MAINTAIN SAFETY FOR PROCESSES OPERATORS IN YOUR INDUSTRY

DISCOVERY

SECURITY

About Us

More than **17** years of experience

Our job is to ensure that industries with their critical operations are protected from cyber threats.

The Alfa and Omega Security protects against "operational interruptions" caused by "Cyber threats, intrusions and human errors, providing visibility, control and protection", and is always dedicated to analyzing solutions and making the best of each technology to minimize problems , always offering the best solutions in your delivery.

The Alfa and Omega Security has carried out this work for all these years with maximum mastery, as well as guiding technological evolution so that its customers always have the most up-to-date information in terms of Cybersecurity, providing everyone with the certainty and comfort that more advanced Cybersecurity policies will be implemented.

SECURITY

Industry

Pharmaceutical

Health

Chemical

Maritime

Mining

Security

Transport

Automotive

Energy

Sanitation

Manufacturing

Gas and Oil

Pharmaceuticals - Industries

The pharmaceutical industry moves billions of units of medicines daily. **The Alfa and Omega Security** assists in the manufacturing process.

In this way, medicines are manufactured in accordance with all norms and quality standards.

The risks of a possible cybersecurity incident directly interfere with the manufacturing of medicines, which, in turn, interferes with the prestige of the end consumer in relation to the manufacturer.

The Alfa and Omega Security protects Operational Technology, manufacturing processes and intellectual property through cybersecurity techniques.

Over the years, the pharmaceutical industry has become increasingly automated in order to meet quality standards. Connectivity provides great efficiency, agility and cost advantages.

Health - Industries

There is a significant increase in smart equipment that aims to treat and monitor patients in more depth. The technology is also available for healthcare institutions and databases. The Alfa and Omega Security protects and ensures patient confidentiality during the processes and systems in question. The protection of patient interests, confidentiality and optimism regarding medical technology are one of the main motivations. It is essential to ensure the protection of technology employed in healthcare. The use of electronic medical records has increased significantly, which requires high-level security controls to ensure privacy and confidentiality. It is crucial that information technology and security experts work together to ensure that cyber risks do not get in the way. the advantages arising from new technologies. Our services provide assistance with the security of hospital networks, IT infrastructure, implementation mechanisms and medical machines in general. The Alfa and Omega Security and its professionals have the necessary knowledge to meet all requirements and regulations that concern public safety, with the aim of protecting the patient's life..

Chemical - Industries

A Alfa e Omega Security has extensive experience in the field of chemical safety. It is of paramount importance to protect employees in risky environments and ensure the production of chemical products safely. The chemical industry is a field with a wide variety of regulations, which implies unique challenges. Every day, new technological resources emerge for the dangerous environment of this area. A breach of OT cybersecurity can cause damage to the physical integrity of civilians, in addition to damage to the environment and revenue. Regardless of taking advantage of IIoT and its benefits, A Alfa e Omega Security helps protect and protect your organization's cybersecurity. Our goal is reduce cybersecurity risks through rigorous security control and training to protect artificial intelligence systems. We have extensive experience in the area of chemical safety. It is extremely important to protect employees in risky environments and ensure the production of chemical products safely. The chemical industry is a field with a wide variety of regulations, which implies unique challenges . Every day, new technological resources emerge for the dangerous environment of this area. A breach of OT cybersecurity can cause damage to the physical integrity of civilians, as well as damage to the environment and revenue. Regardless of taking advantage of IIoT and its benefits, we help protect and protect your organization's cybersecurity.

Manufacturing - Industries

Manufacturing has been affected by automation and digitalization, which has improved production techniques and created new business opportunities. IIOTs provide greater agility and efficiency in production lines, while our services help to securely obtain commercial advantages. In the manufacturing ecosystem, complex industrial control systems are used, which makes it possible to manage all production variables. production. It is essential to ensure strict cybersecurity control for Operations Technologies (OT), **The Alfa and Omega Security** aims to ensure that manufacturing structures follow the best cybersecurity practices, identifying unwanted spaces in security and presenting ways to ensure a low risk in manufacturing processes. As time passes, more and more devices are used in manufacturing environments.**The Alfa and Omega Security** assists in protecting this OT environment against manipulation and copyright theft. The manufacturer is responsible for ensuring that the products are of good quality and with us. To do this, it is necessary to meet strict safety standards, especially in the production of "dangerous" foods or products. **The Alfa and Omega Security** evaluates your control systems to ensure guidelines are followed, such as Good Manufacturing Practices (GMP) or IEC 62443 cybersecurity requirements.

