

27001, una de las metas
del canal para el 2025.

Pág 19



Partners 2025



Pág 22

¡Lo último!

**Llega un nuevo gigante
de Ciberseguridad
a Domotes.**

Pág 15

Hefesto: La Herramienta Estratégica
que Potencia tu Negocio.

Pág 6

islonline

**Usa ISL Online como tu
herramienta de soporte y
acceso remoto.**

Pág 12

Artículo

**¿Conoces el Verdadero
Valor de tu Empresa?**

ÍNDICE

- 
- 4** Tendencias de ciberseguridad para el 2025
 - 6** Usa ISL Online como tu herramienta de soporte y acceso remoto
 - 7** **ISL Online:** Soporte, Acceso y Teletrabajo
 - 8** **Backup todo en 1:** Ofrece la mejor experiencia en backup
 - 9** **Sophos:** Los ciberdelincuentes se conectan cuando nos desconectamos
 - 10** **4 errores** más frecuentes en los comerciales este 2024
 - 11** **Nakivo Nueva Versión:** Nakivo Backup & Replication v.11
 - 12** ¿Conoces el verdadero valor de tu Empresa?
 - 14** **Nakivo:** Solución #1 de backup Virtual, Física, Cloud, NAS y SaaS
 - 15** **Hefesto:** Auditoría de Firewall y Gestión de Amenazas
 - 16** El impacto del ransomware en aumento
 - 18** Ahora Domotes ofrece servicio técnico a otras marcas
 - 19** 27001, una de las metas del canal para el 2025
 - 21** **Comprometidos con el cambio:** Domotes y el Poder de la Innovación Social
 - 22** Un gigante de tecnología de seguridad informática ahora hace parte del portafolio de Domotes
 - 23** SonicWall ZTNA y CASB
 - 24** **Más allá de los parches:** Vicarius, la vanguardia en la gestión de vulnerabilidades
 - 26** **BDRSuite #1:** Software de Backup Rentable
 - 28** **Bonus:** Obtén descuentos y promociones por tus compras
 - 29** Eventos destacados del año en Domotes
 - 30** Una alianza estratégica para el éxito
 - 31** Impulsa tus ventas con nuestro pack exclusivo para partners de tecnología



Domotes llega a Centroamérica

► Fortaleciendo aún más nuestra **presencia**.

Juntos, como parte de su equipo, nos dirigimos hacia un **2025** lleno de oportunidades y crecimiento en la región.



Tendencias de ciberseguridad para el 2025

Es unánime, todos los vendedores de seguridad coinciden en que la IA generativa es uno de los grandes retos a afrontar el próximo año.

Si bien la IA ha ayudado mucho a las organizaciones a aumentar sus niveles de seguridad, el panorama digital se vuelve más complejo, ya que los ciberdelincuentes están aprovechando las herramientas de IA para diseñar ataques más sofisticados.



Según Google, estas son las principales amenazas a tener en cuenta.

Phishing e ingeniería social:

Los ciberdelincuentes utilizan IA para crear mensajes de phishing, vishing y SMS que parezcan más auténticos, lo que dificulta que los usuarios los detecten.

Deepfakes para fraude de identidad:

El aumento en el uso de deepfakes permite a los atacantes eludir los protocolos **Conozca a su cliente** (KYC) para el robo de identidad y el fraude.

IA en la investigación de

vulnerabilidades: Los actores de amenazas están utilizando IA en la identificación y el reconocimiento de vulnerabilidades para explotar las debilidades de manera más efectiva.

Demanda clandestina de IA sin

restricciones: Los actores maliciosos en foros clandestinos buscan cada vez más herramientas de IA sin restricciones para fines ilícitos.



Así que para el 2025 seguiremos viendo avances en el desarrollo y uso de tecnologías de inteligencia artificial en la cadena del ataque.

Aumento en el uso de servicios SOC y MDR por parte de las organizaciones. Esta es una oportunidad que el canal debe saber aprovechar. Las empresas necesitan brindar monitoreo continuo y respuesta ante incidentes para mejorar su postura de seguridad y la falta de personal capacitado en seguridad informática y el alto costo que implica para las organizaciones contar con el recurso humano adecuado, obliga a las empresas a contar con estos servicios. No cabe duda de que la capacidad de automatización y la orquestación SOAR jugarán un papel importante en la gestión eficaz de incidentes, necesarias en las complejas demandas de la seguridad en la nube en particular a medida que las compañías migran sus servicios críticos a estas plataformas.

Confianza Cero: La seguridad del perímetro cada vez más obsoleta.

Según Forbes, se prevé que el mercado de confianza cero se triplique de \$31,45 mil millones a \$95,22 mil millones para 2030. Los principios de confianza cero brindan a las organizaciones una visión más granular de la actividad de la red y el comportamiento de los usuarios. El enfoque de cero confianzas autentica continuamente a todos los usuarios, dispositivos y tráfico de red, lo que



protege contra amenazas internas y movimientos laterales de cibercriminales.

La microsegmentación es otro aspecto clave de la arquitectura Zero Trust. Al dividir la red en segmentos más pequeños, las organizaciones pueden limitar el impacto potencial de una vulneración. Cada segmento opera de forma independiente, lo que garantiza que una vulneración en un área no afecte a toda la red.

En 2025, las OT serán cada vez más relevantes en el ámbito de ciberseguridad por varias razones, entre las que se destaca la ya mencionada conectividad entre dispositivos OT y la gran cantidad de datos que recopilan. También, muchos de estos sistemas son fundamentales para el funcionamiento de infraestructuras críticas, con lo cual es atractivo para los criminales un ataque a esta tecnología, dado que tiene el potencial de causar grandes estragos.

Los OT son sistemas informáticos y dispositivos utilizados para controlar procesos industriales y físicos en diversos sectores, como la energía, manufactura, agua y gas, entre otros.

Estos sistemas gestionan equipos como PLC (Controladores Lógicos Programables), SCADA (Sistemas de Control Supervisorio y Adquisición de Datos) siendo su función principal la automatización de procesos.

Aumento en el gasto de tecnología

A pesar de esta cautela, el optimismo persiste: según una encuesta de Forrester, el 91% de los responsables de la toma de decisiones tecnológicas a nivel mundial planean aumentar el gasto en TI, y más de la mitad espera que el crecimiento supere el 5%, superando la inflación. Forrester pronostica que la economía digital crecerá a una tasa anual compuesta del 6,9% entre 2023 y 2028.

