BASC NOTICIAS

BOLETÍN MENSUAL DE LA ALIANZA EMPRESARIAL PARA UN COMERCIO SEGURO - BASC PERÚ

Más de 25 años generando confianza en la cadena de suministro del comercio internacional.

Nº 176 Edición **Abril 2024**

BASC PERÚ capacitó a funcionarios de organizaciones vinculadas al comercio exterior peruano

INFORMATIVO BASC PERÚ

Boletín mensual de la Alianza Empresarial para un Comercio Seguro - BASC PERÚ, Asociación sin fines de lucro adscrita al World BASC Organization - WBO, con presencia en 17 países.

COMITÉ EDITORIAL

Director:
César Venegas Núñez

Edición y Diagramación:
Anyanela Torres Palo
Rafaella Gonzales Laos
Gianella Golac Zamora

CONTENIDO BASC

Edición | Abril - 2024

BUSINESS ALLIANCE FOR SECURE COMMERCE

DIRANDRO

DICAPI

Palabras del Director Ejecutivo

CÉSAR VENEGAS NÚÑEZ

Estimados colaboradores de nuestras empresas certificadas BASC, reciban un cordial saludo a nombre del equipo de BASC PERÚ. Como parte de nuestra labor diaria, quisiera informarles sobre los logros obtenidos durante el mes de abril: **el capítulo logró la capacitación de más de 1,850 colaboradores de empresas BASC a través del desarrollo de más de 40 capacitaciones, entre presenciales y *online***. Asimismo, **identificamos más de 320 aportes al comercio internacional mediante la ejecución de más de 72 auditorías de certificación y recertificación BASC**, las mismas que se orientan a la mejora continua con base en la trazabilidad de la cadena de suministro.

Manteniendo nuestro compromiso de promover un comercio internacional seguro entre todos los actores que intervienen en la cadena de suministro, se capacitó gratuitamente a un grupo de funcionarios pertenecientes a organizaciones vinculadas al comercio internacional.

Finalmente, a nombre de World BASC Organization (WBO), hago extensiva la invitación para que participen en el **"11vo congreso Mundial BASC"**, que se realizará los días 25 y 26 de setiembre en la ciudad de Miami, Estados Unidos. Este importante encuentro nos permitirá seguir promoviendo el trabajo conjunto entre el sector público y privado, así como **generar confianza en los negocios** entre empresas BASC a nivel global.

¡TODOS SOMOS BASC!

IMPACTO DE BASC PERÚ

Abril 2024

1,851 COLABORADORES CAPACITADOS

42 CAPACITACIONES REALIZADAS

320 APORTES AL COMERCIO EXTERIOR

72 AUDITORÍAS EJECUTADAS

#JuntosSomosBASC

Aportes del SGCS BASC a la seguridad de operaciones del comercio exterior

Durante los días 15 y 16 de abril se desarrolló con éxito el curso de **"Aportes del Sistema de Gestión en Control y Seguridad (SGCS) BASC en la seguridad de las operaciones de comercio internacional"**. Este evento estuvo dirigido a las autoridades y organizaciones vinculadas al comercio exterior peruano, con las cuales mantenemos convenios interinstitucionales.

El Director Ejecutivo de BASC PERÚ, **Sr. César Venegas**, dio la bienvenida a los participantes, quienes fueron capacitados por expertos en temas fundamentales como logística del contenedor, gestión de precintos de seguridad, ley de protección de datos personales y el sistema de gestión en control y seguridad BASC.

Agradecemos y felicitamos a los representantes de SUNAT, APN, DIRANDRO, DICAPI, DEVIDA, Ministerio Público y PromPerú, cuya participación reafirma el compromiso que mantienen con la seguridad del comercio peruano.

