BUSINESS ALLIANCE FOR SECURE COMMERCE

Cargo Security

PUBLICACIÓN ESPECIALIZADA EN SEGURIDAD DE LA CADENA DE SUMINISTRO INTERNACIONAL

EDICIÓN N° 52 - JULIO 2025

Inteligencia Artificial para una eficaz ciberseguridad en la cadena de suministro

Artículos Especializados

Entrevista:
Carmen Zegarra,
Principal Corporate Counsel de Microsoft

Entrevista:
Oscar Andrade,
Vicepdte. del Directorio de WBO y Pdte. de la Junta Directiva de BASC Guatemala

Artículo:
Nicolás Rocca,
Regional Head Security & Operational Resilience SSA / PE DHL Global Forwarding

www.bascperu.org

Confían en ti, confía en BASC

CONTENIDO

Cargo Security® es una publicación trimestral promovida por la Alianza Empresarial para un Comercio Seguro (BASC por sus siglas en inglés), Asociación Civil sin fines de lucro adscrita a la World BASC Organization Inc. (WBO).

La seguridad cibernética en tiempos de intensos cambios

Sr. Aldo R. Defilippi
Presidente del Directorio
BASC PERÚ

Cada vez más, la ciberseguridad es motivo de interés y preocupación para el mundo de los negocios debido a la persistencia del incremento de los riesgos para la seguridad informática de organizaciones y personas involucradas en el uso de internet y redes sociales. El actual contexto internacional de la geopolítica es el principal factor de preocupación por sus implicancias directas en la economía mundial y simultáneamente, en el estado de los riesgos y las amenazas potenciales que año a año se incrementan.

La historia enseña que los grandes conflictos bélicos generan significativos avances tecnológicos. Después del final de la II Guerra Mundial, las tecnologías de la información y comunicaciones (TIC's) han evolucionado rápidamente, tanto que hoy podemos ver episodios de "guerra cibernética" en la guerra entre Israel e Irán, por ejemplo. El tema es que las herramientas utilizadas hoy podrían ser utilizadas después en el ámbito empresarial también. Llegado el momento, esto planteará un desafío más complejo porque los riesgos serán más sofisticados.

Hace poco, el Foro Económico Mundial afirmó que el 71% de los líderes cibernéticos creen que *"las pequeñas organizaciones ya han llegado a un punto de inflexión crítico en el que ya no pueden protegerse adecuadamente frente a la creciente complejidad de los riesgos cibernéticos"*. En este contexto negativo, en Latinoamérica, solo el 18% de empresarios están seguros de que el país donde operan está bien preparado para responder a incidentes cibernéticos que afecten infraestructuras críticas; una cifra muy baja con relación a Norteamérica, donde el indicador es de 65%.

En un escenario regional, donde las pequeñas empresas se sienten desprotegidas frente a ciberataques, los líderes empresariales están llamados a transmitir conciencia de que sí es posible enfrentar a los ciberataques utilizando la Inteligencia Artificial (IA). Esta herramienta nos permite ser predictivos y preventivos, ya no reactivos. Así, podemos enfrentar la sofisticación de los ciberdelincuentes que utilizan la automatización, la IA y la ingeniería social. Con la IA, los atacantes pueden crear con más facilidad un malware evolutivo (programa malicioso con capacidad de cambiar su código o comportamiento para evadir programas antivirus), automatizar ataques, robar datos de dispositivos corporativos, generar *"deepfakes"* (contenidos digitales manipulados con IA) para fraudes e ingeniería social, etc.

Si decidimos enfrentar la ciberdelincuencia con la IA, la política de seguridad de la organización debe conservar los fundamentos de las mejores prácticas de seguridad. Por ejemplo, fortalecer la cultura de ciberseguridad porque la mayoría de los incidentes se deben a errores humanos, por lo que la concientización y formación permanente de los empleados es ineludible

También la implementación de programas "confianza cero" fundamentado en "nunca confiar, siempre verificar", favorece el combate al riesgo de acceso no autorizado. Además, la "gestión de riesgos de terceros" que comprende el buen manejo del sistema de interconexión segura con proveedores y socios externos, es inevitable.

Ahora, la ciberseguridad es una prioridad crítica para toda organización, por lo que la inversión en tecnologías de seguridad avanzadas, particularmente las impulsadas por IA, es una decisión necesaria.

Tengamos presente que una pequeña empresa puede ser proveedora de una gran corporación, siempre que sus servicios sean seguros y confiables.

En la **Organización Mundial BASC** estamos conscientes de la importancia de la Ciberseguridad, tanto así que en sus Estándares se dedica todo un capítulo a la Seguridad de la Información y permanentemente se realizan cursos, charla, foros sobre la ciberseguridad.

UN ATAQUE CIBERNÉTICO NO AVISA, DESTRUYE.

NO PONGAS EN JUEGO LA SEGURIDAD
DE TU INFORMACIÓN.

BUSINESS ALLIANCE FOR SECURE COMMERCE

**Confían en ti,
confía en BASC**

La Inteligencia Artificial

Esta revolución tecnológica transforma la sociedad humana desde su aparición hace 70 años. Aunque antes fue necesaria la aparición de la computadora, cuyo primer diseño fue hecho en el siglo XIX

El término "inteligencia artificial" (IA) fue mencionado por primera vez en 1956, cuando John McCarthy (1927 – 2011), un científico en computación, expuso en la Conferencia de Dartmouth en New Hampshire, EE. UU., evento en que algunos de los mejores científicos de la época discutieron la posibilidad de crear una máquina que sea capaz de pensar como un ser humano. Aunque las nuevas generaciones podrían dudar de que la computación ya existía en esa fecha del siglo XX, lo cierto es que el diseño de la primera computadora digital automática fue hecho en el siglo XIX por el matemático inglés Charles Babbage (1791–1871). El diseño contenía todos los conceptos esenciales presentes en las que se utiliza actualmente.

Los avances que ha experimentado la IA en los últimos 70 años abrieron nuevos modos de generación de valor para empresas, industrias, individuos y la sociedad en general. Ha adquirido tanta relevancia que está avanzando indefectiblemente en prácticamente todos los aspectos de la vida humana a través de sus aplicaciones que son infinitas.

Definición

El universo científico está de acuerdo en que, desde 1956, cuando se usó por primera vez el término IA, ha surgido un amplio espectro de definiciones. En consecuencia, no existe a la fecha una definición única generalmente aceptada de IA.

En este sentido, por ejemplo, la NASA sostiene que es difícil una definición única y simple de IA porque "las herramientas de IA son capaces de realizar una amplia gama de tareas y resultados." Dicho esto, si se deseara regularlo, por ejemplo, no sería posible porque para ello es necesario definir qué es la IA. Pero, aun cuando se lograra una definición legal, esta diferiría significativamente de las definiciones de otras disciplinas porque son definiciones de trabajo, según afirma Jonas Schuett (A Legal Definition of AI, 2019).

- **Prueba de Turing:** Posiblemente la definición más conocida. En 1,950, Allan Turing propuso una prueba que denominó "juego de imitación". "Se refiere a cualquier computadora que supere la "prueba de Turing", que se refiere a un juego con tres participantes: (1) un humano, (2) una computadora y (3) un juez humano. El juez está separado de los otros participantes. Solo pueden comunicarse por texto. La prueba es superada si el juez humano no puede distinguir eficazmente entre el humano y la computadora.

- En 2007 **John McCarthy** publicó el artículo "¿Qué es la Inteligencia Artificial?" en que define la IA. "Se refiere a la ciencia e ingeniería que crea máquinas inteligentes. "Inteligencia" se refiere a la parte computacional de la capacidad para alcanzar objetivos en el mundo.

- Para la **NASA**, son válidas las siguientes definiciones:
  - "Cualquier sistema artificial que realiza tareas en circunstancias variables e impredecibles sin supervisión humana significativa, o que puede aprender de la experiencia y mejorar su rendimiento al exponerse a conjuntos de datos."
  - "Un sistema artificial desarrollado en software, hardware físico u otro contexto que resuelve tareas que requieren percepción, cognición, planificación, aprendizaje, comunicación o acción física similares a las humanas."
  - "Un sistema artificial diseñado para pensar o actuar como un humano, incluyendo arquitecturas cognitivas y redes neuronales."
  - "Un conjunto de técnicas, incluido el aprendizaje automático, diseñado para aproximarse a una tarea cognitiva. Un sistema artificial diseñado para actuar racionalmente, incluido un agente de software inteligente o un robot encarnado que logra objetivos utilizando la percepción, la planificación, el razonamiento, el aprendizaje, la comunicación, la toma de decisiones y la acción."

- **Google**: "La IA es un campo de la ciencia relacionado con la creación de computadoras y máquinas que pueden razonar, aprender y actuar de una manera que normalmente requeriría inteligencia humana o que involucra datos cuya escala excede lo que los humanos pueden analizar."

- **IBM**: "Es una tecnología que permite a las computadoras y máquinas simular el aprendizaje, la comprensión, la resolución de problemas, la toma de decisiones, la creatividad y la autonomía humanas." Para esta empresa "las aplicaciones y dispositivos equipados con IA pueden ver e identificar objetos. Pueden comprender y responder al lenguaje humano. Pueden aprender de nueva información y experiencias. Pueden hacer recomendaciones detalladas a usuarios y expertos. Pueden actuar de forma independiente, eliminando la necesidad de inteligencia o intervención humana (ejemplo, el auto autónomo)."

Según la IBM, desde el 2024 la mayoría de los investigadores, profesionales y titulares relacionados con la IA están centrándose en los avances en **IA generativa *(IA gen)***, una tecnología capaz de crear texto, imágenes, vídeos y otros contenidos originales. Para comprender plenamente la IA generativa, es importante comprender primero las tecnologías en las que se basan sus herramientas: Machine Learning (*ML*) y Deep Learning (*DL*).

Para esta compañía, una forma sencilla de pensar en la IA es como una serie de conceptos anidados o derivados que han surgido a lo largo de más de 70 años.

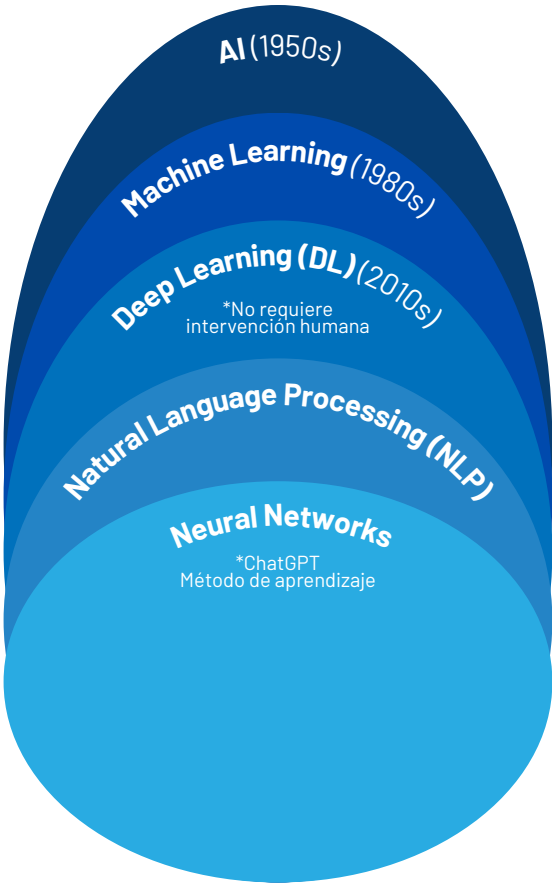
En efecto, es posible esquematizar la evolución de la IA en principales áreas de desarrollo como figura en el siguiente gráfico donde se distingue a la IA como el campo madre y algunas otras herramientas que son utilizadas.

- **Machine Learning**: un campo de la IA enfocado en permitir que los sistemas aprendan de los datos sin una programación explícita. Es decir, dotar a las computadoras la capacidad de aprender y mejorar basado en la experiencia, como los humanos. Pueden analizar datos, identificar patrones y realizar predicciones o tomar decisiones basadas en lo aprendido.

- **Deep Learning (DL)**: como método de trabajo en IA es un subconjunto de Machine Learning que implica redes neuronales con múltiples capas.

- **Natural language processing**: es un subconjunto del Deep Learning que entrena a las computadoras para comprender, interpretar y manipular el lenguaje humano.

- **Neural Networks**: es un método para entrenar a las computadoras a procesar datos de una manera inspirada en el cerebro humano, utilizando una estructura interconectada y en capas inspirada en las neuronas.



Beneficios

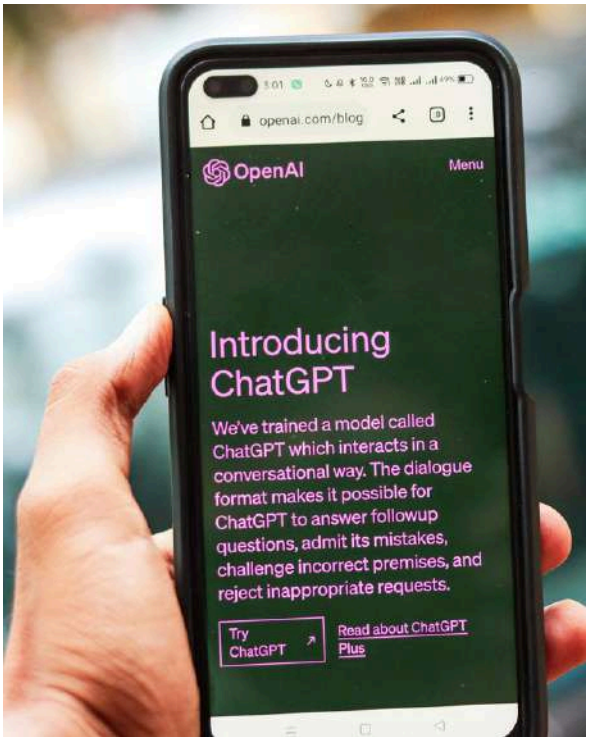
Sin duda, la IA ofrece innumerables beneficios en la economía y la vida diaria de empresas y personas mediante diversas aplicaciones. Las más comunes incluyen:

- Automatización de tareas repetitivas.
- Mayor y más rápida comprensión de los datos.
- Mejor toma de decisiones.
- Menos errores humanos.
- Disponibilidad 24/7.
- Reducción de riesgos físicos.

Para Google la IA es un campo amplio con muchas disciplinas como la informática, el análisis y la estadística de datos, la ingeniería de hardware y software, la lingüística, la neurociencia y hasta la filosofía y la psicología. En el mundo empresarial, a nivel operativo la IA es un conjunto de tecnologías que se basan principalmente en el aprendizaje automático y el aprendizaje profundo que se usan para el análisis de datos, la generación de predicciones y previsiones, la categorización de objetos, el procesamiento de lenguaje natural, las recomendaciones, la recuperación inteligente de datos y mucho más.

Además, es común contar con el uso de sus aplicaciones siguientes:

- Reconocimiento de voz.
- Convertir automáticamente una frase hablada en un texto escrito.
- Reconocimiento de imágenes.
- Identificar y categorizar diversos aspectos de una imagen.



- Traducción, traducir palabras escritas o habladas de un idioma a otro.
- Modelado predictivo.
- Extraer datos para prever resultados específicos con altos niveles de detalle.
- Análisis de datos.
- Encontrar patrones y relaciones en los datos para la inteligencia empresarial.

Uso de la IA en la industria

Las industrias disfrutan el alto potencial de la IA en experiencia, servicio y soporte al cliente.

Pueden implementar **chatbots y asistentes virtuales** para gestionar consultas de clientes, tickets de soporte y más.

Detección de fraude: Mediante Machine Learning y Deep Learning pueden analizar patrones de transacciones e identificar anomalías, como gastos inusuales o ubicaciones de inicio de sesión, que indiquen transacciones fraudulentas.

Marketing personalizado: Los minoristas, bancos y otras empresas pueden usar IA para crear experiencias personalizadas y campañas de marketing para los clientes, mejorar las ventas y evitar la pérdida de clientes. Basándose en datos del historial de compras y comportamientos de los clientes, vía Deep Learning puede recomendar productos y servicios e incluso generar textos personalizados y ofertas especiales para clientes individuales en tiempo real.

Recursos humanos y reclutamiento: Las plataformas de reclutamiento basadas en IA pueden agilizar la contratación mediante la revisión de currículums, la vinculación de los candidatos con las descripciones de puestos e incluso la realización de entrevistas preliminares mediante análisis de video.

Desarrollo y modernización de aplicaciones: Las herramientas de generación de código de IA generativa y las herramientas de automatización pueden agilizar las tareas de codificación repetitivas asociadas con el desarrollo de aplicaciones y acelerar la migración y modernización (reformateo y replanteo) de aplicaciones heredadas a escala.

Mantenimiento predictivo: Los modelos de Machine Learning pueden analizar datos de sensores, dispositivos del Internet de las Cosas (IoT) y Tecnología Operativa (OT) para prever cuándo se requerirá mantenimiento y predecir fallas en los equipos antes de que ocurran. El mantenimiento preventivo basado en IA ayuda a prevenir tiempos de inactividad y le permite anticiparse a los problemas en la cadena de suministro antes de que afecten el resultado final.

“Es inevitable el uso delictivo de la IA, así como es requisito ineludible tomar todo tipo de precauciones para su uso seguro”.

El impacto del uso de la IA genera dos campos: beneficios y perjuicios. El lado de los beneficios está lleno de elogios por capacitar a la humanidad para resolver muchos problemas y necesidades en la vida diaria. También es criticada por el lado negativo, como las consecuencias de la automatización en el mercado laboral (por ejemplo, la preocupación por el desempleo), según afirman Blauth, Gstrein and Zwitter (Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI, 2022). Estos aspectos positivos y negativos de la tecnología se condicen en el campo de la seguridad, lo cual ha generado la aparición de campos especializados como la ciberseguridad (prácticas de protección contra la perpetración de delitos) y la ciberdelincuencia (prácticas ilícitas en contra de personas y organizaciones). La IA se puede utilizar para mejorar y protegerse, como también para perjudicar y atacar.

La ciberseguridad consiste en proteger las computadoras y otros dispositivos. La mayoría de los ataques se producen a través de Internet y debido a estos ataques las

organizaciones pueden perder muchos recursos. Un ciberataque es cualquier acción intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital de una organización. Los recientes avances tecnológicos han demostrado que un solo ataque podría destruir empresas y negocios. Es más, para muchos investigadores, estos pueden tomar formar en las nuevas formas de terrorismo contra los países (Enhancing Cybersecurity through AI and ML: Strategies, Challenges, and Future Directions, 2024).