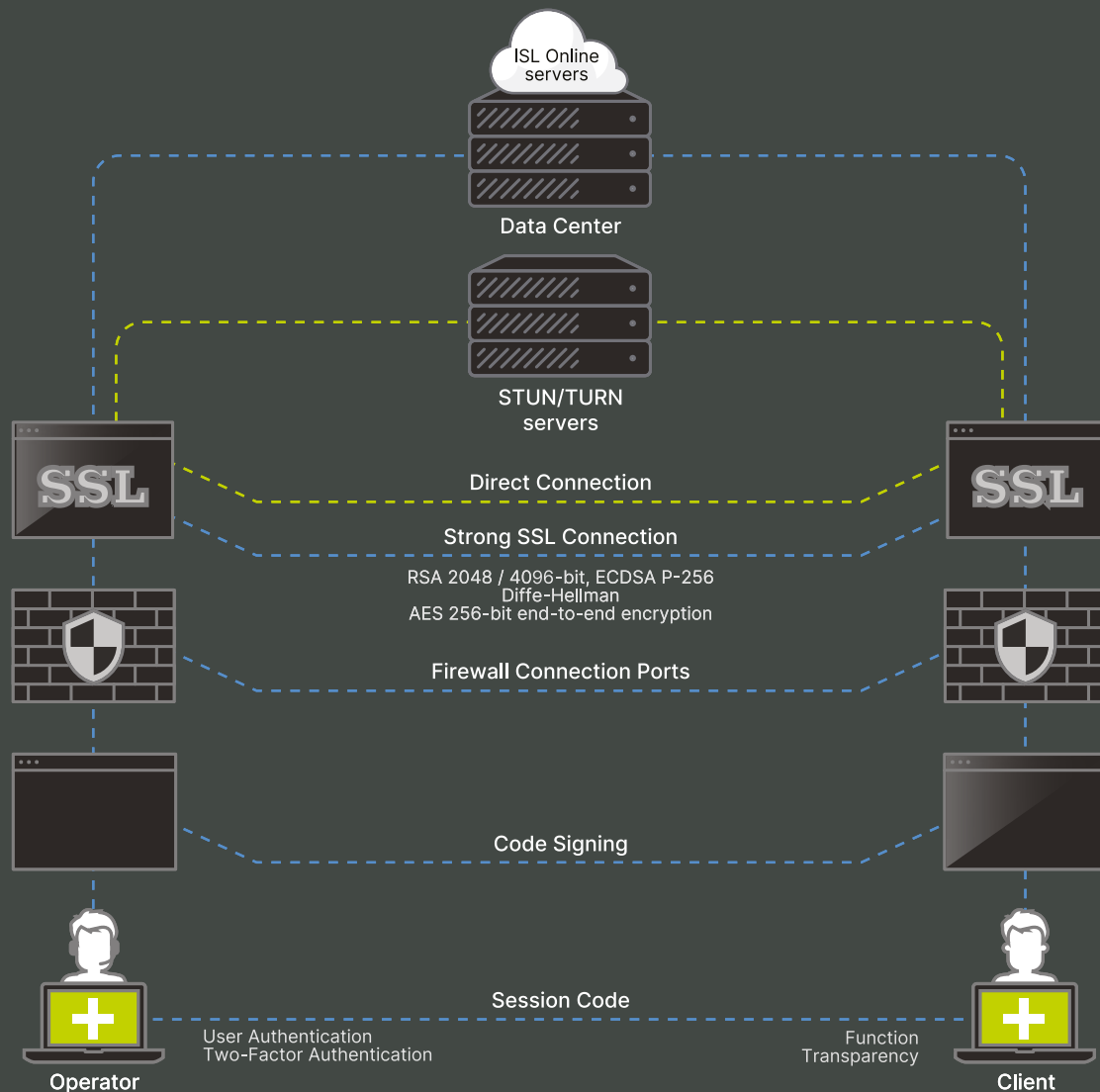
Sería bueno que el canal profundice en estas tendencias y verifique si su empresa se alinea con las necesidades digitales de sus clientes y así podrá hacer cambios en sus modelos comerciales y establecer estrategias para desarrollar en este y los años que vienen.



Luis Burgos
Director Comercial Domotes

Casi nadie presta atención a la seguridad en el acceso remoto. Y eso es muy poco inteligente.

ISL Online utiliza encriptación avanzada y métodos de intercambio de claves para garantizar sesiones de escritorio remoto seguras y robustas.



Usa ISL Online como tu herramienta de soporte y acceso remoto, y ofrece a tus clientes una experiencia de soporte excepcional.

Accede a una prueba gratuita escaneando este código QR.
Contáctanos para obtener 3 meses de licenciamiento NFR



islonline

REMOTO

Soporte. Acceso. Teletrabajo



Salva la vida de tu negocio sin
mojarte ni despeinarte



www.islonline.com

*Ofrece la mejor experiencia en
Backup de información para
diferentes ambientes*



NAKIVO®

asustor
ASUSTOR Inc.

 **SEAGATE**



Backup todo en 1

Porque cada cliente es diferente te asesoramos,
ofreciendo siempre lo mejor a precios competitivos



Los ciberdelincuentes se conectan cuando nos desconectamos.

El 90% de los ciberataques se producen fuera del horario laboral. Proteja su compañía 24/7 con el servicio gestionado de detección y respuesta ante amenazas.



**Sophos Managed
Detection and Response**

SOPHOS MDR le ayuda a mejorar la posición de ciberseguridad de su compañía integrándose también con herramientas de ciberseguridad de terceros.

Más información en: es.sophos.com/mdr

[] Datos obtenidos por el Informe Active Adversary 2023 para líderes tecnológicos de Sophos X-Ops*

4

Errores más frecuentes en los comerciales este 2024

Este 2024 vino lleno de muchos retos a nivel país, a nivel economía mundial, elección del nuevo presidente en EE. UU. y demás cambios que no se pueden controlar y que causan un impacto en nuestra labor.

A pesar de que no se pueden controlar, hay situaciones que sabemos que van a pasar y que la mejor manera de mitigar el impacto negativo es preparándonos con anticipación.

