer cada detalle técnico de un ataque, pero sí comprender sus implicaciones para el negocio. Cada amenaza puede afectar la continuidad, la reputación, el valor de la empresa y la confianza de sus grupos de interés.

Entender los tipos de ataque más relevantes permite priorizar decisiones, asignar recursos con criterio y liderar una respuesta efectiva. No se trata de prevenirlo todo, sino de estar preparados para lo que realmente puede impactar el negocio.

5 ATAQUES CLAVE QUE TODO LÍDER DEBE ENTENDER

Phishing y fraude ejecutivo	Engañan a personas para obtener acceso o transferencias ilegítimas. Impacto directo en pérdidas financieras y confianza.
Ransomware y extorsión digital	Bloquean operaciones o cifran información para exigir pago. Impacto en la continuidad y costos de recuperación.
Compromiso de terceros	Proveedores o aliados son la puerta de entrada. Impacto por contagio en la cadena de valor.
Fuga de información	Exposición o filtración de datos sensibles. Impacto legal, regulatorio y reputacional.
Suplantación y manipulación	Usan identidad y canales legítimos para manipular decisiones o desviar pagos. Impacto en el gobierno y el control.

> Comprender el ataque no es un ejercicio técnico. Es una responsabilidad de **liderazgo.**

Phishing, spear phishing y fraude ejecutivo

Estos ataques no explotan vulnerabilidades técnicas: explotan a las personas. Se basan en la **decepción**, la **confianza**, la **urgencia** y la **autoridad** para inducir decisiones que generan impacto financiero, operativo y reputacional.

> "La confianza sin verificación puede convertirse en fraude."

01 Phishing

Mensajes masivos y engañosos que buscan atraer a muchas personas haciéndose pasar por entidades confiables para robar credenciales, datos o instalar malware.

02 Spear phishing

Ataques dirigidos y personalizados que usan información especifica sobre la víctima o la organización para ganar credibilidad y lograr que realice acciones específicas.

03 Fraude ejecutivo

Los atacantes se hacen pasar por ejecutivos, directivos o proveedores para solicitar transferencias, cambios de cuenta o acciones sensibles, aprovechando la autoridad y la confianza.

PREGUNTA EJECUTIVA

¿Quién valida una instrucción financiera sensible antes de ejecutarla?

SEÑALES DE ALERTA

- Urgencia inusual
- Cambio de cuenta bancaria
- Solicitud fuera del proceso
- Presión por confidencialidad

Ransomware y extorsión digital

El ransomware puede paralizar operaciones, cifrar información crítica, interrumpir la continuidad del negocio y activar decisiones de liderazgo difíciles en minutos. No es solo un incidente técnico: es una prueba de resiliencia, prioridades y toma de decisiones bajo presión.

OPERACIÓN

Los sistemas críticos pueden quedar inutilizados. La producción se detiene, los procesos se interrumpen y los equipos trabajan a ciegas, sin visibilidad ni herramientas.

FINANZAS

Los costos se disparan: rescates, recuperación, forense, multas y horas hombre. Además, el impacto financiero se extiende en el tiempo.

REPUTACIÓN

La confianza de clientes, socios e inversionistas puede erosionarse rápidamente. La percepción del mercado cambia en cuestión de horas.

DECISIÓN

Bajo presión, el liderazgo debe decidir sin toda la información: ¿pagar o no pagar? ¿Comunicar o contener? Cada decisión tiene consecuencias.

PREGUNTA EJECUTIVA

¿La organización sabe operar si sus sistemas críticos no están disponibles durante 72 horas?

DOBLE EXTORSIÓN

No solo bloquean la información; también amenazan con exponerla.

> Una crisis de ransomware no solo prueba la tecnología. **Prueba el liderazgo.**

RIESGOS DE TERCEROS

Tu nivel de seguridad nunca será mayor que el de tu eslabón más débil.

Proveedores, socios y aliados amplían capacidades, pero también tu superficie de ataque. Gestionarlos no es una opción, es una responsabilidad estratégica.

PROVEEDORES CRÍTICOS
Accesos privilegiados, soporte remoto y manejo de información sensible.

SERVICIOS EN LA NUBE
Configuraciones incorrectas, permisos excesivos y dependencias ocultas.

SOFTWARE DE TERCEROS
Vulnerabilidades no parchadas que pueden ser la puerta de entrada.

RIESGO CONTRACTUAL
Falta de cláusulas de seguridad, auditoría y notificación de incidentes.

Gestionar terceros no es burocracia, es gestión de **riesgo inteligente.**

Los desfases de seguridad

El riesgo crece en el espacio entre lo que creemos controlar y lo que realmente hemos preparado.

En toda organización existen brechas que no siempre se ven, pero que condicionan la resiliencia. Los desfases de seguridad aparecen cuando hay desalineación entre lo que se declara y lo que se ejecuta, entre lo que se tiene y lo que se necesita, entre lo que se percibe y lo que realmente ocurre. Comprenderlos es el primer paso para cerrarlos.

> *La madurez empieza cuando la organización deja de confundirse con su propia narrativa.*

Política vs. práctica	VS.	Las políticas pueden estar bien redactadas, pero si los procesos y comportamientos diarios no las reflejan, el riesgo persiste.
Tecnología vs. cultura	VS.	La tecnología puede ser avanzada, pero si la cultura no promueve el cumplimiento y la responsabilidad, las defensas se debilitan.
Cumplimiento vs. capacidad real	VS.	Cumplir un estándar no siempre significa estar preparado para enfrentar un ataque real. La capacidad se demuestra en la práctica.
Percepción ejecutiva vs. exposición real	VS.	La dirección puede tener confianza en los reportes, pero la exposición real puede ser mucho mayor de lo que se percibe.
Incidente técnico vs. decisión corporativa	VS.	Un incidente no se resuelve solo en lo técnico. Requiere decisiones ejecutivas rápidas, claras y alineadas al impacto del negocio.

Identificar desfases a tiempo evita falsas sensaciones de seguridad.

INTELIGENCIA ARTIFICIAL, DATOS Y NUEVAS EXPOSICIONES

La innovación trae oportunidades,
pero también nuevos vectores de riesgo.

MODELOS DE IA

Pueden ser manipulados, envenenados o revelar información sensible.

DATOS SENSIBLES

Más datos, más valor, más atractivo para los atacantes.

AUTOMATIZACIÓN

Errores de configuración o lógica pueden escalar impactos.

NUEVAS SUPERFICIES

APIs, integraciones y herramientas de IA abren puertas invisibles.

La adopción responsable de IA y datos
debe estar guiada por principios de seguridad.

CON VISIÓN AL SUR

CIBERSEGURIDAD • DECISIONES • SUDAMÉRICA

SUR / 01

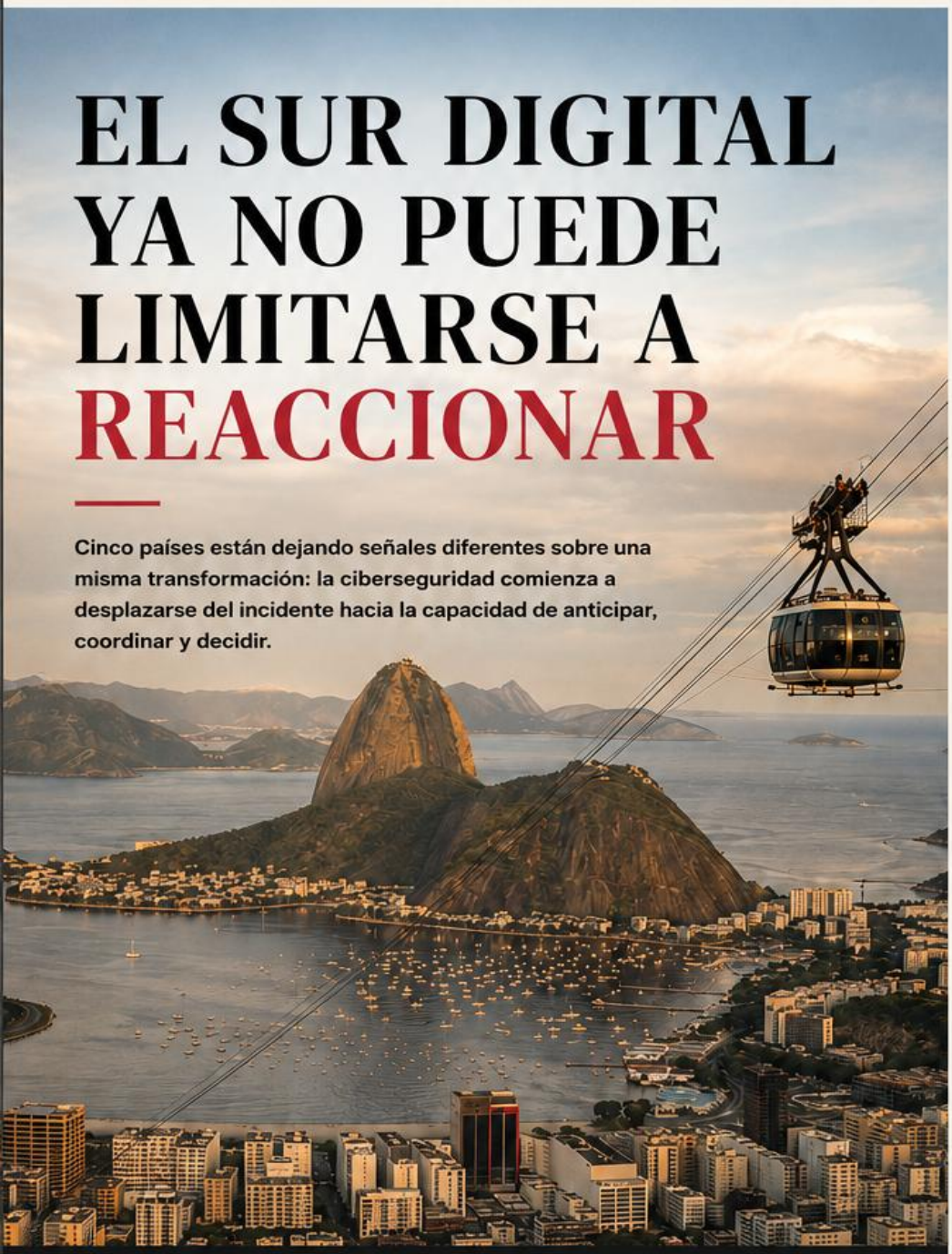
- BRASIL •
- CHILE •
- PERÚ •
- ARGENTINA •
- COLOMBIA •

SUR

NORTE

EL SUR DIGITAL YA NO PUEDE LIMITARSE A REACCIONAR

Cinco países están dejando señales diferentes sobre una misma transformación: la ciberseguridad comienza a desplazarse del incidente hacia la capacidad de anticipar, coordinar y decidir.



Durante años, buena parte de la conversación regional estuvo concentrada en cuánto estaban creciendo los ataques. Esa pregunta comienza a quedarse corta.

Lo verdaderamente relevante ahora es otra cosa:

¿qué están aprendiendo los países después de descubrir dónde realmente están sus dependencias digitales?

Este reportaje reúne los movimientos más relevantes que marcan la agenda de ciberseguridad en Sudamérica y lo que cada uno implica para quienes toman decisiones en organizaciones públicas y privadas.

LA SEÑAL DEL SUR

Proveedores estratégicos comprometidos, identidades vulneradas, ejercicios nacionales de respuesta, nuevas capacidades institucionales y una inteligencia artificial que también está transformando el fraude dibujan una nueva realidad para la ciberseguridad sudamericana.

> *"El verdadero desafío regional no será impedir el próximo incidente. Será decidir mejor antes de que ocurra."*

HECHOS QUE IMPORTAN
Lo que está ocurriendo.

DECISIONES QUE MULTIPLICAN O REDUCEN RIESGOS
Por qué importa al nivel ejecutivo.

APRENDIZAJES QUE VIAJAN
Cómo trasladar la señal al norte.

PERSPECTIVA REGIONAL
Tendencias que conectan a Sudamérica.

Hechos verificados en fuentes oficiales. Contexto y análisis son elaboración editorial de DECIDE FIRST.

EL SUR DIGITAL YA NO PUEDE LIMITARSE A REACCIONAR

Brasil, Chile, Perú, Argentina y Colombia están dejando señales que merecen ser observadas más allá del incidente. Proveedores estratégicos comprometidos, identidades vulneradas, ejercicios nacionales de respuesta, nuevas capacidades **institucionales** y una **inteligencia artificial** que también está **transformando el fraude** dibujan una nueva realidad para la ciberseguridad sudamericana.

> *La madurez digital de un país no se mide solo por cuánto digitaliza, sino también por su capacidad para proteger aquello que decidió convertir en infraestructura digital.*

BRASIL

Cuando comprometer al proveedor puede ser más importante que atacar al cliente

El 21 de mayo de 2026, el Centro de Prevención, Tratamiento y Respuesta a Incidentes Cibernéticos de Gobierno de Brasil, CTIR Gov, informó sobre un **incidente relacionado con Dígito Tecnologia**, compañía brasileña dedicada a soluciones de defensa e inteligencia.

La alerta oficial calificó como **crítico** el incidente por la naturaleza de los servicios de la empresa e indicó la exposición masiva de bases de datos, repositorios de código fuente y archivos internos. El organismo señaló además que la compañía suministra sistemas de interceptación y monitoreo a más de 150 instituciones gubernamentales y organismos de seguridad pública.

El episodio permite observar un problema mucho mayor que la organización directamente comprometida.

LA SEÑAL

Una filtración vinculada con Dígito Tecnologia, proveedor de soluciones de defensa e inteligencia utilizado por más de 150 instituciones públicas y organismos de seguridad, expuso bases de datos, repositorios de código fuente y archivos internos.

Fuente: CTIR Gov (Brasil) – Recomendación 05/2026
21 de mayo de 2026.