Bajo este contexto, las organizaciones deben implementar estrategias que garanticen la protección de su información. La competencia puede atacar a una organización para obtener una ventaja sobre una empresa. Estas consideraciones requieren la aplicación de la ciberseguridad con la finalidad de, por ejemplo, la información confidencial y privada cuenten con medidas adicionales para garantizar el correcto acceso a ella. Este factor garantiza que las personas y las organizaciones estén más seguras.

¿Cuáles son las amenazas de ciberseguridad?

- **Malware:** Software malicioso, como virus, gusanos, troyanos y ransomware, que se puede instalar en sistemas y redes para causar daño.
- **Phishing:** Engaño que utiliza correos electrónicos, mensajes SMS o sitios web falsos para robar información personal o financiera.
- **Denegación de servicios (DoS):** Sobrecarga de un servidor o red con tráfico para impedir que los usuarios legítimos accedan a él.
- **Ransomware:** Software malicioso que cifra los archivos de una víctima y exige un pago para liberarlos.
- **Suplantación de identidad:** El atacante se sitúa entre dos partes en una comunicación, interceptando y modificando los datos.
- **Ataque a la cadena de suministro:** Los hackers dirigen sus ataques a los proveedores de software, proveedores de materiales y otros proveedores de servicios de una empresa.

¿Cuáles son las aplicaciones de IA en Ciberseguridad?

- **Detección de amenazas en tiempo real:** Las herramientas de IA pueden analizar grandes cantidades de datos en tiempo real para detectar patrones y anomalías en el tráfico de la red. Esto permite una detección temprana de actividades sospechosas y una respuesta rápida para evitar un posible ciberataque.
- **Análisis de comportamiento de usuarios:** La IA puede analizar el comportamiento de los usuarios de una red para detectar actividades sospechosas y comportamientos anormales. Esto puede ayudar a prevenir ataques de phishing y otras formas de ingeniería social.
- **Detección de malware y virus informáticos:** Las herramientas de IA pueden analizar archivos sospechosos en busca de patrones de comportamiento malicioso y características de código malicioso. Esto permite una detección temprana de malware y virus informáticos antes de que se propaguen.
- **Análisis de vulnerabilidades:** Las herramientas de IA pueden analizar una red para identificar vulnerabilidades y debilidades de seguridad. Esto permite a las empresas y organizaciones corregir estas vulnerabilidades antes de que sean explotadas por atacantes.

Fuente: IBM, Microsoft, Google, Fortinet, Kaspersky

La IA ha demostrado ser una herramienta muy útil para mejorar la ciberseguridad. Las aplicaciones referidas en el cuadro son solo algunas de las muchas formas en que la IA se está utilizando para proteger a las empresas y organizaciones contra las amenazas cibernéticas. De hecho, es la tecnología por naturaleza dedicada a mejorar la protección de los sistemas informáticos, las redes y los datos contra las ciber amenazas.

Las empresas digitales proveedores de servicios coinciden que esto incluye el uso de aprendizaje automático para detectar amenazas, analizar grandes volúmenes de datos, identificar patrones y responder a incidentes de seguridad en tiempo real. La IA puede automatizar tareas repetitivas, liberar a los analistas de seguridad para que se enfoquen en tareas más estratégicas y mejorar la capacidad de anticipar y neutralizar las amenazas antes de que causen un daño crítico.

El futuro de la ciberseguridad impulsada por la IA resulta prometedor porque a medida que las tecnologías avancen, las organizaciones y los profesionales de la seguridad digital deberán estar preparados para aprovechar al máximo sus capacidades. En este escenario de constante cambio, la colaboración entre humanos y máquinas es fundamental para lograr un entorno digital seguro.

Estamos firmemente comprometidos con el planeta, la sociedad en la que vivimos y los productos que cultivamos, transformamos y distribuimos en todo el mundo. Lo demuestran nuestras 15.000 hectáreas de tierras cultivadas, nuestro modelo de cultivo integrado verticalmente y la trazabilidad total de nuestra cadena productiva y de distribución, que garantizan calidad y sostenibilidad. Además, contamos con el soporte de 19.000 colaboradores y nuestras operaciones tienen un impacto positivo en el medio ambiente, en la comunidad local y en los clientes que confían en nuestros productos y valores: **innovación, sostenibilidad, calidad, fiabilidad y enfoque en las personas.**

www.virugroup.com

Viru®

naturally ahead

La protección de datos personales

El origen del concepto de privacidad personal se pierde en la historia, pero su definición más aceptada data de 1890, fecha desde cuando adquiere un cuerpo legal hasta llegar al ahora conocido como datos personales. Su evolución legal va de la mano con el avance de las tecnologías de la información

De acuerdo con la International Association of Privacy Professionals (IAPP) actualmente 144 países han promulgado leyes nacionales de privacidad de datos, por lo que el 82% de la población mundial está protegida por algún tipo de legislación nacional de privacidad de datos. Esta entidad señala que en 2024 países como Perú y Chile "realizaron modificaciones, sustituciones o disposiciones de implementación importantes en sus leyes de privacidad de datos." El Perú modificó su ley estableciendo un plazo más estricto para las notificaciones obligatorias de violaciones de datos, exigiendo su presentación en un plazo de cuarenta y ocho (48) horas, junto con mayores obligaciones de seguridad para las entidades sujetas que procesan datos personales.

A nivel mundial Europa cuenta con la mayor cantidad de leyes de privacidad de datos debido a la norma denominada "General Data Protection Regulation – GDPR" (Reglamento General de Protección de Datos) promulgada por la Unión Europea (UE). Esta norma, que está vigente desde mayo de 2018, es un referente a nivel mundial por ser considerada como uno de las más estrictas y completas. La GDPR se aplica a todas las empresas y organizaciones que procesan datos de ciudadanos de países europeos miembros de la UE, independientemente de dónde estén ubicadas. Su objetivo, en primer lugar, es dar a las personas más control sobre cómo se utilizan sus datos personales en un ambiente en que empresas como Facebook y Google intercambian el acceso a los datos de las personas para brindarles sus servicios. En segundo lugar, la UE pretende dar a las empresas un entorno jurídico más simple y claro para operar.

En el campo del derecho, para legislar sobre un asunto es esencial definir su definición. En el caso de la protección de datos personales se requiere la definición de "datos personales". Según Nadezhda Purtova, profesora de leyes y computación de la Universidad de Utrecht en Países Bajos, la ley GDPR define datos personales como: "cualquier información relativa a una persona física identificada o identificable (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona." (The law of everything. Broad concept of personal data and future of EU data protection law, 2018).

Historia

La legislación de la protección de datos personales es resultado de una sucesión histórica de acciones realizadas en varios países. Su evolución responde a la preocupación por la privacidad y la necesidad de controlar el uso de la información personal, y ha progresado desde la inicial noción de derecho a la intimidad hasta la necesidad de crear leyes específicas para regular el manejo de la información personal en los ámbitos público y privado.
Los antecedentes de las leyes de protección de datos personales se remontan al surgimiento del derecho a la intimidad y la autodeterminación informativa, reconocidos en 1919 en la Constitución de Weimar (primera constitución democrática alemana adoptada en 1919).

En Estados Unidos, el ensayo "The Right to Privacy" de Warren y Brandeis (1890) sentó las bases de la noción de privacidad, y es considerada como la definición más aceptada. En esta obra la privacidad se define como "...el derecho de una persona a no ser objeto de intrusiones o revelaciones sobre su vida privada, asuntos o información personales...". Incluye el control sobre cómo se recopila, utiliza y divulga su información personal, así como la protección contra la divulgación no autorizada de información personal.

En Europa, las primeras leyes en esta materia surgieron en la década de 1970 en países como Alemania, Francia y Dinamarca, impulsadas por la creciente importancia de la informática en la gestión de datos. En 1981, el Convenio Nº 108 del Consejo de Europa estableció la primera norma jurídica vinculante en este tema.

Además de estos hitos, otros hechos importantes fueron: la Declaración Universal de Derechos Humanos en 1948 al reconocer en su artículo 12 el derecho a la vida privada; la aprobación en Alemania de la ley de Hesse en 1970 dirigida específicamente a los datos personales en poder de organismos públicos. Esta ley buscaba proteger los derechos de las personas en relación con la recopilación, almacenamiento y el uso de sus datos; Suecia aprobó en 1973 una ley de datos, lo que representó un avance internacional de la conciencia sobre este tema.

Para la profesora Nadezhda Purtova el mundo avanza hacia una situación en que todo será o contendrá datos personales, lo cual conducirá a la necesidad de proteger los datos de todo. Como resultado de su estudio del concepto de datos personales en la norma General Data Protection Regulation – GDPR de la Unión Europea, ella concluye que "en el mundo virtual de la inteligencia basada en datos, que está en pleno desarrollo, pronto todo quedará comprendido en la definición de datos personales."

Situación internacional

De acuerdo con la reciente publicación "Protection Laws of the World Handbook 2025" de la firma global de abogados DLA Piper's, en la actualidad el panorama mundial de la legislación sobre protección de datos y privacidad continúa evolucionando a un ritmo sin precedentes. "Con la aparición de nueva legislación en jurisdicciones de todo el mundo, las empresas se enfrentan a una creciente necesidad de mantenerse informadas y adaptarse con agilidad a estos cambios. Este año promete nuevos avances y desafíos (...) en este campo en constante evolución.", señala el documento.

En **Estados Unidos** actualmente 14 estados cuentan con leyes integrales de privacidad de datos, y seis leyes estatales entrarán en vigor en el presente 2025 y principios de 2026. A nivel federal, entre otros cambios, el nuevo gobierno ha anunciado un cambio en las prioridades de aplicación de la ley en este tema. Además, se ha reinstalado el enfoque en la regulación de la inteligencia artificial (IA) alejándose de la regulación y promoviendo la innovación.

Según Shawn Marie Boyne, profesora de la Universidad de Minnesota en Estados Unidos, este país tiene un enfoque sectorial para la protección de la privacidad de los datos. "No existe una legislación federal integral que garantice la privacidad y la protección de los datos personales. En cambio, la legislación a nivel federal protege principalmente los datos dentro de contextos sectoriales específicos" (Data Protection in the United States, 2018).

Para Boyne, aunque el marco legal de protección de la privacidad de Estados Unidos puede parecer menos sólido que la norma GDPR europeo, "en algunos aspectos, el marco estadounidense brinda mayor protección que en Europa." Esto podría ser explicado a grandes rasgos por la diferencia conceptual de los cuerpos legales europeo y estadounidense. Es decir, según Boyne, mientras que los europeos expresan una profunda desconfianza para las corporaciones, los estadounidenses, en cambio, están más preocupados por controlar a su gobierno para que no invada su privacidad.

Las leyes de protección de datos establecidas en **Europa** siguen evolucionando. De acuerdo con Euractiv, en mayo pasado la Comisión Europea ha reabierto el Reglamento General de Protección de Datos (RGPD) para hacer una reforma que lleve a aliviar la carga de cumplimiento de dicha norma por parte de empresas con menos de 750 empleados. Una intención es eximir a las empresas con menos de 250 empleados de las normas que les obligan a conservar registros de datos personales que manejan, salvo que se considere que suponen un riesgo para los derechos individuales.

Según DLA Piper's, en Asia la protección de datos está cambiando con mayor rapidez y de forma más radical que en ninguna otra región. Han sido dadas nuevas leyes en India, Indonesia, Australia, Arabia Saudí, China y Vietnam. En estos países hay una tendencia a regular categorías de datos más amplias (más allá de los datos personales), lo que plantea retos de cumplimiento normativo para las empresas multinacionales.

En general, los especialistas señalan que el acceso a los datos, la regulación del constante avance de la inteligencia artificial (IA), la creación de mercados digitales más justos y la protección de las infraestructuras críticas frente crecientes amenazas de ciberataques, siguen impactando el campo de la protección de datos personales.

Legislación en Perú

La Ley de Protección de Datos Personales, Ley N° 29733 aprobada en 2013, es la norma que legisla este tema en Perú. El Reglamento de esta ley es el Decreto Supremo N° 016-2024-JUS publicado el 30 de noviembre de 2024. Según la abogada Catherine Escobedo este nuevo reglamento es más que una actualización porque "establece un marco normativo que introduce nuevos conceptos, obligaciones y derechos, y que coloca al país a la vanguardia de la protección de datos en América Latina y a la par con los estándares internacionales."

Entre los cambios de este nuevo reglamento figuran la ampliación de la definición de datos personales incorporando información sobre localización y de identificación en línea, además de considerar que la información concierne a aspectos físicos, económicos, culturales o sociales de las personas naturales. También se incorpora en la definición de datos sensibles a los datos neuronales.

Además, el derecho a la portabilidad es incorporado como una manifestación del derecho de acceso. Así, el titular del dato puede solicitar recibir sus datos personales al responsable o encargado de su tratamiento. Para las personas jurídicas agrega las obligaciones de contar con una política de seguridad documentada y la de implementar controles de acceso para mantener áreas seguras y para mantener equipos seguros dentro y fuera de las instalaciones, así como se categorizan nuevas infracciones en categorías leves (información incompleta, etc.), graves (no inscribir o actualizar los bancos de datos personales en el Registro Nacional, etc.) y muy graves (no realizar el tratamiento de datos personales sensibles con las medidas de seguridad pertinentes).

Tips de protección de datos personales

Cuidado al hablar con desconocidos. Los estafadores pueden engañar usando números telefónicos legítimos o nombres reales de funcionarios. Si lo amenazan o le incomodan, cuelgue.

Crear contraseñas seguras y únicas. Use contraseñas diferentes para cada cuenta. Si un hacker vulnera una cuenta, no podrá acceder a las demás.

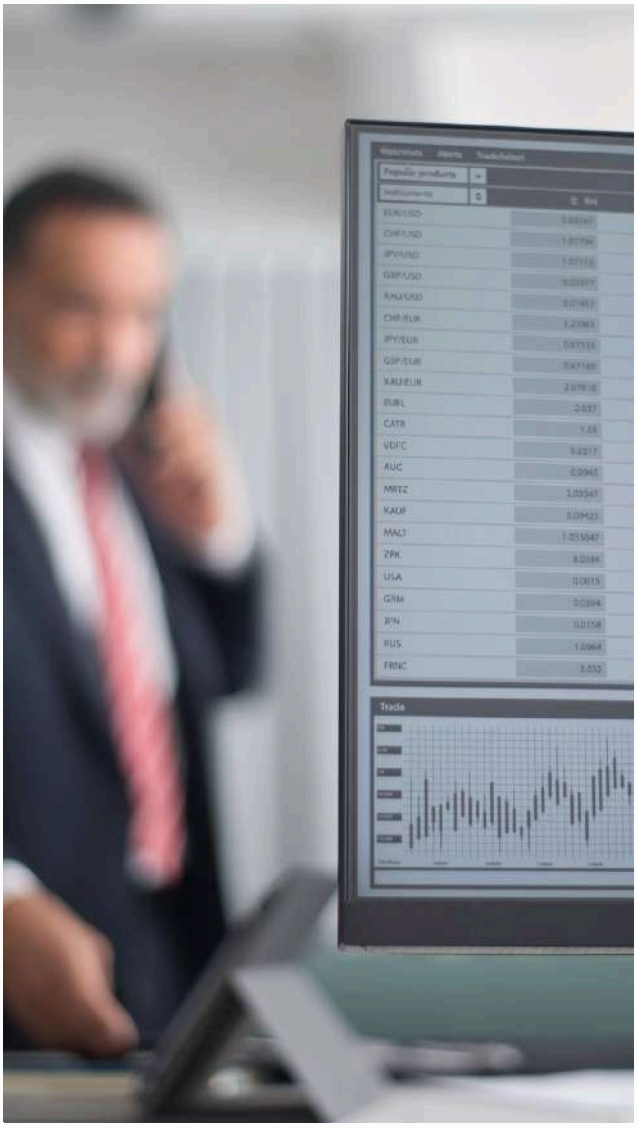
No proporcionar información personal o financiera en respuesta a una llamada o mensaje no solicitado, y nunca publicarlo en redes sociales.

Destruya documentos en papel que contengan información personal (nombre, fecha de nacimiento, etc.)
Proteja su teléfono del acceso no autorizado creando un PIN, agregando una función de huellas dactilares o usando reconocimiento facial. Agregar una contraseña y ajustar el tiempo de bloqueo automático de la pantalla. Revise regularmente sus cuentas bancarias para detectar operaciones sospechosas. Solicitar su informe crediticio anual gratuito de las agencias de crédito (TransUnion, Equifax).

Evite las amenazas de internet instalando un antivirus en sus dispositivos electrónicos. Use una Red Privada Virtual (VPN) para mantenerse seguro en redes wifi-públicas. No realice actividades en redes wifi-públicas que involucren datos confidenciales (compras y operaciones bancarias en línea).

Protegerse en las redes sociales personalizando su configuración de seguridad y eliminando las cuentas sin uso. Revise mensajes sospechosos de sus contactos, ya que los hackers podrían crear cuentas falsas de conocidos.

Nunca hacer clic en ningún enlace enviado por correo electrónico o mensaje de texto no solicitado. Proporcione información únicamente en sitios web seguros.



Dra. Carmen Zegarra
Principal Corporate Counsel de Microsoft

"Implementar tecnologías IA con estrategias claras y controles adecuados"

*Conversamos con la **Dra. Carmen Zegarra, Principal Corporate Counsel de Microsoft**, sobre los desafíos actuales en ciberseguridad e inteligencia artificial. Destaca cómo las organizaciones pueden fortalecer sus cadenas de suministro con un enfoque proactivo y estratégico. Además reflexiona sobre el valor del trabajo que impulsa BASC PERÚ en favor de la seguridad del comercio internacional*

¿Cómo observa Microsoft la evolución mundial de la ciberseguridad en el siglo XXI y su impacto para el sector de comercio internacional? ¿La computación cuántica hará alguna diferencia para facilitar los ataques o mejorar las defensas por parte de las empresas?

La ciberseguridad se ha convertido en uno de los factores más influyentes en el comercio internacional en el siglo XXI. A medida que las cadenas de suministro se digitalizan, los sistemas logísticos se integran en la nube y las operaciones transfronterizas dependen cada vez más de plataformas conectadas, también crece la superficie de ataque para los actores maliciosos. Para ilustrarlo: en Microsoft registrábamos en 2021 unos 579 ataques de contraseñas por segundo; en 2024, esta cifra superó los 7.000 por segundo. Este ritmo impone nuevos desafíos, pero también abre espacio para soluciones más inteligentes.

Un factor clave en esta transformación es el papel dual que desempeña la Inteligencia Artificial (IA). Por un lado, los ciber atacantes han comenzado a utilizar IA para automatizar fraudes, generar contenido malicioso y escalar ataques de ingeniería social con una velocidad sin precedentes. Por otro lado, esta tecnología también es el mayor aliado de los equipos de seguridad. En Microsoft, por ejemplo, hemos desarrollado herramientas como Microsoft Defender XDR y Microsoft Security Copilot, que permiten detectar amenazas en tiempo real, analizar patrones anómalos y responder a incidentes complejos, incluso antes de que el daño ocurra.

