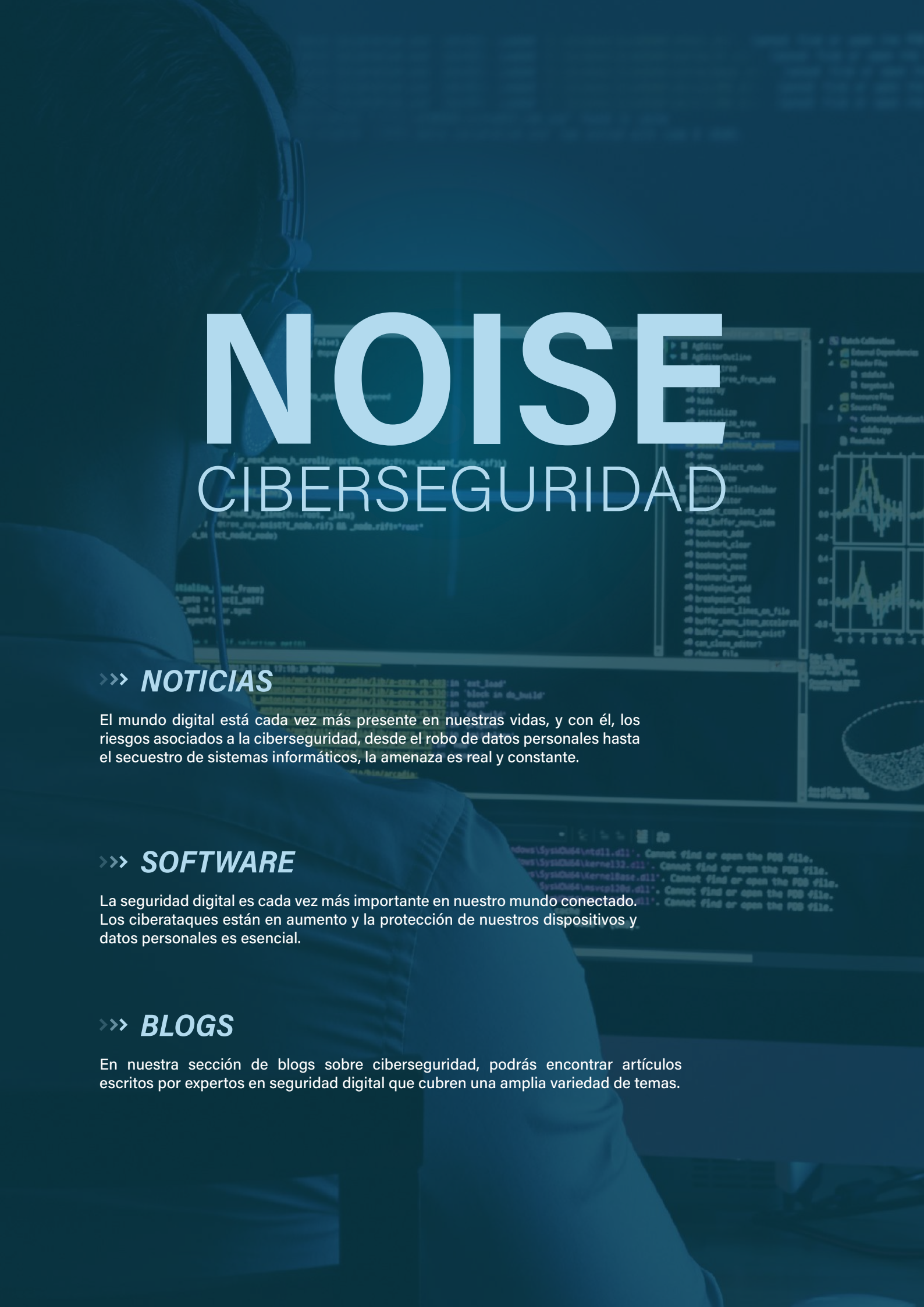


NOISE
CIBERSEGURIDAD

›› NOTICIAS

El mundo digital está cada vez más presente en nuestras vidas, y con él, los riesgos asociados a la ciberseguridad, desde el robo de datos personales hasta el secuestro de sistemas informáticos, la amenaza es real y constante.

›› SOFTWARE

La seguridad digital es cada vez más importante en nuestro mundo conectado. Los ciberataques están en aumento y la protección de nuestros dispositivos y datos personales es esencial.

›› BLOGS

En nuestra sección de blogs sobre ciberseguridad, podrás encontrar artículos escritos por expertos en seguridad digital que cubren una amplia variedad de temas.

¿QUIÉNES SOMOS?

NOISE Ciberseguridad nace como una empresa de Consultoría y Gestión de Riesgos Informáticos, con la finalidad de proveer servicios profesionales especializados en la gestión del riesgo, la ciberseguridad y el cumplimiento regulatorio.

A través de su marca comercial NOISE Ciberseguridad ofrece sus servicios a Latinoamérica con servicios de alta calidad.

NOISE Ciber Seguridad incorpora diferentes metodologías que están respaldadas por las certificaciones de sus consultores que, debido a su amplia experiencia en diferentes industrias, aportan un conjunto de conocimientos adquiridos que nutren cada uno de los proyectos que realiza.

NUESTROS SERVICIOS

Seguridad de la información

- Gestión de riesgo.
- Análisis de impacto de negocio (BIA).
- Plan de continuidad del negocio (BCP).
- Test de ingeniería social.

Gestión de servicios

- Gestión de servidores.
- Soporte de gestión bajo AWS.
- Mantenimiento preventivo y correctivo de servidores Linux (debían, redhat, etc).
- Instalación y configuración Docker y Kubernetes.
- Soluciones de infraestructura opensource (balanceado de carga, firewalls, virtualización, etc).

Seguridad informática

- Análisis de tráfico en redes.
- Análisis de vulnerabilidades y pentest.
- Análisis de código (php, java, c#) y aplicaciones móviles.
- Diseño e implementación de redes empresariales.

Forense y rescate

- Recuperación de información (nivel lógico).
- Peritaje forense de PCs y dispositivos móviles.

Otros

- Creación y personalización web (wordpress).
- Dominio y hosting de sitios web.
- Instalación, configuración e implementación de plataformas de aprendizaje (Moodle).

GÁNATE LA CONFIANZA DE TUS VISITANTES

Resuelva las preocupaciones de los visitantes sobre malware, virus y phishing y muestre la seguridad de su sitio.

