NEWSLETTER

grupobeit.com

BLOG DEL CEO

El cierre del sector tecnológico en el 2026 ¿Qué nos espera para el 2027?

El 2026 ha sido un año definitorio para el sector tecnológico. Por un lado, la Inteligencia Artificial y las soluciones que esta ofrece han abandonado su etapa experimental y se han hecho cada vez más presentes en el día a día de personas y empresas.

EDICIÓN 66

El riesgo de los agentes autónomos generó la necesidad del AI Agent Identity

Cada día, agentes de IA comienzan a actuar por su cuenta de manera tan rápida que los equipos de seguridad humanos no pueden seguirles el paso al monitorearlos y controlarlos, y ese hecho ha abierto importantes brechas de seguridad.

EVENTOS BEIT

Esta semana, el día 3 de noviembre durante un evento clave de colaboración, nos reunimos en una sesión estratégica con dos de nuestros principales clientes para presentar la oferta de soluciones de nuestro aliado helppeople

NOTICIA BEIT



Japón declara emergencia cibernética: una advertencia para las organizaciones de todo el mundo

PARTNERS BEIT

Workshop Proof Point y Sophos

Los días 28 y 29 de octubre tuvimos la oportunidad de asistir a dos workshops de gran importancia, esto junto a Proofpoint y Sophos

Edición 66



El cierre del sector tecnológico en el 2026 ¿Qué nos espera para el 2027?

Por: Elías Cedillo, Fundador y CEO GrupoBeIT

El 2026 ha sido un año definitorio para el sector tecnológico. Por un lado, la Inteligencia Artificial y las soluciones que esta ofrece han abandonado su etapa experimental y se han hecho cada vez más presentes en el día a día de personas y empresas. Por el otro, esto genera nuevos retos y oportunidades que moldearán el 2027 a fin de aprovechar esta tecnología, que poco a poco se vuelve más esencial, de una manera más eficaz y segura.

Uno de los pilares principales para estos cambios será el Cybersecurity as a Service (CSaaS), que ha dejado de lado el enfoque reactivo en busca de consolidar un modelo preventivo. Para ello se prevé que el próximo año se formará una combinación entre IA y automatización, en la que de forma automática se buscarán vulnerabilidades y fallos en el entorno digital de las empresas para solucionarlas antes de que sean explotadas, revolucionando completamente la forma en que se protege nuestra información más valiosa. Asimismo, para evitar posibles brechas de seguridad causadas por los mismos agentes autónomos, se verá un aumento en la adopción de AI (agent identity), que provee a los agentes de una identidad digital única, con privilegios específicos y comprensión contextual que será imprescindible para la protección de datos, puesto que se estima que en 2028 el 25% de las brechas de seguridad en empresas se deberán a agentes de IA mal implementados.

Otro frente tecnológico de suma importancia es el de infraestructura, donde las tendencias para el 2027 llegarán a lugares que antes sólo podíamos concebir en la ciencia ficción con el Wetware as a Service. La computación wetware, que integra cientos de miles de neuronas humanas vivas en una computadora para realizar procesamiento, existe desde 2025 luego de años de pruebas, pero hasta el próximo año se prevé su generalización como servicio. Si bien todavía enfrenta retos como el soporte vital o el filtrado de desechos necesarios para mantener vivas las neuronas, el simple hecho de que se pueda acceder a esta herramienta a través de la nube es un avance tecnológico sin precedentes.

Sin embargo, no todo es brillante para este ramo, puesto que hay que tener presente el consumo desmedido de recursos por parte de la IA, que actualmente ya causa un aumento considerable en los precios de los componentes de memoria, que no disminuirá durante 2027. De la misma forma en que los servidores dedicados a IA aumentarán su demanda energética un 30% anual hasta 2028. Paradójicamente, la adopción tan grande que ha tenido esta tecnología retrasará proyectos de Data Center relacionados con la misma IA, ya que su consumo energético causará cuellos de botella que pondrán una enorme presión en la red. Pero también cabe mencionar el enorme potencial de la IA para, en un futuro, optimizar el consumo energético de manera tan eficiente que pueda prevenir y solucionar crisis relacionadas con la energía. Habrá que ver de qué manera se solucionan estos retos tan grandes.