NUESTROS ALUMNOS

DEVIDA
Comisión Nacional para el Desarrollo y Vida sin Drogas

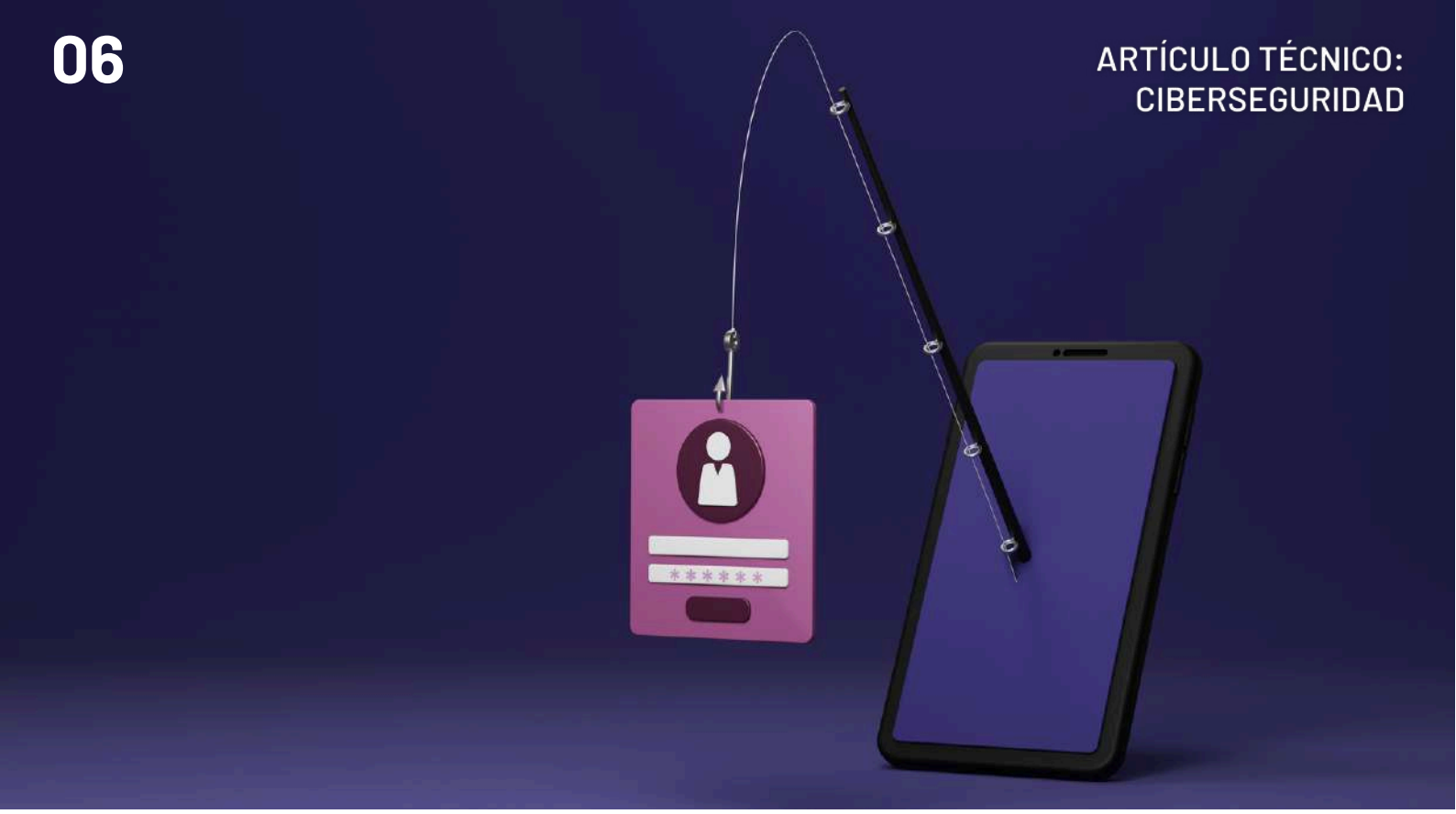
Agradezco a BASC PERÚ por habernos brindado el curso de "Aportes del SGCS BASC a la seguridad de operaciones del comercio exterior" . Ha sido una experiencia que nos ha permitido aprender sobre la seguridad dentro de las actividades del sector logístico.