POR QUÉ IMPORTA

Durante años, la ciberseguridad empresarial concentró gran parte de sus esfuerzos en proteger el perímetro propio.
Ese perímetro prácticamente ha desaparecido.

Proveedores tecnológicos, plataformas, integradores, servicios **especializados, aplicaciones y terceros forman parte de arquitecturas en las que diferentes organizaciones** comparten información, accesos y dependencias.

Eso significa que una organización puede hacer muchas cosas correctamente y continuar expuesta a una decisión de seguridad tomada fuera de sus fronteras.

El caso brasileño pone nuevamente sobre la mesa una pregunta **¿sabemos realmente cuánto riesgo hemos delegado?**

Evaluar a un tercero al momento de contratarlo ya no es suficiente. Hay que comprender qué información procesa, qué accesos mantiene, qué sistemas conecta, qué otros proveedores utiliza y, sobre todo, qué podria ocurrir con nuestra organización si ese tercero deja de ser confiable.

El riesgo de terceros ha dejado de ser únicamente contractual. Puede convertirse en riesgo sistémico.

BRASIL (CONTINUACIÓN)

El riesgo no siempre se materializa desde fuera de la organización. A veces aparece en un eslabón de la cadena de confianza que procesa nuestra información, conecta nuestros sistemas o comparte nuestros servicios.

La ciberseguridad moderna exige visibilidad, evaluación continua y responsabilidad compartida.

MÁS ALLÁ DEL INCIDENTE

El caso brasileño no es únicamente un incidente técnico. Es una señal estratégica sobre cómo el riesgo se ha desplazado desde el perímetro hacia el ecosistema.

La próxima discusión no será solamente sobre cómo evitar que nos ataquen, sino sobre cómo asegurarnos de que nuestras dependencias digitales no se conviertan en nuestro punto ciego.

> *¿Sabemos realmente cuánto riesgo hemos delegado?*

QUÉ OBSERVAR

- Evaluación profunda de terceros críticos y subproveedores.
- Visibilidad continua sobre accesos, sistemas e información.
- Contratos que incluyan controles, obligaciones y auditoría.
- Planes de respuesta que contemplen incidentes en la cadena de suministro.
- Métricas que midan concentración de riesgo en terceros.

Fuente:
CTIR Gov (Brasil) – Recomendación 05/2026
21 de mayo de 2026.

CHILE

No siempre hay que romper la infraestructura para acceder a lo sensible

Durante 2026, una denuncia sobre la posible exposición de información de instituciones públicas generó alarma nacional. El Gobierno descartó una intravención masiva y se concentró la investigación en el robo de credenciales de un funcionario.

En paralelo, Chile decidió fortalecer su sistema de identidad digital. Desde mayo, ClaveÚnica —utilizada para acceder a cerca de 1.700 servicios públicos— incorporó voluntariamente un segundo factor de autenticación mediante códigos temporales. Más de 16 millones de personas cuentan con ClaveÚnica activa.

No fue una obligación regulatoria. Fue una decisión estratégica frente a una realidad: una identidad comprometida no necesita romper la infraestructura para generar impacto.

LA SEÑAL

La atención se centró en la vulneración de credenciales y la identidad digital volvió al centro de la conversación.

Fuente: Gobierno Digital de Chile – Mayo 2026
Fortalecimiento de ClaveÚnica y autenticación multifactor.

POR QUÉ IMPORTA

Una identidad con privilegios adecuados puede abrir la puerta a información sensible, incluso en infraestructuras robustas. La gestión de accesos y la confianza digital son decisivas en la estrategia de seguridad.

MÁS ALLÁ DEL INCIDENTE

Proteger sistemas sin comprender quién puede acceder a ellos, desde dónde y bajo qué condiciones, deja una superficie que ninguna tecnología puede cerrar por sí sola.

QUÉ OBSERVAR

- Gobernanza y administración de identidades privilegiadas.
- Autenticación multifactor y accesos adaptativos.
- Detección de comportamientos anómalos en accesos.
- Revisión periódica de privilegios y accesos críticos.
- Educación continua y cultura de verificación.

Fuente: Gobierno Digital de Chile – Mayo 2026
Información pública sobre ClaveÚnica.

PERÚ

La resiliencia también necesita ensayo

El 16 de julio, Perú desarrolló **SIMAC 2026**, su cuarto Simulacro Nacional de Ataques Cibernéticos.

Los resultados comunicados por la Presidencia del Consejo de Ministros indican que 152 entidades participaron en un ejercicio técnico diseñado para poner a prueba capacidades de detección, respuesta y recuperación ante incidentes de seguridad digital.

El ejercicio se produce además en un contexto en el que el país ha venido desarrollando su propuesta de Estrategia Nacional de Ciberseguridad 2026–2028, orientada a construir un ciberespacio seguro, resiliente y confiable y a proteger infraestructuras críticas, activos digitales y derechos ciudadanos.

POR QUÉ IMPORTA

Un plan de respuesta puede ser impecable sobre el papel y fracasar en los primeros minutos de una crisis.

Porque los incidentes reales introducen elementos que ningún procedimiento escrito puede resolver por si solo: presión, incertidumbre, información incompleta, decisiones simultáneas, responsabilidades cruzadas y necesidad de coordinación.

Ahí aparece el verdadero valor de simular. No para demostrar que todo funciona.

Para descubrir qué no funciona mientras todavía existe tiempo para corregirlo.

Una organización que nunca ha ensayado una crisis desconoce cuánto tardará en reconocerla, quién tendrá autoridad para decidir, cómo se coordinarán las áreas técnicas con la dirección, cuándo deberá comunicarse con clientes o autoridades y qué ocurrirá si varios servicios fallan simultáneamente.

MÁS ALLÁ DEL INCIDENTE

El simulacro revela la madurez real de un país en cuatro dimensiones clave:

01 PREPARACIÓN
Evalúa si los planes existen, están actualizados y son comprendidos por quienes deben ejecutarlos.

02 COORDINACIÓN
Pone a prueba la comunicación entre instituciones, la claridad de roles y la toma de decisiones conjuntas.

03 CAPACIDAD OPERATIVA
Mide herramientas, recursos, procedimientos y habilidades técnicas bajo presión.

04 RECUPERACIÓN
Permite validar tiempos de restauración, continuidad del servicio y aprendizaje posterior.

La resiliencia no debería descubrirse durante el incidente.

La resiliencia que nunca se practica sigue siendo una hipótesis.

QUÉ OBSERVAR

- ¿Cuánto tardan las entidades en reconocer un incidente realista?
- ¿Están claras las responsabilidades y los niveles de escalamiento?
- ¿Funcionan los canales de comunicación bajo presión?
- ¿Existen acuerdos previos con proveedores críticos?
- ¿Se ejecutan los planes de continuidad cuando fallan varios servicios a la vez?
- ¿Qué tan rápido se aprende después del ejercicio?

Fuente:
PCM Perú – 16 de julio de 2026
Estrategia Nacional de Ciberseguridad del Perú 2026–2028 (propuesta)

> *"Ensayar no elimina el riesgo, pero nos revela lo que aún no estamos listos para enfrentar."*

Un país que ensaya hoy será un país que decide mejor cuando el incidente ocurra mañana.

ARGENTINA

Construir capacidad antes de necesitarla

El Decreto 941/2025 creó el **Centro Nacional de Ciberseguridad** como organismo encargado de planificar, ejecutar y supervisar políticas, programas y acciones destinadas a proteger el ciberespacio de interés nacional, las infraestructuras críticas de información, los activos digitales estratégicos del Estado y los sistemas tecnológicos utilizados para prestar servicios públicos esenciales.

El Centro fue presentado oficialmente en mayo de 2026 y durante el año continuó desarrollándose su estructura normativa y técnica.

POR QUÉ IMPORTA

Digitalizar un país aumenta su capacidad. También aumenta aquello que debe proteger.

Servicios públicos, energía, telecomunicaciones, sistemas financieros, salud, transporte, administración pública e identidad digital dependen progresivamente de infraestructuras conectadas.

Por eso, la madurez digital de una nación no puede medirse únicamente por la cantidad de servicios que logra digitalizar. Debe medirse también por su capacidad para anticipar, proteger, coordinar, responder y recuperar aquello que decidió convertir en infraestructura digital.

Prepararse antes de necesitarlo también es una forma de defensa.

MÁS ALLÁ DEL INCIDENTE

La ciberseguridad nacional necesita tecnología. Pero necesita igualmente institucionalidad, responsabilidades definidas, coordinación y capacidad de decisión.

No se trata solo de detectar amenazas. Se trata de comprender quién decide, con qué información, bajo qué marco y con qué impacto para el país.

> *La madurez digital de una nación no puede medirse únicamente por la cantidad de servicios que logra digitalizar. Debe medirse también por su capacidad para anticipar, proteger, coordinar, responder y recuperar aquello que decidió convertir en infraestructura digital.*

QUÉ OBSERVAR

Este nuevo organismo nacional deja señales que conviene seguir de cerca:

- Coordinación entre órganos del Estado y sector privado.
- Protección efectiva de infraestructuras críticas.
- Desarrollo de capacidades técnicas y talento especializado.
- Gestión de riesgos digitales en proyectos estratégicos.
- Cooperación internacional y estándares comunes.

Fuente: Decreto 941/2025 – República Argentina
Presentación del Centro Nacional de Ciberseguridad
Mayo 2026

La ciberseguridad nacional no solo protege sistemas, protege decisiones, servicios esenciales y derechos ciudadanos.

PREPARARSE ANTES DE NECESITARLO TAMBIÉN ES UNA FORMA DE DEFENSA.

COLOMBIA

Cuando el engaño también aprende

Colombia introduce una variable diferente en esta lectura regional: inteligencia artificial.

En abril de 2026, el **Ministerio de Tecnologías de la Información y las Comunicaciones** informó que, aunque durante 2025 se había registrado una reducción de incidentes, el Gobierno elevaba la alerta frente al incremento del fraude digital y al uso de inteligencia artificial para desarrollar ataques dirigidos contra sectores estratégicos como salud, energía, defensa y telecomunicaciones.

No estamos solamente ante nuevas herramientas para atacar. Estamos frente a una transformación en la escala y credibilidad del engaño.

> *La inteligencia artificial permite producir comunicaciones coherentes, adaptar lenguaje, personalizar mensajes y generar grandes cantidades de variaciones con un costo marginal extraordinariamente bajo.*

POR QUÉ IMPORTA

El phishing tradicional tenía defectos: errores ortográficos, mensajes genéricos, traducciones deficientes, contextos poco convincentes.

Muchas de esas señales están desapareciendo.

La inteligencia artificial permite que el engaño parezca más humano y más convincente.

El desafío para las organizaciones no será conseguir que una persona memorice una lista infinita de amenazas.

Será conseguir que pueda detenerse ante una situación aparentemente normal y reconocer cuándo algo merece ser cuestionado.

LA SEÑAL

Alerta nacional emitida en abril de 2026 sobre el incremento del fraude digital y el uso de inteligencia artificial para ataques más sofisticados.

Fuente: Ministerio TIC de Colombia – Abril 2026
Informe sobre el panorama de ciberseguridad y fraude digital en Colombia.

MÁS ALLÁ DEL INCIDENTE

El fraude digital no es únicamente tecnológico. Es también psicológico y contextual.

La IA permite analizar grandes cantidades de datos públicos, comprender patrones de comportamiento y generar mensajes que imitan con precisión el tono, el estilo y el contexto de una comunicación legítima.

Esto significa que:

- Los correos son más creibles y personalizados.
- Los mensajes se adaptan al rol y al momento de la víctima.
- Los ataques pueden escalar rápidamente con bajo costo.
- El engaño puede incluir audio, imágenes y documentos falsos altamente convincentes.

Por eso la defensa necesita algo más que enseñar a buscar errores. Necesita desarrollar criterio y cultura de verificación constante.

QUÉ OBSERVAR

- ¿Nuestra organización tiene visibilidad sobre cómo se usa la IA para ataques?
- ¿Qué tan preparados están nuestros equipos para identificar engaños sofisticados?
- ¿Contamos con controles efectivos para proteger identidades privilegiadas?
- ¿Evaluamos continuamente comportamientos anómalos y riesgos emergentes?
- ¿Promovemos una cultura donde preguntar antes de actuar sea lo normal?

Lo peligroso no siempre parecerá peligroso.
La mejor defensa es la desconfianza consciente, no la desconfianza paralizante.

Cuando el engaño aprende, la mejor defensa es la desconfianza consciente, no la desconfianza paralizante.

La preparación no consiste solo en tener tecnología, sino en desarrollar criterios, verificar y decidir con intención.

LA SEÑAL DEL SUR

Cinco países, cinco movimientos, una misma tendencia

No conforman una única historia.
Pero sí dibujan una tendencia.

Sudamérica está descubriendo que la siguiente etapa de la ciberseguridad no se resolverá únicamente incorporando más herramientas. Será necesario comprender dependencias, identidades, capacidades, comportamientos, coordinación y decisiones.

El perímetro se expandió. La superficie de ataque cambió. Los adversarios también.

Y mientras la transformación digital continúa conectando organizaciones, gobiernos, ciudadanos y servicios esenciales, la diferencia entre resistir un incidente y quedar condicionado por él dependerá cada vez más de algo que ocurre mucho antes del primer indicador de compromiso:

haber pensado qué hacer.

MÁS ALLÁ DEL INCIDENTE

De medir incidentes a medir decisiones

Durante demasiado tiempo hemos utilizado el incidente como principal unidad de medida de la ciberseguridad.

- Cuántos ataques.
- Cuántos registros.
- Cuántas vulnerabilidades.
- Cuánto tiempo de indisponibilidad.