Los impactos que más se dieron este 2024 en general, según nuestro estudio y labor diaria con clientes, fueron:

- 1 Pérdida de vista de sus renovaciones:** los canales llevan sus renovaciones por monto, esto es lógico; lo que no es lógico es que dejan de hacer gestión en los que los montos son bajos, sin detallar realmente el % de participación de los negocios con montos pequeños. Esto, a su vez, es dejar a elección solo por precio al cliente final.
- 2 Actualización de conocimiento:** El cliente final llega a notar qué tanto conocimiento o manejo técnicos tiene el asesor que lo atiende; es poco o ninguno, por lo cual decide cambiar de proveedor o incluso de solución.
- 3 Seguimiento a los negocios:** Puntualmente en los negocios nuevos se evidencia un abandono de cuenta por dos motivos:
 1. No es significativo el monto del negocio.
 2. Falta de organización.
- 4 Ser vendedores y NO asesores:** Un “comercial” que no se capacita, que es tomador de pedido, que no hace feeling, que no entrega sus respuestas a tiempo y con las necesidades aclaradas NO se puede llamar COMERCIAL y mucho menos ASESOR ESTRATÉGICO. Solo es un vendedor esporádico.

Te doy mis consejos para que no estés en este grupo de vendedores y comiences a ser llamado un: **Asesor Estratégico**

Lo inicial es enfocarte en la necesidad del cliente, para esto debes estudiar a tu cliente, saber por lo menos cuál es el Core de negocio de tu cliente, mostrar interés en que quieres AYUDARLO y no solamente venderle un producto.

Debes de conocer mejor que cualquier persona lo que está ofreciendo como servicio o producto, conocer sus beneficios y sobre todo conocer sus carencias, PERO OJO, no dejes de lado a tus competidores; debes conocer a tu competencia y tener con claridad sus beneficios y sus carencias. Esto te ayudará a saber dar una respuesta ante alguna comparación u objeción que te presenten.

Ten en cuenta que TODOS tus clientes son igual de importantes para ti; no interesa el monto del negocio o el tamaño del cliente, ellos deben sentir que para ti son importantes. La empatía es una virtud que debes desarrollar.

La **organización** es la **clave**; llevar tu **CRM** al día es **obligatorio** si quieres ser una **gran asesor estratégico**.

Estudia el mercado, nacional e internacional, ten presente los acontecimientos, así como le dedicas 30 minutos al TikTok o Instagram para ver cosas de risa, dedícalo en estas mismas plataformas para ver personas que mantienen las últimas tendencias, acontecimientos. No interesa si va o no de la mano tu producto; recuerda que haces negocios con personas y nunca sabes qué conversación puede llevarte a crear feeling.



Los 30 minutos de risa NO los dejes; esos deben estar. Te puedo asegurar que si aplicas estos consejos, puedes tener mucho más tiempo de risas.



Ing. Edison Jesús Pérez Ríos.



Nakivo Nueva Versión:

Nakivo Backup & Replication v.11



Nos complace anunciar el lanzamiento de **NAKIVO Backup & Replication v11**, una solución innovadora diseñada para optimizar la gestión y protección de datos en entornos virtuales. Esta versión, que ya está disponible tras una exitosa fase de pruebas beta, ofrece una serie de mejoras y nuevas funcionalidades que no solo fortalecen la seguridad de los datos, sino que también amplían las oportunidades para enriquecer su portafolio de servicios.

Principales Novedades

Backups Sin Agente para Proxmox VE:

Permite realizar copias de seguridad de máquinas virtuales directamente a nivel de host, eliminando la necesidad de instalar agentes y optimizando el uso de recursos.

Mejoras en Backup de Microsoft 365 y NAS:

Se han integrado nuevos destinos de almacenamiento, incluyendo plataformas en la nube, y se ha mejorado la protección contra ransomware, facilitando la implementación de estrategias de backup 3-2-1-1.

Cifrado de Backups en Origen:

Aumenta la seguridad de los datos cifrando la información antes de su transferencia, cumpliendo con las normativas de protección de datos.

Repositorio Federado:

Ofrece una solución escalable para la gestión de backups en grandes entornos, garantizando la continuidad operativa incluso ante fallos de almacenamiento.

Panel de Control para MSP:

Proporciona una visión centralizada de múltiples inquilinos, mejorando la eficiencia en la gestión y supervisión de las actividades de protección de datos.

Interfaz en Español:

Facilita el uso de la solución a los usuarios hispanohablantes, mejorando la accesibilidad y la experiencia del cliente.

Replicación en tiempo real (Beta) para VMware:

Compatibilidad con vSphere 8.0
Mejore sus capacidades de recuperación ante desastres y proteja las cargas de trabajo de VMware que se ejecutan en vSphere 8 contra desastres imprevistos o ataques de ransomware.



Con estas innovaciones, **NAKIVO Backup & Replication v11** no solo refuerza la protección de datos, sino que también brinda a nuestros partners una oportunidad única para diversificar y potenciar su oferta de servicios de seguridad. *Les invitamos a descargar la versión de prueba gratuita para explorar todas las capacidades de esta solución avanzada.*

Aprovechen esta oportunidad para fortalecer su portafolio y ofrecer a sus clientes una protección de datos robusta y confiable.



▶ **Escanea el código QR** y habla con un experto.



¿Conoces el verdadero valor de tu **Empresa**?

Con bastante frecuencia las familias empresariales en **América Latina** nos preguntan: *¿Por qué debería preocuparme por conocer el valor de mi empresa?*

La respuesta está radicada en la visión de largo plazo de cualquier empresa en funcionamiento.

Además de considerar la generación de ingresos, rentabilidad y liquidez, es fundamental comprender cómo cada decisión influye positivamente en la generación y maximización de valor.

Contar con esta comprensión permite tomar decisiones informadas con el objetivo claro de maximizar el valor en beneficio de los propietarios. Realizar una valoración financiera de forma periódica, permite conocer el valor de mercado del negocio y comprender los factores que lo impulsan. Brinda la oportunidad de diseñar una estrategia centrada en la maximización de valor para los accionistas y cada decisión es en un motor de crecimiento en la ruta hacia la prosperidad sostenible de los dueños.

A continuación, se desarrollan algunas de las razones que respaldan la importancia de llevar a cabo una valoración financiera periódica.

1 Impulsa significativamente el desempeño financiero de la Empresa.

La búsqueda exclusiva de rentabilidad y generación de caja es una trampa que limita el verdadero potencial de maximización de valor en cualquier compañía.

Complementar el análisis financiero tradicional con un ejercicio de valoración financiera incorpora dentro de los resultados el objetivo fundamental de las empresas, que es la maximización de valor para los accionistas.

Está comprobado que realizar un ejercicio de valoración financiera recurrente permite comprender las necesidades de inversión para apalancar el crecimiento de los ingresos; determinar el nivel preciso de endeudamiento externo requerido para apalancar las inversiones requeridas que garantice la optimización del costo de capital que tiene un impacto directo en la generación de valor.