Este uso estratégico de la IA está ayudando a cambiar el paradigma de la ciberseguridad de uno reactivo a uno proactivo. En el contexto del comercio internacional, donde un incidente puede detener envíos, vulnerar información sensible o afectar la relación con autoridades aduaneras y socios logísticos, contar con capacidades avanzadas de detección y respuesta no es solo una ventaja, sino una necesidad.

En cuanto a la computación cuántica, es importante abordar el tema con claridad. Esta tecnología aún se encuentra en fases de desarrollo, pero su potencial es enorme. En el futuro, permitirá resolver problemas computacionales de manera exponencialmente más rápida, lo que implica tanto oportunidades como desafíos. Por ejemplo, algunos algoritmos criptográficos actuales podrían volverse vulnerables ante la capacidad de cálculo de un computador cuántico.

Sin embargo, la industria ya está avanzando en el diseño de criptografía avanzada para responder a estos riesgos y Microsoft es uno de los actores que está liderando este proceso desde la investigación y la implementación responsable.

Nuestro enfoque es optimista. Creemos que, así como la tecnología evoluciona, también deben evolucionar nuestras defensas, nuestras alianzas y nuestra cultura organizacional. Por eso, desde Microsoft trabajamos estrechamente con empresas, gobiernos y organismos internacionales para anticiparnos a los riesgos emergentes y construir, juntos, un entorno más seguro, resiliente y preparado para el futuro.

La inteligencia artificial (IA) se ha vuelto accesible para empresas de todos los tamaños y sectores. En ese contexto, ¿cuáles cree usted que son los principales riesgos en ciberseguridad que pueden surgir cuando esta tecnología se implementa sin una estrategia adecuada o sin los controles necesarios?

La democratización de la inteligencia artificial es uno de los hitos más importantes de nuestra era tecnológica. Hoy, empresas de todos los tamaños—desde grandes corporaciones hasta pymes—tienen acceso a capacidades de IA que antes estaban reservadas a algunas pocas organizaciones. Esto ha abierto enormes oportunidades para optimizar operaciones, mejorar la toma de decisiones y elevar la productividad. Sin embargo, también plantea riesgos muy significativos si esta tecnología se implementa sin una estrategia clara ni controles adecuados.

Uno de los principales riesgos es la exposición involuntaria de información sensible. Modelos de IA mal entrenados, o sin salvaguardas ("*guardrails*" por su denominación en inglés), pueden filtrar datos confidenciales, amplificar sesgos o tomar decisiones erróneas que afectan directamente la reputación, la seguridad y la gobernanza de las organizaciones. Esto es especialmente delicado en sectores como el comercio internacional, donde la integridad de la cadena logística y la protección de datos estratégicos son pilares fundamentales de la confianza entre actores. Existe el riesgo de que la IA se adopte como una solución puntual, sin una arquitectura de seguridad de base.

La IA no es una herramienta aislada, sino un componente que debe integrarse dentro de un marco de gobernanza, cumplimiento normativo y cultura organizacional sólida.

La seguridad no puede ser una ocurrencia tardía, sino un principio desde el diseño.

En este contexto, en Microsoft estamos comprometidos en acompañar a organizaciones de todos los sectores en la implementación segura y responsable de sus estrategias de ciberseguridad e IA. Nuestro objetivo es ayudar a fortalecer su resiliencia, proteger sus operaciones críticas y garantizar que la innovación tecnológica se traduzca en ventajas competitivas sostenibles y seguras. Este compromiso se enmarca en nuestra visión de una IA responsable, que sea transparente, segura, inclusiva y centrada en el ser humano. Promovemos principios éticos en el desarrollo y uso de la IA, y trabajamos activamente para que su adopción esté guiada por estándares de gobernanza, privacidad y seguridad desde el diseño.

¿Qué productos, mecanismos, y/o estrategias de defensa puede su empresa recomendar a las empresas peruanas dedicadas al comercio internacional para que puedan enfrentar con éxito las amenazas de ciberataques?

Tanto para la industria del comercio internacional, como en general para múltiples sectores de la economía, la ciberseguridad es un habilitador estratégico para la continuidad operativa, la confianza con socios y la protección de información crítica. Las empresas peruanas que participan en cadenas de suministro, logística, exportación o servicios transfronterizos enfrentan amenazas cada vez más sofisticadas, automatizadas y dirigidas. Por eso, es clave adoptar un enfoque de defensa integral.

Desde Microsoft recomendamos comenzar por un modelo de Confianza Cero ("*Zero Trust*"). Este enfoque parte de la premisa de que ninguna identidad, dispositivo o aplicación debe ser automáticamente confiable. Se basa en verificación continua, acceso con privilegios mínimos, autenticación multifactor ("*MFA*") y segmentación de redes. Es un cambio cultural y tecnológico que reduce la superficie de ataque y dificulta el movimiento lateral de posibles intrusos dentro de la infraestructura.

A esto se suma la necesidad de herramientas de detección y respuesta avanzadas. Soluciones como Microsoft Defender for Cloud, Microsoft Defender XDR y Microsoft Security Copilot permiten identificar amenazas en tiempo real, automatizar la respuesta y contener incidentes antes de que escalen. Estas capacidades son especialmente valiosas en sectores como logística, exportaciones y operaciones aduaneras, donde el mínimo incidente puede interrumpir procesos clave o vulnerar datos sensibles.

Además, **recomendamos la importancia de una cultura de seguridad activa. Capacitar a los colaboradores, simular ataques controlados y adoptar prácticas de higiene digital—como el manejo seguro de contraseñas o la verificación de correos sospechosos**—son elementos que complementan la tecnología y fortalecen la resiliencia de la organización.

¿La plataforma Detección y Respuesta Extendidas (XDR) es una solución al que toda empresa puede aspirar y obtener? ¿Bajo qué requerimientos y condiciones serían, para los interesados?

Las plataformas de Detección y Respuesta Extendidas (XDR) representan un salto cualitativo en la forma en que las organizaciones abordan su ciberseguridad. Lo más relevante es que hoy cualquier empresa, sin importar su tamaño o industria, puede aspirar a implementar una solución XDR como parte de su estrategia de defensa digital, siempre que lo haga con una visión progresiva y basada en sus necesidades específicas.

Lo más valioso de una plataforma XDR es su capacidad para centralizar la detección de amenazas, automatizar la respuesta y ofrecer una visión contextual de los incidentes. Esto reduce la carga operativa de los equipos de seguridad y permite actuar con la velocidad que exige el panorama actual de amenazas.

Desde Microsoft, hemos desarrollado Microsoft Defender XDR como una solución flexible, escalable y nativamente integrada con herramientas que muchas empresas ya utilizan. Esto permite una adopción gradual, sin necesidad de reemplazar por completo la infraestructura tecnológica existente. En este sentido, XDR no requiere condiciones técnicas inalcanzables, sino más bien un compromiso estratégico con la mejora continua de la postura de seguridad.

Para que una organización pueda adoptar con éxito una solución XDR, recomendamos contar con ciertos elementos clave: **una política clara de seguridad; una infraestructura conectada que permita la recolección de señales desde múltiples frentes—correo electrónico, endpoints, identidades, nube, etc.— y el acompañamiento de un equipo especializado o un socio tecnológico que facilite la implementación, personalización y operación de la plataforma.** También es fundamental promover una cultura organizacional abierta al cambio, que vea la ciberseguridad no solo como una necesidad técnica, sino como una inversión estratégica para la continuidad del negocio, la protección de datos y la generación de confianza con clientes, socios y autoridades.

Como empresa proveedora de productos de defensa contra los ciberataques, ¿Cuál es su recomendación para las empresas con relación a políticas internas de ciberseguridad? En el caso de Microsoft es de suponer que también cuenta con una política corporativa al respecto. ¿Puede bosquejarla brevemente?

Una política interna de ciberseguridad efectiva no debe entenderse como un documento estático, sino como una herramienta dinámica de gestión del riesgo que esté plenamente integrada a los 3 ejes fundamentales para la transformación digital exitosa de una organización: tecnologías, procesos y personas de la organización. Nuestra recomendación principal es que las empresas formulen sus políticas con una visión estratégica y transversal, conectada con los objetivos del negocio y alineada con los estándares regulatorios y de cumplimiento que les apliquen.

Estas políticas deben construirse sobre ejes fundamentales como la gobernanza, la cultura organizacional y la tecnología. Desde la gobernanza, es clave definir con claridad los roles y responsabilidades en seguridad, los procedimientos para la gestión de incidentes, la clasificación y protección de datos, y los criterios de acceso a sistemas críticos. En el plano cultural, es indispensable fomentar una conciencia continua sobre ciberseguridad en todos los niveles de la organización. Esto implica capacitar regularmente a los colaboradores, realizar simulaciones de ataques y establecer canales seguros para reportar vulnerabilidades o comportamientos sospechosos, así como definir protocolos para el manejo óptimo de dichas situaciones.

Desde el punto de vista tecnológico, tal como se ha mencionado líneas arriba, recomendamos que las políticas internas adopten el enfoque de Confianza Cero ("Zero Trust"), el uso de autenticación multifactor (MFA), la

segmentación de redes y la supervisión constante de identidades, dispositivos y accesos. Este modelo promueve una verificación continua que se adapta bien a los entornos híbridos y distribuidos de las organizaciones actuales.

En nuestro caso, en Microsoft en efecto contamos con una política de seguridad. En línea con ello, vivimos principios rectores internamente arraigados y que se traducen, entre otros, a través de iniciativas como la Secure Future Initiative (SFI) - lanzada en 2023 - que redefine nuestras prácticas de desarrollo de productos y servicios desde la seguridad por diseño.

Además, seguimos estrictas políticas de privacidad de datos y controles de acceso, y nuestros modelos de IA no se entrenan con información de clientes sin su consentimiento. Todo esto está alineado con marcos regulatorios internacionales y con nuestro compromiso ético en el desarrollo y uso responsable de la tecnología.

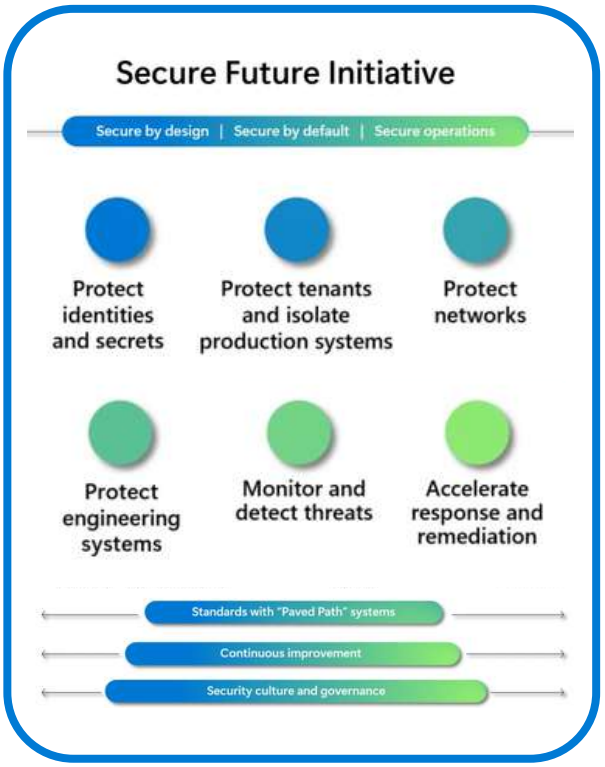
Considerando que es de su conocimiento las actividades que BASC PERÚ realiza en favor de la seguridad de la cadena de suministro del comercio internacional de Perú, ¿Cuál es su impresión de nuestra organización que viene operando cerca de 30 años en nuestro país?

Es indiscutible la importancia del objetivo que orienta el trabajo de BASC PERÚ, el cual radica en fomentar prácticas seguras y mecanismos de facilitación en la cadena de suministro del comercio internacional peruano. Su trayectoria de casi 30 años no solo evidencia una visión de largo plazo, sino también la capacidad para adaptarse a los desafíos emergentes que enfrenta el comercio global.

He tenido la oportunidad de colaborar con BASC PERÚ en iniciativas vinculadas a la ciberseguridad y la gestión de riesgos en el comercio internacional, tanto como panelista en eventos como en espacios de diálogo técnico. Desde esa experiencia, valoro especialmente su apertura a integrar perspectivas diversas y su compromiso con fomentar conversaciones relevantes para el ecosistema empresarial.

Desde Microsoft, creemos que la seguridad no es solo un requisito técnico, sino un habilitador del desarrollo económico y la transformación digital.

En esa línea, saludamos los esfuerzos de organizaciones como BASC PERÚ, que promueven una cultura de colaboración y resiliencia en favor de la seguridad y la estabilidad del ciberespacio.



PERÚ CERTIFICATION

Certifica. Destaca. Lidera.

Sobre nosotros

PERÚ CERTIFICATION, casa matriz de certificaciones en sistemas de gestión ISO. Nuestro enfoque integral nos convierte en el principal socio estratégico hacia la mejora continua, fortalece la competitividad y genera confianza en los negocios de nuestros clientes.

ISO 9001:2015
Calidad

ISO 37001:2016
Antisoborno

ISO 37301:2021
Compliance

paula.lopez@bascperu.org

946 454 057

Sensibilización y simulacros preventivos de ciberseguridad

En tanto que la vida humana parece marchar hacia una interdependencia absoluta basada en el ciberespacio, ***la concientización y los simulacros sobre los ciberataques son vitales para las organizaciones***

La ciberseguridad para las empresas, como parte de la sociedad, actualmente es un asunto ineludible que debe ser asumido con altos niveles de responsabilidad. Como señalan los autores Yuchong Li y Qinghui Liu, "la mayoría de las actividades e interacciones económicas, comerciales, culturales, sociales y gubernamentales de los países, a todos los niveles, incluyendo individuos, organizaciones no gubernamentales e instituciones gubernamentales, se llevan a cabo en el ciberespacio" (A comprehensive review study of cyber-attacks and cybersecurity; Emerging trends and recent developments, 2021) porque el mundo actual depende cada vez más de la tecnología electrónica, proteger los datos es un gran desafío. Los ciberataques tienen como objetivo perjudicar a las empresas, así como, inclusive, pueden tener fines militares o políticos.

El bajo costo de cometerlo, el anonimato, la incertidumbre del origen, el impacto dramático y la falta de transparencia pública en el ciberespacio, han dado lugar a actores fuertes y débiles en este espacio, incluyendo gobiernos, grupos organizados y terroristas e incluso individuos que amenazan con la guerra cibernética, el ciber crimen, el ciber terrorismo y el ciber espionaje. En cuanto a las posibles consecuencias de los ciber ataques, existen diversos escenarios de daños físicos o económicos graves que pueden ser generalizados, incluyendo el ataque de un virus a los documentos financieros de una organización o perturba el mercado de valores de un país, o provoca la paralización de una central eléctrica y el sistema de control del tráfico aéreo, por ejemplo.

Por este motivo, las organizaciones de todo tipo utilizan, como parte de su estrategia de seguridad, **diversas soluciones para prevenir los daños que pueden causar los ciber ataques**. Dos herramientas han surgido como parte del proceso de investigación y desarrollo de estrategias preventivas. **La sensibilización y los simulacros son dos de esas herramientas que han demostrado ser muy útiles.**

La sensibilización

Perseguir el factor humano se ha convertido en la forma más fácil de atacar a una organización y obtener acceso a datos valiosos de la empresa. Los ciberdelincuentes cambian continuamente sus tácticas y utilizan sofisticadas técnicas de ingeniería social para infiltrarse en las redes corporativas. De acuerdo con el blog MetaCompliance, mediante la ingeniería social, los ciber delincuentes, por ejemplo, podrían durante un periodo hacer un seguimiento a las redes sociales de un trabajador objetivo elegido para después poder acceder a las redes de su organización. **Los trabajadores son la primera línea de defensa contra la ciber delincuencia. Inculcarlos con buenas prácticas de**

prevención es la mejor manera de defenderse. Enseguida algunos criterios clave:

- **Debe comenzar el primer día.** Una empresa debe asegurarse de que su personal entiende la importancia de la ciber seguridad en su lugar de trabajo, y para ello **es vital que la formación en ciberseguridad comience desde el primer día de trabajo.** El desarrollo y la inculcación permanente hacia los trabajadores de una cultura de ciber seguridad puede llevar tiempo, pero si se aplican programas desde el principio, aprenderán a actuar con responsabilidad comprendiendo que sus acciones contribuyen a la seguridad general de la empresa.

- **Relievar la formación.** La ciber sensibilización debe ser específica para la organización porque se enfrentan a diferentes amenazas, por lo que la formación debe reflejar las amenazas reales a las que se enfrenta todo el personal en el día a día. La empresa pudo haber enfrentado casos de correos electrónicos de suplantación de identidad o estafas de Business Email Compromise (BEC).

- **Aprobación de la alta dirección.** Para que el personal se tome en serio las ciber amenazas, **el equipo directivo de una organización debe hacer suya la ciber seguridad y apoyar los procedimientos y la formación para enfrentar todos los riesgos.** El tono que se establezca desde arriba será una potente fuerza para crear una cultura sobre la ciberseguridad.