Todos son indicadores necesarios. Pero ninguno responde por completo una pregunta más importante:

> *¿Qué tan preparada estaba la organización para decidir cuando algo dejó de funcionar como esperaba?*

Quizá ahí se encuentre una de las transformaciones más relevantes que la región necesita impulsar.

Pasar de organizaciones preparadas para reaccionar técnicamente a organizaciones capaces de decidir estratégicamente bajo presión.

Porque el próximo incidente llegará con una tecnología diferente, una vulnerabilidad distinta o un método que todavía no conocemos.

Lo que sí podemos construir antes de que ocurra es la capacidad para reconocerlo, interpretarlo, contenerlo, comunicarlo y decidir frente a él.

Haber decidido mejor antes de que ocurra es la verdadera ventaja estratégica.

LO QUE ESTA REGIÓN NOS ESTÁ MOSTRANDO

- **Proveedores en el centro del riesgo.** Una organización puede ser impecable y seguir expuesta por decisiones tomadas fuera de sus fronteras.
- **La identidad como nuevo perímetro.** Saber quién accede, desde dónde y con qué privilegios es hoy tan crítico como proteger los sistemas.
- **Resiliencia que se practica.** Simular antes de necesitarlo es descubrir a tiempo lo que no funciona.
- **Capacidad institucional.** Los países que construyen estructuras y coordinación hoy, estarán mejor preparados mañana.
- **El engaño que evoluciona.** La inteligencia artificial está incrementando la escala, realismo y credibilidad del fraude.

El próximo incidente no es cuestión de si ocurrirá, sino de cuándo. Lo que sí podemos decidir hoy es cómo estaremos listos para enfrentarlo.

Decidir antes es proteger después.

La ciberseguridad no comienza cuando aparece la amenaza. Comienza cuando alguien, en algún lugar, decide que proteger lo importante es parte de su responsabilidad.

Esa es la señal que el sur está dejando al norte.

CON VISIÓN AL SUR

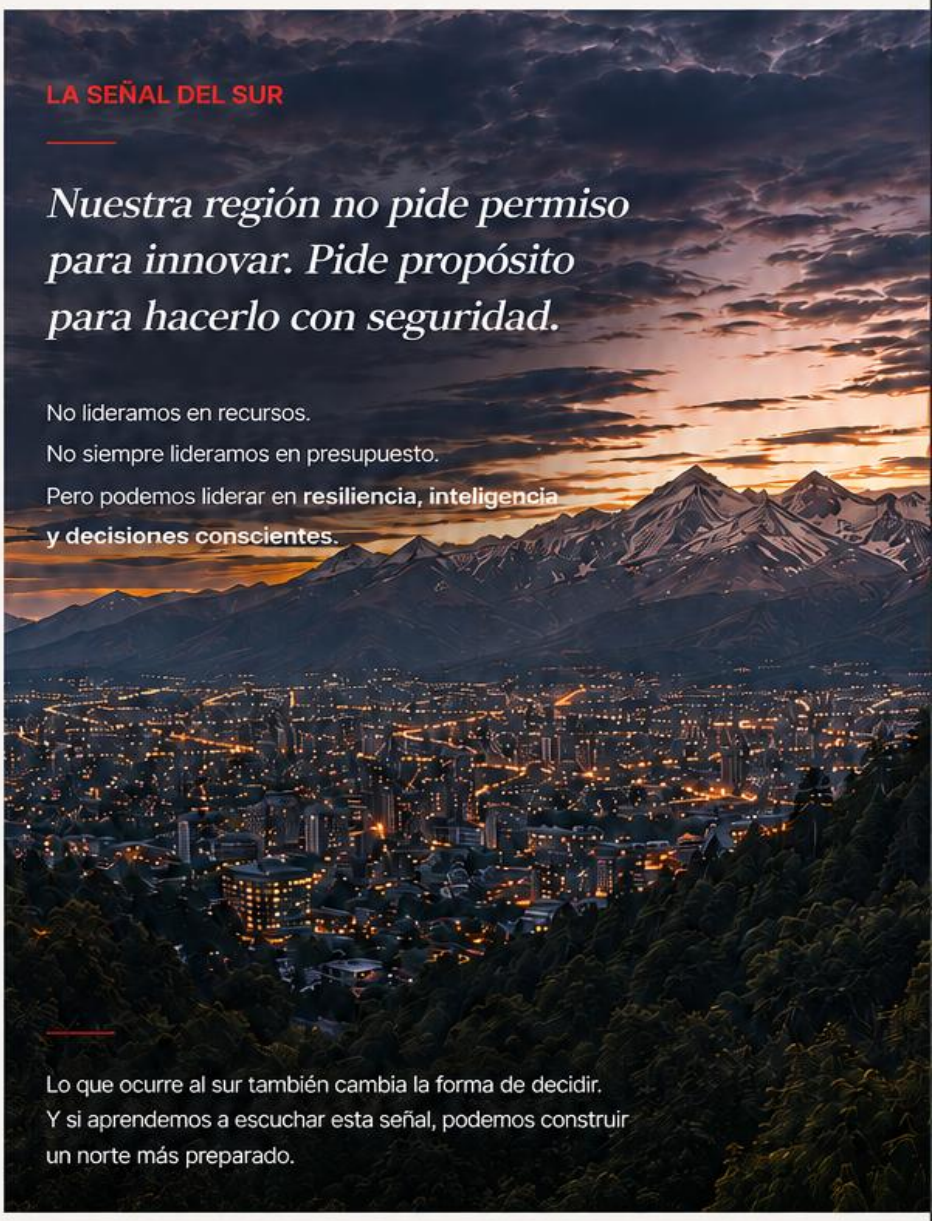
CIBERSEGURIDAD • DECISIONES • SUDAMÉRICA

QUÉ OBSERVAR

Para las juntas directivas, comités de auditoría y líderes ejecutivos, estas son preguntas que ya no pueden esperar.

- ¿Tenemos visibilidad real sobre quién accede, **desde dónde** y con qué privilegios?
- ¿Evaluamos continuamente riesgos, comportamientos anómalos y dependencias críticas?
- ¿Nuestros **proveedores** y terceros cumplen con los mismos estándares que exigimos internamente?
- ¿Contamos con planes de respuesta probados y equipos entrenados?
- ¿Qué decisiones tomaremos si mañana un incidente nos deja sin una capacidad esencial?

> *Las organizaciones que hoy lideran en ciberseguridad no son las que tienen más tecnología, sino las que toman mejores decisiones, más rápido y con más claridad.*



LA SEÑAL DEL SUR

Nuestra región no pide permiso para innovar. Pide propósito para hacerlo con seguridad.

No lideramos en recursos.
No siempre lideramos en presupuesto.
Pero podemos liderar en **resiliencia, inteligencia y decisiones conscientes.**

Lo que ocurre al sur también cambia la forma de decidir.
Y si aprendemos a escuchar esta señal, podemos construir un norte más preparado.

LA PREGUNTA QUE VIAJA AL NORTE

¿Estamos escuchando lo que el sur ya entendió?

Lo que Sudamérica está viviendo no es el futuro. Es el presente. Y quienes seguimos mirando hacia el norte en busca de respuestas, haríamos bien en mirar también hacia el sur para encontrar señales que ya están encendidas.

Porque la ciberseguridad no es una carrera de tecnología. Es una carrera de decisiones.

Y decidir bien es lo único que realmente nos protege mejor.

Proteger el presente es importante. Sostener el futuro es estratégico.

La verdadera madurez no se compra, se construye.

Decisiones conscientes hoy. Resiliencia real mañana. Confianza que permanece.

ScaleUp
ISRAELI HITECH IN LATIN AMERICA

ESCANÉAME · VER VIDEO

Visita:
scaleup-global.com

ANOTACIONES DEL CISO

Apuntes estratégicos sobre riesgo, ciberseguridad y decisiones ejecutivas.

El objetivo no es evitar todo riesgo. Es tomar mejores decisiones.

LIDERAR. PROTEGER. DECIDIR.

Tres verbos. Una responsalbilidad.
El futuro se asegura con estrategia.

ANOTACIONES DEL CISO

Perspectiva. Experiencia. Responsabilidad.

IA sin seguridad no es innovación, es exposición

Por qué la ciberseguridad debe liderar la adopción responsable de la Inteligencia Artificial

La Inteligencia Artificial ya no es una promesa lejana; es parte de nuestras operaciones, decisiones y productos. Pero su adopción acelerada está ocurriendo más rápido que nuestra capacidad para comprender y gestionar los riesgos que introduce.

Como CISO, mi preocupación no es si vamos a usar IA, sino cómo lo estamos haciendo. La IA no es solo otra herramienta tecnológica: es un nuevo modelo operativo que amplía nuestra superficie de ataque, transforma el perfil de riesgos y exige repensar los principios de confidencialidad, integridad, disponibilidad y, sobre todo, confianza.

La IA como multiplicador de riesgos

Los modelos de IA aprenden de datos. Y los datos, en la mayoría de las organizaciones, son nuestro activo más valioso y también el más expuesto.

Cuando conectamos modelos a fuentes internas, los alimentamos con información sensible o les damos capacidad de actuar, estamos otorgando poder. Y donde hay poder, hay riesgo.

Los ataques ya no se centran únicamente en vulnerar sistemas; ahora buscan envenenar datos de entrenamiento, manipular modelos, extraer información confidencial a través de consultas o abusar de automatizaciones para escalar accesos y moverse lateralmente.

La IA amplifica lo bueno. Pero también amplifica lo malo.

Riesgos clave que debemos gestionar desde ciberseguridad

Fuga y exposición de datos sensibles
Los modelos pueden memorizar información. Sin controles adecuados, esa información puede ser extraída por actores internos o externos.

Envenenamiento de datos y modelos
Datos manipulados pueden inducir comportamientos erróneos o maliciosos en los modelos, afectando decisiones críticas.

Inyección de prompts y abuso de salidas
Entradas manipuladas pueden provocar que los modelos revelen información, omitan controles o generen contenido no autorizado o dañino.

Uso indebido de automatizaciones
Agentes de IA con permisos excesivos o sin supervisión pueden ejecutar acciones no previstas o ser utilizados como vectores de ataque.

Riesgos legales, éticos y reputacionales
Decisiones sesgadas, falta de explicabilidad o incumplimiento normativo pueden generar impactos legales y pérdida de confianza.

Nuestra responsabilidad como CISOs

No podemos delegar la seguridad de la IA solo al equipo de datos o al área de tecnología.
Debemos liderar un enfoque integral que incluya:

- ✓ Gobernanza de datos y modelos
- ✓ Evaluación de riesgos específica para IA
- ✓ Controles de acceso y monitoreo continuo
- ✓ Pruebas de seguridad ofensiva para modelos y sistemas de IA
- ✓ Transparencia, explicabilidad y trazabilidad
- ✓ Colaboración entre ciberseguridad, legal, cumplimiento y negocio

> La IA es el motor. La ciberseguridad es el cinturón de seguridad y los frenos.
> Sin seguridad, la innovación no solo se detiene... puede destruir.

CISO
Decide First

ANOTACIONES DEL CISO

IA sin gobernanza es exposición: por qué la ciberseguridad debe liderar su adopción

La inteligencia artificial no es solo una nueva tecnología; es un multiplicador de riesgos que exige una visión de ciberseguridad desde el diseño.

La conversación sobre inteligencia artificial (IA) ha evolucionado rápidamente. Pasamos de la experimentación a la adopción acelerada. Sin embargo, en muchas organizaciones, la pregunta clave sigue sin responderse: ¿estamos abordando la IA como una capacidad estratégica segura o como un experimento tecnológico aislado?

Desde la perspectiva del CISO, la IA no es un proyecto de TI ni un tema exclusivo de innovación. Es un nuevo vector de riesgo empresarial que debe gestionarse con el mismo rigor —o mayor— que cualquier iniciativa crítica de seguridad.

La nueva superficie de ataque

Los sistemas de IA amplían la superficie de ataque en formas que aún estamos aprendiendo a dimensionar:

Datos como objetivo.
Los modelos de IA se alimentan de grandes volúmenes de datos, muchos de ellos sensibles. Su robo, envenenamiento o manipulación puede tener consecuencias directas en la operación y la reputación.

Modelos vulnerables.
Los modelos pueden ser manipulados a través de ataques de envenenamiento de datos, extracción de modelos o evasión de prompts, generando respuestas incorrectas o sesgadas que impactan decisiones y procesos críticos.

Dependencias opacas.
Muchos modelos provienen de terceros o de fuentes abiertas. Sin visibilidad sobre su entrenamiento, código o controles, heredamos riesgos que no podemos gestionar.

Nuevos vectores humanos.
La IA es explotada a través de ingeniería social más sofisticada, deepfakes, automatización de phishing y suplantación de identidad a escala.

La IA no solo puede ser atacada, también puede ser usada para atacar. Debemos asumir ambos escenarios.

Riesgos que no debemos subestimar

Más allá de los riesgos técnicos, la IA introduce desafíos de gobernanza, cumplimiento y ética que, si no se gestionan desde la ciberseguridad, pueden convertirse en crisis estratégicas.

Entre los más relevantes:

- **Falta de trazabilidad y explicabilidad:** ¿Podemos explicar por qué un modelo tomó cierta decisión? Si no, ¿cómo gestionamos el riesgo legal, regulatorio o reputacional?
- **Sesgos y discriminación algorítmica:** Un modelo entrenado con datos sesgados puede amplificar desigualdades y generar impactos éticos y regulatorios.
- **Cumplimiento normativo:** Regulaciones como la AI Act de la UE, NIST AI RMF o ISO/IEC 42001 están marcando expectativas claras. La ciberseguridad debe asegurar conformidad desde el diseño.
- **Shadow AI:** El uso no autorizado de herramientas de IA por parte de colaboradores puede provocar fugas de información, violaciones de datos y pérdida de control.

