



BUSINESS ALLIANCE FOR SECURE COMMERCE

CAPÍTULO PERÚ

Cargo Security

PUBLICACIÓN ESPECIALIZADA EN SEGURIDAD DE LA CADENA DE SUMINISTRO INTERNACIONAL

YEAR XII / 2019 - 38

CYBER CRIME: A LATENT THREAT

Cybersecurity culture in companies

Human behavior may be the most difficult risk to control. Culture is key in this case and that's why there are models to build it. (Page 8)

Quantification of cyber risk

Cyber-attacks on a global scale generate the need to develop quantification models for organizations.

Cybersecurity and the new global competition conditions
(Page. 13)

BASC World Congress 2019: Public and private sector meeting
(Page. 18)

Attention to the events that reshape the world
(Page. 21)



**“EN EL
MARCO DEL
BICENTENARIO”**

Hotel los Delfines | 08 y 09 de Setiembre 2021 | www.bascperu.org

Información: congresobasc2021@bascperu.org | +511 612 8300

Comité Editorial / Editorial Board

Patricia Siles Álvarez
Ricardo Bernales Parodi
César Venegas Núñez

Director / Director
César Venegas Núñez

Edición / Redacción / Editor / Writer
Unices Montes Espinoza

Coordinación / Coordinator
Anyanela Torres Palo

Suscripciones y Publicidad / Subscription & Advertising
anyanela.torres@bascperu.org

Diagramación e Impresión / Design and Press
Grupo Visión Publicidad S.A.C.



BUSINESS ALLIANCE FOR SECURE COMMERCE

Alianza Empresarial para un Comercio Seguro
(Capítulo BASC PERÚ)

Jirón Francisco Graña 335, Magdalena del Mar
Lima - Perú
Teléf.: (511) 612-8300
www.bascperu.org

Consejo Directivo / Directors Board**Presidente del Directorio**

Sociedad de Comercio Exterior - COMEX
Patricia Siles Álvarez

Vicepresidente

Sociedad Nacional de Pesquería - SNP
Ricardo Bernales Parodi

Director Secretario

Asociación de Servicios Aeroportuarios Privados - ASAEPP
Arturo Cassinelli

Director Tesorero

Cámara de Comercio Americana del Perú - AMCHAM
Aldo Defilippi Traverso

Director

Sociedad Nacional de Industrias - S.N.I.
Oliver Joerk

Director

Asociación Peruana de Operadores Portuarios - ASPPOR
César Ballón Izquierdo

Director

Guillermo Acosta Rodríguez

Asociación Marítima del Perú - ASMARPE**Director**

Jaime Miró Quesada Pflucker

Asociación de Agentes de Aduana del Perú - AAAP**Director**

Sabino Zaconeta Torres

Asociación Peruana de Agentes Marítimos - APAM**Past President**

Raúl Saldías Haettenschweiler

Gerente General

César Venegas Núñez

Cargo Security® es una publicación trimestral promovida por los gremios que conforman la Alianza Empresarial para un Comercio Seguro (BASC por sus siglas en inglés), asociación civil sin fines de lucro adscrita a la Organización Mundial BASC.

Las opiniones vertidas en los artículos firmados son de exclusiva responsabilidad de sus autores.

Derechos reservados. Se permite la difusión del material contenido en esta revista siempre que se cite la fuente.

REGISTRO DE MARCA: Certificado N° 00153963
(Resolución N° 010346-2009/DSD-INDECOPI)

Content

EDITORIAL

- 2 Cybersecurity: A new battle front for BASC

COVER PAGE

- 3 Quantification of cyber risk
6 Cyber-attack on public services infrastructures
8 The cybersecurity culture in companies

INTERVIEW

- 11 One of the most important assets of the business is information" César Faro Flores, Head of IT Products and Security of Telefónica Móviles S.A.

COVER PAGE

- 13 Cybersecurity and the new global competition conditions.

INTERVIEW

- 16 Peruvian Navy creates the Cyber Defense Command. Interview with Rear Admiral (AP) Enrique Arnáez Braschi, Commander of this new command.
18 BASC World Congress will be held in Colombia. Interview with Emilio Aguiar, Chairman of the Board of Directors of the World BASC Organization.
19 The digital transformation of a company must consider cybersecurity risks. Interview with Mr. Alexander García Rivas, Director of PricewaterhouseCoopers - PwC Peru.

TRENDS

- 21 Attention to the facts that reshape the world

INTERVIEW

- 25 A strategy that protects, detects and responds to security threats is essential. Interview with Héctor Figari Costa, Legal and Corporate Affairs Director of Microsoft South Region.

TERRORISM

- 28 Groups considered terrorist organizations.

BASC WORLD

- 31 • The WORLD BASC Organization (WBO) with the support of BASC PERÚ trains the public sector and holds rapprochement meetings with Argentine private sector associations on the OAS program and BASC certification
• Peru signs Mutual Recognition Agreement with the Andean Community. Prominent participation of BASC in COMALEP meetings in Paraguay, BASC World Congress 2019 "Residence and Risk Management: The Route of Security and Competitiveness"
• BASC at the 5th Meeting of the Latin American Anti-Smuggling Alliance

BASC WORLD PERU

- 38 • Security in Shipments of Maritime Goods
• BASC PERÚ trains Chiclayo and Trujillo companies in prevention of risks
• Quality Management Forum
• Forum on Environmental Management in Organizations
• IV Annual Meeting of Internal Auditors BASC
• Seminar - Fight Against Cybercrime



Cybersecurity: A new battlefield for BASC

Computer science, and technology in general, is increasing its predominance in new business models globally, as well as its influence on the forms of commercial negotiation at an international level by leaps and bounds; It has also brought great opportunities for those who walk outside the law.

Computer criminals, those involved in cybercrime, have their own agenda and, just like parasites, can inflict enormous damage to society, not only to companies and any type of organization, but also to countries, regardless of their political or economic status, even considering them to be a threat to national security.

In Peru, Law 30999 on Cyber Defense has just been published, whose main objective will be to protect sovereignty, national interests, critical assets and key resources to maintain capacities against threats or attacks in and through cyberspace, when these affect National security. The road to combat this scourge has already been formalized.

This situation leads to the emergence of "Cybersecurity", another combat front for organizations such as BASC PERÚ, with the purpose of looking for tools and strategies that minimize the risks of being victims of cybercriminals, who do

not have a definite physical location or an easily detectable face in police files.

This task has just begun and BASC PERÚ, according to its mission and responsibility with international trade, is on the front line. This was demonstrated on June 20th with the Free Seminar "Fight Against Cybercrime", an event organized for BASC certified companies with speakers from prestigious companies and institutions, such as Microsoft - South and Central America Regions, participated; PricewaterhouseCoopers (PwC) Peru; Telefónica Móviles S.A.; and the Cyber Defense Commander of the Peruvian Navy.

This is the beginning of a future, abundant and dynamic agenda that we will organize for our associated companies and the general public, those that require a lot of institutional support to successfully face the permanent threat of cybercrime. This threat feeds on risks within organizations, so this aspect has a special emphasis on the safe practices that we promote through our BASC Control and Security Management System (SGCS).

Patricia Siles Álvarez
President
BASC PERU



Quantification of cyber risk

The increased risk of cyber-attacks on a global scale is leading to the development of quantification models. Public services, banks, corporations and governments, seek to use them as part of the business and / or risk management. Insurance companies seek to protect themselves from the cyber risk of third parties, large banks seek protection from risk within the organization, while multinationals seek a combination of both.

As part of its deep global concern, the world's leading organizations have been deploying their best efforts to conceive, design, organize and execute the best strategies to address threats against cybersecurity that, depending on their content and scope, could potentially affect the entire world.

For example, the World Economic Forum - WEF recognizes that this is a central issue on the global agenda and is "fundamental for sustainable growth and stability," according to the document "Quantifying Systemic Cyber Risk" (Global Cyber Risk Quantification Network 2018).

This document is the result of what was discussed during the 2015 edition of the WEF, when emphasis was placed on investigating

cybersecurity in this connected world to get an idea of the quantified effects on the global economy in the event of a cyber-attack.

The Global Cyber Risk Quantification Network (GCRQN), composed of representatives from governments, academia and industry, was formed to do such research. In May 2017, the GCRQN focused on the issue of connection in cyber risk, and the members shared innovative experiences and ideas on methodologies for quantification of risks related to the economy, policy formulation, risk management and society.

Globalization shows its negative side in the connection of technologies to cyberspace through a certain premise: as the connection increases, the risk of attack also increases.



Recall the following examples:

- In August 2016, the Mirai botnet infected poorly protected Internet devices by identifying the usernames and passwords of those who still used the factory default ones. This malware turned networked home devices into remotely controlled “bots” that were used for large-scale network attacks (The Mirai botnet was aimed at Internet of Things devices, routers being its main objectives, digital video recorders and surveillance IP cameras).
- In May 2017, WannaCry cyber-attacks worldwide targeted computers running the Microsoft Windows operating system through data encryption and the demand for ransom payments. The ransomware quickly spread through 300,000 patched systems, which paralyzed organizations in its path.
- In June 2017, the NotPetya cyber weapon was launched worldwide, which mainly affected Ukraine, where more than 80 companies were attacked, including the National Bank of Ukraine.

The GCRQN group warns that attacks are advancing in their power and range. In the political field, democratic processes in important countries have been disturbed by attacks and spreading false news, while in the civil field there were attacks on critical infrastructure, such as the Central Bank in Bangladesh and Ukrainian power networks, which have gave rise to global fears about the possibility of unprecedented attacks. Hence, this organization raises the following questions: What are the

reasonable levels of security in cyberspace? What efforts should be made to achieve this? Who should take responsibility for those efforts? How can we ensure that these efforts are continuously maintained to be effective and economical?

The quantification of cyber risk is no longer the exclusive domain of insurance companies and academic centers. Public service entities, banks, corporations and governments are increasingly using quantification approaches as part of their business and / or risk management. There are organizations that are using the benefits of cyber risk quantification approaches to limit their exposure to cyber risk. In some cases, such as insurance, this mainly refers to the cyber risk of third parties. In other cases, such as large banks, this refers to the management of cyber risk within the organization. For multinational companies it is a combination of both.

There are different methodologies and tools that range from sophisticated cyber risk benchmarks to management oriented approaches. Uses range from technology-oriented and threat-oriented approaches to business value-oriented approaches. For the EMF group all known approaches have something in common: they do not yet have efficient and reliable tools to take into account correlations, dependencies or systemic risk. There are four interrelated challenges that cause this limitation:

- **Priority:** Paradoxically, the urgency of cybersecurity at the level of individual



organizations limits the amount of attention devoted to systemic risk.

- **Change:** innovations involving connected technologies and cyber threats develop more and more rapidly, which requires keeping up with the evolving risks.
- **Complexity:** the large number of elements that interact and change require innovative approaches.
- **Data:** companies are not collecting relevant data because it is not clear what data is necessary. In addition, there is a reluctance to share data that is available.

Analysts reveal that the cybersecurity effort is predominantly carried out by individual organizations. Larger organizations tend to have better cybersecurity than smaller ones, due to the high costs involved in achieving a good cybersecurity protection capability. In addition, in relation to physical security, the study suggests leaving the “Wild West” individual defense on the issue of public safety, “Over the centuries, society has learned that it is economically stimulating and more efficient to organize security publicly,” says the document.