SECURITY

Maritime - Industries

Deploying new connected technology allows new vessels to increase convoy efficiency, improve routes and profit margins. It is crucial that manufacturers follow recognized and recognized OT cybersecurity practices.**The Alfa and Omega Security**, broadly speaking, protects crucial maritime assets, whether on-shore or offshore. Our professionals identify threats and provide clear methods to alleviate security challenges. Our experts accompany and guide the manufacturer in the initial development of offshore installations. Additionally, they assist in creating an operations security structure in accordance with regulations and industry policies, providing guidance on best practices aimed at reducing operational risk.
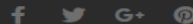
Mining - Industries

Mining has become increasingly dependent on machines, sensors and automated equipment. Mining areas, often remote, have a unique level of cybersecurity, which makes operations more genuine and protects teams amidst such a dangerous ecosystem. Artificial intelligence technologies (IIOT) enable the mining industry gather and analyze data, which makes the strategy more accurate and secure. This is due to improved mining methods, such as the use of sensors and predictive maintenance techniques. Security is a crucial factor in mining, but the science of cyber risk is still small. Assessing and mitigating risks from cyber incidents will help keep production running smoothly. **The Alfa and Omega Security** implements consistent and solid cybersecurity practices. We support cyber threat analysis and mitigation in connected mining systems, as well as protect automated methods of critical infrastructures.
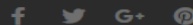
SECURITY

Transport - Industries

New technologies have been fundamental to the transport sector, both in trucks and ships, trains and planes. The ability to manage transport is crucial, as this way it is possible to extract the greatest benefits from intelligent connectivity. It is essential to carry out the necessary maintenance in low-risk operations. This way, it is possible to ensure the safety of the people involved, profit margins and avoid unwanted pauses in the economic sector due to delays in the supply chain. Our services provide assistance to the transport industry in identifying risks and minimizing risks. We have the knowledge of how to apply best practices that bring security to control systems, allowing business to be conducted safely.

Sanitation - Industries

It is crucial to protect the availability of critical systems, such as water management, with an effective cybersecurity strategy.

The Alfa and Omega Security's cybersecurity professionals are trained to protect water infrastructure, combating cyber threats, through a thorough analysis of facilities and a very well-defined governance strategy.

The Alfa and Omega Security understands the challenges faced by dealerships and their particularities when introducing strong security procedures. To ensure safe plant protection, it is crucial that methods that have already been tested and validated in accordance with IEC 62443 are used.

Automotive - Industries

The automobile industry has shown itself to be increasingly proactive and efficient. Therefore, it is crucial to establish effective cybersecurity that protects passengers and manufacturers.

How to ensure that smart car users are safe?

New technologies in the automotive sector continue to bring benefits, such as: fuel economy, greater traffic safety and greater comfort for passengers.

In addition to all the tests and inspections for the physical safety of passengers, which are already being implemented in the automobile industry, it is essential to introduce OT cybersecurity practices in automobile production.

The Alfa and Omega Security helps automotive industry professionals create security technologies and assess the risks that exist in current automotive systems. This increases cybersecurity, agility and reliability in the production of vehicles before they are launched on the market.

Energy - Industries

It is crucial that energy generation, transmission and distribution networks function consistently, thus supplying countries.**The Alfa and Omega Security** aims to protect and protect the energy industry, enabling new technologies and automation to be deployed efficiently.

The energy industry has improved significantly. With the progress of IoT, smart grids have been increasingly deployed, along with new generation and transmission technologies. The benefits arising from new technologies are notable, but, at the same time, new problems arise. Due to new technologies, network security vulnerabilities are exposed, such as a lack of protection against malware, which creates gaps in critical infrastructures.