En cuanto a los Field Services 2.0, durante el próximo año veremos el desarrollo e implementación de agentes de IA autónomos enfocados a la voz, también conocidos como Speech Reasoning Models, disminuyendo el uso de agentes de IA de texto tradicional. Estos agentes serán capaces de comprender contextos e intenciones dentro de una conversación antes de ejecutar una acción, siendo en extremo útiles para servicio al cliente al dar asistencia directa sin necesidad de utilizar nada más que la voz. Al mismo tiempo, se le dará impulso a los World Model, agentes de IA que son capaces de comprender tiempo, espacio e incluso causalidad, lo que les permite predecir y comprender las consecuencias de sus propias decisiones antes de ejecutarlas, mejorando la seguridad en entornos industriales que requieren de maquinaria autónoma en campo.

El crecimiento del mercado será otra consecuencia de las tecnologías aquí listadas, ya se prevé que en 2027 el gasto en TI aumentará un 15% con respecto a este año, alcanzando $7.35 billones de dólares, enfocándose sobre todo en la monetización de las capacidades de la IA, que verá una mayor presencia no sólo en software sino también en infraestructura.

En Grupo BelT estamos a la expectativa de la evolución que tendrá la industria durante el 2027, y estamos seguros de que podremos trabajar a tu lado en la adopción de las nuevas tendencias que revolucionarán la forma en que trabajamos y vivimos. No dudes en acercarte a nosotros para recibir un assessment y llevar tu empresa al siguiente nivel.

Referencias:

- https://www.gartner.com/en/newsroom/press-releases/2026-10-20-gartner-identifies-the-top-strategic-technology-trends-for-2027
- https://iea.blob.core.windows.net/assets/b8a83930-5c77-4da7-b795-270ab6a6c272/EnergyandAI.pdf
- https://www.forbes.com/sites/peterhigh/2026/10/22/gartners-top-10-strategic-technology-trends-for-2027/
- https://www.gartner.com/en/newsroom/press-releases/2026-10-21-gartner-forecasts-worldwide-it-spending-to-grow-15-percent-in-2027-totaling-7-point-35-trillion
- https://www.intelligentliving.co/wetware-computing-living-cells/
- https://www.okta.com/identity-101/what-is-ai-agent-identity/

Edición 66

NEWSLETTER BeIT

El riesgo de los agentes autónomos generó la necesidad del AI Agent Identity

Cada día, agentes de IA comienzan a actuar por su cuenta de manera tan rápida que los equipos de seguridad humanos no pueden seguirles el paso al monitorearlos y controlarlos, y ese hecho ha abierto importantes brechas de seguridad. De acuerdo con Gartner, los incidentes de seguridad empresariales relacionados con agentes de IA con privilegios mal gestionados y poco vigilados alcanzarán un 25% del total de incidentes registrados para 2028. Como medida de prevención para esto, surgió el AI Agent Identity, del que se espera su generalización a lo largo del próximo año.

El IAM (Identity and Access Management) tradicional, que es el marco que define que las personas correctas tengan acceso a los recursos necesarios en tiempo y forma, ya no es suficiente, y esto se debe a la forma misma en la que fue ideado y que se basaba en la predictibilidad: un trabajador humano inicia sesión con sus credenciales y desarrolla sus tareas. Con los agentes de IA, dada la velocidad con la que trabajan, eso no ocurre puesto que operan de forma continua, pueden usar múltiples herramientas en cuestión de segundos, e incluso pueden tercerizar sus credenciales, lo que crea vulnerabilidades en cadena conforme este proceso avanza. Y todo esto ocurre muchas veces sin que la parte humana se entere.

El concepto de AI Agent Identity consiste en dotar a los agentes de una identidad digital única e irrepetible, en la que se engloba qué funciones tienen, quién es el dueño y cuál es su nivel de autorización para trabajar, así como un ciclo de vida para estas credenciales, ya que actualmente al dejarle una tarea a un agente de IA, este puede tercerizar una parte de esa tarea a otro agente y legarle sus mismas herramientas y accesos, y es ahí cuando se crean las vulnerabilidades. Y es que los riesgos no son pocos: uno de los más grandes es que los agentes utilizan credenciales sin supervisión, incluso cuando estas ya han sido comprometidas, y a su vez, conforme van desempeñándose van acumulando accesos y solicitando herramientas que van más allá de lo que originalmente tenían aprobado, siendo esta una acumulación de vulnerabilidades que con el Agent Identity se mitigan enormemente.



De igual manera, esta tecnología no solo hará que las empresas estén más seguras, sino que también protege a los colaboradores: actualmente los agentes de IA actúan por su cuenta en nombre de uno o varios usuarios, con el detalle de que su actividad es indistinguible de la actividad humana, por lo que, en caso de un incidente, no queda claro si la causa fue el agente o la persona, pero con el AI Agent Identity eso se acaba, generando verdadera gobernanza y responsabilidad.

