Número 111 | Febrero 2026

NTT DATA

Radar

El magazine de ciberseguridad

La ciberseguridad empieza, y termina, en las personas

Por Francisco Javier García Lorente

Durante años, la ciberseguridad ha sido tratada como un problema eminentemente tecnológico. *Firewalls* más robustos, herramientas de detección más sofisticadas o inteligencia artificial aplicada a la monitorización de amenazas. Todo eso es necesario. Todo eso es valioso. Pero no es suficiente. La realidad, respaldada por datos y por experiencia, es contundente: la mayoría de los incidentes de seguridad siguen teniendo un origen humano. No por mala fe, sino por desconocimiento, exceso de confianza o simples hábitos mal adquiridos.

Aquí es donde entra en juego un concepto clave que muchas organizaciones aún subestiman: la cultura de ciberseguridad. Y, más concretamente, el papel del liderazgo humano como motor de esa cultura.

Hablar de cibercultura no es hablar de normas colgadas en un portal corporativo ni de formaciones obligatorias que se olvidan al cerrar la ventana del navegador. Hablar de cultura es hablar de comportamientos repetidos, de decisiones cotidianas, de actitudes ante el riesgo. Y la cultura, nos guste o no, se modela desde arriba.

El liderazgo como ejemplo: lo que se hace pesa más que lo que se dice

Las organizaciones no cambian porque se les envíe un correo. Cambian cuando sus líderes actúan de forma coherente y visible. En ciberseguridad esto es especialmente crítico. Un directivo que comparte contraseñas “por agilidad”, que evita el doble factor “porque es incómodo” o que minimiza un incidente porque “no ha pasado nada”, está enviando un mensaje claro al resto de la organización: la seguridad es secundaria.

Por el contrario, un liderazgo que integra la ciberseguridad en su toma de decisiones, que pregunta, que se interesa, que respeta los procesos y que habla abiertamente de riesgos y aprendizajes, genera un efecto multiplicador. No hace falta que los líderes sean expertos técnicos. Hace falta que sean conscientes de su influencia.

La cultura no se impone. Se contagia.

Uno de los errores más habituales en los programas de ciberseguridad es tratar a los empleados como el “eslabón débil”. Esa narrativa, además de injusta, es contraproducente. Las personas no son el problema; son la solución, siempre que se les dé el contexto, las herramientas y el respaldo adecuados.

Aquí el liderazgo vuelve a ser clave. Un liderazgo que fomenta una cultura del miedo —al error, a la sanción, a “meter la pata”— provoca silencio. Y el silencio, en ciberseguridad, es letal.

Los incidentes no se reportan, los correos sospechosos se ignoran y los errores se esconden hasta que ya es demasiado tarde.

Un liderazgo humano, por el contrario, normaliza el error como parte del aprendizaje, promueve la notificación temprana y reconoce las buenas prácticas. Convierte a los empleados en sensores activos de riesgo, no en usuarios pasivos de normas.

La ciberseguridad como valor, no como freno

Otro reto cultural importante es la percepción de la ciberseguridad como un obstáculo para el negocio. “Esto ralentiza”, “esto complica”, “esto no es práctico”. Cuando ese discurso cala, la seguridad se vive como una imposición externa.

El liderazgo tiene la responsabilidad de reencuadrar el mensaje: la ciberseguridad no frena el negocio, lo protege y lo hace sostenible. No es un coste, es una inversión en confianza, reputación y continuidad. En un entorno donde los clientes, los socios y los reguladores exigen cada vez más garantías, la seguridad deja de ser opcional. Cuando los líderes integran este enfoque en su discurso estratégico, la organización empieza a entender que trabajar de forma segura es trabajar correctamente.

Liderazgo humano en un entorno digital complejo

Vivimos en un contexto de hiperconectividad, trabajo híbrido, cadenas de suministro digitales y amenazas cada vez más sofisticadas. Pretender controlar este entorno solo con tecnología es una ilusión peligrosa. La variable humana es inevitable, y precisamente por eso debe ser gestionada con inteligencia.

El liderazgo humano en ciberseguridad implica empatía, comunicación clara y coherencia. Implica adaptar los mensajes a distintos perfiles, entender las presiones reales del día a día y diseñar medidas de seguridad que acompañen al usuario, no que lo enfrenten al sistema. La tecnología protege y el liderazgo alinea.

Formación continua, no eventos puntuales

Una cultura sólida no se construye con campañas aisladas. Se construye con constancia. Aquí el liderazgo vuelve a marcar la diferencia: cuando la formación en ciberseguridad es percibida como algo estratégico, recurrente y alineado con la realidad del negocio, deja de ser una obligación para convertirse en una herramienta útil.

Los líderes deben impulsar una formación viva, práctica y contextualizada, que evolucione con las amenazas y con la organización. No se trata de saberlo todo, sino de saber reaccionar.

Conclusión: liderar es proteger

En última instancia, hablar de cultura de ciberseguridad y liderazgo es hablar de responsabilidad. La ciberseguridad no es solo una cuestión de sistemas; es una cuestión de personas, decisiones y valores. Y los valores se lideran.