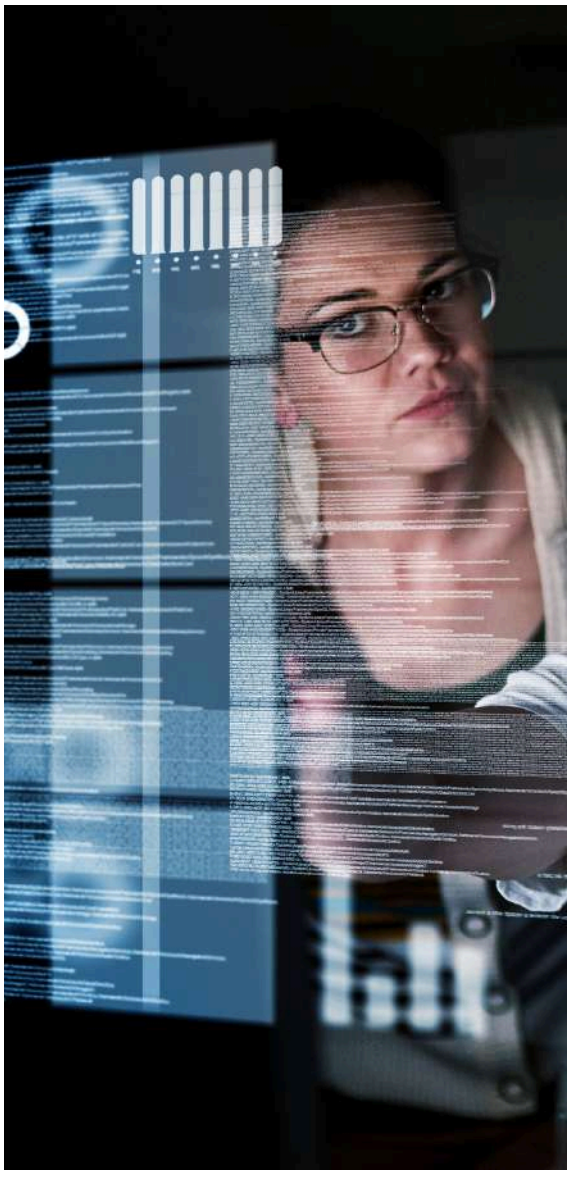
- **Educar sobre el alto costo de la violación de datos.** Explicar didácticamente el precio de una caída en la cotización de las acciones, daños a la reputación, pérdida de clientes o multas para la empresa. **El trabajador debe comprender el impacto real de una violación de la seguridad y cómo podría afectar a su empresa y su empleo.**

- **Formación periódica.** Formar a los trabajadores una vez al año en ciber seguridad no es suficiente para estar preparados para enfrentar los ataques. Este enfoque tradicional ya no es suficiente cuando **ahora las organizaciones son atacadas continuamente y de variadas formas y métodos.**

- **La importancia de la ciber seguridad en el trabajo y en el hogar.** La clave de una buena ciber seguridad en el lugar de trabajo es enseñar a los empleados a adoptar estas prácticas cuando están en casa. Los ciber atacantes pueden pasar semanas investigando a sus víctimas en las redes sociales antes de intentar acceder a las redes de la empresa. Si el personal puede aplicar los buenos hábitos cibernéticos en casa, estos comportamientos se trasladarán al lugar de trabajo.

- **Promover la notificación de incidentes.** A medida que los trabajadores adquieren mayor conciencia y mejor conocimiento de las amenazas, se les debe estimular a informar de cualquier incidente de seguridad a la alta dirección.

- **Comprobar el resultado.** Para evaluar con precisión el nivel del aprendizaje y conciencia es importante poner a prueba a los trabajadores. En este caso **los simulacros ayudan a las organizaciones a determinar el grado de susceptibilidad de su empresa a las estrategias utilizadas por la ciber delincuencia y a identificar al personal que requiere formación adicional.** Las pruebas de simulación controladas ayudarán a los empleados a reconocer, evitar e informar de las posibles amenazas que podrían pasar desapercibidas.



Los simulacros

Los simulacros de ciber ataques también son conocidos como ejercicios de simulación de incidentes. Estos son prácticas controladas que imitan un ataque cibernético real en la infraestructura tecnológica de una organización. Se realiza con el objetivo de evaluar la respuesta y resiliencia de sus sistemas y equipos.

Según Kaspersky, entre los beneficios de estos simulacros se consideran a la identificación de vulnerabilidades, **ya que estos ejercicios revelan puntos débiles en la seguridad que pueden ser corregidos antes de que sean violados**. También permite mejorar la respuesta ante incidentes al permitir a los equipos practicar su respuesta a un ataque y lograr la mejora de los tiempos y la eficacia de sus acciones. Además, elevan la conciencia sobre la ciber seguridad entre los empleados, enseñándoles a reconocer y responder ante posibles amenazas, y finalmente estas prácticas ayudan a cumplir con regulaciones que exigen pruebas periódicas de los mecanismos de seguridad y respuesta ante incidentes.

La organización de simulacros de ciber ataques, requieren una planificación en detalle, definiendo objetivos claros, escenarios realistas y establecer las reglas de juego. También facilita involucrar a todos los niveles de la empresa, desde el equipo de TI hasta la alta dirección, todos deben participar. Asimismo, se debe utilizar las herramientas adecuadas, como emplear software y herramientas diseñadas para simular ataques específicos y medir la respuesta. Para el análisis post ejercicio requiere evaluar el desempeño, identificar áreas de mejora y ajustar las políticas y procedimientos de seguridad en consecuencia.

Existen diversas herramientas y plataformas que pueden ayudar a simular diferentes tipos de ciberataques. Los especialistas señalan que están disponibles desde inyecciones SQL hasta DDoS y ransomware. Herramientas como Kali Linux, Metasploit y Wireshark, entre otras, son esenciales para llevar a cabo estos ejercicios de manera efectiva.

La frecuencia ideal de este tipo de simulacros depende del tamaño de la organización y de la evolución del panorama de amenazas, pero se recomienda realizarlos al menos una vez al año. **Los simulacros de ciberataques no necesariamente interrumpen las operaciones de la organización, si se planifican y ejecutan correctamente los simulacros no deberían causar interrupciones significativas.** Es importante comunicar y programarlos adecuadamente. En cuanto a la participación de las personas, mientras que el enfoque puede estar en los equipos de TI y seguridad es beneficioso involucrar a empleados de diferentes departamentos para mejorar la concienciación y preparación a nivel de toda la organización. La medición del éxito del simulacro depende de cuánto se logran los objetivos establecidos, tales como la identificación de vulnerabilidades, la mejora en los tiempos de respuesta y el aumento de la concienciación sobre ciberseguridad.

Simulación de phishing

Una simulación de phishing es un ejercicio de ciberseguridad que pone a prueba la capacidad de una organización para reconocer y responder a un ataque. Consiste en un correo electrónico, mensaje de texto o mensaje de voz fraudulento, diseñado para engañar a las personas para que descarguen un programa maligno (como ransomware), revelen información confidencial (como nombres de usuario, contraseñas o datos de tarjetas de crédito) o envíen dinero a personas no autorizadas.

Durante una simulación de phishing los trabajadores reciben correos electrónicos simulados que imitan intentos reales de phishing. Los mensajes emplean las mismas tácticas de ingeniería social (por ejemplo, suplantar la identidad de alguien conocido o de confianza del destinatario, creando una sensación de urgencia) para ganarse la confianza del destinatario y manipularlo. La única diferencia es que los destinatarios que caen en la trampa (por ejemplo, al hacer clic en un enlace malicioso, descargar un archivo adjunto malicioso, introducir información en una página de destino fraudulenta o procesar una factura falsa) simplemente no superan la prueba, sin que esto afecte negativamente a la organización.

Los empleados que hacen clic son redirigidos a una página de destino que indica que fueron víctimas de un ataque de phishing simulado, con información sobre cómo detectar mejor las estafas de phishing y otros ciber ataques en el futuro. Tras la simulación, las organizaciones también reciben métricas sobre las tasas de clics de los empleados y, a menudo, realizan un seguimiento con formación adicional sobre concienciación sobre phishing.

Las simulaciones de phishing bien diseñadas ayudan a mitigar el impacto de los ataques de dos maneras importantes: Proporcionan la información que los equipos de seguridad necesitan para **capacitar a los empleados para reconocer y evitar mejor los ataques de phishing reales.** También ayudan a los equipos de seguridad **a identificar vulnerabilidades, mejorar la respuesta general a incidentes y reducir el riesgo** de filtraciones de datos y pérdidas financieras.

Fuente: MaillngBlack

Ing. Oscar Mauricio Andrade
Vicepresidente del Directorio de WBO y
Presidente de la Junta Directiva de BASC Guatemala

"El reto (para las *PYMES*) es eliminar la barrera mental"

*El **Ing. Oscar Mauricio Andrade**, arquitecto de soluciones de seguridad informática, comparte su visión sobre el uso de inteligencia artificial para detectar y responder a ciberamenazas en la cadena de suministro, destacando sus aplicaciones más disruptivas en un entorno logístico digital*

Como arquitecto de soluciones de seguridad informática con Inteligencia Artificial (IA), ¿cuáles considera que son las aplicaciones más disruptivas de la IA en la protección de la cadena de suministro frente a ciberamenazas emergentes? ¿Qué papel juega la IA para detectar y responder oportunamente ante estos riesgos?

La IA redefine la fortaleza de la cadena de suministro frente a las ciber amenazas emergentes. Además se está consolidando como el arma de mayor impacto en el arsenal de ciber seguridad para la protección de las cadenas de suministro globales.

Al pasar de un enfoque reactivo a uno predictivo y autónomo, la IA no solo optimiza la eficiencia, sino que redefine fundamentalmente la forma en que las empresas se anticipan, detectan y responden a las ciber amenazas emergentes que ponen en jaque la integridad de sus operaciones.

Las cadenas de suministro modernas, caracterizadas por su complejidad, infraestructura digital y dependencia de una multitud de proveedores y socios, presentan una superficie de ataque cada vez más amplia y atractiva para los ciber delincuentes.

Frente a este panorama, la IA introduce un cambio de paradigma a través de aplicaciones que van más allá de la tradicional.

El tipo de aplicaciones más disruptivas de la IA en este ámbito se pueden agrupar en tres áreas fundamentales:

- **Análisis predictivo de amenazas y gestión proactiva de vulnerabilidades:** La capacidad más transformadora de la IA reside en su habilidad para predecir y prevenir ataques antes de que ocurran. Mediante el uso de algoritmos de "machine learning" (aprendizaje automático) y el análisis de vastos conjuntos de datos, la IA posee la capacidad de Identificar patrones anómalos con lo que puede analizar en tiempo real flujos de datos provenientes de toda la cadena de suministro (desde sensores de IoT y Sistemas de Gestión de inventario hasta comunicaciones con proveedores) que podrían indicar una brecha de seguridad incipiente.

  Esto incluye desde un patrón de acceso inusual en un portal de proveedores hasta una desviación en los tiempos de tránsito de una mercancía que podría sugerir una interceptación.

- **Análisis de riesgo de terceros:** la IA puede analizar de forma automatizada informes de seguridad, vulnerabilidades conocidas y la huella digital de los proveedores para asignar una puntuación de riesgo dinámica. Esto permite a las empresas tomar decisiones informadas sobre con quién asociarse y qué medidas de seguridad exigir.

- **La inteligencia de amenazas predictiva:** procesa información de fuentes externas (como foros de la *dark web*, informes de inteligencia de amenazas y noticias sobre nuevas tácticas de ataque) para anticipar las amenazas emergentes que podrían afectar a la cadena de suministro. De esta forma, se pueden implementar medidas de forma proactiva, en lugar de esperar a que un ataque sea conocido públicamente.

- **La detección y respuesta autónoma a incidentes:** al detectar que un ataque es inminente o ya está en curso, la velocidad de respuesta es crucial. La IA está revolucionando este aspecto al permitir una reacción casi instantánea y automatizada como los sistemas de detección de intrusiones (IDS) Potenciados por IA, a diferencia de los sistemas tradicionales basados en firmas, los IDS con IA pueden identificar "malware" (programa maligno) de día cero y técnicas de ataque novedosas al reconocer desviaciones del comportamiento normal de la red y los sistemas.

Así como una Orquestación, Automatización y Respuesta de Seguridad (SOAR) impulsada por IA puede automatizar flujos de trabajo de respuesta a incidentes. Por ejemplo, si se detecta un comportamiento malicioso en el dispositivo de un socio que se conecta a la red de la empresa, la IA puede aislar automáticamente ese dispositivo de la red, revocar sus credenciales de acceso y notificar a los equipos de seguridad pertinentes en cuestión de segundos, minimizando así el impacto potencial.

Al utilizar el análisis forense acelerado, en el caso de una brecha, la IA puede analizar rápidamente gigabytes de logs y datos para identificar la causa raíz del incidente, el alcance del compromiso y los datos que han sido comprometidos, cuyas tareas para un analista humano podría llevar días o semanas.

Fortalecimiento de la Integridad y Autenticidad en la Cadena de Suministro

Más allá de la defensa contra ataques externos, la IA juega un papel crucial en garantizar la integridad y la autenticidad de los productos y datos que fluyen a través de la cadena de suministro:

- **Detección de falsificaciones y fraudes:** mediante el "*machine learning*", la IA puede analizar imágenes de productos, empaques, códigos de barras y otros marcadores para detectar productos falsificados con un alto grado de precisión. Esto es vital para industrias como la farmacéutica, la electrónica y la de bienes de lujo.

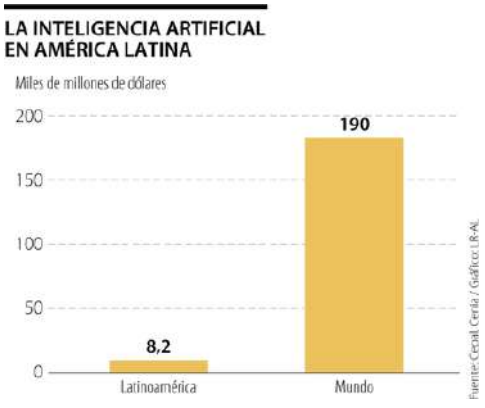
- **Control de acceso adaptativo y basado en el comportamiento:** donde la IA puede ir más allá de las contraseñas y la autenticación multi factor. Al analizar el comportamiento del usuario (patrones de escritura, movimientos del "mouse", horarios de acceso, ubicación geográfica), puede crear un perfil biométrico conductual. Si se detecta una desviación significativa, el sistema puede requerir una verificación adicional o bloquear el acceso, frustrando así los intentos de secuestro de cuentas.

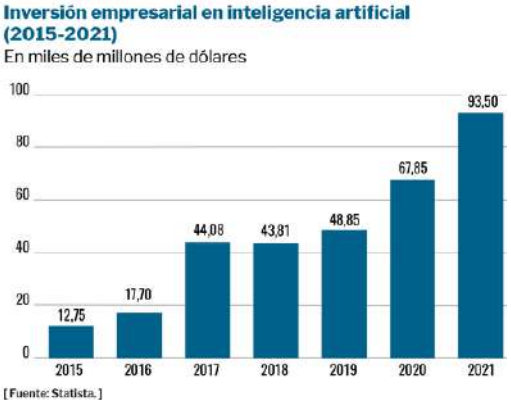
En conclusión, la IA no es simplemente una herramienta de mejora incremental para la ciberseguridad de la cadena de suministro.

Sus aplicaciones más disruptivas están transformando la defensa de un ejercicio de reacción a uno de anticipación, permitiendo a las organizaciones no solo construir muros más altos, sino también prever la trayectoria del atacante y neutralizar la amenaza antes de que impacte en sus operaciones.

La adopción de estas tecnologías se está convirtiendo en un diferenciador clave para garantizar la resiliencia y la confianza en el complejo ecosistema del comercio global, más que una herramienta o conjunto de herramientas, el poder contar con el liderazgo de la alta gerencia para agenciar recursos y alcanzar los objetivos deseados es crucial.

Como cualquier proyecto que involucre tecnología, el reto final es siempre la implementación y el mantenimiento adecuado de la infraestructura.





Muchas empresas pequeñas o medianas creen que aplicar IA o ciberseguridad avanzada es algo solo para grandes corporaciones. ¿Qué les diría a estos empresarios? ¿Por dónde pueden empezar?

El reto fundamental es eliminar la barrera mental, a esos empresarios de pequeñas y medianas empresas les diría lo siguiente:

Entiendo perfectamente su perspectiva. Durante años, la tecnología de punta como la IA y las soluciones de ciber seguridad avanzadas han parecido un lujo exclusivo de las grandes corporaciones con presupuestos millonarios. Sin embargo, pensar que la ciber seguridad avanzada es "demasiado" para su empresa es, hoy en día, uno de los mayores riesgos que puede asumir.

Los ciber delincuentes ya no solo apuntan a los grandes nombres. De hecho, a menudo ven a las **PYMES** como el objetivo perfecto: tienen datos valiosos (de clientes, financieros, operativos) pero suelen tener defensas más débiles. **Son un punto de entrada fácil para atacar a empresas más grandes en su cadena de suministro.**

La buena noticia es que el panorama ha cambiado drásticamente en los últimos años. La ciber seguridad y la IA ya no son un monolito inalcanzable, han evolucionado a un menú a la carta, donde las empresas pueden empezar con lo esencial y escalarlo en la medida que lo necesite, en su propia realidad y la de sus partes interesadas, siempre teniendo en cuenta la gestión del riesgo.

¿Por dónde pueden empezar? Un plan de acción práctico y asequible: No necesita contratar un equipo de ingenieros militares para dar el primer paso, ni tener todo a mano o definido. **El camino se inicia con pasos lógicos, enfocados en maximizar la protección con una inversión inteligente**.

Para esto se pueden seguir las siguientes fases:

Fase 1

La base fundamental (bajo costo, alto impacto): Esta es la "higiene digital" esencial que cierra las puertas más obvias a los atacantes.

- **Concienciación y formación del personal:** Este es el punto de partida más rentable y efectivo. El eslabón más débil suele ser un empleado bien intencionado pero desinformado. Invierta en formación básica para que su equipo pueda reconocer correos de phishing (suplantación de identidad), crear contraseñas seguras y desconfiar de enlaces o archivos sospechosos. Hay cursos "on line" asequibles e incluso recursos gratuitos. Un ejemplo sencillo después de una formación basada en phishing es usar herramientas gratuitas para realizar simulaciones de phishing interno para evaluar la eficacia de la formación y reforzar en caso de encontrar desviaciones.

- **Gestor de contraseñas y autenticación multifactor (MFA):** como implemente un gestor de contraseñas para todo el equipo (ej. Bitwarden, 1Password). Esto elimina el riesgo de contraseñas débiles o reutilizadas. Inmediatamente después, active la MFA (el código que llega a su teléfono o una App) en todas las cuentas posibles, especialmente en el correo electrónico y sistemas bancarios. Esto frustra el 99% de los ataques de robo de credenciales.

- **Copias de seguridad (backup) robustas:** ¿qué sucedería si se pierden todos los datos de la empresa mañana por un ransomware? ¿Podría operar? Establezca una regla "3-2-1": 3 copias de sus datos, en 2 tipos de medios diferentes, con 1 copia fuera de la oficina (en la nube, por ejemplo y encriptado). Servicios como Backblaze o incluso las versiones de negocio de Google Drive/OneDrive son un buen comienzo.

Fase 2

Primeras capas de inteligencia y automatización: Aquí es donde la tecnología "inteligente" empieza a trabajar para usted sin requerir una gran inversión.

- **Seguridad del Endpoint (EDR/XDR para PYMES):** el antivirus tradicional ya no es suficiente. Las soluciones modernas de "Endpoint Detection and Response" (EDR) actúan como un guardia de seguridad inteligente en cada ordenador y servidor. Utilizan IA para detectar comportamientos sospechosos, no solo virus conocidos. Proveedores como SentinelOne, Sophos o Microsoft Defender for Business (incluido en algunos planes de Microsoft 365) tienen ofertas escalables para PYMES que son bastante accesibles.