So, how is cybersecurity quantification predicted? For the document, communities will be key to ensuring cyberspace, this being also the natural place to start collecting the necessary data and start quantifying systemic cyber risk. Instead of generating a high level of trust to directly exchange data, quantification models can act as intermediaries for that trust and can serve to accumulate information from the lowest

operational levels of individual organizations to community levels, community communities and eventually at the level of countries and global regions.

In the coming years, more precise models will be developed that will take advantage of machine learning techniques and artificial intelligence. Some models have already been developed to help quantify systemic cyber risk. It is considered that all models that attempt to quantify cyber risk will have three key components: attack activity, combined cyber risk control, and the impact of cyber abuse. In this way, progress is being made in the development of models designed for large groups following dependency alignments related to the attack (several organizations that suffer the same attack), controls, impact, and higher order dependencies (interrelationships between dependencies).



Cyber-attack on public services infrastructures

In 2015 an electricity distribution company in Ukraine was attacked by cyber criminals. As a training activity, the incident had no major consequences, but it gives rise to fear that the goal may be a manufacturing plant for weapons of mass destruction.

The current central concern and the biggest fear of international business is the disruption of supply chains. Unlike recently, when the emphasis was to find the best way to manage the supply chain (supply chain management), executives now appeal to security as a fundamental tool so that this chain is not interrupted by causes that could occur to hundreds or thousands of kilometers of its offices (supply chain security). There are many factors that can cause a disruption of the flow of goods, from natural to human causes.

Cyberterrorism is one of the most recent and the most silent and artful human causes that can cause the breakdown of any supply chain, whether commercial or not. By its nature, this activity is in full swing and its scope is unlimited or progressing along with the progress of computer science and computing. Geographically its scope also has no limit. The document "Identifying and anticipating cyber-attacks that could cause physical damage to industrial control systems" recently published by the Massachusetts Institute of Technology

(MIT) states that physical control systems are increasingly controlled by reconfigurable devices, network enabled, to increase flexibility and facilitate commissioning and maintenance. "Such capacity creates vulnerabilities. The devices can be reprogrammed remotely by a malicious actor to act inadvertently, causing physical damage to mechanical equipment, infrastructure, life and physical integrity," says MIT.

In the industrial field, control systems are increasingly linked to the Internet to allow remote monitoring and control, creating new vulnerabilities. The intention to simplify processes and facilitate the installation and commissioning of industrial systems, makes it flexible but introduces the potential for misuse.

This means that the cyber threat is not limited to the theft of credit cards, data or other personal information, hackers or other malicious actors can now remotely access the hardware, change settings or reprogram devices to cause real

physical damage on an unlimited scale, “It is typical in engineering training to see physical failures as statistically independent events, based on principles such as the average time to fail. However, a cyber-attack can occur at any time and impact many devices simultaneously. This has important consequences that must be carefully considered,” warns the document.

Example in Ukraine

The document cited provides an example of such threats to what happened in Ukraine, on December 23, 2015, when the lights went out in the Ivano-Frankivsk region. Months earlier, phishing emails had been sent to workers at three power companies, which allowed the perpetrators to enable macros in an attached Word document to install BlackEnergy3 malware which allowed hackers to have a backdoor to reach systems in the electrical substation. The attackers conducted surveillance of the network and were able to obtain the login credentials for remote access to SCADA systems (Supervisory Control and Data Acquisition, or supervisory control and data acquisition).

The attack had several different struts. UPS (Uninterruptible Power Supplies) that provided backup power for control systems were disabled. Then, hackers used access to SCADA systems to

open switches that distributed power to the network. Fortunately, the firmware that controlled the serial controllers to the Ethernet network was poorly operated, which prevented further control of the switches. In addition, hackers installed a denial of service telephone number in the call centers of the energy company, which angered the public.

Finally, they used a program called KillDisk to make the computers in control centers malfunction, avoiding any additional action on the part of the company’s operators. Although there was no electricity for only one to six hours, the attack affected seven 110 kV and twenty-three 35 kV substations, which caused cuts to 225,000 customers.

Months after the attack, the substations were still operated manually. While the attack simply interrupted the distribution of energy, the potential for physical damage was there. The attackers chose to only send a message, instead of damaging the equipment. Russia was blamed for the attack, but no one has taken a step forward to claim responsibility.



This was said in 2009. What do you think of its validity?

Volatile. Perhaps this is the best word to describe the current world market. Like the economies and financial markets, since supply chains have grown more globally and interconnected, they have also increased their exposure to shocks and disruptions. The speed of supply chains only aggravates the problem. Even minor errors in calculations and actions can have greater consequences, since their impacts spread like a virus through the complex networks of supply chains.

How do supply chain executives manage? As part of our recent Global Survey of Supply Chain Managers, we were talking with 400 senior executives from North America, Western Europe and the Asia-Pacific region responsible for the strategies and operations of their organizations’ supply chains. Our conversations revealed five key findings related to: Cost containment; Visibility, Risk, Privacy with the client, and Globalization. These findings suggest that supply chains (and executives responsible for managing them) are under strong pressure.

As compliance mandates, suppliers and information flows multiply, supply chains become more complex, expensive and vulnerable. In addition, it is increasingly difficult for executives to respond to these challenges, especially with conventional supply chain strategies and designs.

We are not saying that companies have ignored these issues; In our research, we do not see a lack of supply chain improvement projects. But our research suggests that it is no longer enough to create supply chains that are efficient, targeted or even transparent.

Source: “The smartest supply chain of the future.” Global study of supply chain managers. IBM 2009rentes.



The culture of cybersecurity in in companies

The internal threat of human behavior is one of the most difficult aspects of security to control. Are the risks generated by action or omission? People's culture is key. A model to build an organizational culture of cybersecurity is proposed by the Massachusetts Institute of Technology.

Organizational cybersecurity requires more than the latest technology. To ensure an organization, all members of the organization must act to reduce the risk. Leaders have a special responsibility to understand, shape and align the beliefs, values and attitudes of the entire organization with the overall security objectives. Managers need practical solutions to deal with the human side of cybersecurity.

There may be models to describe the cybersecurity culture of an organization, the factors that contribute to its creation and how it can be measured. There are factors that help managers understand and apply recommendations to create a mature cybersecurity culture in their organization.

All companies want to protect their assets against hackers and cyberterrorists. Even the most advanced technological security cannot protect an

organization from cybercrime if the people in the organization fail. It only takes an employee to click on a phishing email to provide an attacker with an entry gap in a company's systems. Once inside, an attacker can block critical information. The internal threat of human behavior is one of the most difficult aspects of security to control. Building a culture of cybersecurity within an organization guide.

A culture of cybersecurity underlies the practices, policies and "unwritten rules" that employees use when they carry out their daily activities. What is the strategy that a company follows? The creation of a resilient cyber culture within an organization will mitigate the weakest link, the person. However, although the culture of cybersecurity has a profound impact on risk, it can be difficult to identify, build and quantify. The examination of other types of organizational culture provides a basis for a cybersecurity culture model. Many organizations have developed a strong safety culture in which all employees know and receive constant reminders of ways to stay safe and reduce the possibility of accidents.

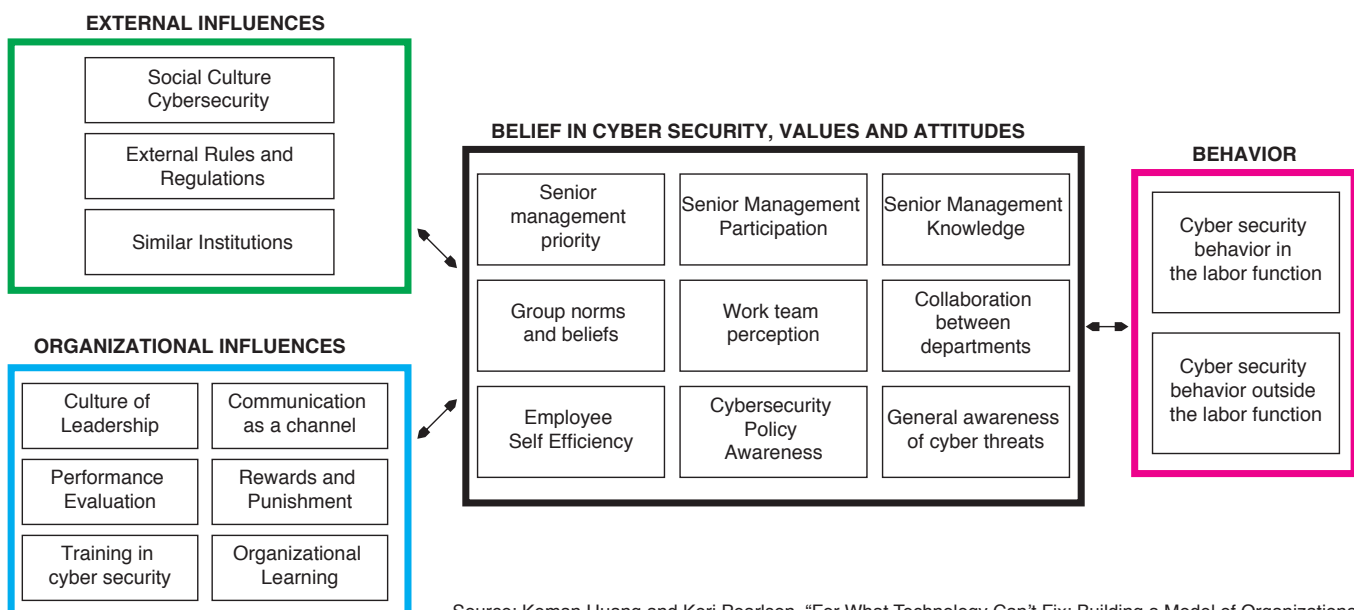
A similar goal for cybersecurity can be said. Each employee must act in a way that keeps the organization cyber safe. How can leaders understand, shape and align the beliefs, values and attitudes of their organization with cybersecurity objectives? A broad-profile model, for example, of creating a "data protection culture" could contain the following.



First, establish an organizational culture of cybersecurity, for which three concepts have to be examined: organizational culture, national culture and information security culture. Second, elaborate the content of the model, which can be achieved by creating a culture of organizational cybersecurity working on the following three factors: beliefs, values and attitudes.

In the field of behavior, which creates or reduces vulnerability in cyberspace, there are two that are the results of a culture of cybersecurity: one in the normal role, and another in behaviors outside the role.

ORGANIZATIONAL CYBERSECURITY CULTURE MODEL



Source: Keman Huang and Keri Pearson. "For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture". Cybersecurity Interdisciplinary Systems Laboratory (CISL). MIT, 2019.

In general, values, attitudes and beliefs are unwritten rules that everyone knows, but few can articulate. However, they can be observed in actions taken by leaders, groups and individuals in the organization. The construction of the safety culture through these three organizational levels follows the leadership behavior of managers and leaders to influence the participation of employees in cybersecurity related activities. **There are three elements that influence the quality of the cybersecurity culture among leaders: their priorities, their participation, and their knowledge of the cybersecurity issue.**

There are three constructs that summarize the level of attitudes, values, and beliefs of the group. The norms and beliefs of the community, the perception of the work team, and the collaboration between departments.

There is another group of elements within cybersecurity within the organization and it is related to the individual beliefs of employees that includes understanding and knowledge of cyber threats, awareness of company policies, and knowledge of personal abilities to cope to the impact of security threats. At this individual level there are three elements: individual effectiveness, level of awareness of cybersecurity policy, and awareness about general cyber threats.