Las organizaciones que entienden esto no buscan culpables tras un incidente, buscan aprendizajes. No confían ciegamente en la tecnología, confían en sus equipos. No delegan la seguridad únicamente en un departamento, la integran en su ADN. Porque en el mundo digital actual, liderar también es proteger. Y proteger empieza por las personas.

Francisco J. Garcia Lorente
Cybersecurity Project Manager

Shai-Hulud 2.0: el día en que el gusano entendió la cadena completa

Cibercrónica por Leire Cubo Arce

Cerramos el año con un mes de diciembre que, una vez más, ha demostrado ser uno de los periodos más activos en el panorama de la ciberseguridad. Mientras muchas organizaciones reducen su actividad debido a las vacaciones y a una menor disponibilidad de personal, los ciberdelincuentes aprovechan este contexto para intensificar campañas que explotan tanto vulnerabilidades técnicas como la confianza de los usuarios.

Uno de los acontecimientos más relevantes del mes ha sido la divulgación de una vulnerabilidad crítica que afecta a MongoDB, identificada como CVE-2025-14847 y conocida como MongoBleed. Este fallo permite a los atacantes extraer información sensible de bases de datos afectadas sin necesidad de autenticación, lo que supone un riesgo significativo para las organizaciones que utilizan instancias de MongoDB expuestas o mal configuradas. Investigadores de seguridad han confirmado intentos de explotación activa poco después de su publicación, reforzando la necesidad de aplicar parches con rapidez y de reforzar los controles de acceso a las infraestructuras de datos.

Diciembre también ha estado marcado por el último Patch Tuesday del año de Microsoft, que ha corregido más de cincuenta vulnerabilidades en su ecosistema de productos. Resultan especialmente preocupantes varios fallos de día cero que ya estaban siendo explotados, y que permiten la ejecución remota de código y la elevación de privilegios. Este hecho vuelve a poner de manifiesto cómo las plataformas empresariales más extendidas continúan siendo un objetivo prioritario para los atacantes que buscan un impacto a gran escala.

Más allá de los entornos tradicionales de TI, la tecnología operacional ha seguido ganando protagonismo. A lo largo del mes, la agencia CISA ha publicado múltiples avisos de seguridad que afectan a sistemas de control industrial y dispositivos médicos de fabricantes ampliamente implantados. Estos avisos ponen de relieve la creciente convergencia entre IT y OT y la exposición cada vez mayor de las infraestructuras críticas a las amenazas cibernéticas, especialmente en sectores donde los ciclos de actualización son largos o las paradas operativas resultan difíciles de asumir.

La actividad de *ransomware* no ha mostrado signos de desaceleración a medida que 2025 llega a su fin.

Los grupos de ciberdelincuentes han continuado atacando organizaciones sanitarias, administraciones públicas y proveedores de servicios, en muchos casos aprovechando credenciales previamente robadas o vulnerabilidades en *software* de terceros. Los analistas han observado que numerosos ataques se basan en accesos iniciales obtenidos tiempo atrás, lo que refuerza la idea de que los atacantes actúan con paciencia y aprovechan el momento más oportuno para lanzar sus operaciones.

Al mismo tiempo, los informes de amenazas publicados durante este mes han revelado la magnitud de la exposición de credenciales en foros clandestinos, con miles de millones de nombres de usuario y contraseñas comprometidos circulando en el ecosistema criminal. Esta disponibilidad masiva de credenciales alimenta ataques automatizados como el *credential stuffing* y la toma de control de cuentas, haciendo que la protección de identidades y el uso de autenticación multifactor sean más críticos que nunca.

Las tensiones geopolíticas también se han reflejado en el ciberespacio. Informes publicados a finales de año indican una actividad cibernética sostenida y a gran escala contra infraestructuras críticas en la región de Asia-Pacífico, especialmente contra entidades financieras, hospitales y organismos gubernamentales. Estas campañas se asocian ampliamente con operaciones de ciberespionaje y estrategias de guerra híbrida, lo que demuestra hasta qué punto la ciberseguridad está cada vez más vinculada a la estabilidad global. Las brechas de datos han seguido teniendo un impacto directo sobre los ciudadanos.

La divulgación de un incidente de seguridad que afectó a un importante portal sanitario en Nueva Zelanda reveló la exposición de cientos de miles de documentos médicos sensibles. Este suceso ha reavivado el debate sobre la protección de datos, la supervisión regulatoria y la responsabilidad de los proveedores de servicios digitales en el ámbito de la salud.

Por último, este ha sido un mes de reflexión para la comunidad de ciberseguridad. Diversos análisis publicados hacia el cierre de 2025 han cuestionado si los marcos de seguridad tradicionales están realmente preparados para afrontar las amenazas emergentes asociadas al uso de la inteligencia artificial. Riesgos como el *prompt injection*, el *model poisoning* o la automatización ofensiva basada en IA están impulsando a las organizaciones a replantear el diseño y la aplicación de sus controles de seguridad en un entorno cada vez más apoyado en estas tecnologías.