- **Seguridad en la nube y correo electrónico:** si usa Microsoft 365 o Google Workspace, ya tiene acceso a herramientas de seguridad potentes. No es complicado activar las funcionalidades anti-phishing, anti-spam y de análisis de archivos adjuntos que ya

vienen incluidas o que se pueden añadir por un costo marginal. Estas herramientas utilizan IA para analizar millones de correos y bloquear amenazas antes de que lleguen a entregarse.

Fase 3 Externalización inteligente (el socio tecnológico)

- **La percepción del costo:** Muchas empresas, especialmente PYMES, ven esto como un gasto inalcanzable. Debemos cambiar la narrativa a una inversión en resiliencia y competitividad. Y la realidad es que muchas de estas tecnologías son cada vez más asequibles a través de modelos de servicio (SaaS).

- **Calidad de los datos:** La IA es tan inteligente como los datos que la alimentan. Nuestro primer paso como empresas es ordenar nuestra casa digital. Hay que asegurar que la información que generamos es precisa, está estandarizada y es accesible.

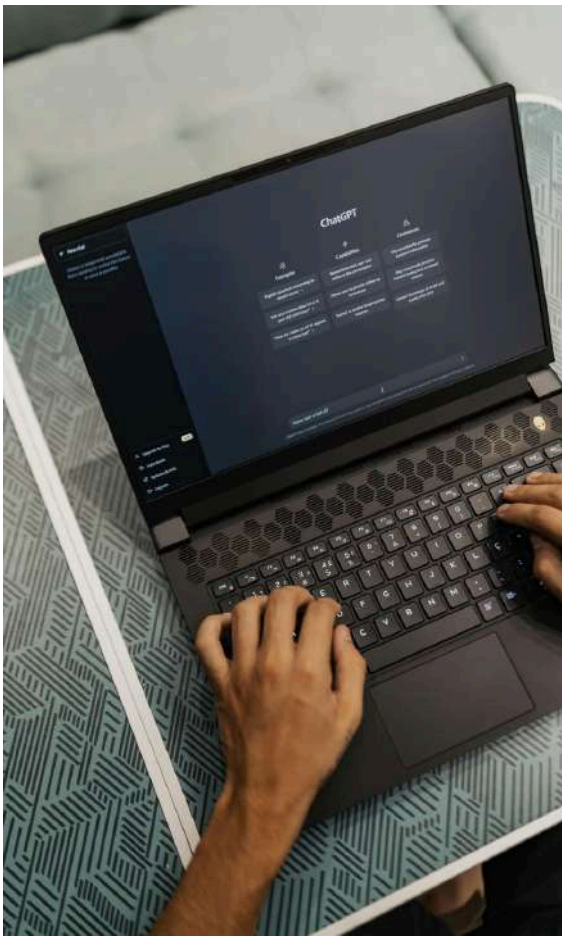
Considerar un socio de ciberseguridad, estas empresas actúan como su departamento de TI y ciber seguridad externo por una cuota mensual predecible. Antes de contratarles se debe evaluar la experiencia y las herramientas avanzadas que utilicen y las ofrecen como un servicio. Se encargan del monitoreo 24/7, la gestión de parches, la respuesta a incidentes y le dan la tranquilidad para que usted se dedique a su negocio.

> **A los empresarios les diría que no vean la ciberseguridad como un gasto, sino como una inversión en la continuidad y la reputación de su negocio.**

No se trata de comprar IA, se trata de adquirir soluciones modernas que utilizan IA para protegerlos de manera más eficaz y asequible que nunca.

Que den inicio hoy con lo básico, que eduquen a su equipo y no subestimen el poder de un usuario bien formado. Luego, que exploren las soluciones de seguridad para sus dispositivos y correos que cuenten con inteligencia integrada. Y cuando estén listos para el siguiente nivel, busquen un socio tecnológico que les dé acceso a la élite de la ciberseguridad por una fracción del costo.

> **"Hacer nada es un lujo que ninguna empresa, sin importar su tamaño, puede permitirse".**

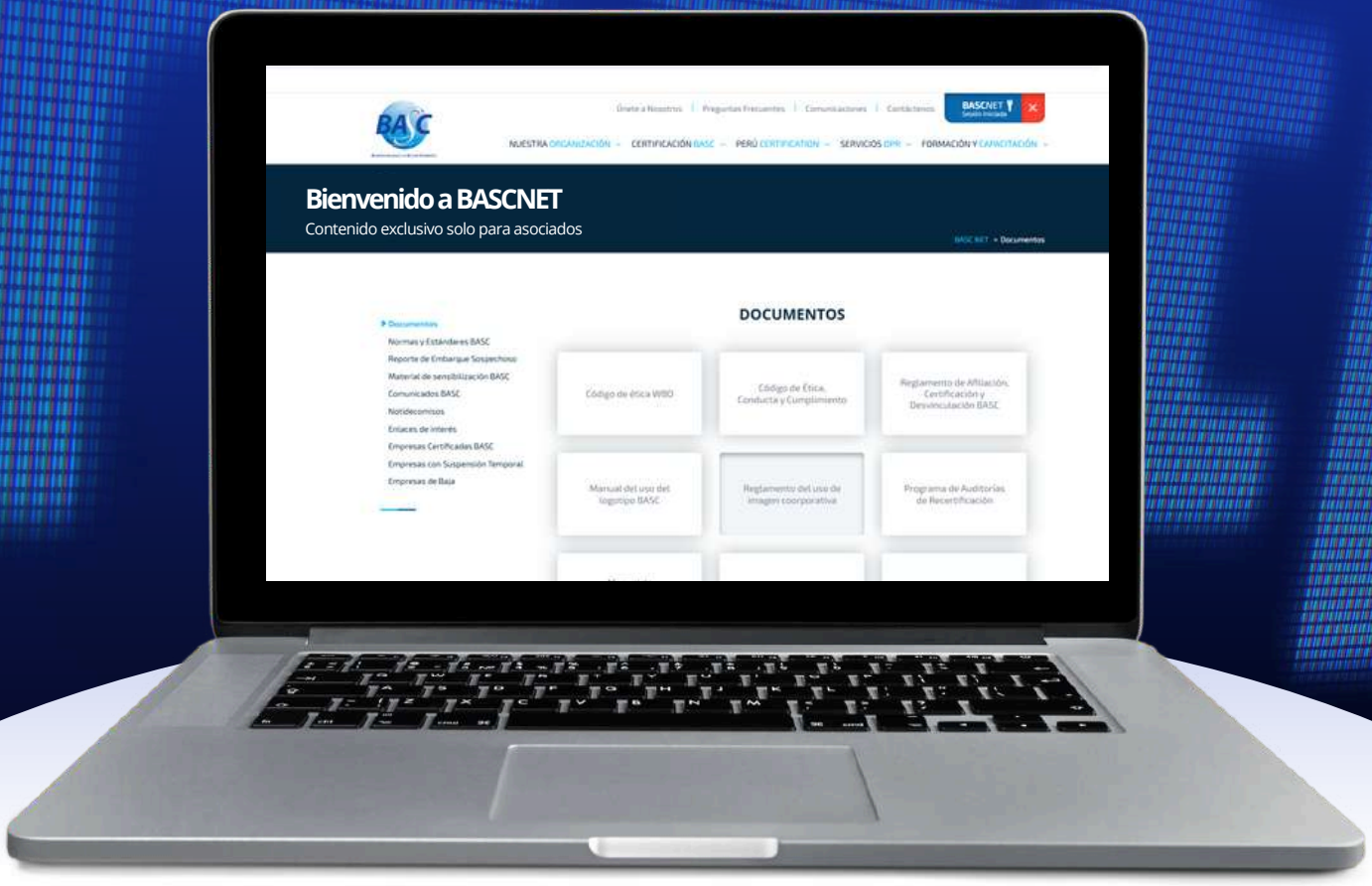


Acceda al BASCNET:

Reporte de embarque sospechoso

Material de sensibilización

Norma y estándares BASC



bascperu.org

Contáctenos para obtener su usuario y contraseña:
silvana.basauri@bascperu.org

Políticas de seguridad cibernética en CTPAT y BASC

Además de otros objetivos, ambas organizaciones trabajan para reducir los riesgos de que una amenaza cibernética sea materializada. La meta es impedir cualquier disrupción de la cadena de suministro

En el campo de la seguridad, una **amenaza** es un evento o circunstancia que puede causar un perjuicio. Ejemplo, un terremoto. El **riesgo** es la probabilidad de que el terremoto ocurra y cause daño. El riesgo será tanto mayor como menor sea la calidad de la construcción de un edificio. Pasa lo mismo en la empresa. La amenaza es un ciberataque y el riesgo es la calidad de su sistema de defensa. Mejor defensa, menor riesgo.

En el actual mundo hiperconectado la ciberseguridad es una preocupación constante para las organizaciones que buscan salvaguardar los activos intangibles más valiosos, como pueden ser la propiedad intelectual, la información de socios comerciales, datos críticos, información financiera, registros de colaboradores, etc. El riesgo de que los sistemas de tecnologías de información de la organización sean violados es latente para empresas de todo tipo y tamaño.

En este escenario, tanto la Customs Trade Partnership Against Terrorism (**CTPAT**) como la Business Alliance for Secure Commerce (**BASC**), comparten el compromiso de brindar a sus empresas miembro las herramientas necesarias para hacer frente las amenazas de potenciales de ataques cibernéticos en todas sus formas. Proteger el Sistema de las Tecnologías de Información (TI) y el cúmulo de datos sensibles para sus miembros, son las bases de las buenas prácticas de seguridad que fomentan ambas entidades.

Las buenas prácticas responden a estándares que provienen de entidades especializadas dedicadas al desarrollo de la calidad de métodos y procedimientos de la comunidad industrial y comercial a nivel mundial.

Customs Trade Partnership Against Terrorism

CTPAT es un programa de colaboración público-privada de la Oficina de Aduanas y Protección Fronteriza (CBP) de EE.UU. Esta entidad fue creada en noviembre de 2001 como reacción estadounidense a los atentados terroristas de setiembre de 2001. Fue **concebida sobre la base de la Business Alliance for Security Commerce (BASC): fortalecer las cadenas de suministro del comercio internacional.**

Así como BASC, el propósito de CTPAT es que las empresas se acojan voluntariamente a la organización para aplicar las mejores prácticas de seguridad, con la finalidad de que sean capaces de protegerse contra el terrorismo y otras actividades ilícitas. Las empresas que participan en CTPAT implementan medidas de seguridad en sus operaciones, incluyendo áreas como la seguridad física, seguridad de unidades de transporte, seguridad de procesos, seguridad de empleados, y seguridad de la información (ciberseguridad).

Las empresas de comercio internacional afiliadas a CTPAT implementan voluntariamente, como parte de su política interna, estrictas medidas de seguridad a cambio de beneficios aduaneros, tales como menos inspecciones de carga y un procesamiento más rápido en los puertos de entrada que están bajo la administración del **U.S. Customs and Border Protection (CBP)**, entidad aduanera del país norteamericano.

Según la misma organización, actualmente cuenta con más de 11,000 empresas miembro entre importadores, transportistas aéreos, terrestres y marítimos, fabricantes extranjeros, consolidadores, agentes de aduanas estadounidenses autorizados, entre otros. Cada miembro se compromete a cumplir en sus cadenas de suministro los Estándares de Seguridad CTPAT, conocidos como Criterios Mínimos de Seguridad (CMS).

Según la misma organización, actualmente cuenta con más de 11,000 empresas miembro entre importadores, transportistas aéreos, terrestres y marítimos, fabricantes extranjeros, consolidadores, agentes de aduanas estadounidenses autorizados, entre otros. Cada miembro se compromete a cumplir en sus cadenas de suministro los Estándares de Seguridad CTPAT, conocidos como Criterios Mínimos de Seguridad (CMS).

Enfrentando las amenazas a la ciberseguridad

En general, los criterios de seguridad de CTPAT están diseñados para sentar las bases de un sistema de seguridad por capas. Si se supera una capa de seguridad, otra capa debería prevenir una brecha de seguridad o alertar a la empresa sobre una brecha. La educación, capacitación y concientización es uno de los aspectos clave para CTPAT. Educar a los empleados sobre las amenazas y la importancia de su rol para proteger la cadena de suministro de la empresa es un factor fundamental para la durabilidad y el éxito de una política de seguridad. Cuando los trabajadores comprenden por qué implementar procedimientos de seguridad, es más probable que los cumplan.

La ciberseguridad es un componente crucial en el programa CTPAT. Cada empresa afiliada debe proteger su sistema de Tecnologías de la Información (TI) contra riesgos cibernéticos, tales como ransomware, malware, phishing y otras estrategias de ciberataque. Estas amenazas pueden interrumpir las operaciones del negocio y causar pérdidas financieras, comprometer su reputación e impactar negativamente en la seguridad de su cadena de suministro. El enfoque de CTPAT para abordar los ciberataques se basa principalmente en sus Criterios Mínimos de Seguridad (CMS).

Los CMS están diseñados para diferentes sectores que operan en la cadena de suministro. En este sentido, si bien no existe un manual específico de CMS para ciberataques, este se incluye en el documento "Minimum Security Criteria – U.S. Importers" (Criterios Mínimos de Seguridad para Importadores Estadounidenses, 2,023) en la sección "Primer área de enfoque: Seguridad Corporativa" bajo el punto 4 "Ciberseguridad".

Aquí se señala que la ciberseguridad "es la actividad o proceso que se centra en proteger ordenadores, redes, programas y datos del acceso, modificación o destrucción no intencionados o no autorizados. Es el proceso de identificar, analizar, evaluar y comunicar un riesgo cibernético, así como aceptarlo, evitarlo, transferirlo o mitigarlo a un nivel aceptable, considerando los costos y los beneficios obtenidos." A continuación, se resume algunos criterios relevantes y cómo deben ser implementados por las empresas.

El primer criterio establece que las empresas CTPAT "deben contar con **políticas y/o procedimientos integrales de ciberseguridad por escrito para proteger los Sistemas de Tecnologías de la Información (TI)**. La política de TI por escrito debe, como mínimo, cubrir todos los criterios individuales de ciberseguridad." Para su implementación se anima a los miembros a seguir los protocolos de ciberseguridad basados en marcos y estándares reconocidos de la industria. El Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés) es una organización de EE. UU. de América 2 (equivalente a INACAL) que proporciona un Marco de Ciberseguridad que ofrece orientación voluntaria basada en estándares, directrices y prácticas existentes para ayudar a gestionar y reducir los riesgos de ciberseguridad, tanto internos como externos.

Este marco puede utilizarse para identificar y priorizar acciones para reducir el riesgo de ciberseguridad. También complementa el proceso de gestión de riesgos y el programa de ciberseguridad de una organización. Como alternativa, una organización que no cuente con un programa de ciberseguridad puede utilizar este Marco como referencia para establecer uno.

Otro criterio señala que **los miembros de CTPAT que utilizan sistemas de red deben comprobar periódicamente la seguridad de su infraestructura informática**. Si se detectan vulnerabilidades, se deben implementar medidas correctivas lo antes posible. Para ello, establece que una red informática segura es fundamental y garantizar su protección requiere pruebas periódicas, lo que se puede lograr programando análisis de vulnerabilidades.

Al igual que un guardia de seguridad comprueba si hay puertas y ventanas abiertas en una empresa, un análisis de vulnerabilidades (AV) identifica las aberturas en los ordenadores (puertos y direcciones IP abiertos), sus sistemas operativos y el software a través del cual un hacker podría acceder al sistema informático de la empresa. El AV compara los resultados de su análisis con una base de datos de vulnerabilidades conocidas y genera un informe de corrección para que la empresa tome medidas. Existen muchas versiones gratuitas y comerciales de análisis de vulnerabilidades. La frecuencia de las pruebas dependerá de factores como el modelo de negocio y el nivel de riesgo. Por ejemplo, las empresas deberían realizar estas pruebas siempre que se produzcan cambios en la infraestructura de red.

Otro criterio importante dice que **las políticas de ciberseguridad deben abordar cómo un miembro comparte información sobre amenazas de ciberseguridad con el gobierno y otros socios comerciales**. Para realizarlo se anima a los miembros a compartir información sobre amenazas a la ciberseguridad con el gobierno y los socios comerciales de su cadena de suministro. El intercambio de información es fundamental para que el Departamento de Seguridad Nacional cree un conocimiento situacional compartido sobre actividades cibernéticas maliciosas. Los miembros de CTPAT pueden unirse al Centro Nacional de Integración de Ciberseguridad y Comunicaciones (NCCIC).

Asimismo, otro criterio establece que **las políticas y los procedimientos de ciberseguridad deben revisarse anualmente o con mayor frecuencia**, según lo exijan los riesgos o las circunstancias. Tras la revisión, deben actualizarse si es necesario. Un ejemplo de una circunstancia que requeriría una actualización de la política antes de lo habitual es un ciberataque. Aprovechar las lecciones aprendidas del ataque ayudaría a fortalecer la política de ciberseguridad de un miembro. Esto puede ser logrado si las personas con acceso a los sistemas de Tecnologías de la Información (TI) deben usar cuentas asignadas individualmente.

Otro criterio importante indica que **las contraseñas deben cambiarse lo antes posible si hay evidencia o sospecha razonable de una vulneración**. Para proteger los sistemas informáticos de las infiltraciones, el acceso de los usuarios debe protegerse mediante un proceso de autenticación.

Las contraseñas o frases de acceso complejas, las tecnologías biométricas y las tarjetas de identificación electrónicas son tres tipos diferentes de procesos de autenticación. Se prefieren los procesos que utilizan más de una medida como la autenticación de dos factores (2FA) o autenticación multifactor (MFA por sus siglas en ingles). La Publicación Especial 800-63B del NIST incluye directrices para contraseñas.

Para las empresas que permiten a sus usuarios conectarse remotamente a una red, otro criterio señala que deben **emplear tecnologías seguras, como redes privadas virtuales (VPN)**, para que los empleados puedan acceder de forma segura a la intranet de la empresa cuando se encuentren fuera de la oficina. Los miembros también deben contar con **procedimientos diseñados para evitar el acceso remoto de usuarios no autorizados.**

El criterio que refiere a que los medios, hardware u otros **equipos informáticos que contengan información confidencial sobre el proceso de importación/exportación**, **deben contabilizarse mediante inventarios periódicos**. Al desecharse, deben desinfectarse o destruirse adecuadamente de acuerdo con las directrices para la "Desinfección de Medios" del NIST que ha desarrollado normas para la destrucción de medios de datos.