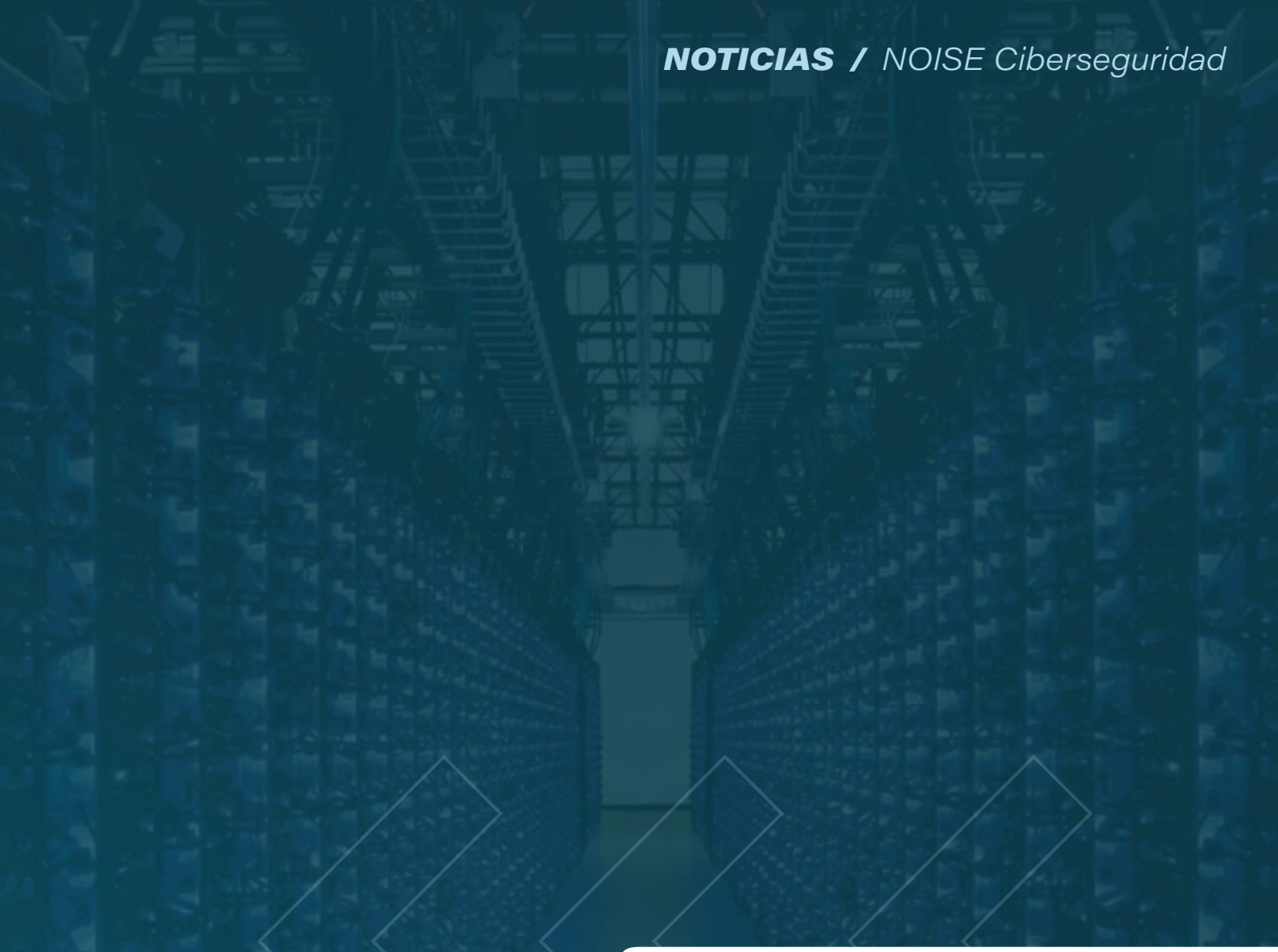
Muestre que su sitio es un negocio confiable con el que los visitantes pueden conectarse fácilmente.

Muestre que su negocio brinda un servicio sobresaliente de manera constante durante todo el proceso de compra.

Proteja a los clientes que califiquen con hasta $100,000 de protección contra robo de identidad.

Obtener certificaciones TrustedSite es el primer paso para aliviar las preocupaciones de los visitantes en su sitio.

TrustedSite



Servidores Exchange vulnerables a los ataques ProxyNotShell

Microsoft lanza parches de seguridad para proteger los servidores Exchange contra los ataques ProxyNotShell.

Microsoft ha lanzado una advertencia sobre dos errores de seguridad, conocidos como CVE-2022-41082 y CVE-41040, que afectan a los servidores Exchange 2013, 2016 y 2019. Estos errores, denominados ProxyNotShell, pueden ser explotados por los atacantes para aumentar los privilegios y obtener la ejecución de código arbitrario o remoto en servidores comprometidos.

Para proteger sus servidores de Exchange de los ataques entrantes, es fundamental que las empresas apliquen los parches de seguridad ProxyNotShell lanzados por Microsoft en noviembre de 2022. Las empresas también deben asegurarse de mantener sus sistemas actualizados y adoptar buenas prácticas de seguridad, como la implementación de medidas de autenticación robustas y la monitorización constante de sus infraestructuras digitales.

La vulnerabilidad de los servidores Exchange es un recordatorio de la importancia de la seguridad cibernética y la necesidad de mantener los sistemas actualizados y protegidos contra las amenazas en constante evolución en el ciberespacio.

Slack: incidente de seguridad en códigos privados de GitHub.

Compromete la seguridad de los repositorios privados de código de la plataforma de comunicación empresarial.

Slack, la popular plataforma de comunicación empresarial, ha sufrido un incidente de seguridad que ha afectado a algunos de sus repositorios privados de código en GitHub. Según la compañía, el incidente fue causado por actores de amenazas que obtuvieron acceso a los repositorios a través de un número limitado de fichas de empleados de Slack que fueron robadas.

Aunque algunos de los repositorios de código privado de Slack se vieron comprometidos, la compañía asegura que la base de código principal y los datos de los clientes no fueron afectados. Slack ha tomado medidas para invalidar las fichas robadas y está investigando el impacto potencial para sus clientes.