Con el cierre de 2025, el mes de diciembre deja un mensaje claro: las amenazas cibernéticas continúan evolucionando en los ámbitos técnico, humano y geopolítico. De cara al nuevo año, la vigilancia constante, la aplicación oportuna de parches y la adopción de estrategias de seguridad adaptativas seguirán siendo elementos esenciales para hacer frente a un panorama de amenazas en permanente transformación.

Leire Cubo Arce
Cybersecurity Consultant

Liderazgo y transformación digital: de controlar empleados a capacitar *firewalls* humanos

Artículo por Isabel Lopez y David Contel

Durante sus inicios, y a lo largo de muchos años, la transformación digital se ha entendido como una cuestión básicamente de implementación tecnológica. Los protagonistas eran herramientas, *software*, seguridad y control, solo para mencionar algunos. Sin embargo, para que una transformación digital sea efectiva, y el campo de la ciberseguridad no es ninguna excepción, no empieza en los sistemas, sino en las personas que la llevan a cabo y en la forma en que son lideradas. A lo largo de la historia, en las organizaciones se han ido conceptualizado múltiples estilos de liderazgo que reflejaban estilos personales, pero también sociales, que a su vez reflejaban los estilos de gobierno político y un determinado inconsciente colectivo de la población.

Liderazgo clásico versus liderazgo moderno

Para contrastar las características de los diferentes liderazgos, se podría simplificar la comparativa en dos tipos.

El que podríamos definir como liderazgo clásico. Históricamente, ha funcionado en las organizaciones y sus acciones partían de asumir una cultura corporativa, en la que debía haber una supervisión de los empleados para que cumplieran sus objetivos. La premisa de partida sería la desconfianza implícita, la supervisión directa y la presencia de riesgo de dejación de responsabilidades o procrastinación.

Un desplazamiento de este paradigma a la seguridad podría propiciar medidas como la limitación de accesos, el bloqueo de sitios web, el control de los empleados mediante un SIEM y, en definitiva, el blindar la organización. La seguridad se entendería como un gasto, una casuística técnica e incluso disciplinaria.

En la práctica, los resultados de la transformación digital tendrían profundas carencias, ya que, a pesar de que los sistemas pudieren están securizados, los verdaderos actores de la transformación, que son los usuarios diarios, no desarrollarían una responsabilidad hacia sus prácticas en ciberseguridad. En otras palabras, no se creerían que ellos también son una parte esencial de la solución para evitar incidentes de seguridad, y contribuir así a la transformación de la cultura corporativa, vital para que una transformación digital sea efectiva.

En el lado opuesto del tablero, encontraríamos el liderazgo moderno. Con todos los matices que pudiéramos señalar en cambio, una de sus premisas de partida es que las personas pueden y deben ser un actor activo del cambio. Este paradigma conlleva, de un modo irremediable, que para que los empleados sean verdaderos protagonistas, deben ser capacitados.

Las competencias que sean necesarias adquirir las definiría cada organización conducida por sus culturas corporativas, pero de un modo más ejecutable, desde sus propias políticas. Al margen de la idiosincrasia propia de cada organización, podríamos partir del clásico binomio de las *hard* y *soft skills*.

Por un lado, los usuarios de la organización deben ser formados en buenas prácticas de seguridad de la información, políticas de seguridad, o competencias más técnicas o *ad hoc* en función del perfil de la persona.

Pero, incluso más importante que los conocimientos, son las competencias personales, y hay una en concreto que debe ser fomentada por la organización a todas sus capas: el empoderamiento. Es básico que los empleados no solo sepan cómo reaccionar ante un posible fraude o incidente se seguridad, sino que también piensen que pueden hacerlo, que pueden ayudar a sus compañeros, y lo que es aún más importante, que pueden hacer propuesta desde los conocimientos operativos de sus respectivas áreas para mejorar la seguridad de la organización. En conclusión, que cada empleado interiorice que es parte de la solución.

Este planteamiento llevado a la práctica conduce al escenario positivo en el que una seguridad técnica es complementada, e incluso podría compensar hasta cierto punto vulnerabilidades de seguridad, gracias a este cortafuegos humano que resultan ser los usuarios empoderados.

El impulso del cambio ¿por qué se da?

A pesar de aplicarse transformaciones en las organizaciones, no todos los líderes impulsan el cambio por las mismas razones. En ciberseguridad las causas que llevan a un cambio de calado suelen ser las regulaciones normativas, los ataques recibidos en la propia organización o de la competencia directa, y la voluntad estratégica.

A lo largo de los últimos años, han surgido **cuerpos reguladores** que empujan a las organizaciones a crear sistemas de gestión de la seguridad de la información (LPIC, NISD o diversas ISOs). Estas regulaciones obligan a las empresas a implementar cambios que desde la perspectiva de las capas ejecutivas de la empresa podría concebirse como un gasto. En cualquier caso, este detonante externo ha sido un motor para estas transformaciones, aunque con muchos matices.

En español existe una expresión popular que puede aplicarse en los escenarios de ciberseguridad: "cuando veas las barbas de tu vecino cortar, pon la tuyas a remojar". El libre mercado por sistema lleva a las empresas a monitorizar qué hace su inmediata competencia.