Organizational mechanisms

On the other hand, considering the organizational mechanisms needed to achieve the security model implies being aware that beliefs, values and attitudes are the unwritten rules and, therefore, are the culture of the organization, but are created by the actions of managers and leaders that are management levers or organizational mechanisms.

To influence the cybersecurity culture, you can identify six management levers that managers can use. Managers make decisions about each of these levers, which in turn drive (and can be driven by) the culture.


First is the leadership in the cybersecurity culture, then come performance evaluations, punishments and awards; organizational learning; cybersecurity training; and the communication channel. This last part, the communication channel, refers to coherent and well-designed messages about cybersecurity communicated through multiple methods and networks. All successful business communications require the right person to hear the right information

at the right time through the right channel.

But what works for one person may not be the same for another. Administrators must create multiple formal and informal channels to report cyber incidents, share dynamic cyber information and even identify potential vulnerabilities. For example, some organizations create similar marketing campaigns based on cybersecurity to influence behaviors by keeping problems at the front and center of employees. Another example is to include brief moments of communication at the beginning of each company meeting to share a cybersecurity message.

Finally, external influence is present as a determining factor. For example, the more the press reports about cybercrime, the more conscious individuals turn against cyber risks. In addition, in some industries, the government or other regulatory body dictates how companies should prepare and defend against cyber threats. For example, the regulations of the General Data Protection Regulation (GDPR) in Europe require organizations to assign a data protection officer so that companies subject to this regulation are more influenced than others.

Three external influencers have a significant impact on the culture of an organization: the cybersecurity culture of society; external regulations and rules; and related institutions (such as BASC PERU).

These four groups of elements create a theoretical model that highlights the organization's cybersecurity culture: beliefs, values and attitudes, in action. The complete model is shown in the included figure. The framework raises a series of relationships between the mechanisms that administrators can use to build a culture of cybersecurity. The absence of these mechanisms is an indicator of a cybersecurity environment that potentially exposes the organization to unnecessary risks. 

Source: Adapted from "For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture". Cybersecurity Interdisciplinary Systems Laboratory (CISL). MIT, 2019.



“One of the most important assets of any business is information”

For the Engineer César Farro Flores, Head of IT and Security Products of Telefónica Móviles S.A., the top management of the companies has the task of understanding this issue to advance in the elaboration of an information security master plan.

What are the main weaknesses in the cybersecurity field of Peruvian companies related to international trade?

Personally, I think that in the first place there is the lack of awareness on behalf of company owners and the collaborators in protecting the most critical information of said companies and, secondly, the lack of knowledge of how to protect critical information despite the fact that some Controls for its implementation are free, based on good practices and company experience.

Due to the following security incidents, among others, companies have been becoming more aware about safeguarding their information; the

Wannacry Ransomware event that occurred on May 12, 2017 attacking more than 230,000 Pcs worldwide in more than 150 countries starting in Asia, Europe and America. This ransomware also affected Peru, we must consider that two to three years ago many companies in Peru suffered other types of ransomware. The other security incident was on Thursday, May 24, 2018, addressed to the Bank of Chile where the Bank's general manager confirmed that the entity was the victim of the theft of about 10 million dollars.

Peru has thousands of companies, but more than 90% are SMEs and, in general, around 20 thousand companies are engaged in foreign trade.



Do cybersecurity risks primarily target larger companies or all alike?

Cybersecurity risks in SMEs are more frequent because they are small businesses that are growing, and many of them do not have dedicated IT staff, much less security, some of them have outsourced IT staff that comes only for hours to the company, they frequently do not have the procedure to generate a backup of their critical information and above all they do not get to try the restore, they do not buy licensed software, for example, from their Windows operating systems, they do not buy an antivirus, they do not buy a perimeter firewall. Therefore, they install a free antivirus, all this generates that when the manufacturer publishes a security patch they cannot update since the non-licensed software does not allow it and they are victims of Viruses, Ransomware, etc.

What strategic guidelines would you recommend to Peruvian companies to establish confidence in their cybersecurity?

The top management of companies must understand that one of the most important assets of the business is the information, of its customers, of its employees, of its critical processes, of its suppliers. For this, **I recommend developing a security master plan that includes the management of security risks alienated to the requirements of ISO / IEC 27001, which is the starting point for managing Information Security in any organization.**

As a strategic point, the company must identify the critical security risks that affect the business in the short, medium and long term. To identify these risks, all areas of the company must be involved and counting as a sponsor to their senior management. **It is recommended to create a multidisciplinary team where the participation of key people from different areas of the company;** such as operations, factory, plant, finance, sales, marketing, IT, and legal personnel, so that all personnel are identified in this group and they are the ones who identify the most critical risks of the company and thus Develop a strategic plan / security director that should be addressed in the short, medium and long term.

What is your impression of the contribution of an organization such as BASC PERÚ in promoting preventive security of international trade activity?

The contribution of BASC PERÚ is key in the issue of calling companies and providing them with content with the objective of raising awareness among companies through conferences, talks, workshops, courses with real examples of what could happen to any organization if it does not have a master security plan, awareness plan aimed at all employees of the company, technical controls of good practices implemented to help protect company information. 🇵🇪



Cybersecurity and the new global competition conditions

Companies are currently going through tremendous changes as a result of new types of interactions between technology, economic-geopolitical power, and business models. They are the main forces that are shaking the current conditions of global trade.

The times that the planet is currently experiencing are tectonic changes for humanity and, in the meantime, businesses and companies are trying to dispel the clouds of uncertainty in order to design new ways of adapting to new circumstances. Technology, economic power linked to geopolitics and business models are the main forces that are driving the changes today.

An example of this is the growing idea of the need to re-found the World Trade Organization (WTO) on

the grounds that this important entity was created to be useful in an era such as the industrial one, based on knowledge and its respective intellectual protection. The WTO was created in 1947 (considering its predecessor GATT).

However, the WTO should be able to respond to the shift towards a global data-based economy, which supports the new Internet-based business models and the move towards machine learning that will lead to the rise of the Internet development

A case in Peru

According to a testimony published in the Andean Agency, in March 2018 a technology equipment retail company of 100 workers was affected by a Ransomware. In a matter of minutes their servers were unusable. The company's logistics database was hijacked and encrypted: the perpetrators asked for 1.5 bitcoins, equivalent to about US \$ 15,000.

The company was paralyzed for hours and its managers decided not to pay the required amount. The technicians formatted the servers, updated the software and the database was restored with data 24 hours ago.

"It was a very big problem. Stock information is updated in real time. Sometimes products were sold that were no longer in stock and had to be solved with the customer," said company spokesmen. While customers continued to arrive, sellers were not sure that the requested products were in the warehouse. Dozens of sales were canceled. After a day and a half, the server resumed its operation. But it took a week for the inventory to be completely updated. It is not necessary if the research to find the authors gave results, but without evidence "it was not worth reporting", said the representative of the company.

According to the security company Eset, in Latin America, 25.1% of ransomware attacks (data hijacking) during 2017 were recorded in Peru, the highest figure in the region.

Source: Adapted from "What are the most common cyberattacks in Peru?" Andean Agency.

of Large-scale things with the advent of 5G telecommunications networks (World Trade Organization 2.0: Reforming Multilateral Trade Rules for the Digital Age. Dan Ciuriak. Center for International Governance Innovation. Canada, July 2019).

Geopolitically, what happened recently between the United States, China and the Huawei company, has been a demonstration of the radical change of the new conditions of economic competition in international trade. For analysts, the WTO is not able to mediate tensions of that nature between a country with a lot of power and another emerging rapidly rising. It follows that any institutional reform would have limited scope to achieve long-term lasting solutions, which leads to a change from the grassroots approach.

The emergence of cybersecurity

In this scenario, as noted, technology has been playing a very important role in shaping the landscape of global risks that stimulate changes. In this regard, the 2019 edition of the Global Risks Report 2019 document published by the World Economic Forum - WEF, points out that one of these risks that the world is increasingly facing is data fraud and cyber-attacks, which are a reflection of technological vulnerability.

Overall, according to the international survey conducted by the WEF, approximately two-thirds

of respondents expect false news and identity theft to increase in 2019, while three-fifths say the same about the loss of corporate privacy. And the governments. In 2018 there were more massive data breaches and new hardware weaknesses were revealed, while warning of the potential uses of artificial intelligence (AI) to design more powerful cyberattacks.

The report reveals that cyber-attacks also pose risks to the critical infrastructure of countries, prompting them to strengthen their "selection of cross-border partnerships" for national security reasons.

What happened during 2018

The Global Risks Report 2019 document reports that malicious cyber-attack protocols and "lax cyber security" led to massive violations of personal information in 2018. The largest was in India, where the government identification database (Aadhaar, equivalent to RENIEC), suffered multiple violations that potentially compromised the registration of 1,100 million citizens. In January of that year it was reported that criminals were selling access to the database at Rs 500 for 10 minutes, while in March a leak at a state utility company allowed anyone to download names and identification numbers.

Cyber vulnerabilities can come from unexpected directions, as happened with the Meltdown and Specter threats in 2018, which implied weaknesses




in computer hardware rather than software. They potentially affected all Intel processors produced in the last 10 years.

As for critical infrastructure. In July, the United States stated that hackers had gained access to the control rooms of utility companies. In this way the potential vulnerability of the critical technological infrastructure is increasingly becoming a national security problem.

The relationship between cyber-attacks and the critical information infrastructure with Artificial Intelligence (AI) information has set strong alert alarms. For example, the potential of malicious acts in synthetic biology to create new pathogens using AI. It is the high negative potential of “affective computing” referring to an AI that can recognize, respond and manipulate human emotions.

In reality, among the most disturbing impacts of AI in recent years has been its role in increasing “echo cameras and fake news from the media.” In

2018, the trajectories of 126,000 tweets were studied and it was discovered that those that contained false news consistently exceeded those that contained true information, reaching an average of 1,500 people six times faster.

One possible reason is that fake news tends to evoke powerful emotions: “False tweets tend to cause words associated with surprise and disgust, while precise tweets combine words related to sadness and trust.” The interaction between emotions and technology is likely to become an increasingly disruptive force, says the World Economic Forum. 



Peruvian Navy creates the Cyber Defense Command

In February 2019 the Cyber Defense Command of the Peruvian Navy was implemented. We interviewed Rear Admiral (AP) Enrique Arnáez Braschi, Commander of this new naval unit, to learn more details of the responsibilities assigned to this new Peruvian foreign trade security ally.

What are the main reasons Cyber Defense Command of the Peruvian Navy were created?

The increase in threats in the new domain known as cyberspace that is global in scope as a result of the constant evolution of technology, motivated the Peruvian Navy to create the Cyber Defense Command.

This decision materializes the permanent concern of the Navy in successfully fulfilling the constitutional role of contributing to the defense of independence, sovereignty and territorial integrity, now even in this new domain.

The current capacities allow to safeguard the integrity of the information, as well as the use of cyberspace in a safe way by the Peruvian Navy and work for the defense of the national critical assets that are assigned.

Where do the hostile digital activities they have detected come mainly from? Are they individuals, organizations or countries?

It is difficult to determine the origin because of how easy it can be to hide the attacker. We receive different types of attacks on a daily basis from many parts of the world. Normally, the attackers are cybercriminals who seek to steal information, identities or credit to sell them on the black Internet market (Dark Web); however, international criminal organizations and even states also act in cyberspace.

The ends of the attacks normally respond to interests linked to the traffic of information, money, or simply hacktivism that is nothing more than ideological or political propaganda.