También, evita sanciones de cumplimiento de las Normas Internacionales de Información Financiera – NIIF. La determinación del valor razonable de ciertos activos y pasivos está respaldada por una

valoración que avala las cifras registradas en los Estados Financieros.

2 Cuando se busca financiación de bancos o inversionistas.

Financiar la empresa con nuevos socios o deuda tradicional es una estrategia sólida para la expansión.

Cuando se considera la opción de inyectar capital fresco o traer inversionistas a la empresa, es fundamental tener claro el valor de la empresa y contar con una valoración sólida antes de iniciar las conversaciones. Los potenciales socios necesitan comprender cómo su inversión impulsará el crecimiento y cómo obtendrán la rentabilidad ofrecida.

Al mostrar cómo sus fondos llevarán la empresa al siguiente nivel, aumentarán su valor y generarán retorno, aumentará el interés de los inversionistas. De otro lado, si el financiamiento elegido para impulsar los planes de crecimiento es financiamiento bancario tradicional, se debe considerar que las instituciones financieras o fondos de deuda privado exigen la valoración financiera para resolver dos preguntas fundamentales: 1) cómo pagarán el préstamo y 2) cuál es la garantía.

3 Venta de la Compañía

El ciclo de vida empresarial incluye también la venta de la empresa en el momento oportuno.

Decidir vender una empresa es una elección crucial para los propietarios, impulsada por diversas razones como falta de herederos, divergencia de intereses, desafíos internos entre socios, entre otras. Anticiparse a este proceso y planificar estratégicamente

la venta es esencial para evitar impactos negativos en el negocio.

En ocasiones y de manera equivocada, los propietarios basan sus estimaciones de valor en datos históricos, estadísticas o percepciones personales, lo cual resulta extremadamente costoso. Para llegar a un rango de valor de mercado de una empresa en marcha, se debe hacer un ejercicio basado en tres enfoques internacionalmente reconocidos:

1 Enfoque de mercado

2 Enfoque de ingresos

3 Enfoque de activos, cada uno con diferentes metodologías

Conclusión

Una valoración financiera es una radiografía que puede convertirse en una brújula en un océano de datos, que, además de ser un espejo reflexivo, es también un faro que ilumina el camino hacia una mayor eficiencia, entregando información certera para establecer objetivos realistas, adoptar decisiones informadas y **¡crear un plan estratégico que maximice la generación de valor para los propietarios!**

¡Esperamos trabajar con ustedes próximamente y apoyarlos a navegar del éxito empresarial al propósito superior de vida!



César Gutiérrez
Managing Director

+57 315 264 0703
cgutierrez@bastioncapital.co

NAKIVO®

#1 Solución de backup

Virtual, Física, Cloud, NAS y SaaS



Rápido

Backup hasta 2 veces más rápido



Asequible

Hasta un 49% menos de TCO



Mejor valorado

Solución altamente calificada





Menu

HEFESTO

SoporteDigital Tech

Audit Firewall: fw-domotes-pro

Dash-Rules

Rules

NAT-rules

SSL-Inspection

Compare-Audit

Compliance-Trend

Certificates

Ips-Settings

System-Services

Wireless-Protection

VPN Settings

Name	keyexchange	AllowReKeying	AuthenticationMode	KeyingMethod
Branch office (IKEv2)	ikev2		MainMode	Automatic
Central_DefaultBranchOffice	ikev2		MainMode	Automatic
Central_DefaultHeadOffice	ikev2		MainMode	Automatic
Clone_Microsoft Azure	ikev2		MainMode	Automatic
Default Profile	ikev1		MainMode	Automatic
DefaultBranchOffice	ikev1		MainMode	Automatic
DefaultHeadOffice	ikev1		MainMode	Automatic

Admin Settings

Certificate: ApplianceCertificate 100%

Threat Protection Status: 3333

Authentication

Connection Security: Simple 0%

Valid Cert Required: Disable

Email Protection - Anti Spam Rules

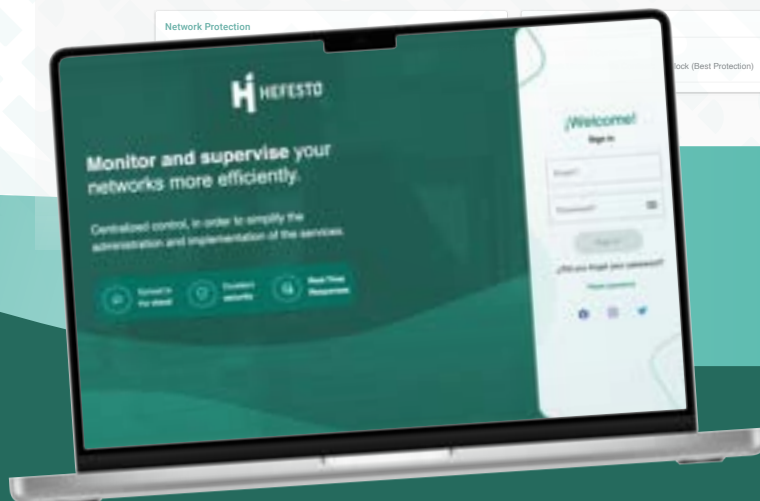
Name: Rule4 POP / IMAP: Prefix Subject Recipient List: Contains SMTP: Reject Sender Email List: Contains	Name: Rule3 POP / IMAP: Prefix Subject Recipient List: Contains SMTP: Prefix Subject Sender Email List: Contains
Name: Rule2 POP / IMAP: Prefix Subject Recipient List: Contains SMTP: Prefix Subject Sender Email List: Contains	Name: Rule1 POP / IMAP: Prefix Subject Recipient List: Contains SMTP: Drop Sender Email List: Contains

Firewall Rules

WAN_TO_ANY	82%
GUESTDDOM	83%
WITHAUTH-LAN-VPN	78%
CLONE_LAN-VPN	78%
LAN-VPN	78%
RICARDOTEST_TO_INTERNET	74%
PRUEBAS_IP-LIBRE	78%

Network Protection

Block (Best Protection)	Deny Unknown Protocol:	SecurityAppliance_SSL_CA	Pharming Protection:
	Https Scanning:		Pua Detection:



Auditoría de Firewall y Gestión de Amenazas, Ahora Nueva Función.



Creación de Archivos STIX para Detecciones Críticas



Informes Más Inteligentes y Accesibles



Velocidad y Rendimiento Mejorados



Interfaz Rediseñada (UX/UI)

Más que una **Herramienta**, tu **Socio Estratégico**

Con **Hefesto.io**, auditar firewalls y gestionar amenazas no solo es más fácil, sino también más estratégico. Maximiza tu protección, mantén el control y prepárate para el futuro de la ciberseguridad.