El rol del CISO: liderar la confianza en la IA

El CISO debe asumir un rol protagónico en asegurar que la IA se adopte de forma segura, ética y alineada al negocio. Esto implica:

- Definir una estrategia de IA segura alineada al apetito de riesgo y objetivos del negocio.
- Evaluar y monitorear continuamente los riesgos de los modelos, datos y proveedores.
- Establecer políticas claras sobre el uso aceptable de IA y promover una cultura de uso responsable.
- Integrar controles de seguridad en el ciclo de vida del modelo (MLOps seguro).
- Medir, reportar y mejorar constantemente la postura de riesgo en IA.

Conclusión

La IA tiene el potencial de transformar nuestras organizaciones, pero también de amplificar nuestros riesgos si no la abordamos con una visión de seguridad integral.

La ciberseguridad no debe reaccionar a la IA. Debe liderarla.

MSIE. Angie Piedra C.
CISO
Decide First

CASO REAL

Cuando una decisión tardía cuesta más que una tecnología ausente

Una historia real. Una lección que evita otras.

EL CONTEXTO

Una empresa en crecimiento pospuso la revisión de su estrategia de ciberseguridad para enfocarse en la expansión comercial.

LO QUE OCURRIÓ

Un incidente de ransomware paralizó operaciones clave por 10 días, afectó clientes estratégicos y generó sanciones regulatorias.

EL IMPACTO

- Pérdidas directas: 2.3 M USD
- Clientes afectados: 19% de la base
- Recuperación operativa: +30 días
- Daño reputacional: significativo

LA LECCIÓN

La tecnología puede esperar.
Las decisiones correctas, no.
La anticipación ejecutiva cuesta menos que la reacción forzada.

DECIDE FIRST

SISTEMAS
ARQUITECTURA
REDES
SEGURIDAD

PROFUNDIDAD QUE PROTEGE

SECCIÓN + TÉCNICO + 01

100% TÉCNICO

Arquitectura, análisis, profundidad y criterio técnico

// ACCESS
// CONTROL
// ENCRYPTION
// INTEGRITY

ARQUITECTURA

ANÁLISIS

PROFUNDIDAD

CRITERIO TÉCNICO

100% TÉCNICO

ARQUITECTURA DE RED
Y CIBERSEGURIDAD

SEGMENTAR PARA CONTENER

Por qué el diseño de red es una decisión de ciberseguridad

Una arquitectura segmentada reduce la superficie de ataque, limita el movimiento lateral y acelera la contención ante incidentes. El diseño de red no es solo infraestructura, es una estrategia de defensa.

> Una arquitectura bien segmentada no evita necesariamente el acceso inicial. Evita que ese acceso se convierta fácilmente en **control de toda la infraestructura.**

En una infraestructura moderna, la seguridad no depende únicamente de firewalls, plataformas de detección o herramientas de protección instaladas sobre los endpoints. Una parte importante de la capacidad defensiva de una organización se define mucho antes: **en la arquitectura de la red.**

Cuando una red ha crecido sin criterios claros de segmentación, separación de funciones o control de flujos, un incidente inicialmente limitado puede transformarse rápidamente en un problema de alcance corporativo.

Por el contrario, una arquitectura segmentada permite reducir la superficie de exposición, controlar el movimiento lateral de un atacante y, sobre todo, ganar tiempo durante las primeras etapas de una intrusión.

Ese tiempo puede marcar la diferencia entre contener un incidente dentro de un segmento específico o enfrentar la propagación hacia sistemas críticos.

UNA DECISIÓN QUE IMPACTA EL NEGOCIO

La segmentación no solo protege la tecnología: protege la continuidad, la reputación, la información confidencial y la confianza de clientes, colaboradores y socios estratégicos.

Reduce el riesgo de propagación de ataques.	Acelera la contención y respuesta ante incidentes.	Protege los activos más críticos del negocio.	Mejora la detección de comportamientos anómalos.	Facilita una administración más ordenada y eficiente.

CONCEPTO CLAVE

LA SEGMENTACIÓN NO EVITA NECESARIAMENTE EL ACCESO INICIAL. EVITA QUE UN ACCESO INICIAL SE CONVIERTA FÁCILMENTE EN CONTROL DE TODA LA INFRAESTRUCTURA.

A lo largo de este artículo exploraremos cómo una arquitectura segmentada contribuye a reducir el *blast radius*, mejora la detección, facilita la respuesta y fortalece la resiliencia operativa de cualquier organización.

> En ciberseguridad, no se trata de si van a intentar entrar, sino de **hasta dónde podrán llegar** si lo logran.

RED PLANA: UN RIESGO QUE MULTIPLICA EL DAÑO

Una red sin segmentación efectiva funciona como una gran autopista interna: todo está conectado con todo. Para la operación puede parecer cómodo, pero para un atacante es una oportunidad.

¿QUÉ OCURRE EN UNA RED PLANA?

Cuando un atacante obtiene acceso inicial en un endpoint, dispone de múltiples caminos para explorar, moverse lateralmente y escalar privilegios.

1. ACCESO INICIAL
2. RECONOCIMIENTO INTERNO
3. MOVIMIENTO LATERAL
4. ESCALAMIENTO DE PRIVILEGIOS
5. ACCESO A SISTEMAS CRÍTICOS

EL MOVIMIENTO LATERAL: EL VERDADERO OBJETIVO

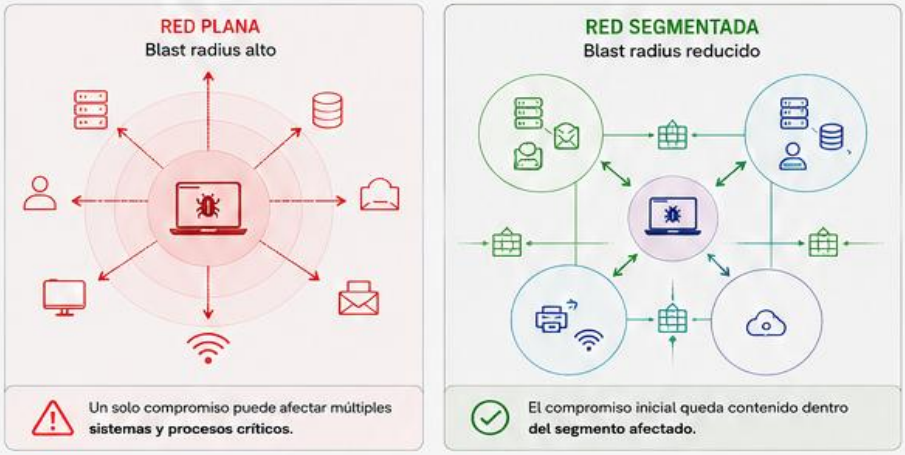
Después del compromiso inicial, el atacante busca expandir su acceso. En redes planas, puede aprovechar protocolos y servicios comúnmente expuestos:

SMB	RDP	SSH	LDAP	Kerberos	WinRM
Compartición de archivos	Escritorio remoto	Administración remota	Servicios de directorio	Autenticación y tickets	Gestión remota en Windows

Cada uno de estos caminos puede conducir a credenciales privilegiadas, servidores críticos, bases de datos, sistemas de respaldo o controladores de dominio.

BLAST RADIUS: CUANTO MÁS CONECTADO, MAYOR EL IMPACTO

El concepto **blast radius** representa el alcance potencial de un compromiso. Una red plana lo expande a toda la organización.



Un solo compromiso puede afectar múltiples **sistemas y procesos críticos.**

El compromiso inicial queda contenido dentro **del segmento afectado.**

CUANDO TODO ESTÁ CONECTADO, NADA ESTÁ REALMENTE PROTEGIDO

Las redes que crecieron sin una estrategia de segmentación suelen heredar reglas permisivas, excepciones temporales que nunca se eliminaron y servicios innecesarios expuestos.

- Más superficie de exposición.
- Mayores oportunidades para el atacante.
- Detección más difícil.
- Mayor tiempo de contención y recuperación.
- Impacto directo en la operación y en el negocio.

SIGNOS DE UNA RED POCO SEGMENTADA

- Equipos de usuarios pueden acceder a servidores administrativos.
- Dispositivos IoT comparten red con sistemas críticos.
- Reglas de firewall amplias y sin revisión periódica.
- Servicios heredados activos sin justificación.
- Múltiples excepciones que se volvieron permanentes.
- Falta de visibilidad del tráfico este-oeste (east-west).

IDEA CLAVE

La tecnología puede ayudar a detectar.
Pero la arquitectura limita.
Una red mal diseñada convierte un incidente de endpoint en un incidente organizacional.

SEGMENTAR NO ES SOLO CREAR VLAN

La segmentación efectiva requiere comprender los activos, sus funciones, dependencias y los flujos permitidos entre ellos. Sin control, la red segmentada sigue siendo vulnerable.

Muchas organizaciones creen que están seguras porque "tienen VLANs". Pero una VLAN por sí sola no protege si no existen políticas que gobiernen las comunicaciones entre segmentos. La verdadera segmentación no se trata de separar por subred, sino de controlar el acceso entre zonas con base en funciones, criticidad y necesidad operativa.

Segmentar es decidir qué puede hablar con qué, por qué, y bajo qué condiciones. Es diseñar límites de confianza, no solo límites de IP.

DE LA SEPARACIÓN LÓGICA AL CONTROL REAL

La segmentación moderna parte de entender cómo funciona tu organización. ¿Qué soporta cada sistema? ¿Qué lo hace crítico? ¿Qué pasaría si se ve comprometido? Desde ahí se construyen zonas con propósito.

Una segmentación efectiva suele incluir al menos: usuarios corporativos, servidores de aplicaciones, bases de datos, infraestructura de administración, dispositivos IoT, redes de invitados, entornos de copias de seguridad, servicios de identidad y zonas de producción y desarrollo.

Cada una de estas zonas debe estar aislada por defecto y permitir únicamente los flujos necesarios para su operación. Todo lo demás debe ser denegado.

EL TRÁFICO EAST-WEST TAMBIÉN IMPORTA

Tradicionalmente, la seguridad se ha centrado en el tráfico north-south: lo que entra o sale de la red. Pero hoy, el mayor riesgo está dentro: en el tráfico east-west, es decir, el que ocurre entre sistemas internos.

Una vez que un atacante compromete un equipo, su siguiente paso será moverse lateralmente para encontrar activos más valiosos. Si no hay controles ni visibilidad sobre ese movimiento, podrá escalar privilegios, acceder a datos críticos o persistir en la red sin ser detectado.

Por eso, es vital aplicar firewalls internos, ACLs entre zonas, microsegmentación cuando sea posible y monitoreo de comportamientos anómalos. La visibilidad del tráfico interno es clave para contener, detectar y responder a tiempo.

CUANDO UNA VLAN NO ES SUFICIENTE

Crear VLANs sin un modelo de comunicación no es segmentación, es ordenamiento. Si todas las VLANs pueden hablar entre sí, un atacante solo necesita comprometer una para tener acceso a todo lo demás.

La clave está en aplicar el principio de mínimo privilegio entre zonas. Solo se deben permitir las comunicaciones estrictamente necesarias para los procesos de negocio. Todo lo que no sea necesario, debe estar explícitamente bloqueado y monitoreado.

EJEMPLOS DE ZONAS TÍPICAS Y COMUNICACIONES CONTROLADAS

ZONA	COMUNICACIONES PERMITIDAS
USUARIOS CORPORATIVOS	A aplicaciones web internas, servicios de identidad y DNS.
SERVIDORES DE APLICACIONES	A bases de datos específicas, servicios internos, repositorios.
BASES DE DATOS	Solo desde aplicaciones autorizadas.
ADMINISTRACIÓN DE INFRAESTRUCTURA	A dispositivos de red, servidores y sistemas de monitoreo.
IOT / OT	Solo a servidores de gestión designados.
INVITADOS	Solo acceso a Internet, sin acceso a red interna.
BACKUPS	A repositorios de respaldo y administración.
IDENTIDAD	A controladores de dominio y servicios relacionados.

> "Segmentar no es dividir por comodidad. Es **controlar por criterio.**"

La segmentación real es dinámica: evoluciona junto con el negocio, se revisa periódicamente y responde a nuevos riesgos. No es un proyecto que se hace una vez, es una práctica continua de seguridad.

Empieza pequeño, enfócate en los activos críticos y aplica controles donde más impacto tengan. Segmentar bien no es solo proteger la red: es proteger el negocio.

Porque no se trata de tener más tecnologia. Se trata de tomar mejores decisiones. ■

> No confiamos por ubicación de red.
> Confiamos porque cada comunicación
> ha sido validada y es necesaria.

MICROSEGMENTACIÓN, ZERO TRUST E IDENTIDAD: EL SIGUIENTE NIVEL DE CONTROL

La evolución natural de la segmentación tradicional es la microsegmentación. Esta permite aplicar políticas de seguridad con un nivel de granularidad mucho más fino, controlando comunicaciones entre cargas de trabajo, aplicaciones o incluso procesos específicos dentro del mismo entorno lógico.

MICROSEGMENTACIÓN: SEGURIDAD DONDE REALMENTE IMPORTA

En entornos virtualizados, contenedores y cloud, la microsegmentación puede aplicarse mediante agentes, hipervisores, firewalls distribuidos o políticas definidas por software. Esto permite controlar qué puede comunicarse con qué, usando qué protocolo y bajo qué condiciones.

Ejemplo clásico de una aplicación de tres capas:

Capa Web	Capa de Aplicaciones	Base de Datos
Solo puede comunicarse con la capa de aplicaciones mediante HTTPS (443).	Solo puede comunicarse con la base de datos mediante el puerto específico del servicio.	No inicia conexiones hacia otros segmentos ni hacia estaciones de trabajo.

Cada capa está aislada y solo puede comunicarse según lo estrictamente necesario.
Si una capa es comprometida, el atacante no puede avanzar libremente hacia las demás.