La ciberseguridad en CTPAT se apoya en instituciones

CTPAT recomienda a sus miembros seguir los protocolos de la ciberseguridad que se basan en normas internacionalmente reconocidas como la ISO 27001 o en organizaciones como el NIST. Por ejemplo, el "NIST Cybersecurity Framework (CSF) 2.0" (2024) es un aporte del National Institute of Standards and Technology (NIST), organismo del Departamento de Comercio de los EE. UU.

Brinda orientación a la industria, agencias gubernamentales y otras organizaciones para gestionar los riesgos de ciberseguridad. Presenta una categorización de resultados de alto nivel que cualquier entidad, sin importar su tamaño, sector o madurez, puede usar para comprender, evaluar, priorizar y comunicar mejor sus iniciativas en este ámbito. El CSF no indica cómo alcanzar estos resultados, pero sí enlaza a recursos en línea que ofrecen guía sobre prácticas y controles que pueden aplicarse para lograrlos.

El CSF está diseñado para ayudar a organizaciones de todos los tamaños y sectores, incluyendo la industria, la administración pública, el mundo académico y las organizaciones sin fines de lucro, a gestionar y reducir sus riesgos de ciberseguridad. Resulta útil independientemente del nivel de madurez y la sofisticación técnica de los programas de ciberseguridad de una organización. Sin embargo, el CSF no adopta un enfoque único. Cada organización tiene riesgos comunes y únicos, así como diferentes niveles de tolerancia al riesgo, misiones específicas y objetivos para lograr dichas misiones. Por necesidad, la forma en que las organizaciones implementan el CSF variará.

Idealmente, el CSF se aplica en conjunto con otros enfoques de gestión de riesgos empresariales, como los financieros, de privacidad, cadena de suministro, reputación, tecnología o seguridad física. Describe resultados esperados de ciberseguridad, de forma que puedan ser comprendidos por un público amplio, incluidos ejecutivos, gerentes y profesionales, sin importar su nivel de conocimiento técnico.

Dado que estos resultados son neutrales, proporcionan a la organización la flexibilidad necesaria para abordar sus riesgos, tecnologías y consideraciones de misión únicos. Los resultados se asignan a una lista de posibles controles de seguridad para su consideración inmediata, con el fin de mitigar los riesgos de ciberseguridad.

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Fuente: NIST Cybersecurity Framework (CSF) 2.0 (2024)

Business Alliance for Secure Commerce (BASC)

BASC fue iniciada en 1996 bajo la forma de una alianza anti-contrabando entre la aduana estadounidense y la empresa privada para implementar mecanismos y procedimientos con la finalidad de evitar que las empresas sean utilizadas por organizaciones ilícitas para transportar narcóticos hacia EE. UU. Esta iniciativa se enfocaba fundamentalmente en el fomento de una conciencia que diera prioridad a una mentalidad preventiva más que represiva o de reacción frente a los hechos consumados. Fue un concepto que rompió los esquemas de esquemas tradicionales y dio inicio al aporte del sector empresarial al desarrollo de políticas de seguridad de la cadena internacional de suministros.

Este nuevo esquema de seguridad preventiva captó crecientemente el interés y el apoyo no solo de las empresas latinoamericanas, sino también de los gobiernos y autoridades, gracias al decidido apoyo de la Aduana de los Estados Unidos. De esta manera, en BASC participan empresas productoras, exportadoras, importadoras, almacenes, terminales portuarios, agencias de aduana, y otras que prestan servicios en las operaciones de la cadena logística del comercio internacional.

En 2005, BASC establece la Norma Internacional BASC y los Estándares internacionales BASC, así como su Sistema de Gestión en Control y Seguridad (SGCS) BASC, que consolida en un solo documento la esencia y las herramientas BASC para su implementación práctica en las empresas. De esta forma, se ofrece la Certificación BASC que es aplicable a empresas de 18 sectores de la cadena logística de comercio internacional.

A la fecha, existen 25 capítulos nacionales en 13 países y 4,500 empresas con certificación BASC. Este logro es fruto del valioso apoyo del sector empresarial latinoamericano y la confianza depositada por parte de una larga lista de instituciones internacionales y supranacionales relacionadas a la gestión del comercio y la seguridad logística a nivel global, tales como la Organización Mundial de Aduanas (OMA), Cámara de Comercio Internacional – (CCI), Asociación Latinoamericana de Cámaras Americanas de Comercio (AACCLA) y AMCHAMS, Banco Interamericano de Desarrollo (BID) Washington, Embajadas de los Estados Unidos, Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDC), Organización de la Naciones Unidas (ONU), Pacific Economic Cooperation (APEC), World Bank, etc.

La más reciente versión de la Norma y Estándares internacionales BASC es la versión 6, lanzada en 2022 con la participación de la Organización Mundial de Aduanas (OMA), Aduana y Protección Fronteriza de los Estados Unidos (CBP), el Programa CTPAT, y autoridades aduaneras de diversos países.

Asimismo, la sexta versión es fruto de la Declaración Conjunta y Plan de Acción entre la Aduana de EE. UU. (CBP) y World BASC Organization (WBO) en 2021, así como de la consideración de los Criterios Mínimos de Seguridad (CMS) del programa CTPAT.

Uno de los cambios introducidos más notorios es la inclusión de la **ciberseguridad**. En concordancia con la Norma Internacional BASC v. 6, los Estándares Internacionales BASC v. 6.0 amplifican su enfoque a la **seguridad cibernética**. En la Guía de Implementación de la Norma Internacional BASC v.6 y los Estándares Internacionales BASC v. 6.0, se orienta a las empresas para que pongan en funcionamiento el Sistema de Gestión en Control y Seguridad (SGCS) BASC.

En la Guía de Implementación de Estándares Internacionales BASC se incluye bajo el título "Seguridad de la Información" el subtítulo "Ciberseguridad y tecnologías de la información", cuyo texto señala:

"Las acciones de ciberseguridad de la empresa deberían ser proporcionales al tamaño, la naturaleza, la criticidad de las operaciones y modelo de negocio. Las empresas que empleen accesos a través de autenticación multifactor, deberían tener en cuenta los factores requeridos para verificar la identidad de los usuarios. Periódicamente se le podría requerir al súper usuario la entrega de las credenciales de acceso a los sistemas y herramientas informáticas que formen parte de la infraestructura tecnológica de la empresa."

Por su parte, el documento "Estándar Internacional de Seguridad BASC v. 6.0.1" incluye en su capítulo 6 "Seguridad de la Información" el subtítulo "Ciberseguridad y las Tecnologías de la Información" donde enlista 22 recomendaciones específicas, entre las que figuran:

- Las empresas que empleen accesos a través de autenticación multifactor deberían tener en cuenta los factores requeridos para verificar la identidad de los usuarios.

- Periódicamente se le podría requerir al superusuario *(aquel que al interior de la empresa puede realizar todo tipo de cambios y acceder a la información del sitio y crear nuevos usuarios en una plataforma tecnológica)* la entrega de las credenciales de acceso a los sistemas y herramientas informativas que forma parte de la infraestructura tecnológica de la empresa.

En resumen, CTPAT no posee una guía o manual dedicado expresamente a la ciberseguridad, sino que está incluida en sus Criterios Mínimos de Seguridad (CMS), donde, a su vez, conduce a las empresas a seguir métodos y estrategias establecidos por otras entidades públicas y privadas dedicadas al desarrollo de herramientas de seguridad según sectores de la industria.

De modo similar a esta entidad estadounidense, BASC recomienda a sus empresas asociadas seguir las mejores prácticas de defensa contra todo tipo de amenaza cibernética, cuyos planes detallados de métodos y estrategias particulares para una actividad especifica, pueden ser encontrados en documentos técnicos producidos en entidades de desarrollo especializadas.

PERÚ CERTIFICATION

ISO 37301:2021
Sistema de Gestión de Compliance

Norma certificable que permite a una organización demostrar su compromiso de cumplimiento con las leyes, requisitos regulatorios, códigos de la industria y las normas que establece a nivel corporativo.

- Crea conciencia y una cultura de cumplimiento.
- Permite identificar riesgos y aprovechar oportunidades de manera estratégica.
- Mejora la confianza entre clientes y socios comerciales.
- Aumenta la transparencia en los procesos.
- Fortalece el buen gobierno corporativo.
- Atiende las necesidades y expectativas de todas las partes interesadas.
- Promueve prácticas comerciales éticas y salvaguarda la reputación.
- Garantiza el cumplimiento de las leyes, regulaciones y estándares éticos.

Destaco dos temas relevantes respecto a certificar en el **Sistema de Gestión de Compliance**:

En primer lugar, **mejora la cultura de cumplimiento** dentro de la organización, es decir, que todos los miembros valoran día a día lo que significa el riesgo de realizar conductas indebidas e ilegales que incluso pueden ser delictivas.

Lo segundo es la **puesta en valor de la organización frente a los colaboradores, clientes y proveedores**, pues genera confianza. Es una forma de decirle al mercado: estamos acá para hacer negocios transparentes con ustedes.

CARLOS CARO
CEO & Socio Fundador

C&A CARO & ASOCIADOS

Certifica. Destaca. Lidera.

946 454 057
paula.lopez@bascperu.org

Ciberseguridad en la Cadena Logística: Aplicación Práctica del Enfoque BASC en América Latina

Nicolás Rocca Aguirre
Regional Head Security & Operational Resilience SSA / PE
DHL Global Forwarding

En el contexto actual del comercio global, la ciberseguridad se ha convertido en un elemento estratégico para las empresas que forman parte de la cadena logística internacional. Transportistas, operadores logísticos, agentes de aduana, importadores y exportadores operan en un entorno cada vez más digitalizado, donde los riesgos no solo están en el robo físico, sino también en la intrusión digital, el espionaje informático y la manipulación de sistemas logísticos.

Frente a este desafío, el estándar BASC ofrece una guía completa y realista para proteger tanto la infraestructura física como los activos digitales que sostienen la continuidad operativa. En América Latina, BASC se ha posicionado como un referente para las organizaciones que buscan blindarse frente a amenazas cibernéticas sin descuidar la seguridad tradicional.

Más allá de muros y candados: el nuevo rostro de la seguridad logística

Durante años, la seguridad logística se asoció casi exclusivamente a medidas físicas: vigilancia, alarmas, control de accesos. Hoy, ese enfoque es insuficiente. La conectividad digital de los sistemas de transporte, almacenaje y despacho exige medidas que vayan más allá del perímetro físico.

El enfoque BASC entiende esta transformación. Su modelo promueve una seguridad integral, que combina la protección física con prácticas concretas de seguridad informática, control de accesos digitales, gestión de dispositivos y protección de datos operativos. No se trata de separar IT de operaciones, sino de integrarlas bajo un mismo sistema de gestión.

Ciberseguridad aplicada: medidas exigidas por BASC

Dentro de los lineamientos BASC, existen exigencias específicas orientadas a la prevención de amenazas cibernéticas que pueden comprometer operaciones críticas.

Entre ellas destacan:

- Reforzar los sistemas de control de acceso digital, aplicando autenticación multifactor (MFA) y perfiles de usuario definidos por función.
- Limitar el uso de dispositivos portátiles (laptops, celulares, USB) solo a equipos institucionales configurados con medidas de seguridad como cifrado, antivirus, y bloqueo por inactividad.
- Prohibir el ingreso de equipos externos no autorizados, especialmente en zonas críticas o conectadas a sistemas logísticos.
- Restringir el acceso a plataformas digitales sensibles (como ERP, TMS, WMS, GPS, cámaras) solo al personal autorizado y según su rol específico.
- Establecer políticas para el registro, custodia y auditoría de credenciales electrónicas, evitando el uso compartido de claves o usuarios genéricos.

Además, BASC recomienda mantener copias de respaldo protegidas, segmentar redes internas, actualizar periódicamente el software y reforzar los protocolos de monitoreo. Toda anomalía debe poder rastrearse y generar un evento auditable.

Protección de instalaciones críticas: la convergencia de IT y seguridad física

La ciberseguridad no se limita al plano digital. Las instalaciones logísticas modernas están equipadas con tecnologías que también deben protegerse: CCTV conectados a la red, sistemas de control de accesos digitales, alarmas inteligentes, sensores perimetrales, entre otros.

BASC insta a que toda infraestructura crítica, muelles, almacenes, salas de servidores, patios de carga, sea evaluada en función de su nivel de exposición. A partir de esa evaluación, se deben aplicar medidas combinadas:

- Controles físicos (barreras, torniquetes, rondas, iluminación).

- Controles electrónicos (biometría, tarjetas, cierres inteligentes).
- Controles digitales (monitoreo remoto, alarmas conectadas, registros electrónicos de acceso).

El enfoque no es únicamente técnico, sino estratégico y organizacional. Cada elemento forma parte de un sistema de prevención que, correctamente administrado, permite anticiparse a eventos que podrían interrumpir o comprometer la cadena de suministro.

Dispositivos portátiles y riesgos humanos: el eslabón más débil

Uno de los vectores más comunes de incidentes cibernéticos es el mal uso de dispositivos personales o institucionales por parte del personal propio o terceros. BASC establece como principio que toda terminal de acceso (computadora, celular, tablet) debe estar regulada por políticas claras, bajo control del área de seguridad o tecnología.

Los equipos deben contar con configuraciones de seguridad aprobadas, estar sujetos a control de versiones, y su uso debe ser exclusivo para actividades autorizadas. Asimismo, se recomienda aplicar listas blancas de software, limitar el acceso a redes públicas y establecer protocolos claros para la conexión de dispositivos externos, si es que se permite.

Una cultura de ciberseguridad sólida implica formación continua del personal, comunicación efectiva sobre buenas prácticas y compromiso institucional desde los líderes hasta el nivel operativo.

Puntos críticos y análisis de riesgo digital

El sistema de gestión BASC exige que cada organización identifique sus puntos críticos, tanto físicos como informáticos. Esto incluye sistemas que gestionan información sensible (valores de carga, rutas, clientes, registros de ingreso), así como zonas físicas con exposición elevada.

La metodología BASC orienta a aplicar análisis de riesgos periódicos, establecer matrices de criticidad y reforzar los controles en función del resultado. Esta lógica de gestión por riesgo permite priorizar inversiones y esfuerzos de seguridad de forma inteligente y efectiva.

Otras normas como referencia

Aunque BASC es el estándar más adaptado a la realidad logística latinoamericana, es totalmente compatible con otros marcos de ciberseguridad y gestión:

- ISO 27001: gestión de la seguridad de la información.
- ISO 28000: gestión de la seguridad en la cadena de suministro.
- NIST CSF: marco de referencia para ciberseguridad organizacional.
- AEO / OEA – CTPAT: programas internacionales de cumplimiento aduanero con enfoque en seguridad.

BASC se integra perfectamente a estos sistemas, actuando como un puente práctico entre la operación diaria y los requisitos globales.

Reflexión final: seguridad sin fronteras

En la logística internacional, los ciberataques, el robo de información y los accesos indebidos ya no son escenarios hipotéticos: son realidades recurrentes. Las organizaciones que adoptan una cultura de ciberseguridad no solo están mejor preparadas, sino que también transmiten confianza, credibilidad y profesionalismo.

El modelo BASC ofrece una ruta concreta para construir esa cultura, adaptada al sector logístico, con criterios verificables, enfoque operativo y reconocimiento regional. En un entorno de amenazas híbridas, proteger la cadena logística implica pensar en digital, actuar con integridad, y trabajar con visión global.

Porque en la seguridad de la carga y la información, lo que hoy se previene, mañana no se lamenta.

Fortaleciendo la ciberseguridad

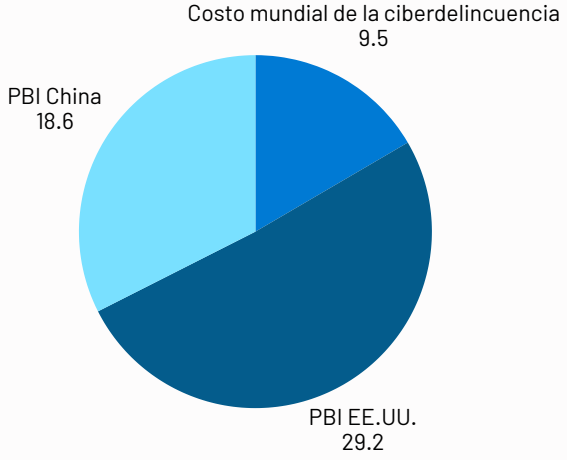
El crecimiento del costo de la ciberdelincuencia es imparable. Su valor ya representaría una hipotética tercera economía mundial después de EE. UU. y China

J.P. Morgan proyecta que el costo global de los delitos cibernéticos será de 23,84 billones de dólares anuales para 2027. Se trataría de un colosal incentivo financiero para que los ciberdelincuentes persistan en desarrollar estrategias cada vez más efectivas y dañinas. Hallar el valor real de este delito es prácticamente imposible porque depende de metodologías, variables a considerar, las ramificaciones entre ellas, los distintos niveles de las economías de cada país cubiertos, etc. También depende del tipo de resultado deseado: ingresos, ganancias, el costo para las economías, etc. Sin embargo, las estimaciones dan una idea de sus dimensiones.

Otra fuente de información de la ciberdelincuencia es Cybersecurity Ventures, empresa que investiga y publica la economía cibernética global y estadísticas sobre ciberseguridad. Esta organización estima que en 2024 la ciberdelincuencia costó al mundo 9,5 billones de dólares. Esta cifra nos dice que la ciberdelincuencia sería la tercera economía más grande del mundo después de Estados Unidos y China.

Valor de la ciberdelincuencia vs. PBI de principales países 2024

**En billones de dólares*



Dicho monto representa el daño total infligido, incluyendo: daños y destrucción de datos, robo de dinero, pérdida de productividad, robo de propiedad intelectual, robo de datos personales y financieros, malversación de fondos, fraude, interrupción del curso normal de los negocios tras un ataque, investigación forense, restauración y eliminación de datos y sistemas pirateados, y daño a la reputación.

Entre los ciberdelitos más lucrativos se encuentran el *ransomware (software malicioso que bloquea o cifra los archivos de una computadora o sistema y luego exige un rescate económico)*, que en 2024 registró un pago promedio de rescate mayor al millón de dólares; mientras que los ataques de *phishing (técnica de fraude digital que busca engañar a la víctima y así obtener información confidencial)*, tuvieron en 2023 un costo promedio de 4.9 millones de dólares por ataque para las empresas. Se estima que en un periodo de 02 a 19 segundos hay un ataque de ransomware a nivel internacional.

Hace cinco (05) años, la revista Cybercrime señalaba que la ciberdelincuencia sería uno de los mayores desafíos que enfrentará la humanidad en las siguientes dos décadas. El rápido crecimiento de esta economía delictiva representa una descomunal (*como desconocida)* transferencia de riqueza en la historia económica mundial, la misma que registra una rentabilidad más efectiva que el comercio de todos los tipos de narcóticos en el mundo.