Conoce más en nuestro nuevo sitio web **www.hefesto.io** y comienza a transformar la seguridad de tu organización hoy mismo.



El impacto del ransomware en aumento



El ransomware continúa siendo una de las amenazas más críticas en el ámbito de la ciberseguridad. Según nuestra reciente encuesta sobre el estado del ransomware en 2024, el 59 % de las organizaciones han sido víctimas de ataques en el último año. Aunque la tasa general de ataques ha disminuido respecto al 66 % de 2023, el impacto en las víctimas ha empeorado, con un costo promedio de recuperación que ha alcanzado los 2,73 millones de dólares, un alarmante aumento del 50 % en comparación con el año anterior.

En 2025, el ransomware seguirá siendo una de las principales amenazas cibernéticas, y Sophos, como líder en ciberseguridad, jugará un papel crucial en la defensa contra estos ataques.

Para mitigar estos riesgos, es fundamental que las organizaciones implementen medidas prácticas en cuatro áreas clave: **prevención, protección, detección y respuesta, así como planificación y preparación.**



Prevención

Las vulnerabilidades sin parches son la principal causa de los ataques de ransomware, por lo que es crucial priorizar la aplicación de parches y la implementación de autenticación multifactor (MFA). La capacitación continua de los empleados en detección de phishing también es esencial para fortalecer la primera línea de defensa.



Protección

Las organizaciones deben establecer bases de seguridad sólidas, como la protección de endpoints y la seguridad del correo electrónico. Utilizar herramientas de protección que incluyan defensas específicas contra ransomware ayudará a detener el cifrado malicioso antes de que cause daños.

¡Somos Centro de Entrenamiento Autorizado por Sophos!



Detección y Respuesta

La adopción de servicios de detección y respuesta gestionada (MDR) y herramientas de detección y respuesta de endpoint (EDR/XDR) es crucial para identificar y neutralizar ataques avanzados, protegiendo así las copias de seguridad y evitando el cifrado de datos.



Planificación y Preparación

Desarrollar un plan de respuesta a incidentes y realizar simulacros, así como la restauración de datos de copias de seguridad, son pasos vitales para asegurar una recuperación rápida tras un ataque.



La ciberseguridad ▶ Es un **compromiso continuo** que requiere atención constante.

Con la información y los recursos adecuados, las organizaciones pueden fortalecer sus defensas y estar mejor preparadas para enfrentar las amenazas cibernéticas del futuro.

Contactate con un **asesor**
escaneando este código QR



Ahora Domotes ofrece servicio técnico a otras marcas

Nuestros servicios se ajustan a las necesidades de soporte y servicio técnico que tenga su compañía trabajando como marca blanca y bajo las siguientes modalidades.



Tercerización completa de los de los servicios técnicos de tecnología que soportamos



Concentración por hora de servicio



Concentración para proyectos puntuales



Servicios técnicos sin costo



Formación y entrenamiento

Tecnologías que Soportamos

FORTINET

SOPHOS

islonline

asustor
ASUSTOR Inc.

vembu

SEAGATE

vicarius

NAKIVO®

aws

Azure

SONICWALL®

Windows

Descarga aquí
nuestro portafolio



Hable
con un asesor





27001, una de las metas del canal para el 2025.

Si el canal vende seguridad informática, una de sus metas para el 2025 debe ser alcanzar la certificación ISO 27001.

En un mundo globalizado y altamente competitivo, las organizaciones deben enfrentarse a desafíos cada vez mayores. Las normas ISO, desarrolladas por la Organización Internacional de Normalización, ofrecen marcos robustos y probados que permiten a las empresas gestionar de manera eficaz y sostenible sus procesos, riesgos y recursos. La implementación de normas como, por ejemplo: ISO 27001 permite proteger los activos de información al garantizar la confidencialidad, integridad y disponibilidad de la información, lo que se traduce en la satisfacción de los clientes. Es por esta razón que es importante que el canal pueda demostrar a sus clientes que en su empresa se cumplen con buenas prácticas de seguridad.

Además, las certificaciones ISO son herramientas competitivas que permiten ingresar a procesos licitatorios, dado que, para algunos

negocios, sobre todo de grandes corporaciones o gubernamentales, solicitan que los participantes estén certificados en dichas normas, entre estas la ISO27001, certificado al que todo canal de venta debe apuntar si quiere ser competitivo.

Tomando en cuenta lo antes visto, **¿cómo puede tu organización prepararse para la certificación ISO 27001?** Desde Domotes queremos compartir 5 pasos que puedes iniciar y que nos ayudaron a nosotros a conseguir esta certificación.





Domotes recibe certificaciones ISO...



ISO 45001

LL-C (Certification)



ISO 9001

LL-C (Certification)



ISO 14001

LL-C (Certification)



ISO 27001

LL-C (Certification)



ISO 20000

LL-C (Certification)

Estructura los procesos de la compañía, definiendo las caracterizaciones de procesos al definir las actividades, responsables, entradas y salidas.

Definir los activos y riesgos de información, define el listado de tus equipos, información sensible y cuáles pueden ser los riesgos de seguridad que pueden impactar a estos activos de información.

Establece los controles de seguridad de información, revisa los 93 controles recomendados por la ISO27001 en el anexo A, y asocia estos controles que puedan eliminar o mitigar los riesgos de información identificados en el paso 2.

Distribuye la responsabilidad de estos controles de seguridad de información en cada responsable de proceso y realiza el seguimiento del cumplimiento de estos controles.

Generar un diagnóstico organizacional frente a la norma ISO 27001, y de forma honesta verificar cómo está la empresa frente a cada requisito.

Si deseas obtener más información sobre esta norma, en **Domotes SAS** estamos aquí para ayudarte a estandarizar tus procesos. Podemos ofrecerte apoyo en el diagnóstico y auditoría de tu empresa en relación con la norma ISO 27001, facilitando así el camino hacia la certificación.



▶ **Escanea el código QR** y habla con un experto.

Comprometidos con el Cambio:

Domotes y el Poder de la Innovación Social

En Domotes creemos que la verdadera innovación no se limita a desarrollar soluciones tecnológicas; también implica transformar vidas y construir un futuro más equitativo. Es por eso que en 2024 lideramos con orgullo la creación de un Aula Inteligente en la Institución Educativa Técnica Policarpa Salavarrieta, en Soledad, Atlántico.