ZERO TRUST: DE LA TEORÍA A LA ARQUITECTURA

El modelo Zero Trust parte de una premisa sencilla: ningún dispositivo, usuario o aplicación debe ser considerado confiable por estar dentro de la red.
Cada solicitud de acceso debe ser verificada antes de permitir la comunicación.

LOS PILARES DE ZERO TRUST APLICADOS A LA RED

VERIFICAR EXPLÍCITAMENTE	USAR EL MENOR PRIVILEGIO	ASUMIR BRECHA	INSPECCIONAR Y REGISTRAR	RESPONDER AUTOMÁTICAMENTE
Autenticar y autorizar cada solicitud de acceso.	Permitir únicamente lo necesario para cumplir la función.	Diseñar la red para que el atacante encuentre barreras en cada movimiento.	Visibilidad completa del tráfico este-oeste para detectar anomalías.	Aplicar controles dinámicos ante riesgos o comportamientos sospechosos.

Zero Trust convierte la red en un sistema dinámico de aplicación de políticas, no en un espacio donde todo está permitido por defecto.

IDENTIDAD Y CONTEXTO: LA NUEVA FRONTERA

La segmentación moderna se apoya cada vez más en la identidad. Ya no es suficiente saber desde dónde se conecta un dispositivo; ya necesario añadir quién desde dónde se conecta un dispositivo; es necesario saber quién es el usuario, cuál es el estado de seguridad del dispositivo, qué rol tiene y bajo qué contexto está intentando acceder.
Esto permite pasar de reglas basadas en direcciones IP a reglas basadas en identidad y propósito.

Ejemplo:

MODELO TRADICIONAL (BASADO EN IP)	MODELO MODERNO (BASADO EN IDENTIDAD Y CONTEXTO)
10.10.20.0/24 puede acceder a 10.10.30.0/24.	Solo usuarios del grupo "Administradores", desde dispositivos corporativos gestionados y con cumplimiento de seguridad, pueden acceder al servidor mediante SSH.

BENEFICIOS DE UN ENFOQUE DE MICROSEGMENTACIÓN Y ZERO TRUST

- **REDUCE EL MOVIMIENTO LATERAL**
  El atacante no encuentra caminos libres para desplazarse dentro de la infraestructura.
- **LIMITA EL IMPACTO DE UN COMPROMISO**
  Cada componente queda confinado a su entorno de operación.
- **MEJORA LA DETECCIÓN**
  Las comunicaciones fuera de lo esperado son más fáciles de identificar.
- **FORTALECE EL CUMPLIMIENTO**
  Las políticas de acceso se alinean con marcos como NIST, ISO/IEC 27001 y CIS Controls.
- **AUMENTA LA RESILIENCIA OPERATIVA**
  La organización mantiene continuidad incluso ante intentos de intrusión.

RETO TÉCNICO: VISIBILIDAD ANTES DE RESTRINGIR

Antes de aplicar controles estrictos, es indispensable entender cómo fluye realmente el tráfico. Herramientas como NetFlow, IPFIX, firewalls internos de observación, análisis de dependencias y soluciones NDR permiten construir un mapa claro de las comunicaciones necesarias.

Segmentar sin comprender puede generar interrupciones.

Segmentar con información genera seguridad sin afectar la operación.

CONTENER PARA RECUPERAR: EL VALOR REAL DURANTE UN INCIDENTE

Una arquitectura de red bien segmentada no solo previene la propagación de amenazas. También facilita una respuesta más rápida, precisa y controlada cuando un incidente ya está en marcha.

La diferencia entre un incidente controlado y una crisis organizacional muchas veces se define en los primeros minutos.

Una arquitectura segmentada le da a su equipo la capacidad de ganar tiempo cuando más importa.

DETECTAR, CONTENER, RECUPERAR: EL CICLO QUE DECIDE EL IMPACTO

Cuando ocurre una intrusión, el objetivo inmediato del equipo de seguridad debe ser evitar que el atacante se mueva lateralmente y comprometa más activos.
La segmentación permite actuar con precisión, sin necesidad de detener toda la operación.

DETECTAR

La visibilidad por segmentos ayuda a identificar comportamientos anómalos con mayor rapidez.

CONTENER

Los controles entre segmentos permiten aislar el origen del incidente y bloquear caminos de propagación.

RECUPERAR

La operación continúa en los segmentos no afectados mientras se normaliza el área intervenida.

AISLAMIENTO INTELIGENTE: PRECISIÓN QUE PROTEGE EL NEGOCIO

En una red segmentada, el aislamiento puede aplicarse a un segmento, a un host o a un conjunto especifico de comunicaciones, sin afectar servicios esenciales.
Esto permite mantener la continuidad operativa mientras se investiga y remedia el incidente.

- Aislar un segmento comprometido.
- Bloquear protocolos o servicios sospechosos.
- Aplicar listas temporales de control de acceso.
- Monitorear y validar antes de restablecer.

LOS RESPALDOS TAMBIÉN NECESITAN FRONTERAS

El ransomware y otras amenazas modernas buscan los respaldos antes que los servidores.
Si la infraestructura de backup no está segmentada, el atacante puede cifrar, eliminar o manipular las copias de recuperación.
Una arquitectura segura debe considerar los respaldos como un activo crítico.

BUENAS PRÁCTICAS PARA PROTEGER RESPALDOS

- Ubicar los repositorios de backup en segmentos dedicados.
- Limitar el acceso administrativo a personal autorizado y desde estaciones especificas.
- Deshabilitar protocolos y servicios innecesarios.
- Implementar inmutabilidad y retención de copias.
- Monitorear accesos y cambios en los entornos de respaldo.

PENSAR COMO ATACANTE, DISEÑAR COMO DEFENSOR

Si un atacante obtiene acceso inicial en su organización, ¿hasta dónde podrá llegar? Si la respuesta es "a casi cualquier sistema", es momento de rediseñar la arquitectura.

ARQUITECTURA QUE ACELERA LA RESPUESTA

Cuando la red está diseñada para contener, el equipo de seguridad puede concentrarse en investigar y remediar, en lugar de apagar incendios.
La contención rápida reduce el costo, el impacto reputacional y el tiempo de recuperación.

> "Una buena arquitectura de red no elimina incidentes. Reduce el daño que pueden causar. Esa es su verdadera fortaleza."

LA SUMA QUE GENERA RESILIENCIA

- **Prevención:** limita la superficie de exposición.
- **Detección:** mejora la visibilidad y el contexto.
- **Respuesta:** permite contener con precisión.

La combinación de estos tres pilares convierte la segmentación en una ventaja estratégica.

5 PRINCIPIOS PARA SEGMENTAR CON CRITERIO

Arquitectura antes que reacción

Una segmentación madura no se limita a separar redes. Define límites de confianza, reduce el movimiento lateral, contiene el impacto ante una intrusión y mejora la detección. No es solo una práctica técnica: es una decisión de arquitectura que determina cuán preparada está una organización para resistir y recuperarse.

La experiencia ha demostrado que los atacantes no siempre entran por la puerta principal, pero casi siempre intentan moverse. Allí es donde muchas redes fracasan: en permitir más de lo necesario entre sistemas que nunca debieron confiar entre sí. La segmentación con criterio corrige ese error de diseño.

A continuación, cinco principios técnicos que todo equipo de seguridad y redes debe adoptar para construir una segmentación que realmente proteja el negocio.

01. Segmentar según función y criticidad.
No todas las cargas ni los usuarios tienen el mismo valor para el negocio. Agrupar por función, sensibilidad y criticidad permite establecer zonas de confianza coherentes y reducir dependencias innecesarias.

02. Aplicar control entre segmentos.
La separación sin control es solo una ilusión de seguridad. Todo flujo entre zonas debe estar explícitamente permitido, documentado y justificado por una necesidad de negocio verificable.

03. Reducir protocolos administrativos.
Los protocolos y servicios administrativos son objetivos frecuentes. Limita su alcance, usa jump servers, credenciales dedicadas y registra cada acción. Menos exposición, menos superficie para el atacante.

04. Observar el tráfico este-oeste.
El mayor riesgo actual no viene del Internet, sino del interior. Visibilidad entre segmentos, análisis de comportamiento y alertas de anomalías son claves para detectar movimiento lateral en etapas tempranas.

05. Diseñar para contener.
Asume que algún día habrá un compromiso. La segmentación debe impedir que ese evento afecte a otras zonas críticas, proteger activos esenciales y facilitar una recuperación rápida y controlada.

CONCLUSIÓN: ARQUITECTURA QUE RESISTE, EQUIPOS QUE RESPONDEN.

La segmentación no es un fin en sí mismo; es una palanca estratégica para reducir el riesgo operativo y aumentar la capacidad de resiliencia. Una arquitectura bien pensada compra tiempo, reduce el radio de impacto, mejora la visibilidad, acelera la detección y permite una respuesta más precisa y con menos fricción.

En un mundo donde la intrusión es cuestión de cuándo, no de si, la pregunta correcta no es cómo evitar ser comprometidos, sino cómo limitaremos los daños cuando ocurra.

El verdadero valor de la segmentación está en diseñar la red pensando en el compromiso. Porque una red que limita el daño, protege el negocio.

ERRORES COMUNES

- ✕ **Permitir todo entre VLAN.**
  El exceso de permisos anula la segmentación. Crea caminos laterales invisibles para el atacante.
- ✕ **Mantener excepciones heredadas.**
  Reglas antiguas que nadie usa... pero todos olvidan. Son puertas abiertas al riesgo y la inconsistencia.
- ✕ **No aislar respaldos y sistemas de gestión.**
  Los respaldos contienen el valor más crítico. Sin aislamiento, el atacante puede alcanzarlo.
- ✕ **No documentar flujos ni dependencias.**
  Sin documentación, no hay control. Sin control, no hay seguridad ni capacidad de respuesta.
- ✕ **Depender solo del perímetro.**
  El perímetro ya fue superado. La defensa real empieza dentro, con arquitectura y límites claros.

CIERRE TÉCNICO

> La segmentación no evita necesariamente el acceso inicial. Evita que un acceso inicial se convierta fácilmente en control de toda la infraestructura.

EL EFECTO DE UNA BUENA SEGMENTACIÓN

PORQUE LA

CIBERSEGURIDAD TAMBIÉN SE PUEDE COMPRENDER JUGANDO.

Aprende, diviértete y fortalece tus habilidades para proteger lo que más importa.

ESTRATEGIA QUE EDUCA

RETOS QUE PREPARAN

DIVERSIÓN QUE DEJA HUELLA

CADA PARTIDA, UNA DECISIÓN QUE TE HACE MÁS FUERTE.

HAZLO TUYO AHORA

+506 8818 1680

Disponible ahora

SPOOK GAMES

JUEGOS QUE ENSEÑAN, EXPERIENCIAS QUE PERDURAN.

SECCIÓN

Desde la pantalla del Hacker

Una mirada al entorno digital desde la lógica del atacante, para entender mejor los riesgos, las señales y las decisiones que las organizaciones no pueden darse el lujo de ignorar.

DESDE LA PANTALLA DEL HACKER

Lo que el atacante ve antes que usted

Desde afuera, una organización revela mucho más de lo que cree: hábitos, exposición, prioridades y silencios operativos. Esa lectura inicial suele definir si un incidente será posible, costoso y difícil de contener.

Por un especialista en seguridad ofensiva con trayectoria en evaluación de entornos empresariales

> *El atacante rara vez entra por lo más complejo; entra por lo que nadie revisó a tiempo.*

Cuando observo una organización desde la lógica del atacante, no empiezo por imaginar un gran exploit. Empiezo por mirar lo evidente. La superficie pública, la huella digital, los servicios expuestos, la forma en que se comunican las personas, la velocidad con la que responden y la disciplina con la que administran accesos. Cada detalle cuenta, porque la mayoría de los incidentes no nacen de una genialidad técnica, sino de una suma de decisiones pequeñas que nadie corrigió a tiempo.

Un atacante experimentado no busca primero lo más complejo; busca lo más rentable. Si encuentra credenciales reutilizadas, privilegios excesivos, activos olvidados, terceros conectados sin suficiente control o colaboradores fatigados por mensajes urgentes, ya tiene una ruta de análisis. Lo que para la organización parece rutina, para el atacante es contexto. Y el contexto bien leído reduce incertidumbre, acelera la selección del objetivo y mejora la posibilidad de movimiento sin levantar sospechas.

Por eso, la pregunta estratégica no es solo si una empresa tiene controles. La pregunta correcta es qué señales proyecta hacia adentro y hacia afuera. Porque desde la pantalla del atacante, una organización no se ve como un organigrama ni como un presupuesto de tecnología. Se ve como un conjunto de oportunidades, fricciones, descuidos y tiempos de respuesta.

LA PRIMERA VENTAJA DEL ATACANTE ES LA VISIBILIDAD

La primera ventaja del atacante no siempre es técnica; suele ser informativa. Cuando una organización desconoce su propia exposición, delega esa comprensión al adversario. Activos públicos sin inventario claro, accesos remotos sobredimensionados, aplicaciones de negocio con configuraciones desactualizadas y huellas digitales mal gestionadas conforman una narrativa de riesgo. No hace falta vulnerar nada para empezar a entender dónde habrá menor resistencia.

En esa etapa, el atacante perfila madurez, anticipa probables debilidades y decide si vale la pena insistir. La ausencia de segmentación, el uso inconsistente de MFA o la falta de gobierno sobre cuentas privilegiadas rara vez aparecen como errores aislados; casi siempre son síntomas de una gobernanza incompleta.

DESDE LA PANTALLA DEL HACKER

La identidad vale más que el perímetro

Hoy el acceso es el activo preferido. Si una cuenta permite entrar sin demasiada fricción, el perímetro pierde protagonismo. Las credenciales expuestas, la reutilización de contraseñas, la proliferación de cuentas huérfanas y los privilegios permanentes ofrecen más valor que una puerta técnica muy ruidosa. Por eso, la madurez real empieza por saber quién accede, a qué, desde dónde y con qué justificación.