CÉSAR ATALAYA
Especialista en monitoreo

prom perú

Con el curso de "Aportes del SGCS BASC a la seguridad de operaciones del comercio exterior" he podido actualizar mis conocimientos sobre logística, seguridad en la cadena de suministro, gestión de riesgos, entre otros. Voy a poder aplicar todo lo aprendido en mi institución con el fin de mejorar las capacidades comerciales de las empresas que exportan alrededor del mundo. De esa forma, en conjunto con los talleres y capacitaciones que realizamos en los "Miércoles del exportador", vamos a poder brindarles apoyo para fortalecer la seguridad de sus operaciones.

JUAN CARLOS GANOZA
Especialista en Logística y Aduanas



La importancia de la ciberseguridad en la cadena de suministro

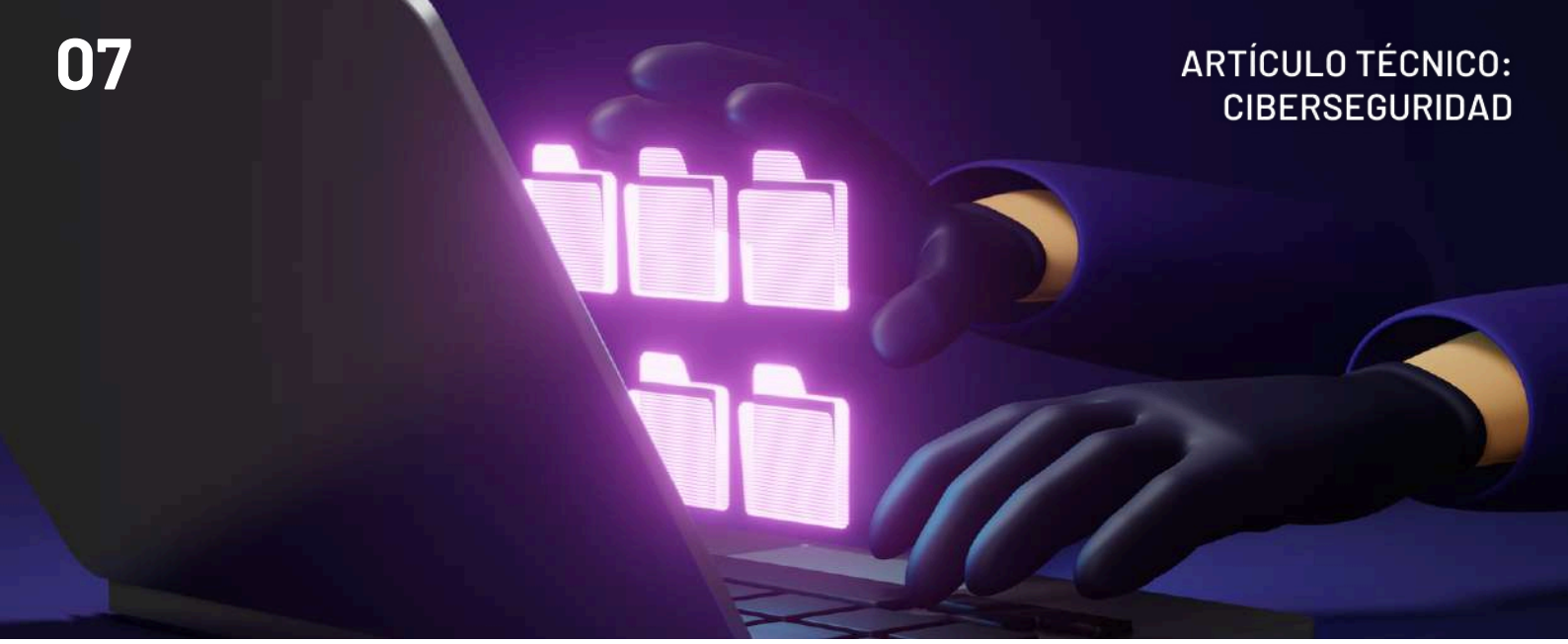
La ciber protección de la cadena de suministro es cada vez más importante: más de un tercio de las organizaciones se han visto afectadas por un ciber incidente en el 2023. ¿Cómo pueden las empresas proteger mejor sus cadenas de suministro?

