Security Audit: What is it and what are the most popular techniques?

Currently, the data contained in computer programs represent the most valuable asset for a company, regardless of its size; To prevent them from being lost or falling into the wrong hands, we must maintain high cybersecurity standards.

The *software* used by businesses is increasingly complex, rich in increasingly specific functionalities and, therefore, more difficult to control: for this reason, it is advisable to carry out a computer **smart contract security audit** to find out about possible failures in our system and prevent catastrophic consequences.
As technology advances, there are new ways to commit crimes and, therefore, cybersecurity in Mexico seeks to be reinforced.

Security audit: what is it?

The security audit is an evaluation of the security maturity level of a company, in which the security policies and processes established by it are analyzed to thoroughly review the degree of compliance. In addition, there are specific technical and organizational measures for greater robustness.
After obtaining the results of this, they are detailed and stored to notify those responsible in order to develop corrective and preventive reinforcement measures and, in this way, achieve more stable systems.

Why is security auditing convenient for companies?

If the company uses or intends to deploy international services - such as the cloud, web servers, CPV connections or email servers - that have the possibility of opening doors to its system and these are misconfigured, the security audit is presented as an excellent option.

It not only works to keep you safe from current operations, but also presents itself as a solution if you want to expand your horizons and use new technologies.

Although it is true that this strategy seeks to protect us against digital problems within the system or even against a cyber attack, it is also necessary to take into account the training of all staff as a preventive measure to prevent your employees from falling into traps such as *phishing*, since that these could compromise the digital health of your organization: in fact, data theft in this way is very common.

Most popular security audit types

This excellent preventive strategy can be of several types.
To begin with, cybersecurity checks can be differentiated depending on who performs them into two subtypes:

Internal

They are made by the company's own personnel with or without the help of external personnel.

External

They are executed by contracted personnel, external and independent of the company.
The ideal option can vary depending on your company's payroll budget; in certain cases, starting a new cybersecurity department would cost more than hiring experts from outside your organisation.
Evaluate all the possibilities!

Now, if we consider the methodology that is applied in the security audit, it can be divided as follows:

Compliance

This type of audit ensures compliance with a certain security standard, whether national or international. For example, ISO 27001 or those that are established in the company's internal policies and procedures.

Techniques

Its objective is only to review computer programs by professionals in systems.
Lastly, security audits are a bit more specific and have a limited range of action when there is an objective to be met, which leads us to the following subtypes:

Forensic

Once the incident has occurred, this kind of security audit seeks to collect all the related data to determine the possible causes that have generated it and the information or systems affected.
Likewise, it intends to search for digital evidence that can assertively guide us to the origin of the fault in order to correct it.

Web applications

They aim to identify potential vulnerabilities in web *apps that could be exploited by cyber attackers.* This type of security audit is also subdivided into:

- **Dynamic Application Analysis**: *Dynamic Application Security Testing* (DAST), based on a real-time review of the web application.

- **Static Application Analysis** – *Static Application Security Testing* (SAST) to find possible vulnerabilities in the code.

Penetration Test

Also called "ethical *hacking* ", it is a cybersecurity technique that tests the computer security measures that the company has, such as *firewalls* and IDS/IPS, among others: everything follows a protocol in the same way that a potential cyber attacker to identify weaknesses that can be corrected.

Physical access control

The platforms are audited and the protection measures that make up the physical perimeter system of a company - such as a door opening mechanism, cameras, sensors, etc.

Net

All devices connected to the network are examined to check their means of protection, such as updating their *firmware, firewall* rules, network access control, antivirus signatures, and network segmentation in VLAN's and Wi-Fi network security, among others.

In conclusion, computer security has grown enormously due to the great changes in conditions and new digital platforms available.
Today, most programs are interconnected, which has opened new horizons for companies to improve their productivity: with this, problems also appear; to prevent them, don't forget to include the **smart contract security audit** in the systems department to protect the structure of your organization.