La gestión de identidad no debe limitarse a un directorio o a la aplicación aislada de MFA. Requiere mínimo privilegio, revisión periódica de permisos, control sobre cuentas administrativas y monitoreo del comportamiento de acceso. Cuando estos elementos faltan, el atacante no necesita improvisar; solo necesita paciencia.

"La cultura no reemplaza a los controles; evita que los controles se vacíen de sentido."

El factor humano se observa, no se improvisa

Desde la óptica ofensiva, la cultura también se ve. Se ve en correos respondidos con prisa, en aprobaciones sin validación, en procesos de excepción que se vuelven norma y en equipos que no distinguen entre urgencia y manipulación. No se trata de culpar a las personas. Se trata de reconocer que un colaborador sin contexto, saturado o presionado opera con menos margen para detectar señales.

Las organizaciones más resilientes no son las que memorizaron mensajes de concientización, sino las que diseñaron condiciones operativas seguras: canales claros para verificar solicitudes, liderazgo que no normaliza la urgencia permanente, reportes sin fricción y ejercicios que conectan seguridad con decisiones reales de negocio.

SEÑALES QUE UN ATACANTE INTERPRETA COMO OPORTUNIDAD

- exposición innecesaria
- privilegios excesivos
- segmentación débil
- terceros sin control
- baja capacidad de detección

DESDE LA PANTALLA DEL HACKER

01 | Los terceros amplían su superficie

En muchas organizaciones, el riesgo no termina en la infraestructura propia. Proveedores, integradores, plataformas SaaS y accesos de soporte amplían la superficie disponible. Desde la visión del atacante, un tercero con menos controles puede convertirse en la vía más eficiente para acercarse a procesos críticos o datos sensibles. Por eso, la relación con terceros debe gestionarse como una extensión del riesgo, no como un tema contractual aislado.

02 | La contención define el desenlace

Ninguna organización sería debería planificar desde la fantasía de invulnerabilidad. La diferencia entre un incidente costoso y uno contenible suele estar en la velocidad con la que se detecta, se decide y se aísla. Segmentación de red, telemetría útil, inventario actualizado, procedimientos de respuesta y autoridad clara para actuar son factores decisivos. Cuando eso existe, el atacante pierde tiempo, contexto y libertad de movimiento.

03 | Decidir antes de lamentar

Si algo he aprendido observando entornos empresariales es esto: la mayoría de las organizaciones no caen por falta absoluta de tecnología, sino por falta de priorización. La seguridad madura no nace de comprar más; nace de entender mejor qué debe verse, gobernarse y ensayarse. Desde la pantalla del atacante, las empresas más difíciles no son las más ruidosas, sino las que saben quiénes son, qué exponen y cómo reaccionan.

La lección para la alta dirección es clara: la ciberseguridad no puede tratarse como una conversación lateral. Es una disciplina de decisiones. Quien reduce visibilidad innecesaria, ordena accesos, exige gobernanza sobre terceros y prepara la contención, le quita ventaja al atacante antes de que el incidente empiece.

DECISIONES QUE REDUCEN LA VENTAJA DEL ATACANTE

- conocer activos y exposición real
- aplicar mínimo privilegio
- segmentar redes y accesos críticos
- gestionar terceros con criterio de riesgo
- ensayar respuesta y contención

> *La mejor defensa no es parecer inexpugnable; es dejarle claro al atacante que será visto, limitado y contenido.*

Qué es una ciberseguridad sana

Seguridad que impulsa, no que paraliza.

Una ciberseguridad sana no se nota en el día a día, pero se siente en los resultados.

Es la que da confianza para operar, reducir la fricción innecesaria y permitir que las personas trabajen mejor y más rápido.

Es la que habilita la innovación sin bajar la guardia, y que enfoca los recursos donde realmente importa.

No se trata de tener más controles, sino de tener los correctos. Ni de bloquear, sino de entender, priorizar y actuar.

Una ciberseguridad sana convierte el riesgo en información útil y la información en decisiones con impacto.

Así, la organización avanza con claridad, velocidad y confianza.

- **DA CONFIANZA:** reduce la incertidumbre y fortalece la toma de decisiones.
- **DISMINUYE FRICCIÓN:** simplifica lo que no aporta valor y elimina obstáculos innecesarios.
- **IMPULSA LA INNOVACIÓN:** protege lo importante para que nuevas ideas lleguen más lejos.
- **ENFOCA RECURSOS:** invierte en lo que importa, no en lo que suena urgente.
- **MEJORA DECISIONES:** más contexto, mejores decisiones, mejores resultados.

> La seguridad no es el freno del negocio. Es su habilitador más inteligente.

SECCIÓN

ÁNGULO LEGAL

ANÁLISIS LEGAL CON VISIÓN ESTRATÉGICA
PARA UN ENTORNO DIGITAL SEGURO
Y EN CUMPLIMIENTO.

DERECHO, TECNOLOGÍA
Y SEGURIDAD
DESDE UNA PERSPECTIVA
QUE PROTEGE Y GENERA VALOR.

DECIDE FIRST
A DIFFERENT WAY TO DECIDE

SECCIÓN

ÁNGULO LEGAL

ANÁLISIS LEGAL CON VISIÓN ESTRATÉGICA
EN CIBERSEGURIDAD Y DELITOS INFORMÁTICOS

Cuando el ataque termina, comienza el expediente:

las decisiones que convierten un incidente de ciberseguridad en evidencia judicial

Un incidente de ciberseguridad no concluye cuando se contiene el ataque. En ese momento comienza su verdadero desafío: transformar lo ocurrido en evidencia válida, lícita y útil para proteger a la organización, sostener investigaciones y responder ante tribunales.

La tecnología puede detectar, contener y registrar. Pero solo el derecho define qué vale como prueba y quién asume las consecuencias.

1. EL MARCO LEGAL QUE SOSTIENE LA DISCUSIÓN

Costa Rica cuenta con un andamiaje jurídico sólido para abordar los delitos informáticos, la protección de datos y la cooperación internacional.

- **Ley N.° 9048 – Ley de Delitos Informáticos (2012):** tipifica conductas como acceso indebido, interceptación de datos, fraude informático y daño informático, entre otros.
- **Código Penal:** contiene disposiciones relevantes como estafa (art. 216), suplantación (art. 274 bis), daño (art. 261) y sabotaje (art. 263).
- **Ley N.° 8968 – Protección de la Persona Frente al Tratamiento de sus Datos Personales (2011):** impone deberes de seguridad, confidencialidad y calidad en el tratamiento de datos (arts. 10 y 11).
- **Convenio sobre la Ciberdelincuencia (Convenio de Budapest, 2001):** Costa Rica es Parte desde 2018 [1], y en abril de 2026, ratificó el Segundo Protocolo Adicional [2], que fortalece la cooperación y facilita la obtención expedita de evidencia electrónica.

2. LA JURISPRUDENCIA QUE MARCA EL CAMINO

La Sala Tercera de la Corte Suprema de Justicia ha emitido criterios clave que delimitan cuándo la tecnología convierte una conducta en delito informático y cómo debe valorarse la prueba digital.

Resolución N.° 951-2024, Sala Tercera (18 de enero de 2024)

Unificó criterio y señaló que la utilización de una tarjeta de débito o crédito previamente sustráída para adquirir bienes o servicios puede constituir el delito de estafa informática (art. 217 bis del Código Penal). La tecnologia es el medio comisivo idóneo para inducir a error y obtener un provecho patrimonial.

Este precedente es relevante porque reconoce que el elemento tecnológico puede elevar una estafa común a estafa informática cuando la conducta se ejecuta mediante sistemas de información, reforzando la necesidad de investigar y documentar técnicamente cada paso del hecho.

3. EVIDENCIA DIGITAL: DEL INCIDENTE A LA SALA

No toda información que se obtiene en un incidente es prueba. Para que sea válida debe cumplir estándares legales y técnicos.

Legalidad de la prueba
El artículo 181 del Código Procesal Penal exige que la prueba sea lícita, pertinente y útil [3].

Cadena de custodia
Debe documentarse cada recolección, traslado, análisis y almacenamiento para garantizar integridad, identidad y no repudio. El Poder Judicial cuenta con un Protocolo de Cadena de Custodia [4] que establece buenas prácticas obligatorias.

Conservación y retención
Los registros (logs), correos, copias forenses e imágenes deben conservarse conforme a políticas internas y plazos razonables, evitando alteraciones o eliminaciones indebidas.

Privacidad y datos personales
El tratamiento de datos en la investigación debe respetar los principios de finalidad, proporcionalidad y necesidad de la Ley 8968 [5].

> “Un incidente técnicamente bien gestionado puede fracasar judicialmente si la evidencia se obtiene sin control, se altera o se pierde su trazabilidad.”

1. Ley N.° 84360, Aprobación del Convenio sobre la Ciberdelincuencia (Convenio de Budapest), 23 de noviembre de 2017; publicación en La Gaceta N.° 229 de 1 de diciembre de 2017.
2. Ley N.° 84362, Aprobación del Segundo Protocolo Adicional al Convenio de Budapest, 15 de abril de 2026.
3. Código Procesal Penal, Ley N.° 7594, art. 181.
4. Protocolo de Cadena de Custodia del Poder Judicial, aprobado mediante circular N.° 193-2017.
5. Ley N.° 8968, arts. 10 y 11.

4. DEL INCIDENTE AL EXPEDIENTE: LAS DECISIONES QUE MARCAN LA DIFERENCIA

Un incidente de ciberseguridad se convierte en un caso judicial cuando existe un hecho ilícito y una víctima que busca justicia. Sin embargo, entre ambos momentos media un proceso silencioso pero determinante: cómo la organización gestiona la evidencia.

La jurisprudencia costarricense ha sido clara: la tecnología es el medio, no el fin. Lo que sanciona el derecho es la conducta que, a través de ese medio, lesiona bienes jurídicos protegidos.

Por ello, actuar con rigor técnico y legal desde el primer minuto no solo ayuda a resolver el incidente, sino que define si será posible sostener una investigación y obtener un resultado en sede judicial.

5. RESPONSABILIDAD ORGANIZACIONAL Y CULTURA DE CUMPLIMIENTO

La ciberseguridad también es una cuestión de gobernanza. El artículo 10 de la Ley N.° 8968 obliga a quienes administran bases de datos personales a adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de la información y evitar su alteración, pérdida, tratamiento o acceso no autorizado.

El incumplimiento no solo genera riesgos operativos y reputacionales, también puede derivar en responsabilidad administrativa, civil e incluso penal cuando la omisión facilita un delito.

La cultura de cumplimiento no es un lujo ni un requisito formal: es la mejor defensa jurídica de una organización frente a un incidente.

EN RESUMEN

La ley no castiga la tecnología, sino el abuso de confianza, el engaño, la intrusión y el daño que esta pueda causar. La evidencia digital, bien gestionada, es la voz que dará credibilidad a la víctima y claridad al tribunal.

6. COOPERACIÓN INTERNACIONAL: UN ENFOQUE SIN FRONTERAS

Los delitos informáticos rara vez respetan fronteras. Por ello, Costa Rica es Parte del Convenio sobre Ciberdelincuencia (Convenio de Budapest) desde 2018 y, recientemente, ratificó el Segundo Protocolo Adicional el 15 de abril de 2026[1].

Este instrumento fortalece la cooperación internacional y facilita la obtención y divulgación expedita de evidencia electrónica entre Estados, acelerando investigaciones y mejorando la eficacia procesal.

Para las organizaciones, esto significa que una correcta preservación y documentación de la evidencia no solo sirve en el ámbito nacional, también puede ser clave para investigaciones que trascienden fronteras.

> No se trata solo de detener al atacante.
> Se trata de construir, desde hoy,
> un expediente que resista mañana.
>
> La evidencia que no se preserva,
> es justicia que se pierde.

1. Ley N.° 84362, Aprobación del Segundo Protocolo Adicional al Convenio sobre Ciberdelincuencia, 15 de abril de 2026.

7. BUENAS PRÁCTICAS LEGALES Y TÉCNICAS: LA MEJOR DEFENSA

La preparación antes del incidente determina la solidez legal después de él. Estas prácticas reducen riesgos y fortalecen la posición jurídica de la organización.

Políticas y procedimientos claros
Definir y documentar políticas de seguridad, respuesta a incidentes y conservación de evidencia digital.

Evaluación y gestión de riesgos
Identificar activos críticos, amenazas y vulnerabilidades. Documentar decisiones y medidas adoptadas.

Preservación inmediata de la evidencia
Aislar sistemas afectados, preservar bitácoras, respaldos y comunicaciones relevantes antes de realizar cambios.

Cadena de custodia rigurosa
Registrar cada recolección, traslado, análisis y almacenamiento de evidencia. Capacitar al personal involucrado.

Asesoría legal temprana
Involucrar al área legal desde el inicio permite tomar decisiones alineadas con el marco jurídico y evitar errores que comprometan la investigación.

Privacidad por diseño y por defecto
Aplicar el principio de minimización de datos y mantener documentadas las bases legales del tratamiento.

FOCO LEGAL

¿POR QUÉ IMPORTA HACERLO BIEN?

Un manejo inadecuado de la evidencia puede generar tres consecuencias graves:

- **Prueba inválida:** lo obtenido ilícitamente o sin trazabilidad puede ser excluido del proceso (art. 181 CPP).
- **Responsabilidad para la organización:** la omisión de medidas de seguridad o la exposición de datos personales puede derivar en sanciones administrativas y civiles.
- **Daño reputacional y pérdida de confianza:** la forma en que se gestiona el incidente impacta directamente la credibilidad ante clientes, reguladores y socios.