Este proyecto no solo fue una inversión en tecnología, sino un compromiso con las nuevas generaciones y su potencial para liderar un mundo digital.

Equipado con herramientas avanzadas de robótica y programación, este espacio educativo marca el inicio de una transformación social tangible. Más allá de las cifras, el impacto real está en las sonrisas de los estudiantes que, por primera vez, accedieron a un entorno diseñado para estimular su creatividad y su capacidad de innovación.



Un Llamado a Nuestros Partners

Como Partners de Domotes, tú también tienes el poder de ser un agente de cambio. Cada acción que tomamos como empresas puede sembrar las bases para una sociedad más justa e innovadora. ¿Por qué no llevar juntos la tecnología y el conocimiento a donde más se necesitan?



El Cambio Está en Nuestras Manos

Imagina el impacto de que más empresas se sumen a iniciativas como estas:

Una comunidad donde los niños tengan acceso a herramientas que despierten su interés por la tecnología.

Universidades apoyadas por programas empresariales que capaciten en ciberseguridad y programación avanzada.

Alianzas estratégicas entre sectores privados y públicos para promover la inclusión digital.

En Domotes no solo estamos comprometidos, somos parte activa del cambio. Queremos inspirarte a unirte a esta misión, porque juntos podemos multiplicar el impacto.



La Oportunidad de Hacer Historia

Proyectos como el Aula Inteligente no son excepciones, son el principio de lo que podemos lograr al trabajar en equipo. Desde tu empresa puedes aportar innovación, recursos o simplemente tu visión para hacer la diferencia.

Este es nuestro llamado a ti, Partner de Domotes: hagamos del impacto social una prioridad empresarial.

Un gigante de tecnología de seguridad informática ahora hace parte del portafolio de Domotes

SONICWALL®

EVOLUCIONANDO CON NUESTROS PARTNERS AHORA CON NUEVAS TECNOLOGÍAS



Network and Access Security



MSP/ MSSP Enablement



Managed Security Services



Cloud Edge Security

SONIC PLATFORM

SinglePane of Glass

Visibility, Reporting and Analytics

AI Powered

User and Device Management

Multi-tenancy and Scale

Topology and Automation

Global Policies

Detection and Response

World-Class Technical Support + Available 24x7x365 Monitoring + Cyber Insurance

3 pilares de SonicWall

Tecnología confiable y accesible

Inteligencia artificial aplicada a la seguridad de sus clientes.

CASB

FIREWALL

Zero Trust

Switchs

SMDR / SOC

Wifi

D-WAN

Red de canales leal

El modelo de negocio ideal para usted

VAR

MSP

MSSP

Capacitación y soporte continuo

Monitoreo 24/7

Soporte a ecosistemas basados en la nube

Protección ininterrumpida

Hágase partner, revolucione la seguridad de sus clientes y disfrute de todos los beneficios que ofrece el programa de canales de SonicWall.

SonicWall ZTNA y CASB

Está su empresa llevando a sus clientes a lo que será el estándar del acceso seguro en el futuro inmediato.

En la actualidad, las organizaciones han trasladado la mayoría (si no la totalidad) de sus aplicaciones y datos a la nube, en gran medida mediante el uso de aplicaciones SaaS. En muchos casos las infraestructuras de las empresas son complejas, con aplicaciones distribuidas en entornos locales, híbridos y multicloud, todo esto sumado al aumento del trabajo remoto supone un gran desafío para las organizaciones en temas de seguridad pues las protecciones tradicionales como controles del firewall en el perímetro o las VPN para las conexiones remotas ya no es suficiente.

De hecho, las soluciones tradicionales centradas en la red, como las VPN heredadas, se han puesto a prueba y han revelado importantes problemas de rendimiento, facilidad de uso y seguridad sistémica que las soluciones provisionales no pueden solucionar. Para abordar estas realidades, se requiere un enfoque escalable e integral para proteger el acceso remoto y las aplicaciones SaaS

Como parte de su evolución tecnológica y estratégica, SonicWall adquiere soluciones de vanguardia (Banyan), esto permitió el desarrollo de SonicWall Cloud Secure Edge (CSE) para ofrecer Zero Trust Security una solución de Servicio de Seguridad de Borde (SSE) que ofrece acceso seguro a cualquier dispositivo y usuario, sin importar dónde se encuentren, mediante políticas de confianza cero y privilegios mínimos, apoyando a las organizaciones a implementar una omnipresencia segura.



Estos son algunos de los beneficios que la tecnología Zero Trust de SonicWall ofrece:

- ✓ Visibilidad profunda de la actividad de los usuarios, dispositivos, aplicaciones y servicio
- ✓ Integración con entornos IaaS, PaaS con un solo clic
- ✓ Fácil implementación, administración y auditoría
- ✓ Seguridad inigualable control granular basado en puntajes de confianza

Cloud Secure Edge ofrece también funcionalidad CASB (Cloud Access Security Broker) brindando una excelente seguridad para aplicaciones SaaS, con políticas de acceso y seguridad consistentes, junto con una visibilidad unificada independientemente de dónde se encuentre la aplicación o el recurso.

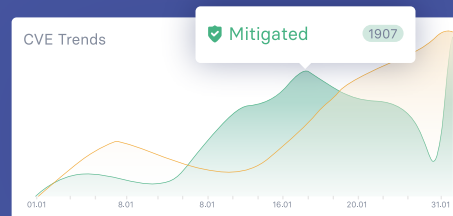
Descubra cómo las tecnologías ZTNA de SonicWall pueden revolucionar su negocio. Le enseñamos cómo puede ofrecerlo a sus clientes y hacer negocios rápidamente.



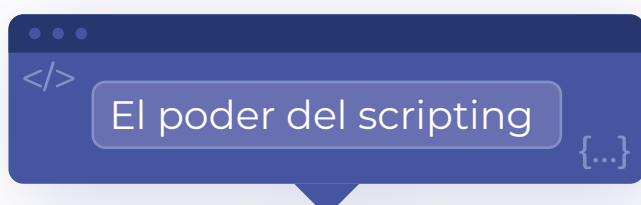
Contáctenos para más información.



Más allá de los parches:



Vicarius, la vanguardia en la gestión de vulnerabilidades



En el panorama actual de amenazas cibernéticas en constante evolución, las empresas se enfrentan al desafío de gestionar un número creciente de vulnerabilidades en sus sistemas y aplicaciones. Los enfoques tradicionales, centrados en la aplicación de parches, a menudo resultan ineficaces y consumen mucho tiempo, dejando a las organizaciones expuestas a riesgos significativos. Vicarius, una empresa innovadora en ciberseguridad, propone un nuevo enfoque para la gestión de vulnerabilidades que va más allá de los parches, priorizando la mitigación proactiva y la automatización inteligente.