Más que una limitante o un freno a las tareas que delegamos a una IA, el Agent Identity es un perímetro de seguridad que nos permite tener control de lo que hacen nuestros agentes mientras trabajan a toda velocidad, eliminando brechas y vulnerabilidades que, por error o por malicia, pueden ser aprovechadas para acceder a nuestra información y nuestros recursos.

En Grupo BeIT comprendemos que la IA ha llegado para quedarse, y no es para menos, dado que desde su aparición ha cambiado la forma en la que trabajamos. Pero su uso también debe hacerse con responsabilidad, y sobre todo con las herramientas necesarias para vigilarla y prevenir riesgos cuando sea necesario. Por esa razón seguiremos el avance del AI Agent Identity con gran interés.

Contáctanos para una asesoría:

WhatsApp: +52 56 5100 8613
E-mail: admmarketing@buromc.com

Referencias:

- https://www.pingidentity.com/en-us/docs/blogs/ai-agent-identity-enterprise-security-perimeter#:~:text=Create%20a%20unique%20identity%20for%20every%20agent,recognized%20in%20logs%2C%20access%20decisions%2C%20and%20investigations.
- https://www.ibm.com/solutions/agentic-ai-identity-management#:~:text=AI%20agents%20reason%2C%20act%2C%20and%20accumulate%20access,faster%20than%20any%20team%20can%20detect%20it.
- https://www.gartner.com/en/newsroom/press-releases/2026-10-20-gartner-identifies-the-top-strategic-technology-trends-for-2027
- https://idm.net.au/article/0015841-ten-trends-gartner-says-cios-must-explore-2027



Japón declara emergencia cibernética: una advertencia para las organizaciones de todo el mundo

NOTICIA BeIT

La reciente declaración de emergencia cibernética nacional en Japón marca un punto de inflexión en el panorama global de la ciberseguridad. Tras una serie de ataques que afectaron a empresas de sectores críticos, servicios al consumidor e infraestructura de transporte, las autoridades japonesas han reconocido oficialmente la magnitud del riesgo que enfrentan las organizaciones en la era de la Inteligencia Artificial.

Más allá del impacto local, este acontecimiento confirma una tendencia que ya está transformando el entorno de riesgo empresarial: la Inteligencia Artificial está acelerando la capacidad de los atacantes para identificar objetivos, automatizar campañas y escalar operaciones con una velocidad sin precedentes.

Lo que anteriormente requería amplios conocimientos técnicos, recursos significativos o barreras idiomáticas, hoy puede realizarse de forma más rápida, precisa y accesible. Como resultado, organizaciones de cualquier tamaño pueden convertirse en objetivo de ataques cada vez más sofisticados.

Para los líderes empresariales, la principal conclusión es clara: la ciberseguridad debe evolucionar al mismo ritmo que la transformación digital.

Las organizaciones más resilientes serán aquellas que fortalezcan su visibilidad, reduzcan su superficie de exposición, protejan identidades y accesos críticos, y desarrollen capacidades sólidas de detección y respuesta ante incidentes.

La pregunta ya no es si ocurrirá un intento de ataque, sino qué tan preparada está la organización para anticiparlo, contenerlo y mantener la continuidad de sus operaciones.

En Grupo BeIT, junto con Buró MC y Elit Infrastructure Services, continuamos ayudando a nuestros clientes a fortalecer su resiliencia operativa y postura de ciberseguridad frente a un panorama de amenazas cada vez más dinámico y sofisticado.

La experiencia de Japón es un recordatorio de que la preparación, la visibilidad y la capacidad de respuesta se han convertido en factores estratégicos para la continuidad del negocio.

Workshop Proofpoint y Sophos

Los días 28 y 29 de octubre tuvimos la oportunidad de asistir a dos workshops de gran importancia, esto junto a Proofpoint y Sophos, empresas con décadas de experiencia en ciberseguridad y dos de nuestros partners más valiosos.

Es nuestro compromiso el mantener alianzas que crean y fomentan herramientas y prácticas para mantener segura tu data más valiosa. De esa manera nos encargamos de crear entornos digitales más seguros y confiables para cualquier institución que lo necesite.



Grupo BeIT

Sesión Estratégica con helppeople

03 de Noviembre, 2026

Durante un evento clave de colaboración, nos reunimos en una sesión estratégica con dos de nuestros principales clientes para presentar la oferta de soluciones de nuestro aliado **helppeople**. Durante el encuentro, destacamos la integración de sus nuevas herramientas de Inteligencia Artificial, orientadas a potenciar la transformación digital y optimizar la operación diaria de nuestros clientes.