Este seguimiento no solo se centra en sus productos, estrategias comerciales o sinergias en el mercado; la **competencia directa** suele ser el espejo de aquello de lo que se podría llegar a ser víctima en algún momento. Un ciberataque es una realidad muy plausible, pero no solo por las consecuencias operativas, sino también por posibles sanciones de los reguladores. Esto acaba siendo a la práctica un gran elemento motivador para el cambio, aunque también con matices.

Ahora bien, el verdadero motivo que lleva a una verdadera transformación es la elección estratégica. En otras palabras, cuando los ejecutivos y lideres de las organizaciones ven la gestión de la seguridad de la información no solo como una inversión, sino también como una oportunidad de marcar una diferencia, proteger la organización y ser un ejemplo como marca en el mercado. Este impulsor interno es el que realmente puede llevar el cambio a todas las capas de la organización, ya que el compromiso de la jerarquía es clave para la eficacia de cualquier acción que se pretenda implementar.

El rol del líder en la transformación digital

Los mandos intermedios son una clave esencial en cualquier la transformación digital, ya que son los que despliegan de facto los cambios en la operativa.

Las mismas bases del liderazgo que hemos comentado anteriormente se aplican en este escalafón de la jerarquía.

No solo depende de ellos el cumplimiento de los objetivos operativos, también el modo en que se llevan a término. Un liderazgo clásico causa dependencia de las instrucciones del mando. Sin embargo, una perspectiva más actual, en la que se ceden no solo competencias, sino capacidad de decisión e iniciativa a los miembros del equipo, permite un despliegue más efectivo, al hacerse estos usuarios responsables de la implementación. Por otro lado, los mandos intermedios son un altavoz de las políticas o nuevas iniciativas de la organización, incluso más efectivo que un área de comunicación.

Conclusión

El liderazgo ha evolucionado con el tiempo para adaptarse a las nuevas realidades del mundo. Sin embargo, el modo de llevarlo a cabo depende de variables culturales, personales y experiencia profesional.

Todo ello indica que las organizaciones y equipos que se conducen de una manera hoy en día variarán en un futuro. Pero al margen de un estilo u otro, lo que está fuera de dudas es que la implicación de todos los usuarios de una organización en un proceso de transformación asegura unos mejores resultados.

Isabel Lopez
Cybersecurity Consultant

David Contel
Cybersecurity Expert Consultant

El camino hacia arriba y hacia abajo es uno y el mismo: ciberseguridad, náutica y liderazgo.

Artículo por Jorge Ortí Navarro

Víctor López Barrantes, Country Manager de NTT DATA Spain, compartió en comunicación corporativa del pasado mes de abril de 2025 que un liderazgo inspirador es esencial para nuestro futuro. En esta misma línea, Abhijit Dubei, Presidente y CEO de NTT DATA, Inc., expresó que el liderazgo no se limita a títulos ni puestos, sino que debemos comprometernos activamente y asumir la responsabilidad por el futuro que construimos, estar listos cada día para inspirar, empoderar y cuidar y nos anima a todos a ser líderes, sea cual sea nuestro rol.

Así, en un mundo como el de la ciberseguridad, donde el desarrollo de nuevas amenazas está a la orden del día y donde pocas son las certidumbres que abrigamos, las organizaciones necesitan más que nunca a líderes capaces de ofrecer dirección y equilibrio sin frenar el progreso.

Puesto que de preguntas y dudas trata el mundo ciber, cabe plantear: ¿cómo instaurar un modelo de liderazgo capaz de impulsar una cultura de seguridad consciente, estable y, sobre todo, capaz de avanzar en un entorno de amenazas en constante cambio?

Los clásicos ya nos enseñaron que el camino hacia arriba y hacia abajo es uno y el mismo. Tomando esta enseñanza por bandera, hemos encontrado la respuesta a esta pregunta donde menos cabria esperarla: en el arte de la navegación.

Empecemos por el principio: los barcos. Dice la RAE que la "vela" es aquella pieza de lona u otro material que se amarra a las vergas para recibir el viento e impulsar la nave. En segundo lugar, afirma que el "ancla" es aquel instrumento de hierro formado por una barra de la que salen unos ganchos, que, unido a una cadena, se lanza al fondo del agua para sujetar la embarcación. Finalmente, la "orza" es aquella pieza que aumenta el calado del barco y procura aportar mayor estabilidad y mejor gobierno para ceñir.

En este sentido, Jesús Terrés publicó el artículo *Ser orza y no ancla* el 5 de marzo de 2022, en el que distinguía tres clases de personas: primero, la "persona vela"; aquella que no duda, que es ímpetu, no tiene miedo a la aventura ni a pasarse de frenada, ni a descarrilar. No le importa empezar la noche en Valencia y terminarla en la discoteca berlinesa Berghain.

Un "vela" decide por puro sentimiento, sin raciocinio alguno. Es pasional, busca lo inesperado; y por ello, no impedirá nunca ir a la deriva, porque su misma esencia es estar a la deriva.