The most common ways to attack seek to penetrate a network, through the vulnerabilities of computer systems or through social methods such as phishing and denial of services, which is nothing more than making thousands of requests to a specific server to saturate it and prevent it from serving users.

Could you give some examples of hostile activities that you have been able to identify?

The most frequent hostile activities are of the type of denial of services. These are performed most of the time by beginners being easily blocked; However, when there is a distributed attack from hundreds or thousands of computers, security may be insufficient.

On the other hand, in cyberspace they are scanning vulnerabilities of the services in an automated way to be able to exploit them (bots). These scans are accompanied by tests that allow the attacker to determine who and how he can attack by penetrating a network.

Finally, the most frequent is the phishing technique that consists of penetrating a network through seduction to some user to click on a link or a file that gives the attacker free access to his computer. In simpler words: **we human beings are the easiest attack vector.**

What is the vision, mission, and scope of the Cyber Defense Command of the Peruvian Navy?

The Peruvian Navy's Cyber Defense Command's mission is to plan and conduct military operations in cyberspace to ensure its effective employment by naval forces in order to achieve national and institutional objectives.


Our vision is to be a leading organization in the region in doctrine and operations of Cyber Defense.

The scope of the Cyber Defense Command, as described by the mission, is the cyberspace of the Peruvian Navy, the areas of operations that are assigned and the critical assets that are granted to the Navy for its protection.

What recommendations would you give to entrepreneurs to minimize the risks of cybercrime?

The best recommendation to minimize the risks of Cybercrime is the training and awareness of the staff in charge, since by experience worldwide **the weakest and most vulnerable link in any organization is the person**, it is no use having the best sensors of security if the personnel in our charge are not aware of the possible threats to which we are exposed and are not indoctrinated to handle risk situations.

For this purpose, we recommend the following measures:

- 1 Verify the origin and content of the emails you receive by checking that the promoter's address is not a false one.
- 2 Set strong passwords, do not share them and change them periodically.
- 3 Do not install software not authorized by the company, and less if it is a pirate.
- 4 Encrypt sensitive information with the methods that the word processor or spreadsheet itself uses.
- 5 Analyze the files we download from the Internet, email or any external device such as USBs, DVDs or external hard drives, among others, with an antivirus; This analysis must be performed before opening the file.
- 6 Block your computer session when it is not present.
- 7 Control with responsibility in the use of the assigned devices, the information they contain and the access to networks, especially public ones. 



BASC World Congress 2019

Emilio Aguiar, brand new President of the Board of Directors of the World BASC Organization for the period 2019-2022, reveals data about the 1st Meeting of Business Members of the Board of Directors of the BASC Chapters - WBO, a new event in the framework of the BASC World Congress to be held next September in Colombia.

Mr. Aguiar, since when do you have a relationship with BASC?

I have the great satisfaction of belonging to BASC since its first years of activity in Ecuador. At the beginning, and attending an invitation to participate in this new security management system, I could see that it was a great help tool to establish safety standards in the activities of companies that are part of the foreign trade logistics chain.

Beyond the honor that it represents to exercise within the WBO Board of Directors, there is the full conviction that the companies that have taken the initiative to belong to the BASC program, we seek to be certain that our activities are developed within a level of trust between our employees and with a vision of development with our related.

What is your vision of the development of BASC and its subsequent international development?

BASC, over time, has been developed as a platform for companies to maintain a track record and can be considered reliable companies, this allows them to project themselves in the world market as companies at the forefront of commercial development.

Our management is aimed at strengthening relations between our affiliates, we seek to expand our number of certified companies. We are contributing to our employers demanding from their suppliers BASC World Congress 2019 safety standards such

as those we offer; to achieve the benefits we want.

Currently, and thanks to the efforts of those who have been in charge of WBO, our organization has achieved a real and strong presence in the different international organizations that have to do with the development of world trade.

We are present and we are an advisory part of the WCO and we share important spaces and meetings with the Customs of the United States (CBP), the International Business Council of the United States (USCIB), the Organization of American States (OAS), the Inter-American Bank of development (IDB) and the Association of Chambers of Commerce of Latin America (AACLA), among others.

At the BASC World Congress 2019, the meeting of the Boards of Directors of WBO is planned. What is the intention of this initiative?

At the BASC World Congress to be held in Cartagena, we are promoting the first Meeting of Entrepreneurs Members of Board of Directors, with the purpose of interrelating entrepreneurs from different countries to tell their experiences about the meaning that BASC certification has had for development and the promotion of its products and services in the field of exports or consumption.

This particular meeting, which we hope will be the beginning of later editions, represents a meeting point for those who are on the Boards of WBO and can tell their experiences of what happens in their respective chapters and thereby achieve the improvements that our members seek. ■



The digital transformation of a company must consider cybersecurity risks

Alexander García Rivas, director of PricewaterhouseCoopers - PwC Peru, says that digitalization projects must be guided by the preventive vision of specialists because in the current circumstances they can present risks and impact the company by putting their survival at stake.

The digital risks for foreign trade companies are the same or different for those operating in developed countries and those that operate in developing markets such as the Latin American region?

Digital risks are a function of the level of dependence that organizations have on their digital assets. In developed countries there is a more intensive use of technology and therefore one might think that their digital risks are greater than in developing countries, but as we have seen in recent weeks, computer attacks do not distinguish geographical area, sector productive or automation level, we are all vulnerable and exposed.

The important thing is what is our strategy to manage, manage and mitigate the digital risks of my organization.

Also, many companies are embarking on digital transformation projects that will determine the future of their organizations, however, they are not considering the cybersecurity risks that may impact their projects and therefore the survival of their business. This is reflected in the fact that the implementation teams of these initiatives do not consider the involvement of cybersecurity specialists who provide a preventive "cyber" outlook on the subject.

What are the main weaknesses in the cybersecurity field of Peruvian companies related to international trade?

One of the main weaknesses is the lack of awareness and awareness that exists in organizations regarding cybersecurity risks. Some executives think that it is a technological or computer security issue, when technology is a means for companies to achieve their business objectives and therefore we must be well informed about it. Likewise, there is no culture of prevention in cybersecurity although we are all very dependent on our mobiles and are connected to social networks.

Another weakness is the lack of an adequate cybersecurity strategy based on risks and more focused on the acquisition of technology. Technology is very important, but if I don't know what to protect, how can I make an adequate investment and protect the most important digital assets of my organization?

In the case of international trade, there is much exchange of information between various parts of the logistics chain in order to meet import and export deadlines, as well as all document management and regulatory requirements. On the other hand, confidentiality aspects are critical for all actors in the logistics chain. In that sense, it is important to have cybersecurity measures that ensure the continuity of the chain and that, given the threat of cyber-attack, processes can be restored. However, not all organizations have properly documented and proven cyber incident response plans that allow them to resist cyber-attacks.

In countries such as ours, there is a lack of awareness and awareness in organizations regarding cybersecurity risks. The culture of prevention in this field is scarce and there is a lack of an adequate risk-based cybersecurity strategy.

What would be the strategic guidelines that you would recommend to Peruvian companies to establish confidence in their cybersecurity?

The strategic guidelines begin and end with the shareholders, board and senior management of our companies, who must be convinced that cybersecurity is not an expense but an investment to ensure the critical business processes that depend on technology, provide the expected benefits.

Once this conviction and awareness is achieved, cybersecurity investments must be aligned with the objectives of the organization to protect their value. In that sense, it is critical to invest in the collaborative cybersecurity prevention culture.

Finally, it is important to constantly challenge the information security team to demonstrate the security levels implemented and to report, with the support of indicators, the state of cybersecurity, and how these align with my products and services.

What is your impression of the contribution of an organization such as BASC PERU in promoting preventive security of international trade activity?

BASC's contribution is to promote the culture of cybersecurity in its associates by sharing information, training and good practices, and also to be an agent of change so that companies engaged in foreign trade are more aware that cybersecurity risks can impact their operations, affect their reputation and cause financial losses.





Attention to the events that reshape the world

Companies have a responsibility to have an accurate panoramic view of the current transcendental problems that occur day by day and which are inevitably reshaping the world in which we live. One of those issues is terrorism, an issue that has become a global concern.

Every day thousands and thousands of news appear around the world, many of them transcendent for a community, city, country, region, continent, and the entire world.

Those that are transcendental for the entire world deserve our full attention because it is an expression of the way the world is changing form and content. It is important that people and organizations committed to the future understand the reasons for the changes made to understand what might come later.

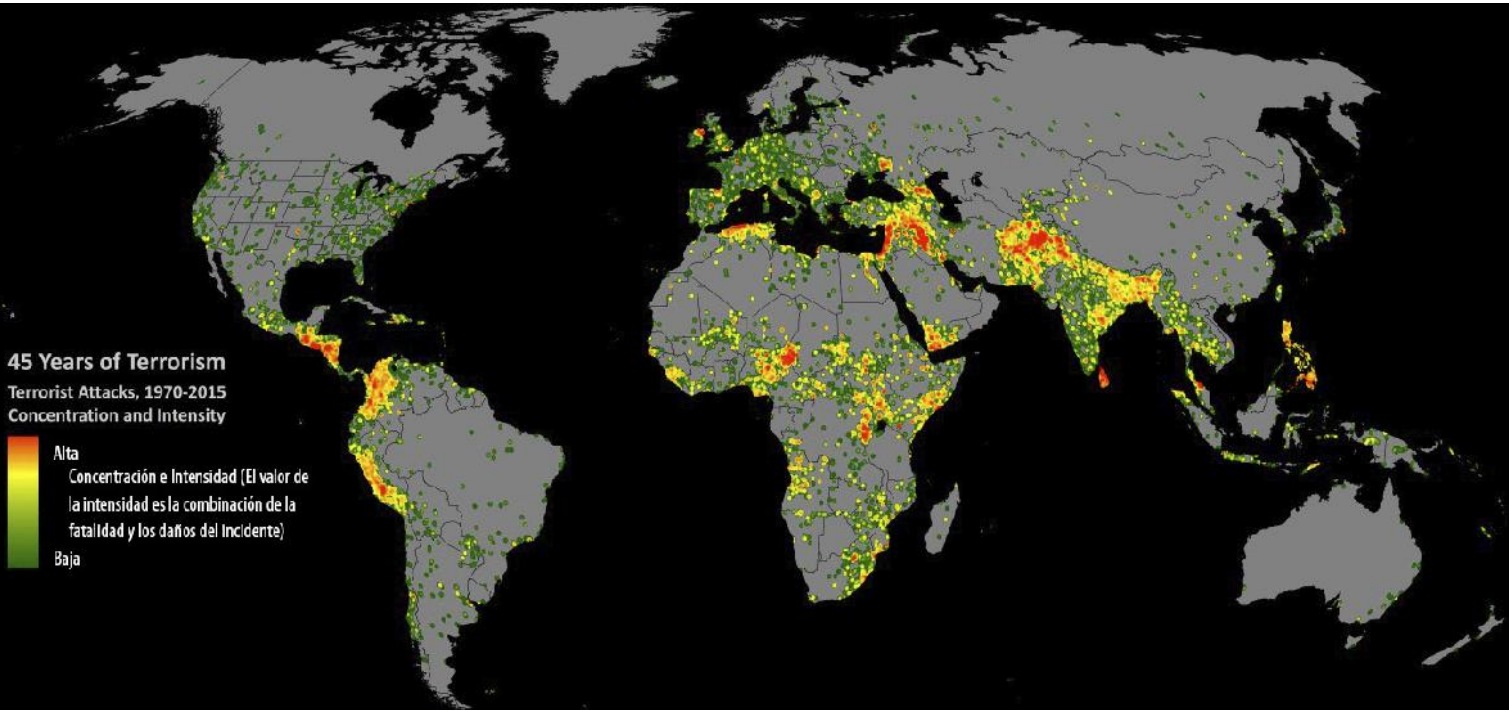
In international business, companies cannot understand what is happening in the world only with daily news. These focus on short-term, particular events, and commonly narrated as isolated events that do not lead us to a panoramic view of significant problems, so it is not possible to perceive the process

path of changes that are reshaping the world in which we live.