Este incidente de seguridad es una llamada de atención para las empresas que utilizan plataformas de comunicación y colaboración en línea. Es fundamental que las empresas adopten medidas de seguridad rigurosas y mantengan una estrecha vigilancia sobre su infraestructura digital para protegerse contra amenazas externas.

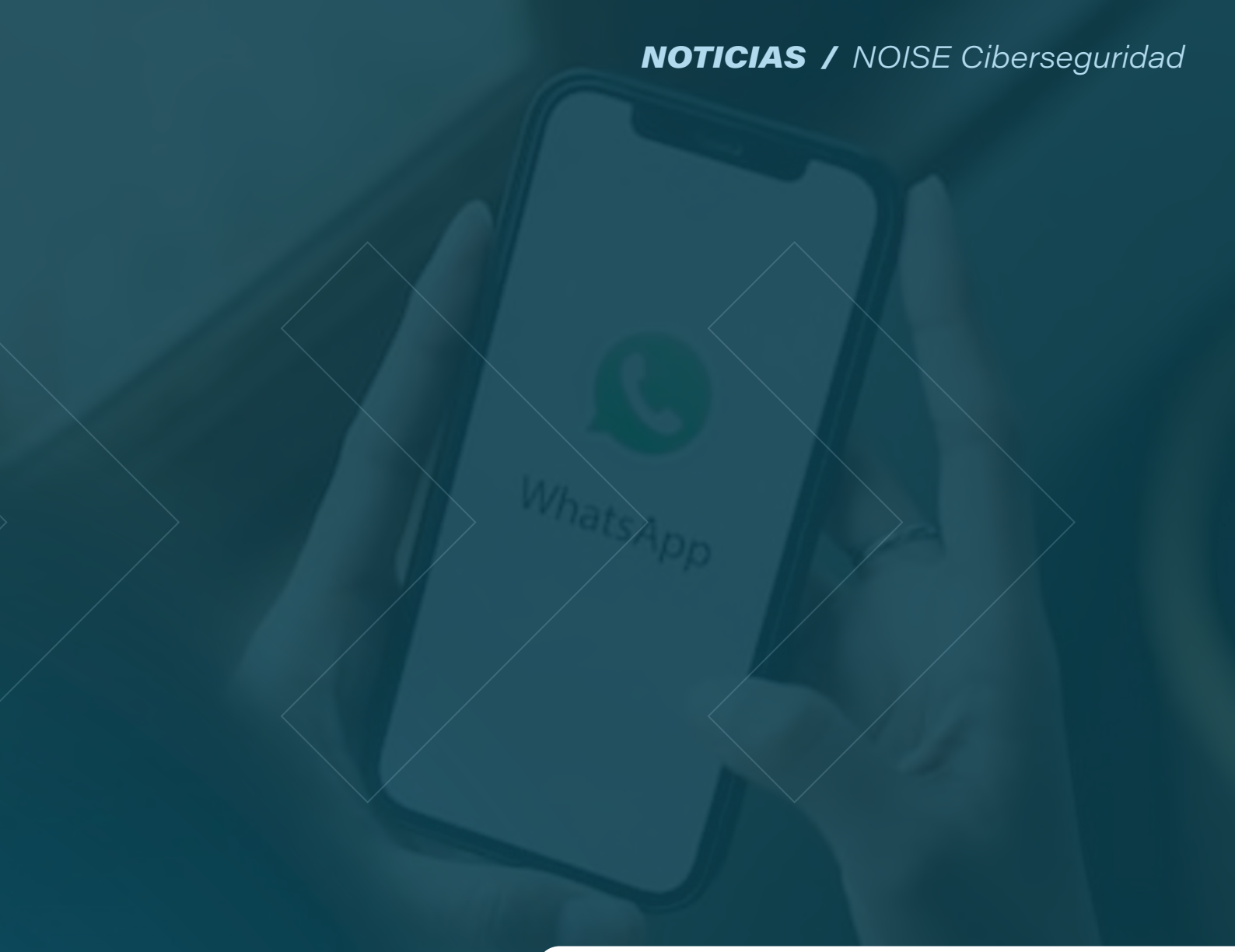
Ransomware Play detrás del ciberataque a los entornos alojados de Microsoft Exchange de Rackspace

Rackspace ofrece licencias gratuitas a los clientes para migrar sus correos electrónicos a Microsoft 365 después del ciberataque del ransomware Play.

La compañía de alojamiento web Rackspace ha confirmado que sus entornos alojados de Microsoft Exchange fueron derribados por el ransomware Play. El grupo de ransomware utilizó un nuevo exploit (OWASSRF) para comprometer los servidores de Microsoft Exchange y obtener acceso a las redes. El exploit permitió evitar las mitigaciones de reescritura de URL de ProxyNotShell proporcionado por Microsoft, probablemente apuntando a una falla crítica CVE-2022-41080.

Desde que se descubrió el ataque, Rackspace ha proporcionado a los clientes licencias gratuitas para migrar sus correos electrónicos desde su plataforma Hosted Exchange a Microsoft 365. Rackspace también ha estado trabajando en estrecha colaboración con las autoridades y los expertos en ciberseguridad para mitigar los efectos del ataque y recuperar los datos perdidos.

Este incidente destaca la importancia de la ciberseguridad en la era digital. Las empresas deben estar preparadas para enfrentar las amenazas de ransomware y adoptar medidas preventivas para proteger sus sistemas y datos valiosos. La colaboración con expertos en ciberseguridad y el mantenimiento de buenas prácticas de seguridad cibernética son fundamentales para mantenerse protegidos contra los ataques cibernéticos.