Dejarse llevar, en definitiva, por impulsos y ser incapaz de frenar a tiempo, terminando varado en puertos desafortunados.

La "persona ancla", en cambio, es aquella que no deja avanzar. Como explica Jesús en su artículo, cuando hablamos de personas que son anclas lo definimos como un lastre, algo o alguien inmóvil que ni se mueve ni te deja avanzar. Se anclan a una roca, a un fondo arenoso que no permite que el barco avance. Puede ser, incluso, que si está echada el ancla mientras sopla un viento inclemente, su fuerza termine quebrando el propio barco precisamente porque el ancla lo mantiene sujeto.

En cambio, la "persona orza" es todo lo contrario. No frena, como el ancla. No impide que se llegue a Berlín. La orza únicamente da estabilidad. Y no en un sentido negativo. Lo estable es aquello que permite avanzar, que permite que nada se frene y, al tiempo, evita que se salga herido por las inclemencias del temporal.

Quizá es esto lo que la náutica y el mar tiene para nosotros: quizá la estabilidad sea la mayor cualidad que pueda haber en una persona y, por extensión, en un líder. Personas a las que llamamos para buscar lo bueno y compartir lo malo, porque es en su estabilidad donde encontramos una calma o, tal vez, algo que todos en algún momento buscamos: un guía.

Un referente que nos permite ir a toda velocidad por los siete mares contra viento y marea y no volcar. No ahogarnos en el caos que en ocasiones encontramos en el mundo de la ciberseguridad.

El "orza" nunca impedirá crecer, avanzar, ser algo diferente, evolucionar. Prestará apoyo a quien lo necesite, se preocupará por sus necesidades y sobre todo y ante todo, siempre con la seguridad de que, en esos cambios, en esas aventuras, en esos proyectos imposibles, no terminaremos varados en una isla desierta o en el fondo del mar; sino que siempre, incluso en el peor de los temporales, con galernas u olas kilométricas, se llegará a puerto seguro.

Es este el líder al que Abhijit Dubei se refiere: aquel capaz de dar la estabilidad necesaria para pensar, recapacitar y seguir luchando. El “orza” no es “vela”, pero nos permite correr con la seguridad de no volcar. Es una pieza que nadie conoce, que puede pasar inadvertida y, no obstante, sin ella el velero estaría destinado a estar siempre a la deriva o anclado. Sustento, apoyo constante, alegría por los triunfos. El impulso sensato para continuar trabajando cada día.

En palabras del ya mencionado Jesús Terrés:

Ser orza y no ancla; tratar de hacer mejores a las personas que quieres (y nunca frenarlas, ser abono y no techo, camino y no fango. Aguantar (juntos) las mareas, poner las cosas fáciles, dejar ser, abiertas las ventanas de par en par, saberte cobijada pero nunca presa, que mi mundo sea tu red, que puedas dejarte caer: ese será mi triunfo [...]. Ser tu orza y no tu ancla.

El camino hacia arriba y hacia abajo es uno y el mismo. Quizá la náutica y la ciberseguridad sean uno y el mismo. Quizá ambas necesiten los mismos líderes. La misma estabilidad. Seamos, pues, orzas que sustenten el entorno en el que trabajamos cada día, y del que todos podamos llegar a sentirnos orgullosos de formar parte.
.

Jorge Ortí Navarro
Cybersecurity Expert Consultant

Tendencias clave de ciberseguridad en 2026

Tendencias por Diego Turiegano de las Heras

En 2026, la ciberseguridad estará marcada por un cambio muy claro en la forma en la que se producen y se defienden los ataques digitales. El avance de la inteligencia artificial generativa, el uso cada vez más realista de los *deepfakes* y la automatización del cibercrimen harán que el panorama sea más complejo y difícil de controlar. Las amenazas ya no dependerán tanto de conocimientos técnicos avanzados, sino de herramientas cada vez más accesibles que permiten lanzar ataques sofisticados con poco esfuerzo. Esto obligará a empresas y usuarios a replantearse cómo se protegen en un entorno donde lo digital forma parte de casi todas las actividades diarias.

La inteligencia artificial tendrá un papel clave y contradictorio. Por un lado, ayudará a mejorar la ciberseguridad, ya que permitirá detectar amenazas con mayor rapidez, analizar grandes volúmenes de datos y apoyar a los equipos de seguridad en la toma de decisiones.

Por otro, será una herramienta muy potente para los atacantes, que la utilizarán para automatizar tareas, crear mensajes más creíbles y adaptar los ataques a cada víctima. Este doble uso de la IA hará que la diferencia entre ataque y defensa sea cada vez más pequeña y que el nivel general de riesgo aumente.

Uno de los aspectos más preocupantes será el uso de *deepfakes* como herramienta de fraude. En 2026, estos contenidos falsos ya no serán algo puntual, sino que se utilizarán de forma habitual para suplantar identidades y engañar tanto a personas como a organizaciones.