An example of this is the social phenomenon known as terrorism that, for decades, occupies spaces in the media worldwide. Behind the violence, chaos and destruction that the news tells about their activities, these movements have increasingly gained notoriety and political weight in the countries where they began to become issues of international concern on a global scale.

Its content and evolution continues to be the subject of important studies for academic, political and military purposes. It is currently an unsolved fact and maintains a growing concern on the part of many governments and supranational organizations for its undoubted impact on the

45 years of terrorist attacks 1970-2015



Fuente: Our World in Data

global situation of social peace and economic progress.

All investigations maintain that the level of global significance of terrorism has its origin in the attacks of September 11, 2001 in the United States.

Strategic objective

The perspective of the most influential country on the planet is extremely important, especially if it has been and is the protagonist of a particular issue such as terrorism. Undoubtedly, its current role in this field is linked to the deadly attacks received in its territory on September 11, 2001 (11S), an event that despite having happened 19 years ago still occupies a priority place in its national security agenda, which can be corroborated in the document "National Strategy for Counter-Terrorism" published by the White House in October 2018 (National Strategy for Counterterrorism of the United States of America. The White House. October 2018).

The document indicates that currently the field of action of terrorism is more fluid and complex than ever and under the expression "we are still a nation at war" in the initial parts of the document, it makes it clear that the main enemy of the United States are Islamic radicals organized into terrorist groups that seek to conduct global attacks under the support of Iran, a country considered the main promoter of these movements.

That is to say, the threat is not only in force but that "it

has changed, it has dispersed and its tactics have diversified, so in order to address this evolution of terrorism, the counter-terrorism approach must also evolve." The book clearly states that it reflects the orientation that US policy follows.

The problem situation

What is the situation of terrorism? At present, as mentioned, this phenomenon has changed, its geographical expansion is a reality, and it now has new tools of action. In their chronological evolution, the studies carried out agree that the attacks of September 11 (11S) represented a break in the long-term trend that it registered until then.

For example, the essay "Do significant terrorist attacks increase the risk of subsequent attacks?" Brian Michael Jenkins, Henry H. Willis, Bing Han. RAN, 2016, notes in their analysis for the USA and Europe in the period 1970 - 2013, that from 1970 to the early years of the 90s, the perpetrators of terrorist actions were domestic groups motivated by ideology or separatism,

which, during the following years were decreasing while that the terrorist activities connected with Islamic extremism (jihadism) were increasing until the culmination of the 11S attacks in 2001, an event “unprecedented in the annals of terrorism.” From that date until 2003, the document indicates that it was a particular period of the post 9/11 adaptation process.

For its part, for the non-profit organization Our World in Data, “the use of terrorism to promote a political cause has accelerated in recent years. Modern terrorism emerged largely after World War II with the rise of nationalist movements in the former empires of the European powers. These first anti-colonial movements recognized the ability of terrorism to generate publicity for the cause and influence global politics.”

According to this organization, what Bruce Hoffman, director of the Center for Security Studies at Georgetown University, says, explains the change in advertising tactics by violent movements. Hoffman says that the ability of these groups to mobilize sympathy and support outside the narrow limits of their real ‘theaters of operations’, led to other foreign movements with causes of struggle, to use terrorism as an effective means to transform local conflicts in international problems.

For Our World in Data, this development paved the way for international terrorism in the 1960s.

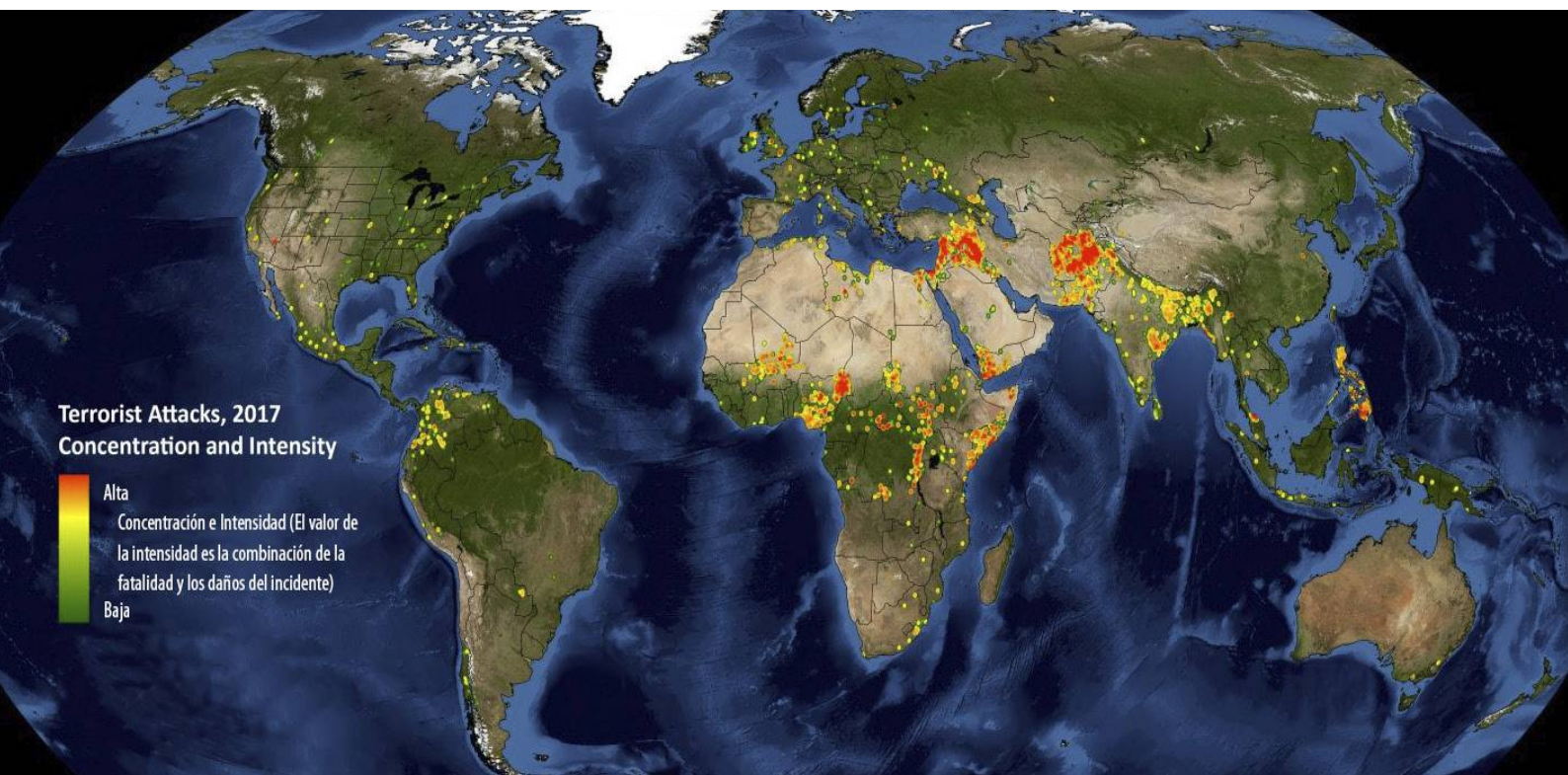
Does the strategy or conditions change?

According to figures from the Global Terrorism Database (GTD) prepared by the Institute for Economics and Peace (IEP) with information from the National Consortium for the Study of Terrorism and Responses to Terrorism (National Consortium for the Study of Terrorism and Responses to Terrorism - START) of the University of Maryland, from 1970 to 2017, more than 170,000 terrorist incidents were recorded.

Only considering the period 1970 - 2008, there were 87,000 terrorist attacks according to the publication Peace and Conflict 2012 of the Center for International Development and Conflict Management (CIDCM) of the Center of Interdisciplinary Research at the University of Maryland. That is, in the last 11 years there were additionally 83,000 such incidents in the world.

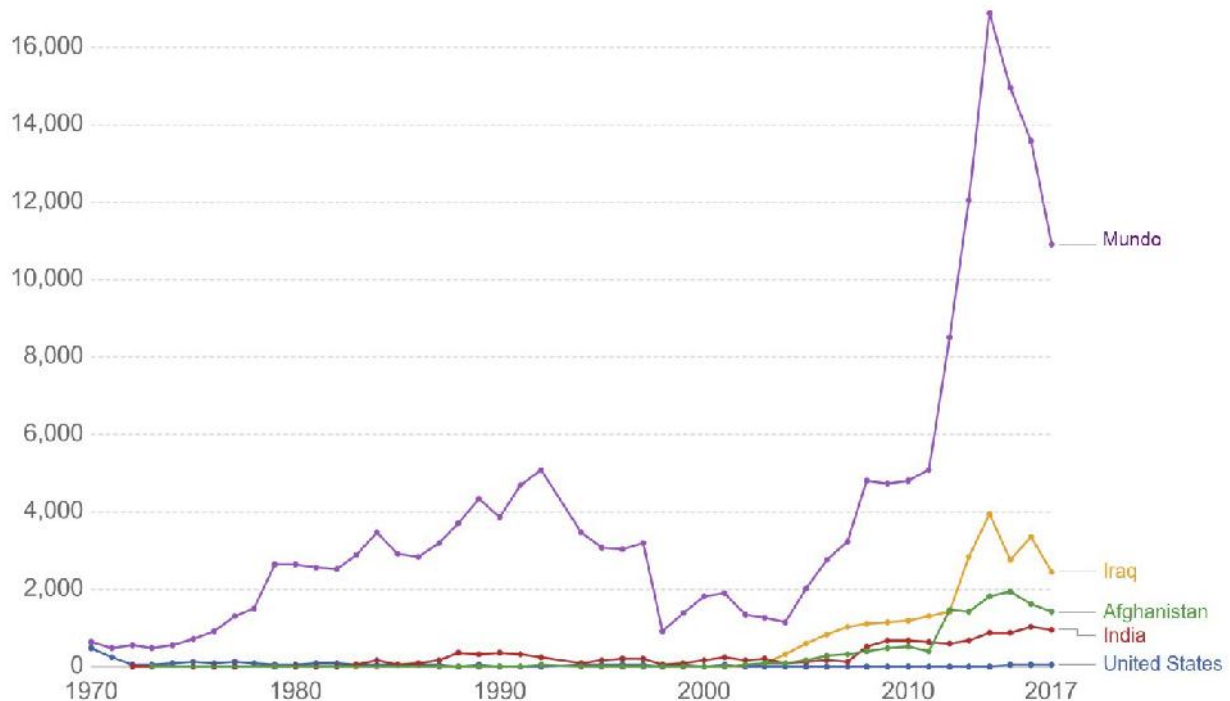
In annual terms the terrorist attacks reached their highest point of the twentieth century in 1992 with 5,120 attacks, while they were drastically reduced in 1998 to levels of the year 1975. A year before 9/11, in 2000, the total attacks were of 1,379 a level close to the total attacks during 1977 and 1978 (1,320 and 1,534, respectively). Then, in the 21st century, the number of attacks rose

Terrorist Attacks 2017



Fuente: Our World in Data

World: Number of terrorist attacks 1970 - 2017



Fuente: Our World in Data

sharply from 2003 when the Iraq war began, so that by 2008 the number of attacks (4,650) approached the record level of 1992 mentioned.