Our services and solutions protect infrastructure, the network and remote locations, ensuring safety for workers, employees and civilians, and preventing energy services from being interrupted. The energy industry is subject to national and international cybersecurity legislation.**The Alfa and Omega Security** offers assistance so that you comply with the required requirements and regulations.
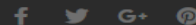
SECURITY

Oil & Gas - Industries

The oil and gas industry provides essential services for people's daily lives.

Companies that deal with oil and gas exploration use complex procedures, in which safety is a crucial aspect.

Safety is, without a doubt, a crucial feature throughout the operation of this industry.

Cases of accidents in this area pose serious risks to the physical integrity of people and the environment.

The Alfa and Omega Security's experience contributes to the creation of evidence-based cybersecurity policies.
We are determined to assist them in implementing new cybersecurity standards such as IEC.62443, NIST SP 800-82 and industry best practices.

SECURITY

Security - Industries

For manufacturers of security systems, it is crucial to ensure that they are operating safely, efficiently and securely.

The Alfa and Omega Security, based on IEC 61508, 61511 and 62443, aims to establish the best operational security practices to maintain a safe situation inside and outside production environments.

By applying the concepts of HAZOP, LOPA and QRA, it is possible to understand the most relevant scenarios, their categorizations and frequencies considered appropriate for certain risk events (hazardous), as well as assign risk categories and determine which Independent Protection Layers (IPLs) must be in operation.

Let us know to understand how your organization can benefit from the strategies proposed by our experts.

Cyber Risk Mitigation

The objective of Cyber Risk Mitigation is to restore existing systems or design new systems. It is essential that the network is designed and configured to meet the performance, resilience and security needs of industrial control systems, in accordance with current practices. most appropriate for each sector.

SECURITY

Monitoring and Response to Cyber Incidents

The objective of the Cyber Incident Monitoring and Response service is to make the necessary corrections in the operational environment of the industrial plant, which comprises procedures, solutions and technologies, as well as identify irregularities, monitor the environment, analyze and respond to incidents

SECURITY

Governance and Compliance

The objective of the Governance and Compliance service is to provide best Governance practices, such as: management, policies and procedures for industrial operations, audits and reports.

SECURITY

Awareness and Trainings

The Awareness and Training service aims to train and certify professionals with the aim of demonstrating their skills and knowledge in industrial cybersecurity and Critical Infrastructures.
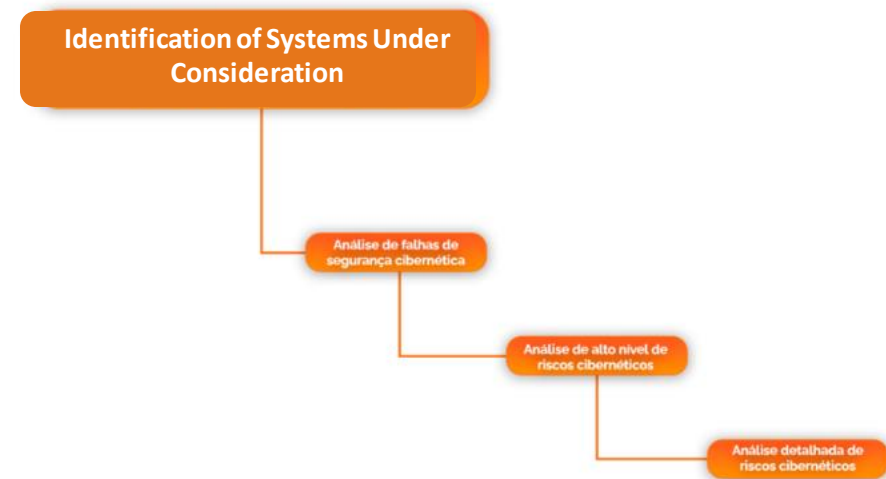
SECURITY

Cyber Risk Assessment

The Cyber Risk Assessment service aims to provide a cyber security assessment for existing and new systems that are present in industrial and critical infrastructure environments. To achieve this, we follow four fundamental steps:

1 - Identification of Systems Under Consideration

2 - Cybersecurity flaw analysis

3 - High-level cyber risk analysis
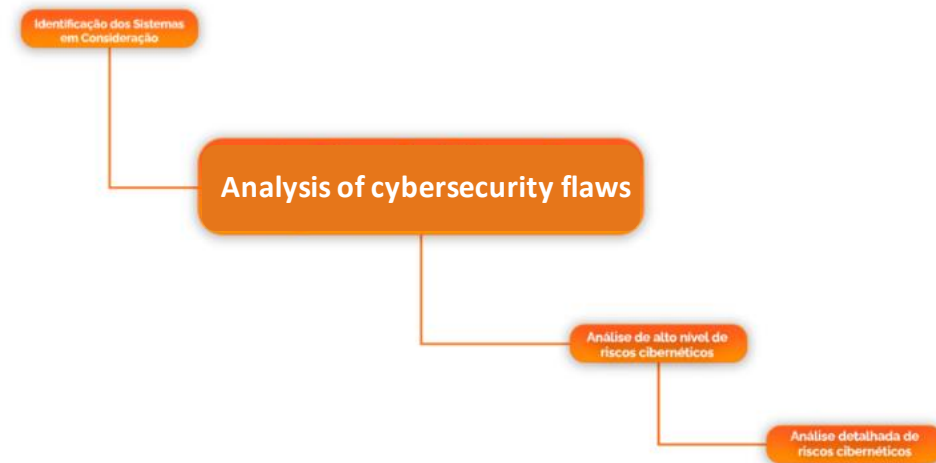
4 - Detailed cyber risk analysis

SECURITY

1-Identification of Systems Under Consideration

In this first stage, we thoroughly identify the systems in question. This is the first step in assessing cyber risks in industrial and critical infrastructure environments. The objective is to identify all elements that are cybernetic in the environment in question. It is now possible to understand how each system operates in an integrated, automatic way, and how it has been used.

Identification of Systems Under Consideration

Análise de falhas de segurança cibernética

Análise de alto nível de riscos cibernéticos

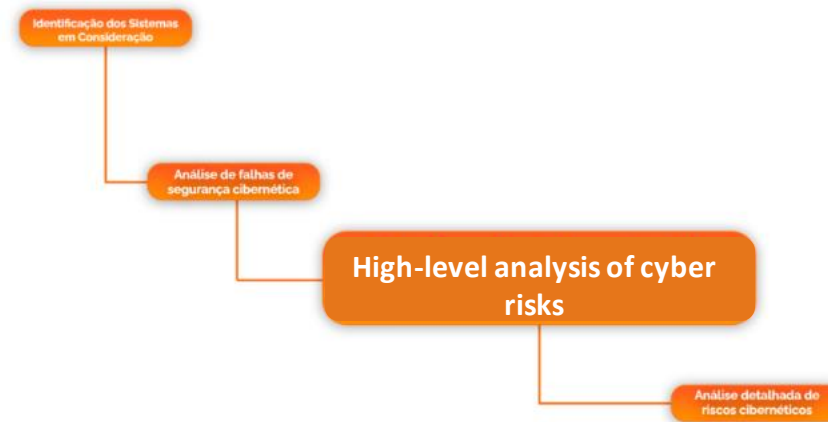Análise detalhada de riscos cibernéticos

2-Analysis of cybersecurity flaws

At this stage, a thorough analysis of the model in use in the organization's environments is carried out, taking into account its pros and cons. This action is extremely important, as the current level of cybersecurity will be assessed.

Identificação dos Sistemas em Consideração

Analysis of cybersecurity flaws

Análise de alto nível de riscos cibernéticos

Análise detalhada de riscos cibernéticos

3-High-level analysis of cyber risks

At this stage, Cyber Risk is deeply analyzed. At this point, the risks present in Industrial Control and Critical Infrastructure systems will be identified, with the aim of determining the consequences and effects of each cyber asset present in the system in question.

Identificação dos Sistemas em Consideração

Análise de falhas de segurança cibernética

High-level analysis of cyber risks

Análise detalhada de riscos cibernéticos

4-Detailed analysis of cyber risks

The last stage is a long-term analysis, with the aim of identifying all risks and their consequences present in the systems in use. Specialists, through safe methods, have control from the beginning of projects. In this way, these systems become more compatible with existing gaps.

Identificação dos Sistemas em Consideração

Análise de falhas de segurança cibernética

Análise de alto nível de Riscos Cibernéticos

Detailed analysis of cyber risks