EL IMPACTO EN NÚMEROS

Hoy en día, uno de los mayores retos a la hora de gestionar los ciberataques en la cadena de suministro es comprender el amplio perfil de amenazas y los controles de seguridad que mantiene la empresa.

Según el estudio realizado por "FortiGuard Labs", laboratorio de análisis en inteligencia de amenazas de Fortinet, el **Perú recibió más de 5,000 millones de intentos de ciberataques durante el 2023**. Sin embargo, este mostró una reducción en comparación al 2022, ya que en dicho periodo se identificaron un total de 15,000 millones de intentos de ciberataques.

A nivel de región se identificó que, durante el 2023, América Latina y el Caribe sufrió 200,000 millones de intentos de ciberataques, lo que representa el 14.5% del total reportado a nivel global. Al respecto, podemos mencionar que los países más vulnerados a nivel de Latinoamérica fueron Brasil, Colombia y México.



Frente a este contexto podemos mencionar que **los ciberataques están siendo diseñados bajo objetivos específicos, lo que los vuelve más sofisticados y con mayor posibilidad de éxito, más aún cuando las organizaciones no cuentan con controles de ciberseguridad automatizadas, integradas y actualizadas**.

Cabe mencionar que el incremento de estos incidentes conlleva a la reflexión sobre la creciente necesidad de abordar la ciberseguridad de la cadena de suministro a nivel global, identificando y reforzando los eslabones más débiles.

¿CÓMO PUEDEN LAS ORGANIZACIONES PROTEGER MEJOR SU CADENA DE SUMINISTRO FRENTE A CIBERATAQUES?

Las cadenas de suministro de todos los sectores se enfrentan al constante reto de ser parte de un entorno dinámico e impredecible. Por ende, somos testigos de que este ilícito ha vulnerado a pequeñas, medianas y grandes empresas, donde logran secuestrar, obtener y afectar la integridad de la información confidencial de las organizaciones, la misma que trae consigo graves impactos en el corto y largo plazo.

La principal causa de este riesgo es la falta de implementación de estrategias, políticas, controles y procesos de detección de posibles ataques cibernéticos, lo que no permite disminuir las brechas de ciberseguridad. Esto, sin duda, tiene grandes implicancias económicas, legales y reputacionales.

Es por ello que la ciberseguridad se ha vuelto un factor determinante para la protección de la infraestructura TI y todo lo relacionado con esta dentro de las organizaciones. Es imprescindible, entonces, crear estrategias y contar con buenas prácticas para el óptimo desempeño de los procesos.

PRÁCTICAS DE CIBERSEGURIDAD A TOMAR EN CUENTA POR TU ORGANIZACIÓN

1 ESTAR INFORMADO

Es importante estar siempre actualizado e informado sobre las últimas tendencias y modalidades que se presentan a nivel nacional e internacional. Este tipo de contenido le permitirá a tu organización tomar decisiones con base en el contexto a fin de prevenir, afianzar o implementar diversos controles de ciberseguridad.

2 CONTRASEÑAS COMPLEJAS

Este tipo de control debe incluir al menos diez (10) caracteres, entre ellos: números, letras mayúsculas y minúsculas, así como, al menos, un carácter especial. De preferencia, no utilizar información personal para elaborar contraseñas.

Adicionalmente, utilice la autenticación multifactor para obtener una doble validación (pin de seguridad, reconocimiento facial, huella, etc.). Este control sirve para sesión de correos electrónicos como para aplicativos de dispositivos móviles.

No olvide cambiar la contraseña con frecuencia (una buena práctica de seguridad está entre 60 a 90 días) y evite usar la misma en diferentes plataformas digitales.

3 REPORTE OPORTUNO DE MENSAJES SOSPECHOSOS

Mantengamos la buena práctica de reportar al área encargada de TI sobre la recepción e identificación de mensajes sospechosos (incluye enlaces, documentos en ZIP, etc.) de origen desconocido. Por ende, es importante reforzar el control de no descargar o abrir archivos adjuntos.