In 2017, deaths from terrorism were 18,814, a 27% lower percentage compared to the previous year and Afghanistan was the country with the most victims. According to START figures, despite severe territorial and financial losses, the Islamic State remains the deadliest terrorist group.

In the long process of terrorism there were also geographical changes. Thus, considering the 10 countries where more attacks occurred in periods before and after 9/11, Latin America stands out for the inclusion of three countries in this region. Colombia, Peru and El Salvador were the main sources of terrorist incidents before September 11, 2001. In the period after September 11, **terrorist activity has shifted to the Middle East and South Asia, where countries such as Iraq, India and Afghanistan top the list.**

Analysts say that the main jihadist terrorist groups such as Al Qaeda and ISIL (also known as the Islamic State of Iraq and Syria, officially known as the Islamic State of Iraq and Syria, officially known as Islamic State or Daesh for its acronym in Arabic language) are clearly focused in recent years on

directing their main efforts and resources on local and regional objectives, among which the defeat of the Bashar al-Assad regime in Syria, a phase for them that would allow them to continue, is a priority objective with the expansion and growth of its foreign attacks. It follows that these movements are less interested, for now, in launching large terrorist attacks in the West, because this objective remains a central tenet of al Qaeda's ideology. This geographical trend in the period 1970 - 2017 can be clearly seen in the two graphic maps that accompany this article. [es](#)



A strategy is essential to protect, detect and respond to security threats

“Peru faces digital risks at rates above world averages,” says Héctor Figari Costa, Legal and Corporate Affairs Director of Microsoft South Region, for whom a good strategy contemplates: best preventive practices (increases the cost of criminal attacks and achieves better users), the promotion of cyber hygiene using genuine programs and good management of personal data and passwords, and the implementation of multifactor authentication to take care of the technological infrastructure.

What are the main digital risks for companies immersed in international trade in the Latin American region?

As part of our commitment to long-term cybersecurity, among many other initiatives, at Microsoft we publish a Security report annually that provides a unique perspective when it comes to trends in the field of digital threats and risks; the most recent is the “Security Intelligence Report 2018” or SIR 2018 for its acronym in English, where we find that the main threats

facing organizations in our region are malware encounters, ransomware, cryptocurrency mining malware and hidden downloads or Drive-by Downloads.

In most cases, the attack vectors detected are characterized by operating stealthily and without the victim taking direct knowledge of their vulnerability

On the other hand, phishing attacks have continued to be a frequent threat to organizations. In that line it is important to highlight that 90% of the intrusions begin with an attack of this

type, which means that 9 out of 10 people will “click” on a link or download an attachment that they should not, thus generating that third parties gain unauthorized access to personal or business information.

Beyond a glance by industry, the attacks have a common denominator and it is the affectation at the economic and reputational level of the victims, which also decays in the loss of confidence in digital environments, confidence that is a fundamental pillar for operations and relationships between the different market players and that, undoubtedly, technology companies seek to generate and preserve.

What is the relationship between digital crime and intellectual property and how do they manifest themselves in the daily life of companies?

It has been shown that there is a very close correlation between non-genuine (pirated) software and computer risk such as malware infections, loss of identity and information theft. Aware of this link and its effects, from Microsoft we have been working permanently in the prevention of computer risk focusing on avoiding the distribution and marketing of pirated software either physically or digitally, as well as actively fighting cybercrime.

In this line, it should also be noted that many of the updates that Microsoft provides to its users are related to security updates. Additionally, the “pirate” software does not have any type of support.

Of the countries where you work in Latin America, what are the three countries where your represented detects a greater activity of cybercrime related to intellectual property?

Looking at some of the main digital risks that impact our region, in terms of malware encounters, our SIR 2018, previously mentioned,

reveals that the markets with the highest encounter rates are Venezuela, Bolivia and Peru; while the markets with the lowest meeting rates are Puerto Rico, Costa Rica and Uruguay.

And when it comes to ransomware meetings, although there is evidence of a decrease of this one by up to 64% in Latin America, the meeting rate in our region is 40% higher than the global average, with markets with rates Highest meeting Venezuela, Bolivia and Honduras; while those with the lowest meeting rates are Canada, the United States and Puerto Rico.

It is important to note that the most vulnerable countries have, in their entirety, piracy rates that currently and historically are above the regional average.

What is the particular situation of Peru?

What are the main weaknesses of Peruvian companies related to international trade in the field of cyber security and intellectual property?

Peru faces digital risks at rates above world averages.

“las inversiones de tecnología deben ir atadas al factor educación; necesitamos usuarios más educados en lo que se refiere a seguridad digital puesto que no es suficiente contar con tecnologías robustas y de vanguardia si (...) quienes la van a emplear no lo hacen correctamente.”

Along these lines, companies must seriously worry about investing in improving their capabilities and the security features of their IT products and services, which should allow them to be permanently protected. In the face of threats that today impress with their increasing frequency, greater level of sophistication and wide range of impact, a strategy that allows organizations to protect themselves, detect and respond to security threats is essential.

On the other hand, technology investments must be tied to the education factor; We need more educated users when it comes to digital security because it is not enough to have robust and cutting-edge technologies if at the end of the day the users who are going to use it do not do it correctly.

Although the scope and consequences of cyber-attacks paint a worrying picture and could mean even greater challenges for smaller organizations with very limited resources, it is no less true that companies of all sizes can develop capacities and strategies that allow them properly manage risk.

In general, what would be the guidelines of the strategy that recommends companies to establish trust in their cybersecurity?

When it comes to best practices around cybersecurity, organizations must be able to prevent incidents. Preventive controls have been shown to increase the cost of attacks for criminals, and prevent users from falling into many attacks.

Likewise, the promotion of cyber hygiene, the use of genuine software, the backup of personal data and password management are some of the most important elements to consider in a security strategy.

In line with this, it is important that the managers of each organization understand the relevance of identity and tools such as, for example, the implementation of multifactor authentication for the protection of their technological infrastructure.


Finally, systems should be updated regularly as they cannot face threats as sophisticated as those we are seeing today.

What is your impression of the role of an organization such as BASC PERU in the security of the activity of international trade?

The promotion of safe practices that generate trust, as well as encouraging the adoption of a culture of prevention to achieve security in international trade operations are objectives with a broadly positive impact on the market and its operators.

Within that context, undoubtedly, paying attention to Cybersecurity and the risks associated with the use of digital environments greatly favors the achievement of these objectives, so the generation of learning spaces must be continued with a view to improving capacities, increasing specialized forums to share knowledge and the strategic use of the power of integration to face a problem that knows no

borders and is configured as a big business and also as a weapon of cyber war against citizens and companies in times of apparent peace.

From Microsoft we reaffirm our commitment to continue actively collaborating with industry partners, governments and other actors worldwide to develop solutions, improve capacities and promote effective public policies that help protect people and build trust through transparency, Compliance and security. 

“Companies of all sizes can develop capabilities and strategies that allow them to properly manage risk.”



Groups considered to be terrorist organizations

The most extensive list of terrorist groups is drawn up by the United States Department of State (68 groups). Historically the most relevant are about 25 groups with presence (current or not) in 73 countries on five continents and activity for at least 19 years. The group with the largest geographical distribution is Hizballah, responsible for terrorist activities in 17 countries.

Defining Terrorism

There is no single definition of terrorism worldwide despite the consensus that its threat must disappear. Different positions are adopted by countries and organizations. Academically, an interesting definition is that of Bruce Hoffman (Inside terrorism. Columbia University Press, 2013) who points out that terrorism is the deliberate creation and exploitation of fear through violence or the threat of violence in the search for political change. All terrorist acts involve violence or the threat of violence. It is designed to have powerful psychological effects and is intended to instill fear, intimidate an "objective audience." It is designed to create power where there is none or to consolidate a weak one. Through violence, terrorists seek to gain influence and power that, otherwise, they cannot have to effect a political change.

According to the European Parliament (newsletter - At a Glance of the European Parliamentary Research Service, November 2015) due to the lack of a unified global definition that could make the fight

against this phenomenon more effective, a framework for global cooperation has been gradually established since 1963 in various international treaties that together provide a catalog of terrorist acts or those that facilitate terrorism so that states can extradite or prosecute their perpetrators.

In September 2001, the UN adopted Resolution 1373 that asks states to "work together urgently to prevent and suppress terrorist acts." The United Nations global strategy against terrorism adopted in 2006, with revision resolutions in 2008 and 2010, was a milestone in improving international cooperation against terrorism.

Since 2000, this organization has promoted a general convention on international terrorism, although progress has been limited. For example, in November 2014, a number of outstanding issues were identified, including a request by the Organization for Islamic Cooperation (ICO) on the differentiation between acts of terrorism and the "legitimate struggle of peoples under foreign occupation (...)" in the exercise of their

Foreign Terrorist Organizations

From	Group Name
10/8/1997	Abu Sayyaf Group (ASG)
10/8/1997	Aum Shinrikyo (AUM)
10/8/1997	Basque Fatherland and Liberty (ETA)
10/8/1997	Gama'a al-Islamiyya (Islamic Group – IG)
10/8/1997	HAMAS
10/8/1997	Harakat ul-Mujahidin (HUM)
10/8/1997	Hizballah
10/8/1997	Kahane Chai (Kach)
10/8/1997	Kurdistan Workers Party (PKK, aka Kongra-Gel)
10/8/1997	Liberation Tigers of Tamil Eelam (LTTE)
10/8/1997	National Liberation Army (ELN)
10/8/1997	Palestine Liberation Front (PLF)
10/8/1997	Palestine Islamic Jihad (PIJ)
10/8/1997	Popular Front for the Liberation of Palestine (PFLP)
10/8/1997	PFLP-General Command (PFLP-GC)
10/8/1997	Revolutionary Armed Forces of Colombia (FARC)
10/8/1997	Revolutionary People's Liberation Party/Front (DHKP/C)
10/8/1997	Shining Path (SL)
10/8/1999	al-Qa'ida (AQ)
9/25/2000	Islamic Movement of Uzbekistan (IMU)
5/16/2001	Real Irish Republican Army (RIRA)
12/26/2001	Jaish-e-Mohammed (JEM)
12/26/2001	Lashkar-e Tayyiba (LeT)
3/27/2002	Al-Aqsa Martyrs Brigade (AAMB)
3/27/2002	Asbat al-Ansar (AAA)
3/27/2002	al-Qaida in the Islamic Maghreb (AQIM)
8/9/2002	Communist Party of the Philippines/New People's Army (CPP/NPA)
10/23/2002	Jemaah Islamiya (JI)
1/30/2003	Lashkar i Jhangvi (LJ)
3/22/2004	Ansar al-Islam (AAI)
7/13/2004	Continuity Irish Republican Army (CIRA)
12/17/2004	Islamic State of Iraq and the Levant (formerly al-Qa'ida in Iraq)
6/17/2005	Islamic Jihad Union (IJU)
3/5/2008	Harakat ul-Jihad-i-Islami/Bangladesh (HUJI-B)
3/18/2008	al-Shabaab
5/18/2009	Revolutionary Struggle (RS)
7/2/2009	Kata'ib Hizballah (KH)
1/19/2010	al-Qa'ida in the Arabian Peninsula (AQAP)
8/6/2010	Harakat ul-Jihad-i-Islami (HUJI)
9/1/2010	Tehrik-e Taliban Pakistan (TTP)
11/4/2010	Jaysh al-Adl (formerly Jundallah)
5/23/2011	Army of Islam (AOI)
9/19/2011	Indian Mujahedeen (IM)
3/13/2012	Jemaah Anshorut Tauhid (JAT)
5/30/2012	Abdallah Azzam Brigades (AAB)
9/19/2012	Haqqani Network (HQN)
3/22/2013	Ansar al-Dine (AAD)
11/14/2013	Boko Haram
11/14/2013	Ansaru
12/19/2013	al-Mulathamun Battalion (AMB)
1/13/2014	Ansar al-Shari'a in Benghazi
1/13/2014	Ansar al-Shari'a in Darnah