En las cadenas de suministro

En el reciente foro sobre ciberseguridad 2025 realizado por el Foro Económico Mundial (FEM) se resaltó la creciente complejidad y el aumento de las amenazas del ciberdelito en las cadenas de suministro, ámbito en que la tecnología digital permite su expansión global pero también las hace vulnerables. *"Un solo ciberataque o una interrupción del servicio de TIC´s puede interrumpir ecosistemas enteros, como se vio en la interrupción global de 2024 causada por una actualización de seguridad defectuosa"*. señala el documento "Global Cybersecurity Outlook 2025" al tiempo de afirmar que "Resulta alarmante que el 54% de las grandes organizaciones identifiquen los desafíos de la

cadena de suministro como el mayor obstáculo para lograr la ciber resiliencia".

Para el FEM, la inestabilidad geopolítica está transformando las estrategias de ciberseguridad. Casi el 60% de las organizaciones afirman que el aumento de las tensiones influye en sus decisiones, desde las alianzas con proveedores hasta las políticas operativas. En este sentido, advierte que las empresas con recursos limitados son vulnerables porque las convierte en blancos fáciles para los ciberdelincuentes sofisticados. En general, durante 2024 se notó una creciente complejidad del escenario internacional en la que el ciberdelito es percibido como una amenaza real y creciente.

Implicancias de ataques cibernéticos

Hace poco, el 23 de junio del presente año, el portal Cybernews reportó que según una investigación 16 mil millones de contraseñas habrían sido expuestas mediante una "filtración de datos que abre el acceso a Facebook, Google, Apple y cualquier otro servicio imaginable". Este portal considera que *"recopilar información confidencial innecesariamente puede ser tan perjudicial como intentar robarla activamente"*. Esta enorme cantidad de datos expuesta respondería a un modelo de explotación masiva vía malware.

Los ciberdelincuentes ahora tendrían acceso sin precedentes a credenciales personales que pueden usarse para el robo de cuentas, el robo de identidad y el phishing altamente selectivo. Además, lo preocupante es la estructura y la actualidad de los datos. No se trata solo de filtraciones antiguas recicladas. *"Se trata de inteligencia nueva y susceptible de ser utilizada como arma a gran escala"*. No está claro quién controla esas grandes cantidades de datos. La mayoría de los conjuntos de datos descubiertos fueron "accesibles temporalmente a través de Elasticsearch o instancias de almacenamiento de objetos no seguras".

¿Qué pueden hacer los hackers con las contraseñas? Si las contraseñas se filtran, el daño puede ir mucho más allá de una sola cuenta. En el peor de los casos, los hackers pueden suplantar la identidad digital. Una vez que alguien accede a un correo electrónico, por ejemplo, puede restablecer las contraseñas de otras cuentas y obtener acceso a prácticamente todo. Puede tomar su cuenta como rehén: el hacker puede iniciar sesión y bloquearle cambiando su contraseña y la información de recuperación. A veces le pedirá dinero para devolverla, mientras usa su perfil virtual para actividades maliciosas sin que usted se de cuenta. Si acceden a su cuenta bancaria o a algún dato personal, pueden hacerse pasar por usted vaciando sus cuentas, creando correos electrónicos o mensajes que parezcan totalmente reales, engañar a sus contactos para que hagan clic en un enlace o compartan información, etc.

Pueden usar su contraseña en otras de sus cuentas, rastrear su actividad en línea, robar y vender su información personal en la *Dark Web (parte oculta de la Internet que no encontrará en Google ni en otros buscadores)*. Para acceder a ella, necesita un software especial como el *navegador Tor (sistema que permite navegar por internet de forma anónima y segura, ocultando tu identidad y ubicación)*. Los ciberdelincuentes la utilizan como mercado para comprar, vender o intercambiar información robada.

Casos de ciberataque

Según Microsoft, alrededor de 600 millones de ciberataques ocurren cada día en todo el mundo. Estos ciberataques están referidos a "señales de seguridad" o "intentos/eventos detectados" por lo que la cifra refleja la cantidad de actividades maliciosas, intentos de ataque, detecciones de malware, escaneos de vulnerabilidades, correos de phishing, y otras señales de seguridad que sus sistemas de defensa y telemetría detectan diariamente. De esta manera, en años recientes sucedieron incontables casos de ciberataques, de los cuales la siguiente relación es una muestra de ejemplos.

Registrados en 2023

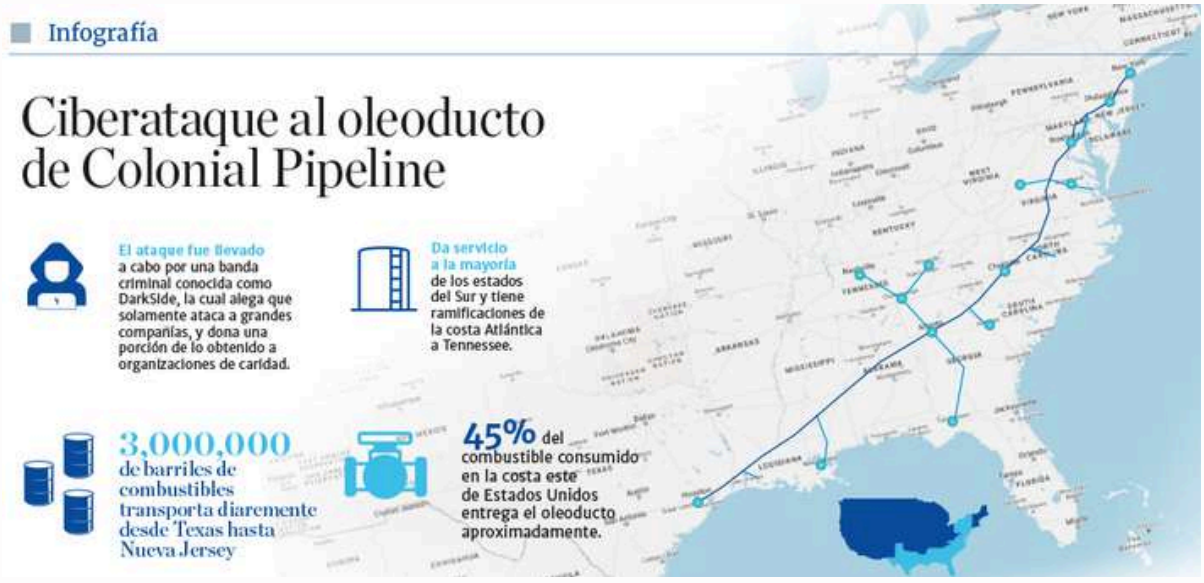
- **Robo de registros del Departamento de Estado de EE.UU.:** Hackers vulneraron Microsoft Exchange y robaron decenas de miles de correos electrónicos con al menos **60,000 correos** extraídos de las cuentas de Outlook de esta dependencia de EE. UU.
- **Fallo de protección de datos de DarkBeam:** La filtración provino de una empresa de protección digital, que expuso **3,800 millones de registros**, convirtiéndola en una de las mayores filtraciones de datos de los últimos tiempos. Fueron afectados correos electrónicos y contraseñas de usuarios.
- **Ataque de ransomware a Royal Mail:** El servicio de correos del Reino Unido sufrió un ciberataque de ransomware que interrumpió sus servicios de correo internacional. Los hackers exigieron un rescate de 80 millones de dólares y el ataque **afectó a 11,500 sucursales de correos**, impidiéndoles gestionar paquetes internacionales.
- **Robo de datos de MOVEit:** Grupos de ciberdelincuentes explotaron vulnerabilidades en el

software de transferencia de archivos MOVEit de Progress Software y lo utilizaron para robar datos de sus bases de datos. Más de 2.000 organizaciones se vieron afectadas, así como los datos de más de 60 millones de personas.

- **Robo de pasaportes en Indonesia:** Los **pasaportes de 34 millones de ciudadanos fueron robados en Indonesia.** El autor fue un *hacktivista* llamado Bjorka. Los datos robados incluían nombres completos, género, número de pasaporte y fecha de nacimiento, el país se preparó para estafas y fraudes de identidad.

Otros casos

- En 2017, la cadena de comida rápida **Chipotle** en EE.UU. descubrió un ataque de malware que atacó la mayoría de sus tiendas. Chipotle lanzó una herramienta de localización para que un cliente verifique si fue víctima del ataque. El malware buscó datos de la banda magnética de una tarjeta a través del dispositivo POS.
- El ransomware llamado **"WannaCry"** hackeó miles de computadoras con Windows en 2017. Exigió un pago en Bitcoin para desbloquearlos. Más de **200.000 computadoras en 150 países fueron atacadas.** Entre las víctimas se incluyen hospitales en Reino Unido, FedEx, Ferrocarriles Rusos, y una fábrica de Honda en Japón.
- En 2017, el malware **"GoldenEye"**, parte del ransomware **Petya**, inutilizó ordenadores en todo el planeta. Afectó sistemas de grandes empresas en **más de 65 países**. Además, el ciberataque comenzó infectando la red eléctrica, el aeropuerto y las oficinas gubernamentales de Ucrania. Luego, afectó también a la petrolera rusa Rosneft, a la naviera Maersk y la farmacéutica Merck.
- En 2021, **el gobierno de EE.UU.** declaró un estado de emergencia regional tras un ciberataque a la mayor red de oleoductos del país. Los atacantes desconectaron y robaron más de 100 GB de información del Oleoducto Colonial, que transporta el 45% del suministro de diésel, gasolina y combustible que consumen los aviones de la costa este.
- También en 2017, la aplicación móvil de **Pizza Hut** en EE.UU. fue hackeada para robar información confidencial de los clientes, incluyendo nombres, correos electrónicos, direcciones y números de tarjetas de crédito. **70,000 personas que hicieron pedidos los días del hackeo sufrieron el robo de su información.**



Fuente: Globalenergy.mx

Estrategias para reforzar la ciberseguridad

Las contraseñas seguras, el uso adecuado de software, la precaución con enlaces sospechosos y la autenticación multifactor resumen los pilares básicos de las buenas prácticas de ciberseguridad tanto para personas como para organizaciones

En un escenario mundial en el que la tecnología de la información participa cada vez más en todos los aspectos de nuestra vida diaria, existe un riesgo creciente de eventos ilícitos basados en esta tecnología que podrían ocurrir y generar consecuencias negativas de diferentes escalas. Las consecuencias pueden causar daños a personas y organizaciones o interrumpir servicios públicos, a diferentes escalas. Para evitar esto hay una sola manera: **desarrollar e implementar las mejores prácticas de ciberseguridad por parte de personas y organizaciones de todo tamaño,** ya sean gubernamentales como privadas.

Para la America's Cyber Defense Agency (ACDA) de EE.UU. l**os fundamentos para una buena ciberseguridad son:**

- Usar contraseñas seguras
- Actualizar el software
- Pensar antes de hacer clic en enlaces sospechosos
- Activar la autenticación multifactor

Estas cuatro prácticas de ciberseguridad parecen resumir el contenido de las recomendaciones que hacen la mayoría de las organizaciones privadas y gubernamentales dedicadas a la protección cibernética. Entre estas buenas prácticas destaca la autenticación multifactor, un método multicapa de protección. Para ingresar, el usuario debe proporcionar una combinación de dos o más autenticadores para verificar su identidad antes de que se le permita el acceso. Si un ciberdelincuente compromete un primer nivel (como la contraseña), no podrá cumplir con la segunda capa de autenticación.

La European Union Agency for Cibersecurity, creada en 2004 para contribuir con la política cibernética de la Unión Europea, comparte las herramientas sugeridas por el ACDA estadounidense y recomienda otras medidas como el desarrollo de la cultura de seguridad y la capacitación del personal, el desarrollo de un plan de respuestas, el uso de la nube, entre otros.

Otra organización estadounidense, la U. S. Small Business Administration, dirige su atención a las pequeñas empresas, considerando que estas se sienten vulnerables a un ciberataque y que muchas no pueden acceder a soluciones profesionales de tecnologías de información (TIC's).

En este sentido, enfoca sus recomendaciones en la **capacitación de los empleados, proteger las redes, habilitar la MFA, usar la nube, y asegurar los procedimientos internos.**

A continuación, estas y otras medidas:

J. P. Morgan

- **Implementar políticas sólidas:** Deben describir las mejores prácticas para los empleados. Abarcar la gestión de contraseñas, la protección de datos y el uso adecuado de los recursos. Revisar y actualizar periódicamente la política
- **Educar y capacitar a los empleados: El error humano es el punto más débil de la ciberseguridad.** Realizar capacitación periódica. Fomente una cultura de vigilancia donde los empleados se sientan cómodos al reportar actividades sospechosas sin temor a represalias.
- **Usar autenticación multifactor:** Usar contraseñas seguras y únicas para todas las cuentas de la empresa.

- **Las contraseñas deben ser largas y complejas:** La MFA requiere dos o más factores de verificación para acceder a una cuenta.
- **Actualizar el software y los sistemas periódicamente:** Las actualizaciones incluyen parches de seguridad para las vulnerabilidades explotadas por los ciberdelincuentes. Automatizar las actualizaciones.
- **Realizar auditorías de seguridad:** Utilizando sus resultados identificar y abordar vulnerabilidades. Fortalecer la estrategia de ciberseguridad y mitigar los riesgos.
- **Hacer copias frecuentes de seguridad:** En una ubicación externa segura para garantizar una rápida restauración de datos.
- **Utilizar tecnologías de seguridad avanzadas:** Esto incluye firewalls, sistemas de detección de intrusiones, software antivirus y cifrado. Pueden detectar y prevenir ciberataques.
- **Supervisar el tráfico de red:** Usar herramientas de monitorización de red para analizar continuamente en busca de actividades inusuales. Tener protocolos claros para responder a las amenazas detectadas y garantizar una respuesta eficaz.
- **Garantizar entornos de trabajo remoto seguros:** Proteger el acceso remoto a su red. Utilice redes privadas virtuales (VPN) para cifrar los datos transmitidos entre los trabajadores remotos y su red.
- **Desarrollar un plan de respuesta a incidentes:** El plan debe describir los pasos a seguir en caso de vulneración. Pruebe y actualice el plan periódicamente.

US Federal Communications Commission

- **Capacitar en principios de seguridad:** Exigir contraseñas seguras, pautas para el uso de Internet y sanciones por infringir las reglas. Establecer normas de comportamiento para manejar y proteger la información de los clientes.
- **Proteger la información, las computadoras y las redes:** Mantener los equipos con software de seguridad, el navegador web y el sistema operativo más recientes. Configurar el antivirus para que analice después de cada actualización.
- **Proteger su conexión a Internet:** Un firewall es un conjunto de programas relacionados que impiden que personas externas accedan a los datos de una red privada. Si hay trabajo remoto, asegúrese de usar esta herramienta.
- **Crear plan de acción para dispositivos móviles:** Estos presentan desafíos de seguridad y administración, especialmente si contienen información confidencial o pueden acceder a la red corporativa.
- **Control del acceso físico a computadoras:** Crear cuentas de usuario para cada empleado. Los privilegios administrativos solo para personal de TI de confianza y al personal clave.
- **Proteger las redes Wi-Fi:** Debe ser segura, cifrada y oculta. Para ocultarla configure su enrutador para que no difunda el nombre de la red (SSID). Proteja el acceso al enrutador con contraseña.
- **Aplicar las mejores prácticas con las tarjetas de pago:** Colabore con los bancos utilizando herramientas y servicios antifraude. **Aísle los sistemas de pago no utilizando la misma computadora para procesar pagos y navegar por internet.**
- **Accesos limitados de empleados a los datos y la información, y para instalar software:** Los empleados solo deben tener acceso a los sistemas de datos específicos que necesitan y no deben poder instalar ningún software sin permiso.
- **Contraseñas y autenticación:** Usar contraseñas únicas. Cambiarlas cada tres (03) meses. Considere implementar la autenticación multifactor.

European Union Agency for Cybersecurity

- **Desarrollar cultura de ciberseguridad:** Designar la gestión de recursos, formación del personal y desarrollo de políticas eficaces. Lograr la aceptación vía comunicación eficaz. Realizar auditorías con independencia. Publicar las políticas de ciberseguridad.
- **Proporcionar capacitación adecuada:** Capacitación periódica a los empleados incluyendo a responsables de la ciberseguridad para garantizar que cuenten con las habilidades y competencias necesarias para realizar su trabajo.
- **Garantizar una gestión eficaz de terceros:** Todos los proveedores, en particular aquellos con acceso a datos o sistemas sensibles, deben tener contratos con la empresa para cumplir con los requisitos de seguridad.
- **Desarrollar plan de respuesta a incidentes:** Un plan formal con directrices claras y responsabilidades documentadas para que los incidentes se respondan de manera oportuna, profesional y adecuada.
- **Acceso seguro a los sistemas: Usar una frase como contraseña.** Habilite la autenticación multifactor. Use un administrador de contraseñas dedicado.
- **Gestión de dispositivos móviles:** En el teletrabajo, emplear Gestión de Dispositivos Móviles (MDM) para controlar el acceso a los sistemas y borrar remotamente datos en casos de pérdida o robo.
- **Mejorar la seguridad física:** En los dispositivos electrónicos activar el bloqueo automático. Supervisar los documentos impresos confidenciales.
- **Sitio web configurado de forma segura:** Proteger cualquier dato personal o financiero. Esto implica realizar pruebas de seguridad periódicas en el sitio web de la empresa.
- **Aprovechar la nube:** Ofrecen ventajas, pero también presentan riesgos que se deben considerar antes de contratar un proveedor.