8. MIRADA HACIA ADELANTE: NUEVOS DESAFÍOS, MISMA EXIGENCIA LEGAL

La inteligencia artificial, el Internet de las Cosas y el trabajo remoto amplían la superficie de ataque y también los desafíos probatorios: cómo recolectar evidencia de sistemas distribuidos, cómo garantizar la integridad de los datos generados por algoritmos y cómo equilibrar la seguridad con la privacidad.

La respuesta no está en evitar la innovación, sino en gobernarla: evaluar el impacto legal de las nuevas tecnologías, documentar decisiones y mantener siempre el principio rector:

> “La tecnología cambia, pero las reglas del debido proceso, la protección de datos y la búsqueda de la verdad se mantienen.”

RECUERDE

La evidencia digital no es solo un conjunto de archivos.

Es la voz que hablará por su organización ante un juez.

Cada decisión que tome hoy puede fortalecer esa voz o hacerla incomprensible.

Prepárese, documente, preserve y actúe con legalidad.

Así, cuando el ataque termine, su expediente comenzará con ventaja.

REFERENCIAS NORMATIVAS Y JURISPRUDENCIALES

- Ley N.° 9048, Ley de Delitos Informáticos, del 25 de octubre de 2012.
- Código Penal de Costa Rica, Ley N.° 4573, del 4 de mayo de 1970 y sus reformas.
- Ley N.° 8968, Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, del 7 de julio de 2011.
- Convenio sobre la Ciberdelincuencia (Convenio de Budapest), aprobado por Ley N.° 84360, del 23 de noviembre de 2017; ratificado por Costa Rica el 20 de junio de 2018.
- Segundo Protocolo Adicional al Convenio sobre Ciberdelincuencia, aprobado por Ley N.° 84362, del 15 de abril de 2026.
- Código Procesal Penal, Ley N.° 7594, art. 181 (legalidad de la prueba).
- Protocolo de Cadena de Custodia del Poder Judicial, aprobado mediante circular N.° 193-2017.
- Resolución N.° 951-2024, Sala Tercera de la Corte Suprema de Justicia, de 18 de enero de 2024 (expediente 20-023214-0042-PE).

El riesgo humano también puede gestionarse estratégicamente.

Convierta la exposición humana en una decisión mejor informada.

SHCRM™

Strategic Human Cyber Risk Management

Solicite información en **oktaritech.com**

ÓKTARITECH

SECCIÓN

TRAS LA ÉGIDA

Mujeres que piensan, deciden y transforman la ciberseguridad.

INTELIGENCIA
para anticipar

ESTRATEGIA
para proteger

LIDERAZGO
para transformar

SECCIÓN

TRAS LA ÉGIDA

Mujeres que piensan, deciden
y transforman la ciberseguridad.

NO LLEGARON PARA OCUPAR UN ESPACIO

LLEGARON PARA CAMBIAR LA FORMA DE PROTEGERLO.

Durante demasiado tiempo, hablar de mujeres en ciberseguridad significó hablar de una ausencia.

Hoy, mientras la industria sigue midiendo representación, muchas mujeres ya están tomando decisiones que determinan cómo organizaciones, instituciones y sociedades enfrentan el riesgo digital.

DISEÑAN, INVESTIGAN, RESPONDEN, LIDERAN, ANALIZAN, CONSTRUYEN, ENSEÑAN Y DECIDEN.

Los números muestran una paradoja. El estudio de ISC2 publicado en 2025 situó en 22% la presencia promedio de mujeres en los equipos de ciberseguridad estudiados.

Sin embargo, entre las profesionales encuestadas, 55% ocupaba posiciones gerenciales o superiores, 7% estaba en C-Suite y 53% participaba en decisiones de contratación.

La representación continúa siendo minoritaria. La influencia, sin embargo, ya no puede considerarse marginal.

EL VERDADERO DÉFICIT

El Global Cybersecurity Outlook 2025 del World Economic Forum señala que dos de cada tres organizaciones reportan brechas de habilidades de moderadas a críticas y que apenas 14% afirma contar con las personas y capacidades que necesita. Mantener barreras que reduzcan el universo de talento disponible no es solo un problema de representación. Es una mala decisión de ciberseguridad.

> *"La ciberseguridad no necesita que las mujeres encuentren un lugar dentro de ella. Necesita reconocer el lugar que ya están construyendo.*

HALLAZGOS CLAVE DEL ESTUDIO DE ISC2 2025

22%
Presencia promedio de mujeres en los equipos de ciberseguridad.

55%
Ocupaba posiciones gerenciales o superiores.

7%
Estaba en posiciones C-Suite.

53%
Participaba como responsable en decisiones de contratación.

FUENTES: ISC2 Women in Cybersecurity Research 2025 | World Economic Forum, Global Cybersecurity Outlook 2025

DE PROTEGER SISTEMAS A INFLUIR EN DECISIONES

La ciberseguridad ya no se limita a la tecnología. Hoy, quien protege también interpreta el riesgo, explica, aconseja y participa en las decisiones que sostienen a las organizaciones.

El rol de las profesionales en ciberseguridad se ha expandido de manera significativa. Ya no se trata únicamente de operar herramientas o responder incidentes. Ahora participan en la estrategia, el gobierno corporativo, la innovación, el cumplimiento, la gestión del riesgo y la resiliencia organizacional.
Su impacto se extiende más allá del entorno técnico y alcanza aquello que realmente define el rumbo de una organización.

MÚLTIPLES CAMINOS, UN MISMO PROPÓSITO

No existe una única ruta para llegar a la ciberseguridad.
Las profesionales provienen de distintos campos del conocimiento y aportan miradas complementarias que fortalecen a los equipos.

TECNOLOGÍA	NEGOCIOS	DERECHO	CIENCIAS SOCIALES	INVESTIGACIÓN
INGENIERÍA, TI, DESARROLLO	RIESGO, FINANZAS, AUDITORÍA	COMPLIANCE, PRIVACIDAD, REGULACIÓN	INVESTIGACIÓN, COMUNICACIÓN, EDUCACIÓN	INTELIGENCIA, FORENSE, ANÁLISIS

NO SE TRATA DE IMITAR, SINO DE APORTAR

La diversidad no significa tener más mujeres en la foto.
Significa valorar perspectivas distintas, fomentar el pensamiento crítico y permitir que cada profesional aporte desde su experiencia y autenticidad.

Los datos de ISC2 2024 revelan que aún existen barreras culturales que impactan la experiencia profesional:

29%
de las mujeres percibió discriminación en el trabajo. (frente al 19% de los hombres)

36%
de las mujeres indicó no poder mostrar su autenticidad en su entorno laboral.

Abrir espacios es el primer paso. Crear entornos donde puedan crecer, decidir y liderar es lo que genera transformación.

FUENTES: ISC2 Women in Cybersecurity Research 2024 | World Economic Forum, Global Cybersecurity Outlook 2025

> *La técnica sigue siendo esencial. Lo que cambió fue el perímetro de influencia.*
>
> *Y ahí es donde su liderazgo marca la diferencia.*

UN NUEVO PERFIL PROFESIONAL

La profesional de ciberseguridad actual combina habilidades técnicas con capacidades estratégicas:

- Comprende el negocio y el contexto.
- Comunica riesgos con claridad.
- Piensa de forma estratégica.
- Colabora en equipos diversos.
- Toma decisiones con propósito.

La ciberseguridad del futuro necesita todas las miradas, todas las voces y todas las capacidades.

LIDERAZGO FEMENINO QUE PROTEGE EL MAÑANA

La ciberseguridad necesita más visión, diversidad y decisiones valientes.

Las mujeres están transformando la ciberseguridad desde el conocimiento, la empatía estratégica y la capacidad de anticipar riesgos antes de que se materialicen.

Hoy lideran equipos, diseñan estrategias, impulsan la innovación y construyen entornos digitales más seguros y resilientes. Su aporte no solo fortalece la industria: la hace más humana, ética y sostenible.

MUJERES QUE TRANSFORMAN

- Construyen estrategias de defensa anticipativa.
- Lideran la respuesta ante incidentes críticos.
- Impulsan la innovación y la resiliencia digital.
- Forman nuevas generaciones de talento.
- Abren el camino hacia una industria más diversa, segura y sostenible.

En un mundo donde los ataques evolucionan cada día, la verdadera fortaleza está en la inteligencia colectiva, en la diversidad de pensamiento y en la capacidad de decidir con criterio. Las mujeres en ciberseguridad no solo participan: lideran, innovan y marcan el rumbo.

Son agentes de cambio que hacen la diferencia.

> *"La verdadera madurez en ciberseguridad no se compra, se construye."*

SECCIÓN

Bajo la *luz* del criterio

Columna de opinión

Perspectivas invitadas que examinan, argumentan y orientan la decisión.

SECCIÓN

Bajo la luz del criterio · Columna de opinión

El peor dato no es el incorrecto: es el dato *incorrecto* que todos consideran confiable

Por ***Ing. Pablo López***

> *"El mayor riesgo no siempre está en los datos que se cuestionan, sino en aquellos que nadie se atreve a cuestionar"*

En gestión de datos solemos preocuparnos por el dato incorrecto.

El campo vacio. El registro duplicado. El código inválido.
La fecha mal digitada. El valor fuera de rango.
La inconsistencia evidente.

Esos errores importan. Pueden afectar reportes, procesos, integraciones, indicadores y decisiones.

Pero existe un problema mucho más peligroso:
el dato incorrecto que parece correcto.

Ese dato que aparece en un dashboard ejecutivo. Ese indicador que se presenta mes a mes sin discusión. Esa cifra que todos citan en reuniones. Ese reporte que tiene apariencia de oficialidad. Esa base de datos que nadie revisa porque "siempre se ha usado asi".

El peor dato no es necesariamente el incorrecto.

El peor dato es el *incorrecto* que todos consideran confiable.

Porque cuando un dato se percibe como confiable, deja de ser cuestionado. Se convierte en referencia. En argumento. En evidencia. En insumo para decisiones.

Y ahí comienza el verdadero riesgo.

> El peor dato es el *incorrecto* que todos consideran confiable.

Cuando el error se vuelve institucional

Un dato incorrecto aislado puede corregirse.

Pero un dato incorrecto que ha sido aceptado por la organización empieza a producir consecuencias más profundas.

Se incorpora en reportes. Alimenta indicadores. Justifica decisiones. Se reutiliza en presentaciones. Se comparte con otras áreas. Se integra a modelos analíticos. Se convierte en insumo para auditorías, proyecciones, presupuestos o planes estratégicos.

Con el tiempo, el dato deja de ser solamente un valor equivocado.
Se convierte en una verdad institucional aparente.

Ese es el punto más delicado: cuando la organización no solamente utiliza un dato incorrecto, sino que construye confianza alrededor de él.

Ya no se trata de corregir una celda.
Se trata de desmontar una creencia.

> La confianza *visual, jerárquica o histórica* puede reemplazar la confianza basada en controles.

La apariencia de confianza puede ser más peligrosa que el error evidente

Un error evidente genera sospecha.

Una cifra absurda, un campo vacío o una duplicidad visible suelen activar alertas. Alguien pregunta. Alguien revisa. Alguien duda.

Pero un dato que parece razonable puede pasar inadvertido durante años.

Si el indicador muestra una variación esperada, nadie lo cuestiona. Si la cifra coincide con la intuición de los líderes, se acepta. Si el *dashboard* tiene buen diseño, se percibe como profesional. Si el reporte viene de una fuente "oficial", se asume que fue validado.

La confianza visual, jerárquica o histórica puede reemplazar la confianza basada en controles.

Y cuando eso ocurre, la organización empieza a confundir presentación con veracidad.

Un dashboard no es confiable porque se vea bien. Un indicador no es confiable porque lo use la alta dirección. Un reporte no es confiable porque exista desde hace años. Una fuente no es confiable porque todos la consulten.

La confianza en los datos debe construirse sobre definiciones, calidad, linaje, responsables, controles y evidencia.

No sobre costumbre.

El dato incorrecto confiable produce decisiones equivocadas con seguridad

Una decisión tomada con datos evidentemente dudosos suele venir acompañada de cautela.

Pero una decisión tomada con datos supuestamente confiables se toma con seguridad.

Ese es el problema.

La organización puede aprobar inversiones, recortar recursos, modificar procesos, priorizar proyectos, lanzar campañas, ajustar presupuestos o evaluar desempeño con base en información que nadie cuestionó.

El dato incorrecto no solo informa mal.

También da confianza para actuar mal.

Y eso es mucho más grave.

La consecuencia no siempre aparece de inmediato. A veces se manifiesta meses después, cuando una decisión no produce los resultados esperados, cuando una auditoría encuentra inconsistencias o cuando otro equipo descubre que la fuente utilizada no representaba realmente lo que se creía.

Entonces surge la pregunta incómoda:

¿Cómo tomamos esta decisión con un dato equivocado?

La respuesta suele ser más incómoda todavía:

Porque todos confiábamos en él.

El problema no siempre es técnico

Cuando aparece un dato incorrecto, la primera reacción suele ser buscar una falla técnica.

Un proceso de carga. Una transformación. Una integración. Una consulta SQL. Un error en el sistema. Una fórmula mal aplicada.

A veces esa es la causa.

Pero muchas veces el problema es más profundo.

El dato puede ser incorrecto porque la definición nunca fue acordada. Porque el responsable nunca fue asignado. Porque la regla de negocio cambió y nadie actualizó el reporte. Porque la fuente dejó de ser oficial. Porque el indicador se heredó de un proyecto anterior. Porque nadie volvió a revisar la fórmula. Porque el dato se siguió usando por costumbre.

En estos casos, el problema no es solamente de tecnología.

Es de gobierno.

Y cuando el problema es de gobierno, no se resuelve únicamente corrigiendo el valor.

Se resuelve corrigiendo las condiciones que permitieron que ese valor incorrecto se volviera confiable.