Las falsificaciones de voz, en particular, serán cada vez más realistas y fáciles de crear, lo que facilitará estafas dirigidas, como llamadas falsas haciéndose pasar por directivos o compañeros de trabajo. Además, la falta de sistemas fiables para identificar contenido generado por inteligencia artificial hará que detectar estos engaños sea todavía más complicado.

También empezarán a ganar importancia los *deepfakes* en tiempo real, capaces de modificar la imagen o la voz durante una vídeollamada. Aunque actualmente requieren cierta complejidad técnica, su evolución constante permitirá que se utilicen en ataques más directos, especialmente en entornos profesionales donde existe un alto nivel de confianza en la comunicación visual y por voz.

Esto pondrá en duda métodos tradicionales de verificación basados simplemente en “reconocer” a la persona que está al otro lado de la pantalla. La automatización del cibercrimen será otro de los grandes cambios.

En 2026, la inteligencia artificial se utilizará en todas las fases de un ataque, desde la creación de *malware* hasta la búsqueda de vulnerabilidades o la distribución de *software* malicioso.

Esto permitirá lanzar ataques más rápidos y a mayor escala, reduciendo el tiempo del que disponen los equipos de seguridad para reaccionar.

Además, el uso de modelos de IA de código abierto, con menos mecanismos de control, facilitará que estas tecnologías se utilicen tanto con fines legítimos como delictivos, complicando el análisis y la atribución de los ataques.

A pesar de todos estos avances tecnológicos, el factor humano seguirá siendo uno de los principales puntos débiles.

El robo de credenciales continuará siendo una de las formas más efectivas de acceder a los sistemas, sobre todo porque muchas personas siguen utilizando contraseñas débiles, repitiéndolas en varios servicios o prescindiendo de la autenticación multifactor.

Los atacantes aprovecharán esta situación mediante técnicas de ingeniería social cada vez más elaboradas, diseñadas para engañar al usuario y hacerle ejecutar acciones que aparentan ser legítimas.

El *ransomware* tampoco desaparecerá. Al contrario, en 2026 será más frecuente y más rápido. Los modelos de ataque como servicio permitirán que personas con pocos conocimientos técnicos puedan lanzar ataques complejos utilizando herramientas ya preparadas.

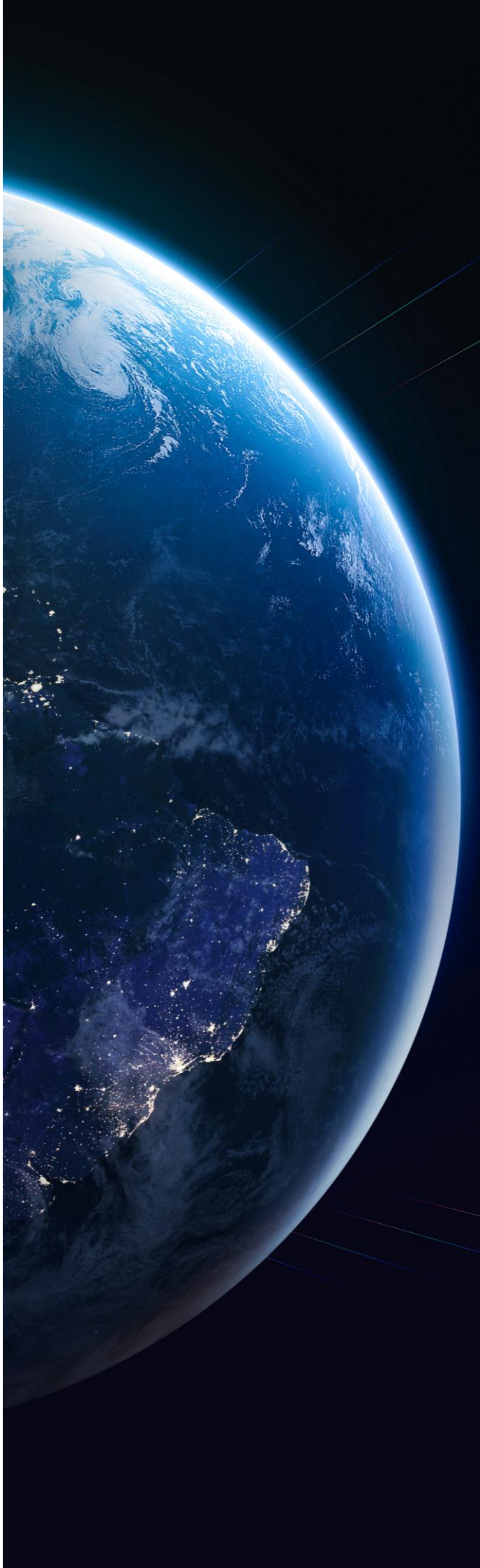
La inteligencia artificial ayudará a automatizar procesos como el cifrado de datos, la exfiltración de información o incluso la negociación del rescate, lo que reducirá el margen de reacción de las víctimas y aumentará el impacto de los ataques.

Por último, la adopción masiva de inteligencia artificial en las empresas traerá nuevos riesgos relacionados con la cadena de suministro digital.