La plataforma vRx de Vicarius ofrece una solución integral para la gestión de vulnerabilidades, que abarca desde el descubrimiento y la evaluación hasta la priorización y la remediación. Mediante el uso de algoritmos de aprendizaje

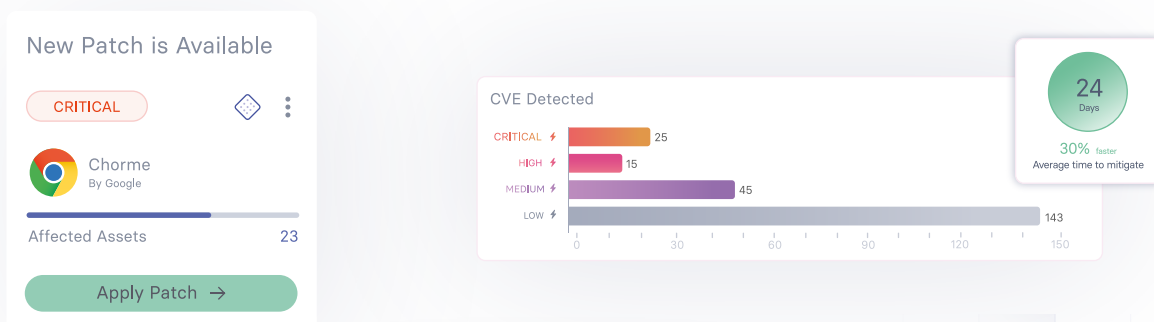
automático y análisis contextual, vRx identifica las vulnerabilidades que representan un mayor riesgo para la organización y recomienda acciones de mitigación específicas. Además, vRx automatiza la aplicación de parches y ofrece opciones de mitigación proactiva, como parches virtuales y configuraciones de seguridad, para proteger los sistemas incluso antes de que un parche esté disponible.

Un elemento central de vRx es su poderoso motor de scripting, que permite a los equipos de seguridad automatizar una amplia gama de tareas, desde la ejecución de comandos en los endpoints hasta la integración con otras herramientas de seguridad. Este motor de scripting proporciona una flexibilidad sin precedentes para adaptar vRx a las necesidades específicas de cada organización, permitiendo la creación de flujos de trabajo personalizados, la automatización de respuestas a incidentes y la orquestación de acciones de seguridad complejas.



Uno de los aspectos más destacados de Vicarius es su capacidad para analizar aplicaciones propietarias y especializadas en busca de vulnerabilidades, incluso sin CVE oficiales. Esto permite a las empresas proteger sus aplicaciones internas y de nicho, que a menudo son ignoradas por las soluciones de seguridad tradicionales. Además, vRx se integra con otras herramientas de seguridad, como SIEM y SOAR, para proporcionar una visión holística del panorama de amenazas y automatizar los flujos de trabajo de seguridad.

Con su enfoque innovador y sus capacidades avanzadas, Vicarius está ayudando a las empresas de todos los tamaños a gestionar sus vulnerabilidades de forma más eficiente y proactiva. Al reducir el riesgo de ciberataques y optimizar los recursos de seguridad, Vicarius permite a las organizaciones centrarse en sus objetivos de negocio con la confianza de que sus sistemas y datos están protegidos.



Contacta a un experto



Noe Linares
Account Executive

+57 315 671 9897
Noe@vicarius.io

Escanea el código QR y contactame





BDRSuite **#1**
By Vembu

Software de Backup Rentable

Ofrezca valor a sus clientes al tiempo que genera beneficios para su negocio

Las amenazas cibernéticas están en aumento, la adopción de la nube se acelera y sectores como la atención médica y las finanzas enfrentan regulaciones más estrictas. En este contexto, BDRSuite está bien posicionado para satisfacer la creciente demanda de soluciones integrales de copia de seguridad y recuperación ante desastres.

BDRSuite ofrece soluciones de copia de seguridad confiables, rentables y de bajo costo, garantizando la continuidad del negocio para sus clientes. Como socio, podrá disfrutar de altos márgenes de beneficio e ingresos recurrentes, lo que convierte a BDRSuite en una valiosa adición a su cartera.

Niels Jensen, destaca que BDRSuite le ha ayudado a ahorrar dinero y le proporciona ingresos mensuales al ofrecerlo como servicio a sus clientes, expresando su satisfacción con la herramienta.

¿Por qué convertirse en socio de BDRSuite? (Reseller/VAR, MSP)

- ✓ Alto margen en cada venta y obtenga ingresos recurrentes con precios competitivos.
- ✓ Libertad para elegir entre modelos de suscripción o de licencia perpetua, sin opciones forzadas, a diferencia de la competencia.

- ✓ No hay presupuestos mensuales ni contratos para que los proveedores de servicios operen sin compromisos.
- ✓ Protección de clientes potenciales para garantizar que sus clientes potenciales estén asegurados y sean exclusivamente suyos.
- ✓ Capacitación y soporte integrales, con recursos técnicos y de ventas para vender y respaldar.
- ✓ BDRSuite con confianza.
- ✓ Oportunidades de marketing en conjunto, incluidos materiales de marca y campañas conjuntas para ampliar su alcance. Gerente de cuenta dedicado que ofrece orientación personalizada para ayudarlo a tener éxito.

¿Por qué BDRSuite es la ventaja competitiva que necesita?

Rentabilidad

BDRSuite ofrece ahorros significativos en comparación con sus competidores, con precios competitivos que garantizan un excelente valor sin comprometer la calidad.



Adrian V, Consultor de Sistemas, destaca que el software es asequible y cumple con todas sus necesidades, mientras que Anand Davda, Director General, menciona que es accesible para empresas con presupuestos ajustados.

1. Gestión centralizada

La consola local de BDRSuite o la consola en la nube BDRCloud permiten administrar fácilmente todo el entorno de copia de seguridad.

John Demattia, Director IT, comenta que BDRSuite ha reducido el tiempo de gestión de copias de seguridad en al menos un 20% y ha disminuido los costos de administración entre un 20 y un 25%.

2. Copia de seguridad desde cualquier ubicación

BDRSuite permite realizar copias de seguridad de cargas de trabajo virtuales, físicas, en la nube y SaaS, asegurando la protección completa de los datos.

Redha Benlaksira, Director de Ventas Técnicas, resalta que la herramienta es integral y permite gestionar copias de seguridad desde cualquier lugar a través de una interfaz web.