Aprenda a reconocer los correos electrónicos de suplantación de identidad, validando siempre la dirección de correo (dominio) y los detalles de escritura del remitente.

4 USO DE ANTIVIRUS

Es importante utilizar y mantener actualizado el antivirus corporativo para la correcta detección de un posible ataque o fuga de información. Recordemos que los "firewalls" son útiles para poder filtrar los puertos de red que no utiliza, evitando cualquier tráfico no deseado o requerido.

5 RESPALDO DE LA INFORMACIÓN

Las organizaciones realizar el respaldo de su información de manera segura y con una frecuencia definida, la misma que puede estar almacenada en un disco duro (físico) o en una nube. Este control es importante frente a un ataque cibernético de "ransomware", ya que permite recuperar o restablecer la información de manera oportuna con el propósito de no detener las operaciones.

6 FOMENTAR UNA CULTURA DE PREVENCIÓN

Como parte de las buenas prácticas es trascendental fomentar una cultura de prevención a través de políticas, capacitaciones y difusiones constantes con el personal, sobre la importancia de mantener la ciberseguridad de nuestra información.
Asimismo, es esencial asignar un equipo interno de trabajo para desarrollar estrategias y respuestas frente a este ilícito, lo que generará mayor compromiso por parte de los colaboradores.

7 CIFRAR DISPOSITIVOS

Actualmente, con el trabajo remoto, la cobertura de la red se ha movido a los dispositivos móviles y laptops en nuestros hogares. Frente a este contexto, es importante que el equipo de trabajo aprenda a cifrar los dispositivos informáticos que utilizan para la gestión laboral, teniendo en cuenta el nivel de vulnerabilidad al que se encuentran.

Anyanela Torres Palo
Auditora Internacional BASC
Auditor Interno ISO/IEC 27001
(Sistema de Gestión de Seguridad de la Información)

Cacería de ballenas: cuando los CEO en el Perú están en la mira de los hackers

Fuente: G de Gestión

El ahora expresidente del directorio de PETROPERÚ, Pedro Chira, no ha sido el único ejecutivo peruano afectado por el avance de la deepfake en el país. Las voces de algunos gerentes de empresas de los rubros de alimentos y de la construcción también han sido manipulados en los últimos meses por la Inteligencia Artificial. Los hackers se aprovecharon de material audiovisual público (incluso privado) para crear contenido que incluía estafas financieras. ¿Hay forma de detener el fraude en línea?

El deepfake es una forma de inteligencia artificial (IA) que se utiliza para crear contenido audiovisual falso y casi indetectable para el ojo humano (un video suyo anunciando el sorteo de un auto, por ejemplo, podría estar dando la vuelta por internet en estos momentos). El término ya no es una novedad. A nivel internacional, se han hecho públicos diversos casos desde el 2019.

En el Perú, las denuncias comenzaron en el 2023. “Ahora internet está lleno de plataformas que permiten crear y manipular contenido. Si el hacker enviara el video falso a 1,000 personas y al menos dos cayeran, podría embolsicarse miles de soles en pocos minutos”, explica Omar Palomino, consultor en seguridad en Kunak Consulting.

En Perú, la empresa Kaspersky alertó que el 75% de peruanos no sabe qué es un deepfake y un 57% no sabría reconocer un video de este tipo.

Pero esta no es la única forma en que los ciberdelincuentes se aprovechan de la IA para cometer fraude. Las temibles llamadas desconocidas son otra puerta de ingreso. El denominado vishing (engaño por teléfono para obtener información confidencial) permite al ciberdelincuente grabar la voz y manipularla con IA para, eventualmente, usarla cuando requiera hacer alguna operación ante un banco u otra empresa a nombre de la persona afectada.

Medidas preventivas:

Los expertos de Kaspersky alertaron que los cibercriminales podrían seguir explotando las herramientas de Inteligencia Artificial (IA) para crear contenidos engañosos más convincentes y accesibles, aumentando los riesgos asociados con los deepfakes. Esta tecnología es usada en imágenes, videos e incluso audios y textos, alterados para mostrar información diferente a la original, por ejemplo, para que una persona suplante a otra.