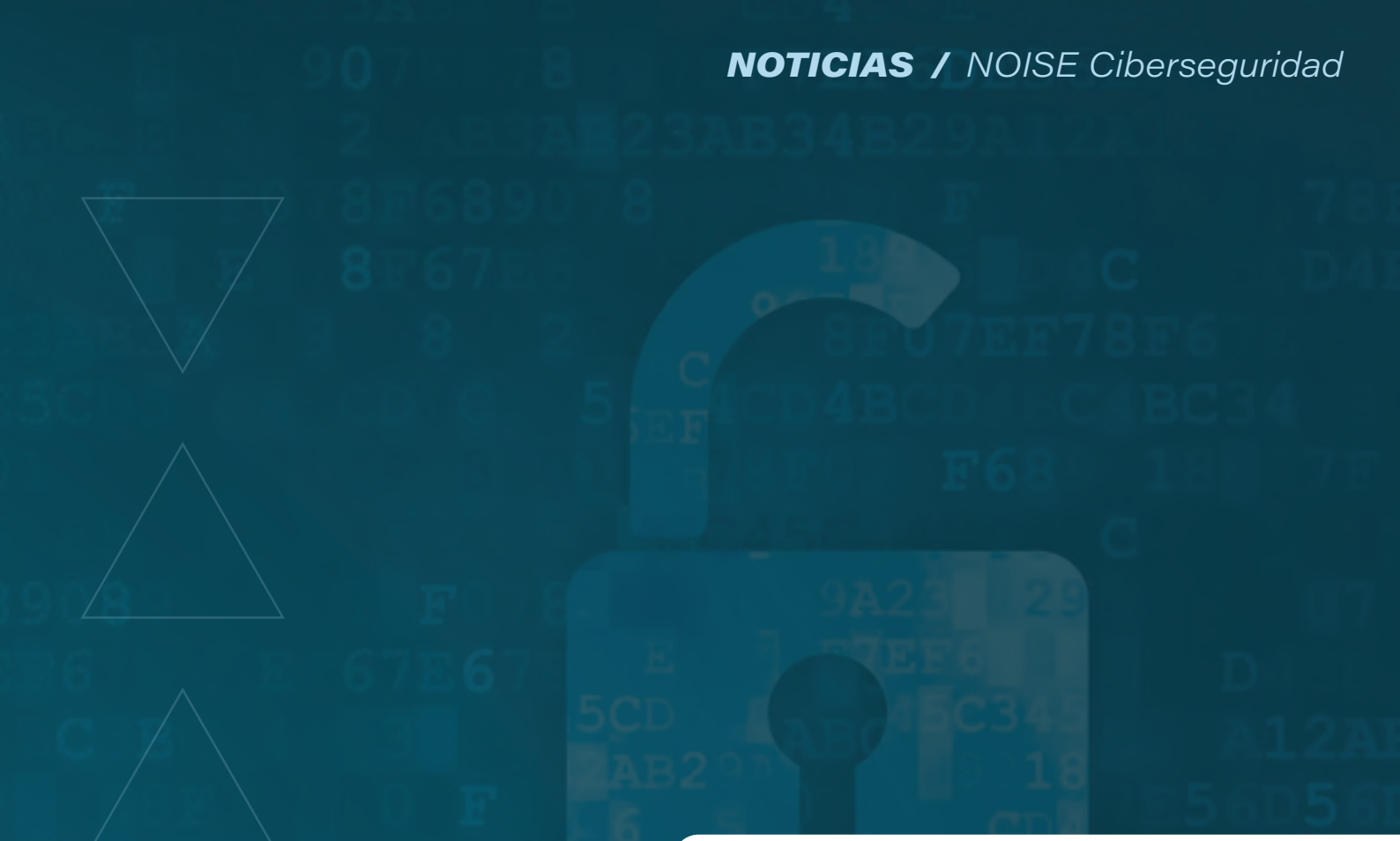
Cuidado con el mensaje de 6 dígitos en Whatsapp: una nueva estafa de robo de cuentas

Los ciberdelincuentes están utilizando la técnica de autenticación de doble factor para engañar a los usuarios y robar sus datos personales.

Los ciberdelincuentes han desarrollado una nueva forma de robar cuentas: la estafa del código de 6 dígitos. Esta técnica se aprovecha de la verificación de doble factor, un proceso que añade una capa extra de seguridad al pedir al usuario que introduzca un código de seguridad después de introducir su contraseña.

A través de un mensaje en Whatsapp, los estafadores solicitan a sus víctimas el código que han recibido por SMS, alegando que lo enviaron por error. Si la persona cae en la trampa y proporciona el código, los ciberdelincuentes tendrán acceso completo a su cuenta.

Los expertos en seguridad advierten que es importante tener precaución y no proporcionar nunca el código de seguridad a nadie, incluso si el mensaje parece legítimo. Si tiene dudas sobre un mensaje que ha recibido, es mejor verificar su autenticidad directamente con la empresa o servicio en cuestión antes de proporcionar cualquier información personal.



Google presenta su nueva herramienta para la protección de la privacidad de los usuarios

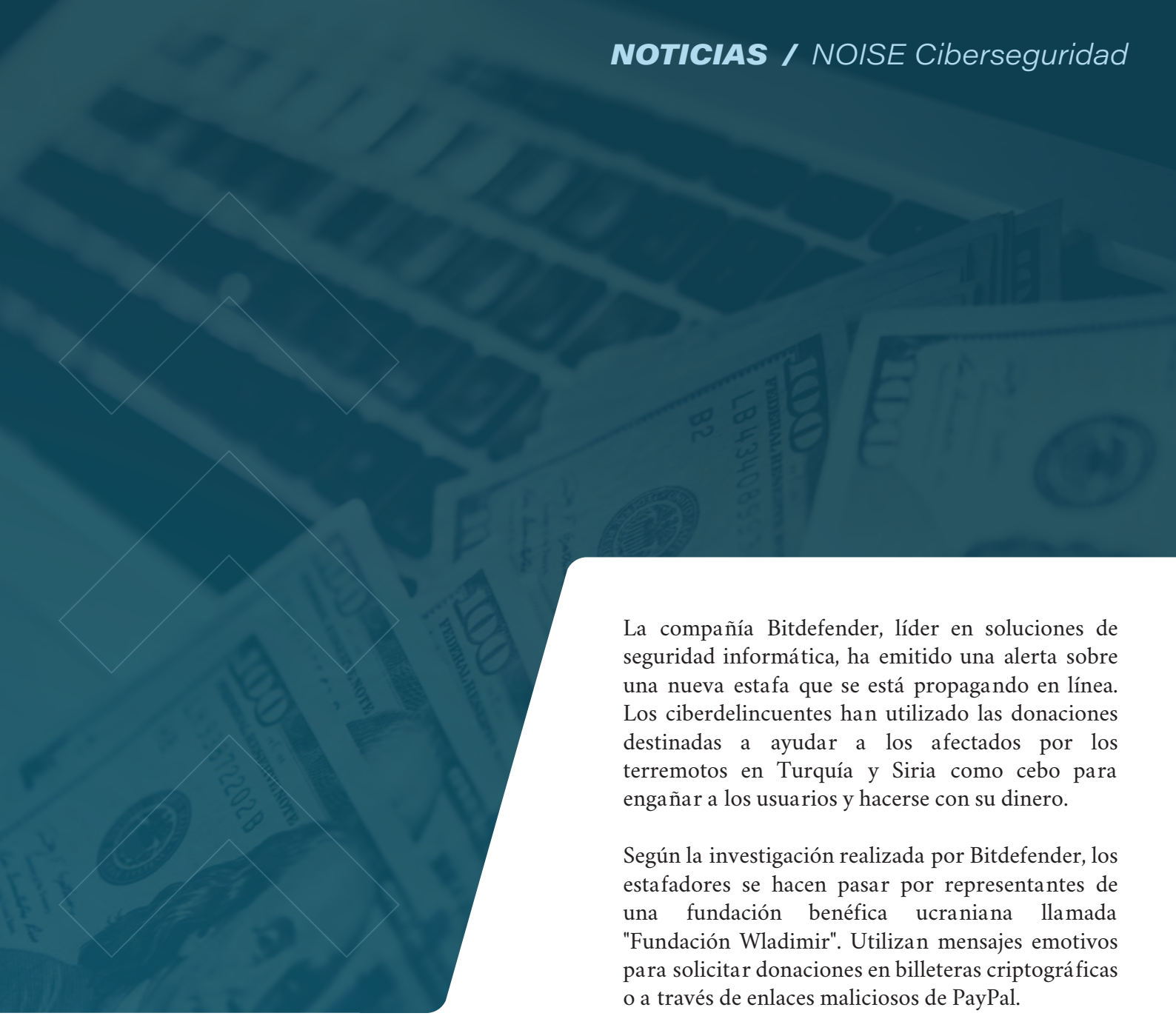
Google se preocupa por la privacidad de los usuarios y presenta una nueva herramienta para retirar información personal de los resultados de búsqueda.