La confianza sin trazabilidad es una ilusión

Una organización debería poder explicar por qué confía en un dato.

No basta con decir que el dato viene del sistema principal. Hay que demostrar qué significa, cómo se genera, qué controles tiene, quién lo aprueba, cuándo fue actualizado, qué transformaciones recibió y para qué usos está autorizado.

La confianza necesita trazabilidad.

Sin trazabilidad, la confianza es una percepción.

Y las percepciones pueden ser peligrosas cuando se convierten en base para decisiones críticas.

Un dato confiable debería poder responder preguntas básicas:

- ¿Cuál es su fuente oficial?
- ¿Qué definición utiliza?
- ¿Quién es responsable de aprobarlo?
- ¿Qué reglas de calidad se aplican?
- ¿Cuándo fue actualizado?
- ¿Qué transformaciones recibió?
- ¿Qué indicadores o reportes lo consumen?
- ¿Qué restricciones de uso tiene?

Si ninguna de estas preguntas puede responderse con claridad, entonces la organización no tiene un dato confiable.

Tiene un dato acostumbrado.

> “La confianza necesita *trazabilidad.*

La confianza heredada debe revisarse

Uno de los grandes desafíos en gobierno de datos es cuestionar datos que llevan años siendo utilizados.

No porque todo dato antiguo sea incorrecto, sino porque muchos datos sobreviven más tiempo que las condiciones que les dieron origen.

Un reporte pudo haber sido correcto hace cinco años, pero utilizar una lógica que ya no representa el proceso actual.

Un indicador pudo haber sido útil en un contexto específico, pero perder relevancia después de una reorganización.

Una fuente pudo haber sido oficial, pero ser reemplazada por otro sistema.

Una definición pudo haber sido aceptada, pero quedar desactualizada por cambios regulatorios, operativos o comerciales.

La confianza no debería ser permanente por defecto.

Debe renovarse.

Un dato crítico necesita revisión periódica, validación de vigencia y control de cambios. De lo contrario, la organización puede seguir confiando en información que ya no representa la realidad.

La inteligencia artificial puede amplificar el problema

Este riesgo se vuelve todavía más importante con inteligencia artificial.

Si una organización alimenta modelos, agentes o asistentes con datos incorrectos que todos consideran confiables, la IA no solo heredará el problema. Puede amplificarlo.

Puede generar respuestas convincentes basadas en información equivocada. Puede recomendar acciones sobre indicadores mal definidos. Puede automatizar decisiones sobre fuentes no validadas. Puede reutilizar documentos obsoletos con apariencia de autoridad.

La IA no siempre sabrá que un dato es incorrecto si la organización lo trata como confiable.

Por eso, antes de entregar datos a modelos de IA, las organizaciones deben preguntarse si esos datos realmente han sido gobernados o simplemente han sido aceptados por costumbre.

La IA no convierte confianza aparente en confianza real.

Solo la procesa más rápido.

El rol del gobierno de datos

El gobierno de datos debe proteger a la organización no solo de los datos incorrectos, sino también de la falsa confianza en los datos.

Esto implica establecer mecanismos para identificar, validar, certificar, monitorear y revisar los datos críticos.

No todos los datos requieren el mismo nivel de control. Pero aquellos que alimentan decisiones relevantes, reportes ejecutivos, cumplimiento regulatorio, inteligencia artificial, atención a clientes o procesos críticos deben tener un nivel de gobierno proporcional a su impacto.

El objetivo no es burocratizar el uso de la información.

El objetivo es evitar que una cifra mal entendida, mal calculada o mal gobernada termine orientando decisiones importantes.

La confianza en los datos no debe ser un acto de fe.

Debe ser una capacidad organizacional.

La cultura del dato también implica cuestionar

Muchas organizaciones hablan de cultura del dato como si significara usar más datos.

Pero una verdadera cultura del dato no consiste solamente en consultar dashboards o tomar decisiones basadas en indicadores.

También implica saber cuestionar.

Cuestionar una definición. Cuestionar una fuente. Cuestionar una fórmula. Cuestionar una variación inesperada. Cuestionar un indicador que nadie sabe explicar. Cuestionar una cifra que todos repiten sin conocer su origen.

No para bloquear decisiones, sino para protegerlas.

Una organización madura no castiga a quien pregunta de dónde salió un dato. Al contrario, entiende que esa pregunta es una señal de responsabilidad.

La confianza no se debilita cuando se cuestiona un dato.

Se fortalece cuando el dato puede responder.

Conclusión

El dato incorrecto es un problema.

Pero el dato incorrecto que todos consideran confiable es un riesgo mucho mayor.

Porque no solo informa mal. También convence. Se reutiliza. Se institucionaliza. Se transforma en decisiones, reportes, inversiones, estrategias y automatizaciones.

Una organización no debería preguntarse únicamente si tiene datos disponibles.

Debería preguntarse:

¿Qué datos consideramos confiables y por qué?

Si la respuesta es “porque siempre los hemos usado”, la confianza es frágil.

Si la respuesta se basa en definiciones, responsables, calidad, linaje, controles y evidencia, entonces la confianza empieza a ser real.

> “La confianza en los datos no debe ser *un acto de fe.*

PREGUNTAS PARA CEO, LEGAL, RRHH Y COMUNICACIÓN

La alineación entre áreas clave
es la base de una protección sólida.

CEO	• ¿Estamos invirtiendo lo necesario para proteger el negocio? • ¿Cómo la ciberseguridad impulsa el valor y mitiga el riesgo?
LEGAL	• ¿Hemos cumplido con las leyes y regulaciones aplicables? • ¿Cómo se gestionan las obligaciones y la notificación de incidentes?
RRHH	• ¿Nuestro equipo está capacitado y es consciente de los riesgos? • ¿Cómo protegemos la información de colaboradores y candidatos?
COMUNICACIÓN	• ¿Cómo comunicamos un incidente de forma clara y oportuna? • ¿Cuál es nuestro plan de comunicación interno y externo?

Las mejores respuestas se construyen en conjunto.

RADAR 506

Detectamos. Analizamos.
Compartimos lo que importa.

SECCIÓN

EL PULSO DE LA CIBERSEGURIDAD EN COSTA RICA

Radar 506 es el nuevo espacio de DECIDE FIRST dedicado a monitorear y analizar lo más relevante que ocurre en Costa Rica en materia de ciberseguridad.

Un punto de observación estratégico que conecta hechos, tendencias, decisiones y oportunidades para fortalecer la resiliencia digital del país.

6 señales que la dirección debe observar

01 | Fraude digital

Riesgo: Smishing, vishing y suplantación de identidad.

Señal: SUTEL aprobó medidas regulatorias para reducir el impacto de ciberataques mediante SMS y llamadas.

Por qué importa: El fraude ya exige respuestas desde la infraestructura de telecomunicaciones, no solo desde la concientización.

Qué observar: Controles anti-smishing, trazabilidad del tráfico fraudulento y nuevas obligaciones para operadores.

02 | Infraestructura pública

Riesgo: Exposición de servicios digitales gubernamentales.

Señal: El CSIRT-CR atendió un evento reportado por la Asamblea Legislativa en uno de sus servidores de servicios digitales.

Por qué importa: Cada incidente pone a prueba detección, escalamiento, continuidad y comunicación institucional.

Qué observar: Tiempo de detección, alcance, recuperación de servicios y coordinación con el CSIRT-CR.

03 | Gobernanza del riesgo

Riesgo: Políticas sin gestión integral del riesgo.

Señal: Un estudio nacional evidenció brechas en evaluación formal del riesgo y visibilidad presupuestaria.

Por qué importa: Tener controles no equivale a conocer, medir y priorizar el riesgo.

Qué observar: Métricas para dirección, responsables claros y presupuesto vinculado a la exposición real.

RADAR 506

Señales para decidir.
Costa Rica en observación.

SEÑALES QUE LA DIRECCIÓN DEBE OBSERVAR

04 | TALENTO Y CAPACIDAD

Riesgo	Déficit de especialistas frente a una superficie de ataque creciente.
Señal	El mismo estudio nacional identifica la escasez de personal calificado como una barrera para el 94,1 % de las instituciones participantes en materia de investigación y desarrollo en ciberseguridad. El financiamiento fue señalado por el 82,4 %.
Por qué importa	La adquisición de tecnologia no compensa indefinidamente la ausencia de capacidad humana para gobernarla, configurarla, supervisarla y responder ante incidentes.
Qué observar	Rotación de especialistas, dependencia de terceros, cobertura operativa del SOC, capacidades internas de respuesta y programas de desarrollo de talento.

05 | RESPONSABILIDAD FINANCIERA

Riesgo	Fraude electrónico convertido en riesgo jurídico y de gobierno corporativo.
Señal	En febrero de 2026 la Asamblea Legislativa aprobó en primer debate el expediente 23.908, relacionado con la protección de consumidores ante sustracciones fraudulentas de fondos. El texto coloca los estándares de ciberseguridad y su demostración como elementos relevantes frente a la eventual responsabilidad de las entidades financieras.
Por qué importa	La ciberseguridad comienza a adquirir una dimensión probatoria: no basta afirmar que existen controles; puede ser necesario demostrar su funcionamiento, trazabilidad y cumplimiento continuo.
Qué observar	Evolución legislativa, reglamentación posterior, criterios de SUGEF y exigencias sobre evidencias técnicas, auditoria y gestión de incidentes.

06 | CAPACIDAD NACIONAL DE RESPUESTA

Riesgo	Amenazas que evolucionan más rápido que las capacidades forenses tradicionales.
Señal	Durante 2026, Costa Rica inició formación técnica especializada vinculada con la implementación del primer Laboratorio de Ciberforense y gestión proactiva de amenazas del pais, con participación del MICITT, la DIS y el OIJ.
Por qué importa	El fortalecimiento de capacidades forenses mejora no solamente la investigación posterior a un ataque, sino también la posibilidad de generar inteligencia, preservar evidencia y comprender patrones adversarios.
Qué observar	Capacidad operativa efectiva del laboratorio, mecanismos para compartir inteligencia, coordinación público-privada y traducción de sus hallazgos en prevención.

LA SEÑAL DE FONDO

Costa Rica está pasando gradualmente de una conversación centrada en "proteger sistemas" hacia otra mucho más amplia: demostrar resiliencia, gestionar riesgo, responder con rapidez y asumir responsabilidad por las decisiones digitales.

DECIDE FIRST
MAGAZINE
A DIFFERENT WAY TO DECIDE.

TE INVITAMOS A SER PARTE

DE LO QUE INSPIRA DECISIONES

DECIDE FIRST Magazine es la publicación que conecta visión, estrategia y liderazgo con las decisiones que construyen organizaciones más seguras y resilientes.

Te invitamos a participar en nuestras próximas ediciones como protagonista, aliado o anunciante.

¿QUIÉNES PUEDEN PARTICIPAR?

01 EMPRESAS
Comparte tu visión, soluciones, casos de éxito o liderazgo en ciberseguridad.

02 PERSONAS
Ejecutivos, expertos y líderes que desean aportar su voz y conocimiento a nuestra audiencia.

03 PROYECTOS E INICIATIVAS
Dale visibilidad a tu proyecto, emprendimiento o iniciativa que genera impacto.

TAMBIÉN TE INVITAMOS A

SER PARTE DE NUESTRA PAUTA PUBLICITARIA

Conecta tu marca con una audiencia ejecutiva y profesional interesada en ciberseguridad, tecnología, innovación, gobernanza y toma de decisiones.

Espacios publicitarios disponibles en nuestras ediciones digitales.

JUNTOS IMPULSAMOS

DECISIONES QUE TRANSFORMAN.

Tu historia, tu visión y tu marca pueden inspirar a otros a decidir mejor.

CONTÁCTANOS →

Estamos listos para escucharte y brindarte toda la información sobre participación editorial y pauta publicitaria.

Gracias por acompañarnos en esta primera edición.

Cerrar una revista también es abrir una conversación. DECIDE FIRST nació con una convicción clara: en un entorno saturado de ruido, velocidad y opiniones, decidir bien sigue siendo una ventaja decisiva. Por eso, esta revista no busca solo informar. Busca ofrecer criterio, contexto y perspectiva para quienes entienden que las mejores decisiones se construyen con visión, análisis y sentido estratégico.

En estas páginas reunimos voces, ideas y miradas que no se conforman con lo evidente. Apostamos por un contenido editorial que conecta ciberseguridad, liderazgo, innovación, gobernanza y visión empresarial desde una posición clara: pensar mejor para decidir mejor. Ese es nuestro posicionamiento y también nuestra promesa.

Si esta edición dejó una pregunta valiosa, una reflexión o una nueva forma de observar, entonces la conversación apenas comienza. DECIDE FIRST quiere consolidarse como un espacio distintivo para líderes, profesionales y organizaciones que buscan profundidad antes que ruido, criterio antes que inercia y futuro antes que complacencia.

Lo que sigue también importa. Muy pronto llegará VOICES TO DECIDE, nuestro suplemento editorial: una extensión natural de esta visión, creada para amplificar voces, perspectivas y conversaciones que merecen continuidad.

Gracias por leernos, acompañarnos y por decidir diferente.

Nos reencontramos en la próxima edición.

“Decidir bien sigue siendo una ventaja estratégica”

DF

Equipo editorial
DECIDE FIRST
A Different Way to Decide.

PRÓXIMA PUBLICACIÓN

VOICES TO DECIDE

El suplemento editorial de DECIDE FIRST

Voces, criterio y visión para decidir mejor.

DECIDE FIRST MAGAZINE

UNA FORMA DIFERENTE DE DECIDIR.

DECIDE FIRST
DF
MAGAZINE
A DIFFERENT WAY TO DECIDE.

Donde la visión, el análisis y la perspectiva se unen para inspirar mejores decisiones.

Una plataforma editorial global para líderes, tomadores de decisión y mentes visionarias.