Muchas soluciones se implantarán sin un análisis de seguridad suficiente, incorporando dependencias y posibles vulnerabilidades. Al mismo tiempo, el uso malicioso de la IA seguirá creciendo, con campañas de *phishing* más personalizadas, *bots* más eficaces para el fraude y los primeros casos de *malware* generado con ayuda de estas tecnologías.

En este contexto, el gran reto de 2026 será encontrar un equilibrio entre aprovechar las ventajas de la inteligencia artificial y controlar los riesgos que introduce, apostando por la prevención, la formación y una gestión más consciente del riesgo.

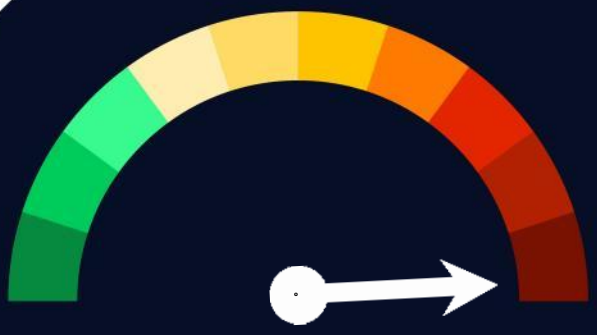
Diego Turiegano de las Heras
Cybersecurity Consultant



Vulnerabilidades

Vulnerabilidad crítica en n8n

Fecha: 26 de diciembre de 2025
CVE: CVE-2025-68668



CVSS: 9.9

CRÍTICA

Descripción

Se ha detectado la vulnerabilidad crítica **CVE-2025-68668** en n8n, una plataforma de automatización de flujos de trabajo de código abierto.

Esta vulnerabilidad permite a usuarios autenticados ejecutar comandos arbitrarios en el sistema subyacente. El fallo se debe a un problema en los mecanismos de protección dentro del *Python Code Node,* lo que posibilita escapar del entorno aislado y ejecutar código con los mismos privilegios que el proceso de n8n.

Aunque requiere autenticación y permisos para crear o modificar flujos, se considera un riesgo elevado por la posibilidad de ejecución de comandos en el *host*.

Solución

Se recomienda actualizar inmediatamente a las versiones con parches oficiales de n8n:

- Versión 2.0.0 o superior.

Como mitigación temporal, se recomienda:

- Deshabilitar el *Code Node* mediante la variable NODES_EXCLUDE: "[\"n8n-nodes-base.code\"]“.
- Desactivar soporte python en el nodo con N8N_PYTHON_ENABLED=false.

Productos afectados

Las versiones vulnerables son:

- De la versión 1.0.0 hasta las anteriores a la versión 2.0.0.

Referencias

- nvd.nist.gov
- thehackernews.com

TLP:WHITE

Vulnerabilidades

Vulnerabilidad crítica en *routers* D-Link DSL

Fecha: 5 de enero de 2026
CVE: CVE-2026-0625

CVSS: 9.3

CRÍTICA

Descripción

Se ha identificado una vulnerabilidad crítica (**CVE-2026-0625**) de ejecución remota de código que afecta a varios *routers* D-Link DSL antiguos ya fuera de soporte.

El fallo se debe a una inyección de comandos en el *endpoint* de configuración DNS (dnscfg.cgi), que permite a un atacante remoto y no autenticado ejecutar comandos con privilegios del sistema.

Está vulnerabilidad está siendo explotada activamente, pudiendo derivar en control total del *router*, secuestro de DNS, espionaje de tráfico o integración en *botnets*.

Solución

No existe parche oficial para la mayoría de los modelos afectados.

Se recomienda:

- Sustituir los dispositivos vulnerables.
- Deshabilitar administración remota.
- Restringir accesos mediante firewall/ACL.

Productos afectados

Routers D-Link DSL (modelos EoL), incluyendo:

- DSL-2640B
- DSL-2740R
- DSL-2780B
- DSL-526B

Referencias

- incibe.es
- thehackernews.com

TLP:WHITE

IBM corrige una vulnerabilidad crítica de omisión de autenticación

Fecha: 31 de diciembre de 2025
CVE: CVE-2025-13915

Crítica

Descripción

IBM ha publicado actualizaciones de seguridad para API Connect con el fin de corregir la vulnerabilidad crítica de omisión de autenticación identificada como **CVE-2025-13915,** con una puntuación CVSS de 9.8.

La falla de seguridad podría permitir al atacante remoto acceder a servicios protegidos sin necesidad de credenciales válidas, comprometiendo la confidencialidad e integridad de las APIs gestionadas por la plataforma.

IBM ha indicado que la vulnerabilidad puede ser explotada de forma remota y sin interacción del usuario, lo que incrementa significativamente el riesgo para entornos empresariales expuestos a Internet. Por ello, se recomienda aplicar cuanto antes las actualizaciones de seguridad.

Productos afectados

Las versiones vulnerables de IBM API Connect son:

- Versiones de la 10.0.8.0 a 10.0.8.5.
- Versión 10.0.11.0.

Solución

Se recomienda:

- Aplicar inmediatamente los parches y correcciones proporcionados por IBM (descargar e instalar la actualización disponible para API Conect desde Fix Central según la versión afectada).