Google ha añadido una herramienta muy útil para que los usuarios puedan retirar su información personal de los resultados de búsqueda. Esta nueva función se encuentra en la sección "Resultados sobre ti" dentro de la aplicación de Google. Al hacer clic en ella, los usuarios pueden solicitar que se retire cualquier información personal que aparezca en los resultados de búsqueda.

Este nuevo apartado permite a los usuarios tener más control sobre su información personal y decidir qué información quieren compartir públicamente. La herramienta es fácil de usar y guía a los usuarios a través de todo el proceso de solicitud, lo que hace que el proceso sea rápido y sencillo.

Una vez que se ha enviado la solicitud, los usuarios pueden comprobar el estado de su petición y ver qué resultados han sido aprobados para su eliminación. Además, esta herramienta es un gran paso adelante en la protección de la privacidad de los usuarios en línea.

En un mundo cada vez más digital, la privacidad y la protección de datos personales son fundamentales. Google ha tomado la iniciativa de ayudar a sus usuarios a controlar su información personal y ofrecer una mayor transparencia en los resultados de búsqueda. ¡Una excelente noticia para la protección de la privacidad en línea!



Advertencia de Bitdefender: Estafas que utilizan las donaciones a Turquía y Siria como cebo.

Los ciberdelincuentes se hacen pasar por una fundación benéfica ucraniana para solicitar donaciones a través de enlaces maliciosos en línea.

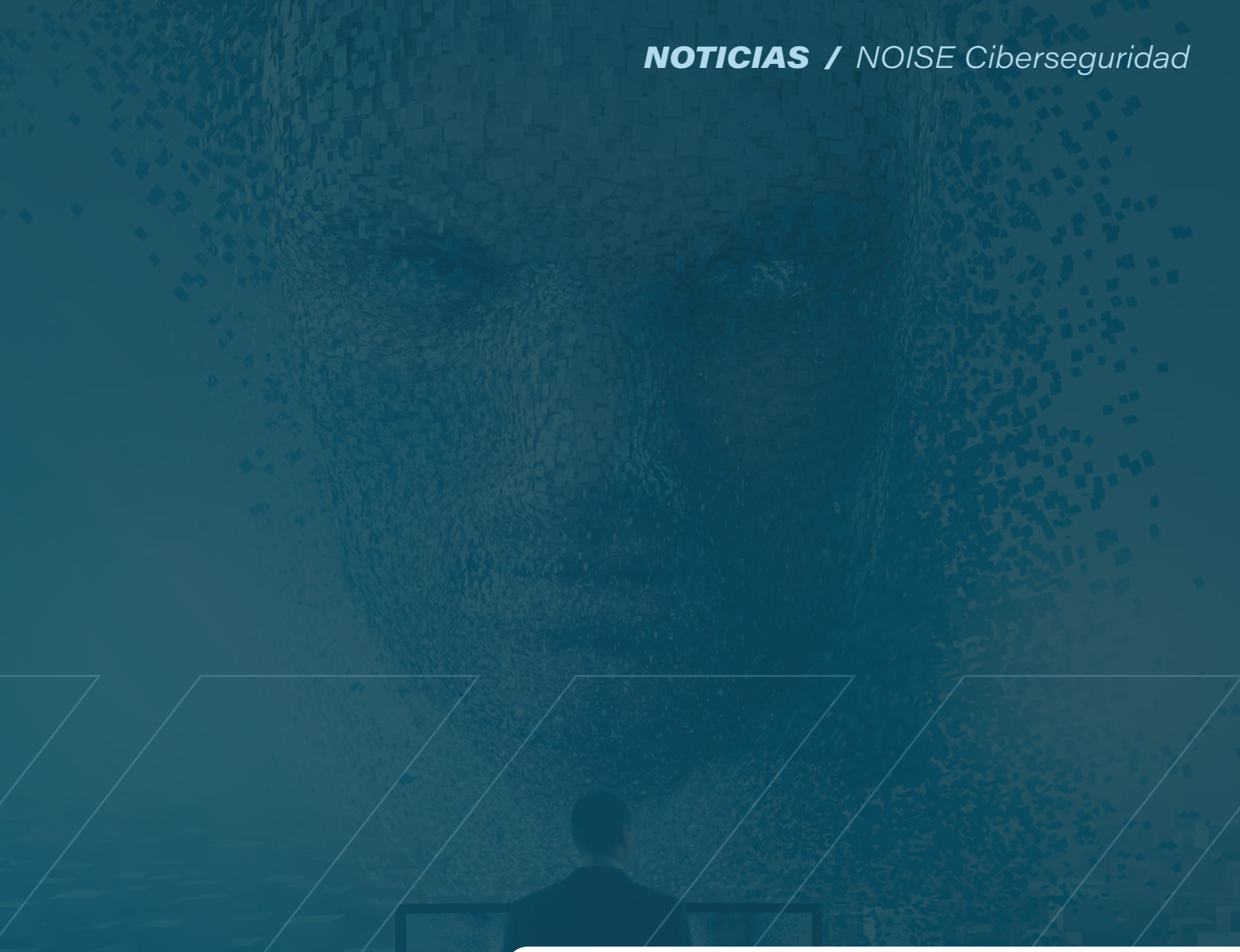
La compañía Bitdefender, líder en soluciones de seguridad informática, ha emitido una alerta sobre una nueva estafa que se está propagando en línea. Los ciberdelincuentes han utilizado las donaciones destinadas a ayudar a los afectados por los terremotos en Turquía y Siria como cebo para engañar a los usuarios y hacerse con su dinero.