Reporte de Embarque Sospechoso

Informa oportunamente a las autoridades competentes sobre la detección de embarques sospechosos.

www.bascperu.org

Glosario: Ciberseguridad en el Sistema de Gestión en Control y Seguridad BASC

La ciberseguridad forma parte de la más reciente versión 06 de la Norma Internacional BASC y de los Estándares Internacionales BASC, dos documentos que dan cuerpo al Sistema de Seguridad de Gestión en Control y Seguridad (SGCS) BASC

El **"Glosario de Términos y Definiciones"** complementa dichos documentos oficiales al poner en claro las ideas y definiciones de la terminología empleada por BASC en su trabajo con las empresas miembro durante la implementación del SGCS BASC. Los siguientes conceptos parten de la terminología citada:

- **Acción correctiva:** Conjunto de actividades que permite eliminar la causa de una no conformidad y evitar que vuelva a ocurrir.
- **Actividad sospechosa:** Son aquellas operaciones inusuales que, de acuerdo con razones objetivas, son identificadas como sospechosas.
- **Acuerdo de seguridad:** Es el compromiso documentado en seguridad que una empresa Certificada BASC acuerda con su asociado de negocio no BASC para que este cumpla con los criterios de Seguridad acordados entre las partes.
- **Área crítica:** Espacio físico en el que se identifica una alta probabilidad de ocurrencia de riesgos (o combinación de estos) que representen un impacto significativo en la seguridad de la empresa.
- **Autenticación multifactor:** Tecnología de seguridad que requiere múltiples métodos de autenticación para verificar la identidad de un usuario. Combina dos o más credenciales independientes: lo que el usuario sabe, como una contraseña; lo que tiene el usuario, como un token de seguridad y qué es el usuario, mediante el uso de métodos de verificación biométrica.
- **Cadena de custodia:** Proceso ordenado mediante el cual se transfiere la responsabilidad de la integridad de la carga, la unidad de carga o la información de un custodio previo al próximo custodio dentro del modelo operativo (cadena logística), evidenciando mediante registros de trazabilidad esta transferencia segura.
- **Ciberdelincuencia:** Acto que infringe la ley y que se comete usando las tecnologías de la información y la comunicaciones (TIC´s) para atacar las redes, sistemas, datos, sitios web y la tecnología o para facilitar un delito.
- **Ciberseguridad:** Proceso de identificar, analizar, evaluar y comunicar un riesgo cibernético y aceptarlo, evitarlo, traspasarlo o mitigarlo a un nivel aceptable, tomando en consideración los costos y beneficios para la empresa. Se enfoca en proteger las computadoras, las redes, los programas y los datos del acceso, el cambio y la destrucción no deseados o no autorizados.
- **Comercio electrónico:** También conocido como comercio por Internet o comercio en línea o *e-commerce*, , consiste en la compra y venta de productos o de servicios a través de internet, tales como redes sociales y otras páginas web.
- **Geolocalización (GPS):** Identificación de la ubicación geográfica a partir de un dispositivo conectado a Internet. Existen muchas tecnologías aptas para determinar la geolocalización de una persona o equipo. Capacidad de rastrear el paradero de un dispositivo utilizando GPS, torres de teléfonos celulares, puntos de acceso Wi-Fi o una combinación de estos.

- **Información sensible:** Información privada de un individuo o empresa, por ejemplo, ciertos datos personales y bancarios, contraseñas de correo electrónico e incluso el domicilio en algunos casos.
- **Seguridad de la información:** Conjunto de controles operacionales enfocados en la prevención y mitigación de los riesgos relacionados con la información.
- **Superusuario:** Es aquel que al interior de la empresa puede realizar todo tipo de cambios y acceder a la información del sitio y crear nuevos usuarios en una plataforma tecnológica.
- **Tecnologías de la Información:** Comprende las computadoras, el almacenamiento, las redes y otros dispositivos físicos, la infraestructura y los procesos para crear, procesar, almacenar, garantizar e intercambiar todas las formas de datos electrónicos.
- **Teletrabajo:** Trabajo que una persona realiza para una empresa desde un lugar remoto de la sede de ésta, por medio de un sistema de telecomunicación.

Asimismo, es importante resaltar los siguientes conceptos del Instituto Nacional de Ciberseguridad (INCIBE). **Glosario de términos de ciberseguridad: Una guía de aproximación para el empresario.** Gobierno de España, s.f.

- ***Adware:*** Software que se apoya en anuncios (normalmente para financiarse) como parte del propio programa. En algunos casos se les considera malware. Común en las versiones gratuitas en las aplicaciones.
- ***Captcha*:** Acrónimo en inglés de Completely Automated Public Turing test to tell Computers and Humans Apart; en español, prueba de Turing completamente automática y pública para diferenciar ordenadores de humanos, es un tipo de medida de seguridad que consiste en la realización de pruebas desafío-respuesta controladas por máquinas que sirven para determinar cuándo el usuario es un humano o un bot según la respuesta a dicho desafío.
- **Cifrado de extremo a extremo:** Es la propiedad de algunos sistemas de comunicación que hace que los mensajes intercambiados sean ilegibles durante la comunicación en caso de interceptación al estar cifrados. Al ser de extremo a extremo, implica que solo emisor y receptor podrán descifrar y conocer el contenido del mensaje.
- ***Cookie:*** Pequeño fichero que almacena información enviada por un sitio web y que se almacena en el equipo del usuario, de manera que el sitio web puede consultar la actividad previa del usuario.
- **Correo *spam*:** Tipo de correo electrónico que se caracteriza por ser no solicitado por el receptor y que

se envía en grandes cantidades con fines publicitarios o como complemento de actividades maliciosas como los ataques de phishing.
- ***Cracker*:** Ciberdelincuente que se caracteriza por acceder de forma no autorizada a sistemas informáticos con la finalidad de menoscabar la integridad, la disponibilidad y el acceso a la información disponible en un sitio web o en un dispositivo electrónico.
- **Doble factor de autenticación:** Esquema de autenticación básica a la que se añade otro factor como puede ser un código enviado a un móvil, huella dactilar, sistema OTP, etc., más seguro que la autenticación simple.
- ***Hacktivista:*** Ciberdelincuente que haciendo uso de sus conocimientos en materia informática y herramientas digitales los usa para promover su ideología política. Entre las acciones que realizan destacan las modificaciones de webs (defacement), redirecciones, ataques de denegación de servicio (DoS), robo de información privilegiada o parodias de sitios web, entre otras. Estos actos son llevados a cabo por estas personas bajo la premisa de potenciar otros actos como la desobediencia civil con el fin último de lograr sus propósitos políticos.
- **Huella digital:** Mecanismo cuyo propósito principal es combatir la piratería digital y defender los derechos de autor mediante la introducción de una serie de bits o datos aleatorios imperceptibles que permiten detectar si la copia es legítima o no.
- ***Plugin:*** También conocida como extensión, complemento o add-on es una aplicación que se relaciona con otra para agregarle una función nueva y generalmente muy específica. Las extensiones son un tipo de software que permite personalizar entre otros los navegadores web.
- ***Ransomware:*** Malware cuya funcionalidad es «secuestrar» un dispositivo (en sus inicios) o la información que contiene de forma que si la víctima no paga el rescate, no podrá acceder a ella.
- ***Troyano:*** Malware diseñado para tener múltiples utilidades, la más común es crear una puerta trasera en el equipo infectado, para poder descargar actualizaciones y nuevas funcionalidades. Esta diseñado para ser controlado desde un centro de comando y control (C&C).
- ***Zero day:*** Son aquellas vulnerabilidades en sistemas o programas informáticos que son únicamente conocidas por determinados atacantes y son desconocidas por los fabricantes y usuarios. Al ser desconocidas por los fabricantes, no existe un parche de seguridad para solucionarlas.

Conoce nuestras Actividades en el año

Como cada año, el Capítulo BASC PERÚ organiza y participa de eventos de interés para el sector. Asimismo, fomenta espacios de encuentro entre empresas certificadas a nivel nacional

14° Encuentro de Auditores Internos BASC PERÚ

El evento fue un espacio clave para actualizar conocimientos, intercambiar experiencias y reflexionar sobre el papel estratégico del auditor interno frente a los nuevos retos del entorno empresarial

Transformación digital, ciberseguridad y liderazgo en la auditoría interna fueron los ejes del XIV Encuentro Nacional de Auditores Internos BASC, realizado el jueves 19 de junio con la presencia de alrededor de **200 auditores internos de empresas certificadas a nivel nacional.**

La jornada reunió a destacados ponentes como el **Sr. Juan García**, especialista en Neuroauditoría; **Sr. Mario Yunis**, experto en transformación digital y la **Sra. Fátima Toche**, referente en derecho digital y ciberseguridad. Cada presentación ofreció una perspectiva sobre cómo la función del auditor debe adaptarse a los escenarios más complejos, tecnológicos y cambiantes en los que vivimos en la actualidad.

"El auditor interno es un actor clave para reforzar la cultura de prevención en su respectiva empresa", destacó el Sr. César Venegas, Director Ejecutivo de BASC PERÚ, quien enfatizó el **compromiso de la organización con el fortalecimiento permanente de las competencias profesionales de su red de auditores internos BASC.**

El evento incluyó un espacio de integración, premios sorpresa y una fotografía protocolar que cerró una jornada de alto valor profesional. Una vez más, **BASC PERÚ** reafirma que **la confianza en los negocios se construye desde la auditoría interna, con ética, visión panorámica y capacidad de transformación.**

BASC PERÚ presente en el Congreso Nacional BASC COLOMBIA 2025

El Director Ejecutivo de BASC PERÚ, Sr. César Venegas, participó en el Congreso Nacional BASC Colombia 2025, llevado a cabo el 05 de junio en la ciudad de Bogotá

Durante esta enriquecedora jornada acerca de **"La seguridad de la cadena de suministro, un compromiso de todos"**, se abordaron temas como el riesgo geopolítico global, la seguridad en la cadena de suministro como compromiso transversal en todos los sectores económicos, la innovación de la IA y gestión de riesgos para el éxito empresarial, el comercio seguro, compliance, estrategias y buenas prácticas para la prevención de delitos, la importancia del trabajo colaborativo entre el sector privado y las autoridades, entre otros.

Estos encuentros contribuyen a **fortalecer la integridad, la confianza y la competitividad en el comercio internacional**, al mismo tiempo, reafirman nuestro compromiso con el desarrollo de cadenas de suministro seguras, éticas, sostenibles y resilientes, en colaboración con los capítulos BASC de la región y en alianza con los sectores público y privado.

Actividades de BASC PERÚ | Junio

Reunión del Comité Técnico de World BASC Organization

Nuestro Director Ejecutivo de BASC PERÚ, Sr. César Venegas Núñez, miembro principal del Comité Técnico de WBO, participó en reuniones de Trabajo el martes 03 y miércoles 04 de Junio en las instalaciones del capítulo BASC Bogotá, Colombia, aprovechando el marco del Congreso Nacional BASC Colombia 2025, para continuar con el **Plan de Trabajo aprobado por la junta directiva de WBO**.

Entre otros temas se revisó el proyecto de Estándar/Reglamento de competencias de Auditores Internos.



Charla de Sensibilización y Ceremonia de Reconocimiento a Empresas BASC en Chimbote

El pasado 12 de junio se realizó en la ciudad de Chimbote una Charla de Sensibilización para Asociados de Negocio de empresas BASC y una Ceremonia de Reconocimiento a empresas que mantienen ininterrumpidamente su certificación BASC por más de 20, 15, 10 y 05 años.

El evento contó con una presentación sobre los "Desafíos de seguridad en el comercio exterior", a cargo de la Srta. Yesica Zevallos, Auditora Internacional BASC. Asimismo, el Sr. Gregorio Zurita, Superintendente de Planta Chimbote de **COPEINCA** brindó un testimonio de agradecimiento por sus más de 15 años ininterrumpidos como empresa certificada BASC y comentó acerca de las buenas prácticas que se implementaron con sus *stakeholders*. El evento contó con la presencia de más de 55 personas.



Actividades de BASC PERÚ | Mayo

Webinar BASC "Ciberdelincuencia: Impacto en la cadena de suministro"

El pasado 22 de mayo se llevó a cabo nuestro webinar "Ciberdelincuencia: Impacto en la cadena de suministro".

El evento contó con las palabras de bienvenida de nuestro Director Ejecutivo, luego la participación de la Sra. Yolanda Chacón, Especialista en Seguridad de la Información en el marco del Plan de Gobierno Digital en el **Ministerio de Salud** del Perú, quien explicó sobre los desafíos que afronta la ciberseguridad en la cadena de suministro, seguido del Ing. Javier Garay, Gerente de Innovación y Transformación Digital en **TLI (Técnica Logística Integral)**, quien expuso sobre las buenas prácticas y estrategias de defensa para resguardar la ciberseguridad de sus operaciones.

Más de 350 asistentes participaron y ampliaron sus conocimientos en este tema que cada vez cobra más relevancia dentro del mundo del comercio internacional.

Ingrese a nuestro **canal de Youtube BASC PERÚ** para acceder al webinar completo.

Charla de Sensibilización y Ceremonia de Reconocimiento a Empresas BASC en Trujillo

El 29 de mayo se realizó en Trujillo una Charla de Sensibilización para Asociados de Negocio no BASC y una Ceremonia de Reconocimiento a empresas que mantienen ininterrumpidamente su certificación BASC por más de 20, 15, 10 y 05 años.

El evento contó con las ponencias del Sr. César Venegas, Director Ejecutivo de BASC PERÚ y del Sr. Javier Mejía, Gerente de Operaciones de **CAMPOSOL**, quien compartió buenas prácticas como empresa certificada desde hace más de 22 años. Reconocemos el compromiso de las empresas y sus asociados por seguir fortaleciendo una cadena de suministro segura.

Actividades de BASC PERÚ | Mayo

Charla de Sensibilización y Ceremonia de Reconocimiento a Empresas BASC en Ica

El pasado jueves 08 de mayo se realizó una charla de sensibilización en la ciudad de Ica para empresas no BASC, contó con la ponencia de nuestro Director Ejecutivo, Sr. César Venegas y del Sr. César Rojas, Gerente General del Puerto de Paracas, quien compartió buenas prácticas como empresa certificada BASC.

Posteriormente, se llevó a cabo una ceremonia de reconocimiento a organizaciones que han mantenido de manera ininterrumpida su certificación BASC por más de 20, 15, 10 y 05 años. En representación de las empresas reconocidas, el Sr. Juan José Córdova Benavides, Gerente General de **Textil del Valle**, compartió su testimonio tras más de 22 años de estar certificados, resaltando cómo BASC ha generado y genera valor real en sus colaboradores, operaciones y relaciones comerciales con marcas globales como Patagonia, Lacoste, Ralph Lauren, Burberry, entre otras. El evento reunió a más de 80 participantes.



Comité de Seguridad BASC: Zona Centro Sur

El pasado 16 de mayo, se llevó a cabo el "Comité de Seguridad – Zona Centro Sur", en las instalaciones del Puerto de Paracas. Este encuentro reunió a más de 30 participantes de 14 empresas certificadas BASC, con el objetivo de reforzar el intercambio de experiencias, buenas prácticas y estrategias orientadas a fortalecer la seguridad en la cadena de suministro internacional.

Como parte de la agenda del evento, se contó con la participación del Sr. Carlos Reyes, Gerente de Operaciones de BASC PERÚ, quien compartió información relevante sobre la gestión de riesgos en el comercio internacional y la ponencia del Coronel PNP José Rengifo Reátegui, representante de la **DIRANDRO**, quien realizó una presentación enfocada en las amenazas actuales del narcotráfico en el ámbito portuario y logístico, así como las acciones articuladas entre el sector público y privado para su prevención.


Actividades de BASC PERÚ | Abril

Charla de Sensibilización y Ceremonia de Reconocimiento a Empresas BASC Chiclayo

El 10 de abril más de 40 asociados de negocio participaron en la charla de sensibilización realizada por nuestro Director Ejecutivo, organizada por BASC PERÚ en Chiclayo, seguida de una ceremonia de reconocimiento a empresas que mantienen ininterrumpidamente su certificación BASC por más de 5, 10, 15 y 20 años.

El Sr. Marco Antonio Claros, Jefe de Planta del **Complejo Agroindustrial BETA**, brindó un valioso testimonio en representación de las organizaciones destacadas.
Agradecemos a las empresas de la región por su compromiso con un comercio internacional más seguro con ética y calidad.

Charla de Sensibilización y Ceremonia de Reconocimiento a Empresas BASC Arequipa

El día 22 de abril, más de 60 asistentes participaron en una jornada especial organizada por BASC PERÚ en Arequipa, que incluyó una Charla de Sensibilización para Asociados de Negocio no BASC realizada por nuestro Director Ejecutivo y posteriormente una Ceremonia de Reconocimiento a empresas que mantienen ininterrumpidamente su certificación BASC por más de 20,10 y 05 años.

Durante el evento, el Sr. Humberto Moreno, Gerente SSOMA de **TASA**, compartió cómo su primera certificación BASC en 2004, fue clave para fortalecer sus procesos, logrando contar hoy, con 11 sedes certificadas. “BASC es un aliado estratégico”, destacó.

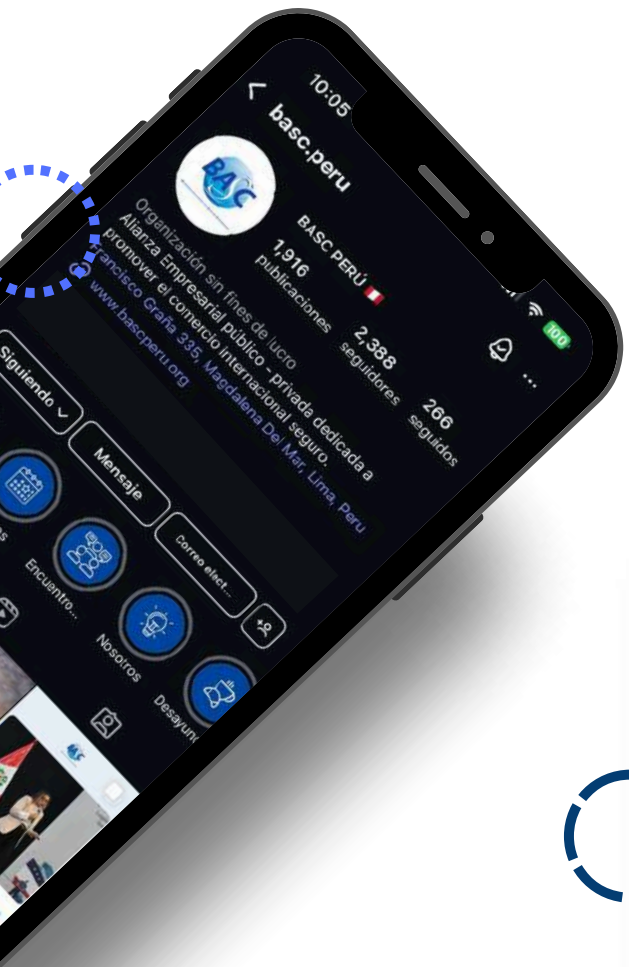
Ceremonia de Bienvenida a nuevas empresas BASC en nuestra sede institucional

El 29 de abril se llevó a cabo la “Ceremonia de Bienvenida BASC”, dirigida a las empresas que certificaron en el periodo diciembre 2024 – marzo de 2025.

El evento inició con unas palabras de felicitación por parte de la Sra. Suzanne Lemaitre, Directora Ejecutiva de World BASC Organization. Posteriormente, el Sr. César Venegas Núñez, Director Ejecutivo del Capítulo, brindó un cordial agradecimiento por la confianza depositada en el capítulo BASC PERÚ y en el SGCS BASC. Asimismo, los jefes de área presentaron los beneficios con los que cuentan nuestras empresas certificadas.

Entérese de todas nuestras novedades:

@bascperu



Revista especializada
elaborada por el Capítulo BASC PERÚ