La mayoría no sabe qué es un deepfake (75%) y tampoco sabe reconocer un contenido de este tipo (57%), aunado a que es una amenaza que se verá constantemente este año, para engañar a altos ejecutivos y potenciales clientes.

En tal sentido, las empresas certificadas BASC deben establecer un procedimiento documentado, con base en la gestión del riesgo y su rol en la cadena de suministro, para:

- Gestionar y proteger el manejo de la información y los recursos informáticos de la empresa, incluyendo las medidas a aplicar en caso de incumplimiento.
- Salvaguardar la información y su confidencialidad, integridad y disponibilidad, en sus diferentes formas y estados.
- Proteger la infraestructura de las tecnologías de la información.

Asimismo, deben implementar diversos controles para dar cumplimiento a los requisitos que detalla el Estándar BASC respecto a Ciberseguridad y las Tecnologías de la Información y algunos de ellos son los siguientes:

- Establecer, documentar y mantener criterios de seguridad que permitan identificar y proteger los sistemas de las tecnologías de la información y recuperarla oportunamente en caso de ser necesario.
- Identificar partes interesadas y su nivel de criticidad en la infraestructura informática (hardware y software) de la empresa.
- Comunicar oportunamente información sobre amenazas de ciberseguridad identificadas a las partes interesadas correspondientes.
- Clasificar la información de acuerdo con la legislación vigente, sistemas y accesos según el nivel de criticidad y establecer políticas de acceso a la misma.

EMBAJADORES
BASC PERÚ

BASC PERÚ reconoce **el compromiso de empresas** que mantienen el Sistema de Gestión en Control y Seguridad (SGCS) BASC por más de 20 años.

Para Security International Moving S.A.C. - SIM ha sido sumamente importante **mantener la Certificación BASC de forma ininterrumpida por casi dos décadas**, ya que esto nos ha permitido desarrollar controles y fortalecer nuestros procesos.

Estamos comprometidos con la seguridad de nuestras operaciones y somos conscientes de su importancia dentro del mercado. Por ello, en SIM nos preocupamos en capacitar a nuestro personal, así como a **continuar implementando acciones que permitan mejorar nuestros procesos de manera continua**.

JUAN GARCÍA
Sub-Gerente General

SIM security international moving

SIM SECURITY INTERNATIONAL MOVING

"EXPERTOS EN GLOBAL MOBILITY"

NOSOTROS

Con más de 50 años en mudanzas internacionales, lideramos el sector ofreciendo traslados seguros y eficientes a nivel global, incluyendo EE.UU, Europa, Asia y Latinoamérica.

MUDANZA INTERNACIONAL

Ofrecemos un servicio completo de **reubicación internacional de puerta a puerta**, que incluye embalaje personalizado, traslado, trámites de aduanas y entrega de pertenencias desde cualquier parte del mundo, a través de **nuestra red global de agentes certificados.**

Nuestros servicios y procesos son auditados periódicamente para mantener los más altos estándares de calidad y seguridad para beneficio de nuestros clientes.

- Mudanza corporativa local y nacional
- Embalaje y traslado internacional de obras de arte
- Servicio de almacenaje
- Traslado internacional de mascotas
- Distribución
- Manejo de proyectos especiales

FIDI IATA IPATA BASC FIDI ACADEMY Omni lacma

CONTÁCTANOS

www.simoving.com.pe +51 994 274 728

Nuevas empresas BASC

AirSeaLog

Manuelita

OSEA GROUP

algaex

CLP OPERADOR LOGISTICO

MEGADUANAS OPERADOR LOGÍSTICO

V13 SEGURIDAD • RESGUARDO • VIGILANCIA

wic logistics

Bretaña Transport E.I.R.L.

Los Olivos De Villacurí S.A.C.
Grupo Vanguard Internacional

JOCYMAS

INKA'S BERRIES GLOBAL GENETICS & GROWERS

Desde el capítulo brindamos una cordial bienvenida a las nuevas empresas certificadas que suman a la comunidad BASC.