Según la investigación realizada por Bitdefender, los estafadores se hacen pasar por representantes de una fundación benéfica ucraniana llamada "Fundación Wladimir". Utilizan mensajes emotivos para solicitar donaciones en billeteras criptográficas o a través de enlaces maliciosos de PayPal.

La compañía ha alertado a los usuarios para que estén alerta y eviten hacer donaciones a través de estos canales no oficiales. En su lugar, recomiendan hacer donaciones a organizaciones benéficas reconocidas y confiables que estén trabajando en el terreno para ayudar a los afectados por los terremotos en Turquía y Siria.

Ante esta situación, la Fundación Wladimir ha emitido un comunicado en el que niega cualquier vinculación con estos mensajes fraudulentos y ha informado que están trabajando con las autoridades pertinentes para identificar a los responsables de esta estafa.

Las autoridades competentes han sido informadas y están investigando el caso para dar con los responsables de esta estafa en línea que están aprovechando la crisis humanitaria para engañar a las personas bienintencionadas.



Microsoft y OpenAI lanzan el nuevo asistente de inteligencia artificial para Bing.

Se espera que este nuevo asistente de inteligencia artificial de Bing cambie la forma en que las personas interactúan con los resultados de búsqueda y haga que la búsqueda de información sea más fluida y fácil.

Microsoft ha iniciado la integración de las capacidades de inteligencia artificial basados en ChatGPT de OpenAI con su buscador Bing, el cual pretenden que sea un asistente en la búsqueda de soluciones integrado con los resultados de búsqueda.

A pesar de un inicio brusco debido a respuestas fuera de tema o con entonaciones agresivas por parte del asistente, Microsoft pretende hacer todo lo posible para que este asistente sea lo mas neutral y certero posible al generar respuestas.

Este es el inicio de una era impulsada por inteligencia artificial donde Bing pasaría de dar resultados de búsqueda a dar soluciones directamente como ya se hace con ChatGPT, mientras tanto Google aún trabaja en su propio motor de AI para competir con Microsoft.

Microsoft integrará esta nueva tecnología con más productos para llegar a más público, próximamente será integrado por el buscador de Windows 11 y mas adelante con las aplicaciones de Microsoft 365.

Ciberataque paraliza la distribución de medicamentos en farmacias catalanas

Alliance Healthcare, uno de los principales mayoristas de medicamentos en España, sufre un ataque informático que afecta a sus sistemas de gestión y entrega de productos.

En las últimas horas, se ha confirmado que uno de los principales mayoristas de medicamentos de las farmacias catalanas, Alliance Healthcare, ha sufrido un ciberataque que ha paralizado sus sistemas informáticos y ha impedido a la empresa entregar productos a las farmacias de manera normal.

Este ataque, que se inició el pasado viernes 24 de marzo de 2023, ha afectado a la página web de la empresa, los sistemas de facturación y los pedidos, lo que ha generado un importante caos en la gestión de los medicamentos en las farmacias catalanas.

Según fuentes cercanas a la empresa, los clientes no han sufrido las consecuencias del ataque, ya que la empresa solo cuenta con información comercial y no personal de los clientes. No obstante, el incidente ha generado una importante preocupación en el sector, ya que se trata de uno de los principales distribuidores de medicamentos en España.

Desde la dirección de Alliance Healthcare han asegurado que están trabajando intensamente para solucionar el problema y restablecer la normalidad en la entrega de productos a las farmacias. Además, han confirmado que han denunciado el ataque a las autoridades competentes y están colaborando activamente con las fuerzas de seguridad en la investigación del mismo.

Mientras tanto, el sector farmacéutico sigue muy de cerca la evolución de la situación y espera que Alliance Healthcare pueda recuperarse lo antes posible del ciberataque para que la distribución de medicamentos vuelva a la normalidad en la región catalana.

Hospital Clínic de Barcelona en crisis por ciberataque que compromete datos médicos

RansomHouse exige el pago de 4,5 millones de dólares para no publicar datos del Hospital Clínic sobre investigaciones y ensayos médicos. El Govern implementa protocolo para prevenir engaños.

El Hospital Clínic de Barcelona ha sufrido un gran apagón en su actividad a causa de un ciberataque de tipo ransomware que ha comprometido la seguridad de sus datos. La empresa de cibercrimen RansomHouse ha reclamado al Govern una cifra de 4,5 millones de dólares (4,2 millones de euros) para no hacer públicos ni revender los datos sustraídos.

Entre los datos que podrían ser publicados se encuentran investigaciones y ensayos sobre cáncer y enfermedades autoinmunes, campos en los que el Hospital Clínic es destacado. La situación ha generado una gran preocupación en la comunidad médica, ya que estos datos podrían poner en riesgo la privacidad y confidencialidad de los pacientes.

Ante esta amenaza, el Govern está elaborando un protocolo de prevención para informar a los profesionales y pacientes del Hospital Clínic sobre el posible envío de mensajes falsos y otras tácticas de engaño. El objetivo es evitar que se produzcan acciones fraudulentas por parte de los delincuentes informáticos y proteger la seguridad de los datos de los pacientes.

El Hospital Clínic ha confirmado que está trabajando intensamente para solucionar el problema y recuperar la normalidad en su actividad. Además, ha asegurado que ha denunciado el ciberataque a las autoridades competentes y está colaborando activamente con las fuerzas de seguridad en la investigación del mismo.