From	Group Name
1/13/2014	Ansar al-Shari'a in Tunisia
4/10/2014	ISIL Sinai Province (formerly Ansar Bayt al-Maqdis)
5/15/2014	al-Nusrah Front
8/20/2014	Mujahidin Shura Council in the Environs of Jerusalem (MSC)
9/30/2015	Jaysh Rijal al-Tariq al Naqshabandi (JRTN)
1/14/2016	ISIL-Khorasan (ISIL-K)
5/20/2016	Islamic State of Iraq and the Levant's Branch in Libya (ISIL-Libya)
7/1/2016	Al-Qa'ida in the Indian Subcontinent
8/17/2017	Hizbul Mujahideen (HM)
2/28/2018	ISIS-Bangladesh
2/28/2018	ISIS-Philippines
2/28/2018	ISIS-West Africa
5/23/2018	ISIS-Greater Sahara
7/11/2018	al-Ashtar Brigades (AAB)
9/6/2018	Jama'at Nusrat al-Islam wal-Muslimin (JNIM)
4/15/2019	Islamic Revolutionary Guard Corps (IRGC)

Fuente: Departamento de Estado de EEUU. Julio 2019.

right to self-determination in accordance with the principles of international law," which is problematic given the ambiguity of what constitutes a 'legitimate struggle' and the use of terrorist tactics by insurgent organizations.

In this scenario, the European Union adopted the Council of Europe Convention for the Prevention of Terrorism (CETS No. 196) in 2005 although it does not provide a definition of terrorism but criminalizes the public provocation to commit a terrorist offense and the recruitment and training for terrorism. The Additional Protocol to the Convention was signed in October 2015 penalizing recruitment, training, and travel to another state for terrorist purposes.


Most active groups

According to the Global Terrorism Index 2018 publication, the Institute for the Economy and Peace (IEP) determines which terrorist groups are the most active and which are responsible for the majority of deaths is difficult due to their particular conformations and the intricate relationship of alliance or cooperation between them and other local, national or regional groups. However, the IEP has managed to establish that in 2017 the four terrorist groups responsible for 56.5% of the deaths (10,632) by terrorist actions were the Islamic State of Iraq and the Levant (ISIL), the Taliban, Al-Shabaab and Boko Haram. In 2012, just before the great increase in terrorist activity worldwide, these four groups were responsible for 32% of all terrorism deaths, while in 2008 they represented only 6%.

Which are groups are considered

The best known list of groups considered terrorists worldwide corresponds to the one prepared by the United States Department of State. This list is called Foreign Terrorist Organizations (FTO) and includes organizations outside the US designated by the Secretary of State of that country in accordance with Article 219 of the Immigration and Nationality Law (INA).

To include a group, the State Department must demonstrate that it is involved in terrorist activities. For this, it analyzes the terrorist attacks carried out or if the group has been involved in planning and preparations for possible future acts of terrorism or if it retains the capacity and intention to carry out such acts. It also defines terrorism as "premeditated and politically motivated violence perpetrated against non-combatant targets by subnational groups or clandestine agents."

The relationship of FTO organizations plays a fundamental role in the fight against American terrorism and represents an effective means to reduce support for terrorist activities and pressure groups to abandon terrorist activity. The State Department also notes that the countries that promote terrorism are Iran (qualification established in January 1984), Sudan (qualification established in January August 1993) and Syria (qualification established in December 1979). 

WORLD BASC ORGANIZATION (WBO) with the support of BASC PERU trains the public sector and holds rapprochement meetings with Argentine private sector associations on the OAS program and BASC certification



Closing of the BASC Auditors Course - OAS



Mr. Carlos Reyes Lazo, Operations Manager of BASC PERÚ; Mrs. María Virginia Garimaldi, Chief (Int.) Of the Authorized Economic Operator Department (OAS) of Argentina; Mr. Fermín Cuza, International President of the World BASC Organization and Mr. César Venegas Núñez, General Manager of BASC PERÚ



Mr. Ignacio Federici, Deputy Director General of the Customs of Argentina; Mr. Fermín Cuza, International President of the World BASC Organization (WBO) and Mr. César Venegas Núñez, General Manager of BASC PERÚ.

The BASC PERU Chapter assumes a new challenge by WBO provision after the training of more than 30 Argentine customs officials on the Authorized Economic Operator Program (OAS) and the importance of BASC Certification, as a platform to achieve the security of the international trade supply chain.

World BASC Organization (WBO) with the support of the BASC PERÚ Chapter was present in Buenos Aires giving the “Course for Auditors of the Public Sector: BASC - OAS” addressed to more than thirty (30) officials, validators of the Authorized Economic Operator Program (OAS) in Argentina. The same, which was developed during the week of August 12 to 16 and had Mr. Carlos Reyes Lazo, Operations Manager of BASC PERÚ, in charge of the meeting.

As part of the training, topics such as the matrix of import and export risks by air, land and sea were addressed; as well as the realization of practical exercises to identify objective evidence based on the requirements of the Validators Guide of the World



Sr. Mr. Carlos Reyes Lazo, BASC Operations Manager Mr. Fermín Cuza, International President of World BASC Org., Mrs. María Virginia Garimaldi, Chief (Int.) Of the Authorized Operational Department (DIREPA) of the General Customs Directorate of Argentina; Mrs. Ana Lía Monfazani, representative of Peru in Argentina and Mr. César Venegas Núñez, Manager of BASC PERÚ.

Customs Organization (WCO).

The closing of the course was attended by senior officials, including; Mr. Ignacio Federici, Deputy Director General of the Customs of Argentina; Ms. Maria Virginia Garimaldi, Chief (Int.) of the Authorized Economic Operator Department (OAS) of the General Directorate of Customs of Argentina; Mr. Fermín Cuza, International President of the World BASC Organization; Mr. César Venegas Núñez, General Manager and Mr. Carlos Reyes Lazo, Operations Manager of BASC PERU.



Mr. César Venegas Núñez, General Manager of BASC PERU; Engineer Oscar Enrique Fernández Choco, Secretary Director of C.E.R.A.; Mg Claudio J. Levalle, Director of C.E.R.A and Mr. Fermín Cuza, International President of the World BASC Organization (WBO).

Within the framework of the training aimed at customs officials and based on the importance of the OAS Program and the BASC Certification, as a support and complement tool for the implementation and maintenance of the OAS program, institutional meetings were organized with the main guilds from Argentina, with the objective of sharing our knowledge and experience managing risks so that companies prepare adequately for the certification of the Authorized Economic Operator Program (OAS) in that country and disseminate how the Control and Security Management System - BASC complements with said Program.

On behalf of BASC participated Mr. Fermín Cuza, International President of the World BASC Organization (WBO) and Mr. César Venegas Núñez, General Manager of BASC PERÚ, who met with the main representatives of unions such as the Argentine Chamber of Commerce (CAC), Chamber of Exporters of the Republic of Argentina (CERA), Chamber of Importers of the Republic of Argentina (CIRA), Customs Brokers Center (CDA), Argentine Association of International Cargo Agents, American Chamber of Commerce of Argentina (AmCham),

Argentine Chamber of Automotive Transport of Dangerous Goods and Residues (CATAMP), Argentine Confederation of Medium Enterprises (CAME), Industrial Chamber of Projects and Engineering Goods of the Argentine Republic (CIPIBIC), the Chamber of Instruments Manufacturers Weigh and Measure (CAFIPEM).

It should be mentioned that this first approach allowed the BASC World Organization to present its experience of more than twenty-two (22) years of presence in the market, generating a culture of risk prevention among its certified companies belonging to the supply chain of the International Trade.

Similarly, meetings and visits to companies belonging to the international trade logistics chain were generated, such as: RICOH (Uruguay), El Rosario Port Terminal, Cargonet Group, IFS Logistics and Speed Transport in Argentina.



Visit of Mr. Fermín Cuza, International President of the World BASC Organization (WBO) to the El Rosario Port Terminal



Mr. Fermín Cuza, International President of the World BASC Organization; Mr. Rubén Oscar García, President of C.I.R.A and Mr. César Venegas Núñez, General Manager of BASC PERÚ.



Mrs. Ana Lia Monfazani, representative of the commercial office of Peru in Argentina; Ms. Alejandra Cerquetella, Foreign Trade Manager and Mr. Cesar Venegas Nuñez, General Manager of BASC PERU.



AAACI representatives: Mr. Jorge Alberto Pererira, President; Mr. German Raña, Vice President; Mr. Jorge J. Mujica, General Manager; Mr. Federico Espeche, Director; Mr. Gustavo Navone, Director; among others



r. Fermín Cuza, International President of the World BASC Organization (WBO); Mr. Jorge Billorou, Vice President of Tarifar; Mrs. Cristina Peteira, General Manager of Tarifar and Mr. César Venegas Núñez, General Manager of BASC PERÚ.



Mr. Fermín Cuza, International President of the World BASC Organization (WBO); Mr. Ricardo Colombo - Partner of the Cargonet Group and Mr. César Venegas Núñez, General Manager of BASC PERÚ.



Mr. Alejandro Díaz, CEO of AmCham and Mr. César Venegas Núñez, General Manager of BASC PERÚ.



Mr. Fermín Cuza, International President of the World BASC Organization (WBO); Mrs. Azucena Siverino, General Manager of Speed Transport and Mr. César Venegas Núñez, General Manager of BASC PERÚ.



Mr. Enrique Martínez, General Director of the ASAPRA Secretariat and Association of Customs Brokers (ADAU) of Uruguay with Mr. Fermín Cuza, International President of the World BASC Organization (WBO).M



CATAMP representatives: Mr. Angel Fuente, President; Mr. Juan D. Segovia, Vice President; Ing. Diego Folch, Director and Mr. Rodolfo Espinosa Liard, Institutional Coordinator.



Mr. Andrés Traverso, Head of the Foreign Trade Department of the CAC; Mr. César Venegas Núñez, General Manager of BASC PERÚ and Mr. Agustín Basso, Coordinator of the Department of Foreign Trade of the CAC.



Mr. Taboada Falero - General Manager, Mrs. Adriana Da Luz - Operational Excellence Manager & Chief Information Officer of the RICOH company of Uruguay, with Mr. Fermín Cuza - International President of the WBO.

Peru signs Mutual Recognition Agreement with the Andean Community

The National Superintendence of Customs and Tax Administration (SUNAT) of Peru signed a Mutual Recognition Agreement (MRA) with its counterpart organizations in Bolivia, Colombia and Ecuador, member countries of the Andean Community of Nations (CAN).