BASC PERÚ
Testimonios

ECOPACKING

Debido al aumento de nuestras operaciones de exportación era necesario generar confianza a nuestros clientes y proveedores seguros, por este motivo la obtención de la certificación BASC logra este objetivo y genera, al interior de la empresa, una cultura integral de prevención de seguridad.

RICARDO PEÑA
Gerente de Operaciones y Proyectos

Los Olivos De Villacurí S.A.C.

Grupo Vanguard Internacional

Una manera de promover sostenibilidad es generando confianza frente a toda la cadena de suministro. Por ello, nos sometimos a la exhaustiva revisión de nuestras políticas y procesos, decididos a obtener la certificación BASC. Nuestro enfoque es de constante prevención y fortalecimiento de nuestra seguridad.

MANUEL YZAGA
Gerente General de Los Olivos de Villacurí
y CEO del Grupo Vanguard Internacional

Auditorías BASC | Abril


Cargueros Terrestres - Lima


Adualink - Lima


Corporación LMJ - Lima


DSM Marine Lipids Perú - Piura

Gráfica Vulcano - Lima

Grupo Homero Logistic - Lima

ISC Perú - Lima

KAR Logistics Perú - Lima

King Real Security - Lima


Limones Piuranos - Piura

Auditorías BASC | Abril

Manuport Logistics - Lima

Quicornac - Lambayeque


Servisegur - Lima


Supply Company - Lima


Ultra Frío - Callao

Airsea Logistics - Lima


ISA Seguridad - Ica

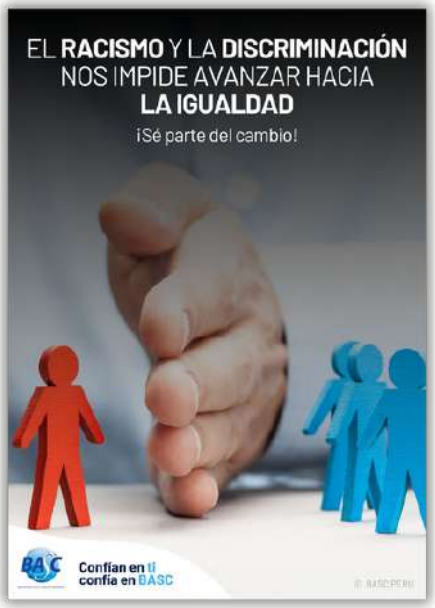

Security Company - Lima


COPEINCA - Piura


Sunshine Export - Piura

AFICHES DE SENSIBILIZACIÓN

BENEFICIOS PARA EMPRESAS CERTIFICADAS BASC



Disponibles en:

www.bascperu.org

¿Conoces el objetivo del 11° Congreso Mundial BASC?

Abordar los retos y tendencias actuales que impactan las operaciones comerciales, así como fortalecer los procesos a través de paneles de discusión, expositores de talla mundial, análisis de tendencias y mejores prácticas de seguridad.

Mayor información:

www.congresomundialbasc.com

Congreso Mundial BASC 2024

Miami | Sept 25 & 26

BASC

BUSINESS ALLIANCE FOR SECURE COMMERCE

BASC PERÚ TRAINING

MAYO 2024

Curso online

Modelo de gestión de riesgos integral: COSO ERM, modelo de las 3 líneas, ISO 31000.

20 de may.
06:00 p.m.

Curso online

Análisis de causas y levantamiento de no conformidades

21 de may.
09:00 a.m.

Curso online

Elaboración de programas de capacitación y medición de su eficacia según el SGCS BASC

28 de may.
02:30 p.m.

Curso online

Seguridad de la información y de los sistemas informáticos

30 de may.0
6:00 p.m.

Inscríbete en www.bascperu.org

BASC PERÚ TRAINING

¡SÍGUENOS!

BASC Perú Training

BASC PERÚ Training

bascperu.training


BASC
BUSINESS ALLIANCE FOR SECURE COMMERCE
Confían en ti,
confía en BASC.
www.bascperu.org