La situación sigue siendo delicada, pero se espera que el Hospital Clínic pueda recuperarse pronto del ciberataque y garantizar la seguridad de sus datos y la privacidad de sus pacientes.

Italia sufre caída de conexión a internet tras masivo ataque de hackers

Telecom Italia, uno de los principales proveedores de servicios de Internet en el país, fue la más afectada por el ataque que comprometió varios sistemas informáticos nacionales.

La compañía Telecom Italia sufrió una caída de la conexión en Internet en toda Italia después de un masivo ataque de hackers que comprometió varios sistemas informáticos nacionales. El equipo de respuesta a incidentes de seguridad informática del país detectó un ataque masivo con un ransomware que explotó las vulnerabilidades de los sistemas operativos.

La capacidad de navegación de Internet en las principales ciudades italianas se vio fuertemente afectada, dejando a muchos usuarios sin conexión durante horas. La empresa Telecom Italia, uno de los principales proveedores de servicios de Internet del país, fue la más afectada por el ataque.

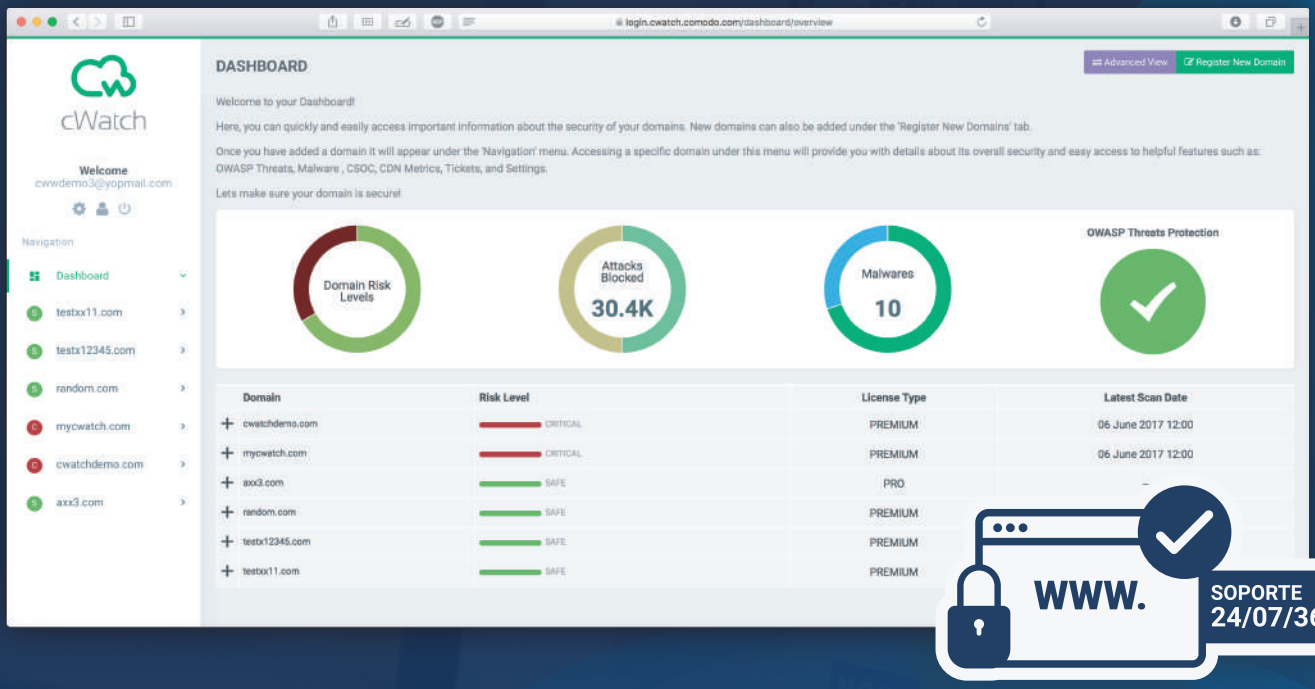
El equipo de seguridad informática de la compañía está trabajando en la solución del problema y en la recuperación de los sistemas afectados. Además, están colaborando con las autoridades para identificar a los responsables del ataque y tomar las medidas necesarias para evitar futuros incidentes.

El ataque ha generado preocupación entre los usuarios de Internet en Italia y ha puesto de manifiesto la importancia de mantener los sistemas informáticos seguros y actualizados para evitar posibles vulnerabilidades.

Las autoridades italianas han emitido una alerta de seguridad y han recomendado a los usuarios de Internet tomar medidas preventivas, como el uso de software de seguridad actualizado y la realización de copias de seguridad regularmente para proteger su información personal y empresarial.

La situación sigue siendo delicada, pero se espera que las medidas tomadas por las autoridades y las empresas de telecomunicaciones permitan una recuperación rápida y completa de la conexión a Internet en todo el país.

PROTECCIÓN COMPLETA PARA TU SITIO WEB



87%
Aumento del rendimiento promedio del sitio web

99%
Resoluciones de tickets de soporte

7,900,000
Vulnerabilidades desconocidas procesadas por nuestra Ai

cWatch

Ciber Resiliencia

Ciber Resiliencia tiene por misión hacer cumplir los objetivos de negocio que dependan de recursos cibernéticos en un ambiente de igual forma, cibernético.

Ante una revolución en las tecnologías y la evolución a una era digital en los modelos de negocio, se debe construir una cultura de seguridad en todos los procesos de las organizaciones, la cual se vuelve igual de importante que los aspectos financieros y operativos.

Nos encontramos en un punto de transformación, donde antes se llenaban papeles de formularios ahora se llenan formularios en línea, donde antes éramos atendidos por un agente para gestionar un proceso, ahora es un proceso automatizado, lleno de validaciones y verificaciones.

Cada vez los procesos son completamente digitales y las empresas saben que este es el futuro al que nos dirigimos, quien no pueda adaptarse al cambio no podrá mantener su puesto en el mercado, se verá opacado por aquellos que logren antes la meta, es una carrera por digitalizar los procesos. Sin embargo, solo pensamos en la meta, no pensamos en las consecuencias, con una transformación digital también se transforman las amenazas y todas las empresas que se unan a esta carrera por la digitalización deben estar conscientes de los riesgos.

La ciber resiliencia debe ser un punto de gran importancia, un punto crítico a considerar durante las operaciones del negocio, de la misma manera en la que se espera una falla eléctrica, un corte en la comunicación también debemos esperar un ataque cibernético.