3. Almacene la copia de seguridad en cualquier lugar

BDRSuite ofrece flexibilidad para almacenar copias de seguridad en almacenamiento local, remoto, en su propia nube pública o en BDRCloud.

Tony Ashvanian, Director de TI, menciona que su empresa utiliza BDRSuite para hacer copias de seguridad desde máquinas hasta la nube, optimizando el proceso.

¡Da el siguiente paso!

Realiza una prueba sin costo: Regístrese hoy para una prueba gratuita de **30 días** y **experimente la diferencia.**



Escanee el código QR o visite www.bdrsuite.com/try

BONUS

Recorta y reclama tus beneficios por ser partner **Domotes**

SOPHOS

- Por compras mayores a **10 mil dólares** recibe **200 dólares** de descuento para dicha orden
- Por compras mayores a **20 mil dólares** recibe **400 dólares** de descuento para dicha orden
- Por compras mayores a **30 mil dólares** recibe **600 dólares** de descuento para dicha orden



Escanea y reclama tu beneficio

islonline

3 meses
Soporte remoto
GRATIS

Para elevar tu servicio al próximo nivel. Simplifica tu trabajo y sorprende a tus clientes con una plataforma segura, eficiente y **¡muy fácil de usar!**



Escanea y reclama tu beneficio



vicarius

¡Nuevos negocios, nuevas oportunidades con **Vicarius!**

Consigue un

5%

de descuento

Exclusivo en tu primera compra. (No válido para clientes con descuentos actuales).



Escanea y reclama tu beneficio

SONICWALL®

Con la promoción **3 & Free** con Cloud Secure Edge de SonicWall

Transforme su acceso y protección digital.

Al adquirir un Essential Protection Service Suite (EPSS) o Advanced Protection Service Suite (APSS) de 3 años, sus clientes obtendrán sin costo, un firewall de próxima generación Gen 7, que brinda una seguridad total y simplifica el acceso a sus recursos desde cualquier dispositivo.

Adicional obtenga el nuevo TZ80:

Un pequeño firewall que protege a lo grande. A partir de 99 dólares FOB*

*Aplica términos y condiciones.



Escanee y reclame su beneficio



SEAGATE

15%
de descuento

En las unidades Flashtor
*[Aplica para las referencias FS6706T y FS6712X y hasta agotar existencias]



Por la compra de
Unidades de discos
Seagate Ironwolf de 20TB

¡Lleva 1 disco
de 2TB gratis!

*Válido hasta agotar existencias



Escanee y reclame su beneficio



Eventos destacados del año en Domotes



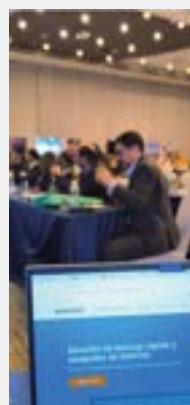
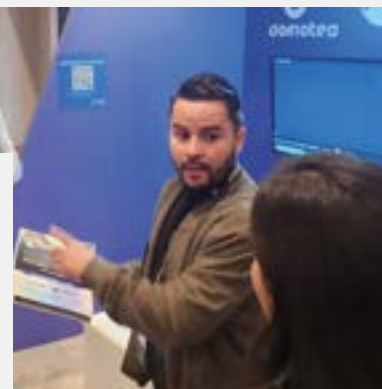
Este 2024 marcamos grandes hitos con nuestra participación en eventos clave como INFOSECURITY Colombia y Ecuador, ANDICOM, y capacitaciones especializadas como las ATC, además de fortalecer relaciones a través de eventos de apoyo al canal y encuentros con Partners.



¡Hagamos Equipo en 2025!

Te invitamos a participar en nuestros próximos eventos y contar con nuestro apoyo para organizar eventos que impulsen el éxito con tus clientes.

¡Somos parte de tu equipo!





Una alianza estratégica para el éxito.

En el ecosistema digital actual, las empresas de ciberseguridad no solo deben proteger a sus clientes, sino también destacar en el mercado. Aquí es donde el marketing digital se vuelve esencial, ayudando a estas empresas a posicionarse como líderes de confianza.



Una tendencia importante en el marketing de ciberseguridad es la educación. Las compañías están creando blogs y webinars que informan a los usuarios sobre las amenazas y las mejores prácticas en seguridad, lo que genera confianza y los establece como referentes en el tema.

También están utilizando contenido visual como infografías y videos para simplificar conceptos difíciles y atraer la atención de potenciales clientes.

Mostrar resultados a través de casos de estudio y testimonios es otra estrategia clave. Los clientes quieren ver cómo una empresa puede proteger sus datos en situaciones reales. La automatización del marketing permite gestionar campañas de email, recordatorios de webinars y segmentar audiencias, optimizando recursos y personalizando la comunicación. La publicidad pagada en plataformas como LinkedIn y Google Ads también es efectiva, ya que permite llegar específicamente a ejecutivos y gerentes de seguridad que buscan soluciones de protección.

Además, el marketing digital ayuda a humanizar una industria que a menudo se percibe como técnica. Facilita que las empresas muestren su lado más accesible y refuercen su misión de proteger a sus clientes. Al comunicar su mensaje de manera clara y sencilla, invertir en contenido educativo y demostrar su eficacia con pruebas sociales, las empresas pueden atraer y convertir leads en clientes.

En resumen, **el marketing digital es clave** para que las empresas de ciberseguridad se diferencien en un mercado competitivo al construir una imagen confiable y apegada a las necesidades de sus clientes.



¡Impulsa tus ventas con nuestro

Pack exclusivo para partners de tecnología!

En un mercado competitivo, **cada detalle cuenta**



Con nuestro **Pack de Campañas** Dirigidas, optimiza tu estrategia y **maximiza tus resultados.**

INCLUYE

Contenido optimizado para **atraer** a tu audiencia

Diseño visual **impactante**

Landing page personalizada para **generar leads**

Campañas de Ads en plataformas claves

Seguimiento y análisis para **mejorar** cada paso

¡No dejes pasar la oportunidad de **crecer!**



Contáctanos hoy y transforma tus esfuerzos de marketing en ventas.

 www.hooki.co

Partners

2025



Esta edición es un reflejo de la confianza y el compromiso que compartimos contigo. Sigamos avanzando juntos hacia un futuro lleno de crecimiento, innovación y éxito compartido.

Escanea en el QR y comparte tus expectativas para este 2025, incluyendo el apoyo que esperas recibir de Domotes. Tu opinión es clave.

Somos parte de su equipo