Referencias

- thehackernews.com
- incibe.es

TLP:WHITE

OWASP Core Rule Set corrige una vulnerabilidad crítica de bypass de seguridad

Fecha: 7 de enero de 2026
CVE: CVE-2026-21876

Crítica

Descripción

Se ha identificado una vulnerabilidad crítica en OWASP *Core Rule Set* (CRS), el conjunto de reglas más utilizado en Web Application Firewalls (WAF) como ModSecurity.

El fallo se encuentra en el procesamiento de peticiones *multipart*, lo que permite a un atacante evadir las reglas de seguridad mediante solicitudes especialmente manipuladas. Esta evasión puede permitir que cargas maliciosas (como inyecciones SQL, XSS u otros ataques web) no sean detectadas ni bloqueadas por el WAF.

Aunque no provoca directamente ejecución de código, la vulnerabilidad reduce significativamente la capacidad defensiva del WAF, facilitando ataques de alto impacto contra aplicaciones web protegidas.

Productos afectados

Los productos afectados por esta vulnerabilidad incluyen:

- OWASP Core Rule Set (CRS).
- Versiones anteriores a 4.22.0 (rama 4.x).
- Versiones anteriores a 3.3.8 (rama 3.x).

Cualquier WAF que integre estas versiones del CRS.

Solución

Se recomienda:

- Actualizar a OWASP CRS versión 4.22.0 o superiores (rama 4.x).
- Actualizar a OWASP CRS versión 3.3.8 o superiores (rama 3.x).

Referencias

- cvedetails.com
- secalerts.co

Eventos

Cyber Security & Cloud Expo Global 2026
4 - 5 de febrero

Evento internacional de referencia que reúne a líderes tecnológicos, CISOs, arquitectos cloud y responsables de innovación para analizar las grandes tendencias en ciberseguridad y computación en la nube. El congreso pone el foco en amenazas emergentes, seguridad en entornos híbridos y *multicloud*, Zero Trust, IA aplicada a la defensa, cumplimiento normativo y resiliencia digital, combinando ponencias estratégicas, casos reales y una amplia zona expositiva con los principales *vendors* del sector.

Enlace

Hcon
6 - 7 de febrero

H-C0N es una conferencia técnica de ciberseguridad con ADN *hacker*, centrada en investigación avanzada, *hacking* ético, *reverse engineering*, *red teaming*, *blue teaming* y seguridad ofensiva y defensiva. Destaca por su enfoque práctico, charlas profundas sin marketing, *workshops* técnicos y una comunidad muy especializada, convirtiéndose en un punto de encuentro clave para profesionales que viven la ciberseguridad desde dentro, con mentalidad *hands-on* y espíritu de aprendizaje continuo.

Enlace

EspañaSec Cyber Summit 2026
10 - 11 de febrero

EspañaSec Cyber Summit es un congreso de alto nivel orientado a la visión estratégica de la ciberseguridad, dirigido a directivos, CISOs y responsables de riesgo, tecnología y cumplimiento. Aborda la seguridad como un habilitador del negocio, tratando temas como gobernanza, gestión del riesgo, regulación, ciberresiliencia, impacto de la IA y toma de decisiones en entornos complejos, con ponentes de primer nivel y un enfoque claro en liderazgo y estrategia.

Enlace

Congreso Ondata – Informática Forense y Ciberinteligencia
18 de febrero

El Congreso Ondata es una cita consolidada en el ámbito de la informática forense y la ciberinteligencia, orientada a profesionales técnicos, fuerzas de seguridad, analistas y expertos en investigación digital. El evento profundiza en análisis forense, respuesta a incidentes, investigación de cibercrimen, OSINT y *threat intelligence*, combinando rigor técnico, casos reales y un enfoque muy práctico que lo convierte en un referente nacional en estas disciplinas.

Enlace

Recursos

➢ *Checklist* de mejores prácticas

Lista actual de acciones ciberseguridad con enfoque operacional: controles de identidad, actualizaciones críticas, *backups* verificados, *vendor controls*... perfecta como *checklist* para inspecciones rápidas o auditorías internas.

Enlace

➢ Global Cybersecurity Outlook 2025 – Foro Económico Mundial (WEF)

Un informe estratégico y global que examina cómo la ciberseguridad está evolucionando frente a tecnologías emergentes, tensiones geopolíticas y retos de resiliencia. Proporciona datos clave sobre riesgos como la dependencia de las cadenas de suministro, la sofisticación de los ataques y disparidades en capacidades entre organizaciones, con recomendaciones para líderes que deben navegar esta complejidad creciente.

Enlace

➢ GCA Cybersecurity Toolkit (Global Cyber Alliance)

Un kit de herramientas y guías prácticas para evaluar tu postura de seguridad, reforzar controles comunes y acceder a soluciones gratuitas con enfoque claro en defensas básicas recomendadas internacionalmente.

Enlace

NTT DATA

Suscríbete a RADAR
up.nttdata.com/suscribetearadar

Powered by the cybersecurity NTT DATA team

es.nttdata.com