La ciber resiliencia puede ser confundida con el cumplimiento o la seguridad de la informática, sin embargo, este concepto trata las cosas desde un punto de vista más general con el único propósito de incrementar la seguridad en la totalidad de la organización y reducir los riesgos o fallas que puedan existir.

Al hablar de ciber resiliencia, se refiere a una cultura de ciberseguridad, no se habla de cumplimiento, no es un estándar definido con su listado de puntos por verificar, ¿Puede la ciber resiliencia ayudar con el cumplimiento? si puede y en gran medida. Se trata de la cultura en una organización, esta se forma en base a los objetivos del negocio y sus valores, la ciber resiliencia requiere que la cultura de la organización sea con orientación a la seguridad, que se capacite al personal no solamente porque hay una ley regulatoria o una norma que nos dice que debemos capacitar al personal (lo cual puede ser percibido como una tarea más) sino porque queremos que el personal sepa la importancia de la seguridad en su entorno laboral, que no solo el personal sino también los ejecutivos sean parte del proceso que sepan que el correo institucional es para cuestiones de trabajo y no para registrarlo sin cuidado en sitios de dudosa procedencia.

La ciber resiliencia también se refiere a la continuidad del negocio, preparar los sistemas para funcionar ante una serie de posibles escenarios que podrían resultar en una catástrofe para la organización, lo cual muchas empresas tienen bastante claro, ya sea por cumplimiento, por prevención o por algún incidente en el pasado que los obligó a tomar acciones al respecto.

Está más que claro que es mucho más fácil hacerse una idea que tratar de implementarlo, un cambio de este tipo no ocurre de la noche a la mañana, esto puede tardar meses o años dependiendo del tamaño de la organización y la cantidad de áreas a cubrir, pero es un beneficio para todos, el personal aprende la importancia de la seguridad de la información la cual puede aplicar dentro y fuera de su horario laboral, los ejecutivos tendrán la seguridad de que el negocio es capaz de resistir las amenazas más comunes y los equipos encargados de la seguridad pueden agilizar los procesos con una visión más clara.

CISCO, realizó una investigación con sus clientes alrededor del mundo donde se determinan algunos puntos importantes para lograr la ciber resiliencia de manera más efectiva, los cuales presentamos con detalle a continuación.

Apoyo de los ejecutivos.

Las organizaciones que tienen el apoyo de los ejecutivos en la organización para los planes de seguridad demuestran ser un 39% más resilientes ante los incidentes, es importante hacer saber a los ejecutivos que los planes de seguridad no son un gasto sino una inversión, recuperarse de un incidente no solo puede afectar los ingresos, sino también la imagen de la organización.

Poca cultura de seguridad.

Aquellas organizaciones en las cuales la seguridad es parte de la cultura tienen un nivel de resiliencia 46% más alto que aquellas que no lo tienen, recordar que los incidentes se pueden dar no solo mediante los sistemas sino también por los empleados e incluso los ejecutivos, es importante dejar bien claro desde el inicio el porqué es importante la seguridad y como un incidente puede afectar los procesos de la organización, ya sea que estos se originen mediante el correo electrónico, la ingeniería social o un sistema desactualizado, una acción puede hacer la diferencia.

Tener el personal suficiente.

Nadie quiere contratar demasiado personal para un mismo puesto o área, pero es mucho más común ver a una sola persona desempeñar varios cargos, esto no solo afecta el rendimiento o eficiencia de una persona sino también de los procesos, CISCO en su reporte hace mención que tener personal adicional al necesario hace una diferencia de 15% en la resiliencia ante un incidente en una organización, la diferencia sería mucho mayor cuando no se tiene el personal suficiente en el área de seguridad y aún más amplia la diferencia cuando ni siquiera se tiene el personal dedicado a esa área.

Una opción es tercerizar el servicio y contratar una empresa que se encargue de la gestión de estos aspectos, así como dar consultoría y soporte con respecto a los temas de seguridad informática.

Infraestructuras complejas.

Sin importar el tamaño del equipo con el que se trabaje, tener una gestión compleja de la infraestructura puede entorpecer y/o ralentizar los

procesos, simplificar el manejo de los activos de infraestructura sin importar que esta sea en sitio, en la nube o hibrida puede mejorar la resiliencia en un 15%, es muy común ver la concepción que una vez implementada la solución esta va a funcionar de forma continua y desatendida, pueden pasar años hasta sin que se piense en un mantenimiento y en algunos casos el personal es diferente al que se encontraba presente al momento de la implementación y hay poca documentación o no existe, lo cual va aumentando el nivel de complejidad con el paso del tiempo.

Pocas capacidades de detección y respuesta.

Si no se tiene una vista sobre los activos que se tienen, no sabes su estado y no sabes cómo protegerlos, esto hace que se reduzca la resiliencia hasta un 45%, actualmente empiezan a surgir los sistemas de detección y respuesta extendida o XDR por sus siglas en inglés, los cuales ya no solamente aplican a equipos individuales como los sistemas de detección y respuesta de endpoints o EDR, sea cual sea la solución a escoger debe ser una que permita tener una visión del estado de los sistemas, el ideal siempre es abarcar todos los sistemas, pero en caso de no poder hacerlo se recomienda hacer un análisis.

Microsoft en su reporte de defensa digital 2022, marca la ciber resiliencia como un punto importante para la gestión de la seguridad dentro de las organizaciones en esta era de rápido crecimiento y digitalización, así como se crean sistemas, se crean amenazas y no hay suficientes recursos para cubrir todas las posibilidades, por esto la seguridad no debe depender de un solo sistema o un área de la organización, debe ser parte de la cultura, parte del día a día de todos los involucrados, dentro y fuera de la organización, desde los ejecutivos hasta el personal que cuida la entrada, todos deben ser conscientes del por qué es importante la seguridad y por qué son así los procesos y los riesgos y consecuencias que pueden existir al no cumplir.

¡NUNCA PIERDAS TU PRECIADO TRABAJO!

Tu solución integral para la protección de sitios web.

Eliminación de malware

Servidores de ensayo

Migración de sitios web

Actualizaciones automáticas de complementos de WordPress

API con todas las funciones

Copia de seguridad de correo electrónico

CodeGuard

NOISE
CIBERSEGURIDAD

Servicios de Seguridad de la Información y Adiestramiento Profesional
informacion@noise-sv.com / ventas@noise-sv.com
www.noise-sv.com