Under this Agreement, the signatory customs commit to recognize among themselves the companies certified with the Authorized Economic

Operator Program (OAS) that carry out foreign trade activities with some of the four markets that make up the CAN. It is worth mentioning that Peru registered in 2017 a commercial exchange with the CAN of 4.705 billion dollars. The agreement was signed during the “Authorized Economic Operator Seminar (OAS)” organized by SUNAT and the CAN.

PROGRAMA OPERADOR ECONÓMICO AUTORIZADO			
Países	Sectores	Cantidad	ARM firmados
Bolivia	Exportadores, Importadores, Agencias de Aduana, Transporte terrestre y Consolidador.	36 empresas	Países que conforman la Comunidad Andina y MERCOSUR (Argentina, Brasil, Paraguay, Uruguay y Venezuela).
Colombia	Exportadores, Importadores y Agencias de Aduana.	80 empresas	Países que conforman la Alianza del Pacífico, Comunidad Andina, MERCOSUR y Costa Rica.
Ecuador	Exportadores	3 empresas	Bolivia, Colombia y Perú.
Perú	Exportadores, Importadores, Agencias de Aduana, Almacenes y Courier	118 empresas	Países que conforman la Alianza del Pacífico, Comunidad Andina, Uruguay, EE. UU. y Corea.



(Left to Right): Mrs. Viviana Caro Hinojosa, representative of the Inter-American Development Bank (IDB); Mrs. Ingrid Díaz, Director of Customs Management DIAN Colombia; Mr. Rafael García Melgar, Deputy National Superintendent of Customs of the SUNAT of Peru; Mr. Jorge Hernando Pedraza, Secretary General of the Andean Community (CAN); Ms. María Eugenia Nieto, National Director of Risk Management and Customs Technical of the National Customs Service of Ecuador (SENAE) and Ms. Marlene Ardaya, Executive President of the Customs of Bolivia.

Outstanding BASC participation in COMALEP meetings in Paraguay



Moments during the intervention of Mr. Álvaro Alpizar on the agenda of the OMA-COMALEP-Private Sector Joint Forum.

As it has been doing consecutively for 15 years, World BASC Organization was present at the meetings of the Multilateral Agreement on Cooperation and Mutual Assistance of the Customs of Latin America, Spain and Portugal (COMALEP), held last May in Asunción, Paraguay.

On this occasion, the BASC delegation was represented by Emilio Aguiar, President, and Alvaro Alpizar, Vice President, of the WBO Board of Directors, respectively, who played a key role in supporting the work agenda of the OMA-COMALEP-Private Sector Joint Forum.

BASC, who occupies the vice presidency of the Regional Private Sector Group (GRSP), worked during the meetings on matters of importance to the

GRSP in relation to the terms of reference and the guidelines of the group before the customs administrations of the Americas and the Caribbean, which were pending approval.

During the meeting, Mr. Alpizar moderated working sessions and discussions on the mechanisms of formal communication between customs and the private sector and their effectiveness in the hemisphere and addressed with different audiences, together with Mr. Aguiar, the contributions of BASC on international standards and voluntary cooperation based on trust.

BASC World Congress 2019 "Research and Risk Management: The Route of Security and Competitiveness"



CONFIANZA Y GESTIÓN DE RIESGO: LA RUTA DE LA SEGURIDAD Y LA COMPETITIVIDAD

World BASC Organization (WBO) and BASC Colombia organize the present edition of the BASC World Congress that takes place in Cartagena, Colombia, on September 19 and 20. The congress, the highest institutional event of BASC, to be held at the Convention Center of the "Hotel Las Américas" in Cartagena, will focus its efforts on trust and risk management, as key factors in the path of security and competitiveness in the supply chain, fundamental tools for the promotion and facilitation of trade.

The event is a unique opportunity where businessmen and leading authorities in foreign trade security analyze the challenges and opportunities to combine tools and strategies that allow to build effective security systems in the organizations that develop in business and global trade.

Please find the content and agenda of the event on the website "www.congresomundialbasc.org".

BASC at the 5th Meeting of the Latin American Anti-Smuggling Alliance

Mr. Álvaro Alpízar, president of REX International, a BASC certified company, and Vice President of the Board of Directors of the World BASC Organization, was invited by the Latin American Anti-Smuggling Alliance - ALAC and the Costa Rican Chamber of Commerce as moderator of the panel "The importance of the SAFE Framework and the Authorized Economic Operator in the fight against smuggling" carried out at the beginning of last May.

Mr. Alpízar made a brief presentation on the

objectives of BASC to promote safe trade, its participation in the World Customs Organization - WCO, the meaning and importance of countries understanding and implementing the WCO SAFE Framework for its contribution to risk management in smuggling, drug trafficking, terrorism, public health, intellectual property, etc.



View of the intervention of Mr. Álvaro Alpízar, in the 5th Meeting of the Latin American Anti-Smuggling Alliance - ALAC in Costa Rica.

Security in Shipments of Goods by Sea



On Thursday, April 11, BASC PERU held a free seminar “Security in Shipment of Goods by Sea” that took place at the facilities of the National Society of Industries (SNI). The event was attended by Mr. Teodoro Agüero, Head of the Port Protection Area of the Protection and Security Unit of the National Port Authority - APN; Commander (PNP) Javier Reategui, Chief of the Maritime Intelligence section of the Anti-Drug Port Division of the National Police of Peru - PNP; and Dr. Alberto García Riega, General Manager of Adualink S.A.C.

The welcome words were given by Dr. Patricia Siles Álvarez, President of the Board of Directors

of BASC PERÚ, who told the more

than a hundred attendees the importance of establishing systems that increase security in their operations in relation to the chain supply of international trade; among them the certification of the Management System in Control and Security (SGCS) BASC.

Among the topics addressed were: maritime exports by the National Port Authority (APN), statistics on illicit drug trafficking and major incidents in the maritime sector by the Port Drug Division of the National Police of Peru (PNP), and the participation of logistics operators in maritime transport by the representative of the certified company Adualink SAC

The invitation was made to the participating companies to disseminate the importance of having a management system, such as that provided by BASC, with the aim of achieving security and traceability in their operations, minimizing the threats to which their goods are exposed by sea.

BASC PERÚ trains Chiclayo and Trujillo companies in risk prevention

With the aim of raising awareness and informing the business sector about the benefits and advantages of having an internal preventive security policy, BASC PERU held on May 14 and 16 free awareness talks in Chiclayo and Trujillo, respectively. The talk brought together more than fifty representatives of companies from various sectors, who were given information on: the international environment, threats to foreign trade and contribution of the BASC Control and Security Management System (SGCS) to prevent emerging risks.

The presentation was given by Mr. César Venegas Núñez, General Manager of BASC PERÚ, who commented on the benefits of having the BASC Management System, emphasizing the norms and safety standards applicable



at international level according to the sector that represents the company in the international supply chain.

Mr. César Cabrejo Vega, Head of Integrated Management Systems (GIS) of SOCIEDAD AGRÍCOLA VIRÚ, BASC certified company for 15 years that participated in the event held in Trujillo. It should be remembered that there are currently more than 800 companies affiliated with BASC PERÚ with a presence in 18 regions of the country, which have worldwide recognition as companies that apply safe international practices in their foreign trade operations.

Quality Management Forum



On May 31, BASC PERU held the “Quality Management” Forum for free, in which Dr. Luis Tenorio, Executive Director of the Industrial Development Center of the National Society of Industries of Peru (SNI) participated.

The welcome speech was given by Mr. César Venegas Núñez, General Manager of BASC PERÚ who told the audience of representatives of BASC certified companies, the importance of implementing a Quality Management System in their operations in relation to ISO 9001: 2015.

For his part, the representative of the Industrial Development Center of the SNI emphasized that the continuous improvement of an organization influences the ability to constantly renew itself, this being the cornerstone of a Quality System. Likewise, recommendations were made for companies to strengthen their capacities through the BASC Control and Security Management System (SGCS) in order to be more competitive.

Environmental Management Forum in Organizations



On June 6, the free forum “Environmental Management in Organizations” was held with the participation of Mr. César Díaz Rodríguez, teacher of CENTRUM Católica Graduate Business School, and Mr. Carlos Verano Zelada, Director of the National Information System Water Resources of the National Water Authority (ANA).

Mr. César Venegas Núñez, General Manager of BASC PERÚ, told the attendees representatives of BASC certified companies, the importance of implementing an Environmental Management System

according to ISO 14001: 2015.

This system identifies the aspects and impacts to respond adequately to changing environmental conditions and propose solutions respecting the ecosystem in which the organization develops. Recommendations were made for companies to strengthen their capacities internally and foster a culture of prevention considering the environmental aspect of their operations.

IV Annual Meeting of Internal Auditors - BASC



On June 28, the “IV Annual Meeting of Internal Auditors BASC” was held, an event that brought together more than one hundred internal auditors of BASC certified companies belonging to different foreign trade sectors.

In his words of welcome, Mr. César Venegas Núñez, General Manager of BASC PERÚ, highlighted the work of our organization for almost a quarter of a century serving as a reference in the security of international trade for exporters, importers, terminals, customs agents, carriers, among others.

The presentations and dynamics were in charge of a panel composed of specialists such as Dr. Luis Tenorio, Executive Director of the Industrial Development Center of the National Society of Industries (SNI) who addressed the topic “Management of Excellence: Tools and Strategies for the Process improvement”; Mr. Manuel Oyarce Postigo, Coaching specialist with the theme “How to create and maintain a team of highly effective internal auditors”; and of Mg. Nicanor Leonoff, clinical psychologist under the theme “Risks related to Human Factors.”

Seminar: Fight Against Cybercrime



On June 20, 2019 BASC PERU held the free “Fight Against Cybercrime” seminar aimed at companies with BASC certification; the same one that took place at the facilities of the National Society of Industries (SNI).

The event was led by a panel made up of Dr. Carmen Zegarra Arce, Director of the Cyber Crimes Unit of Microsoft South Region and Central America; Mr. Alexander García Rivas, Director of

PricewaterhouseCoopers (PwC) Peru; Ing. César Farro Flores, IT Product Manager and Security of Telefónica Móviles S.A. and Rear Admiral (AP) Enrique Arnáez Braschi, Cyber Defense Commander of the Peruvian Navy.

On behalf of our organization, Dr. Patricia Siles Álvarez, President of the Board of Directors of BASC PERÚ, highlighted the importance of implementing management systems that increase security in their operations related to information technology (IT); the same that can paralyze the continuity of the organizational and commercial march of the companies. In this sense, topics such as Cybersecurity and Data Protection, by Microsoft; Cybercrime: Statistics and Trends, by PwC Peru; Impact of Ransomware Attacks on Peruvian companies, by Telefónica Móviles; and Cybersecurity and Cyber Defense, by the Peruvian Navy.

LA CIBERDELINCUENCIA SE ENCUENTRA ENTRE NOSOTROS ¡NO BAJE LA GUARDIA!



Llegadas Internacionales
International Arrivals



BUSINESS ALLIANCE FOR SECURE COMMERCE

www.bascp Peru.org

Fomentamos una cultura
de prevención de seguridad

Denuncie los actos ilícitos al
0800-1-9900 LINEA
GRATUITA
de la Policía Nacional del Perú

The drug
trafficking
route will
lead you
to the abyss



BUSINESS ALLIANCE FOR SECURE COMMERCE

22 years promoting a culture of safety prevention in international trade operations.

www.bascperu.org