



ISOPH FIM FOR COMPANIES SPECIALIZING IN DIGITAL TRANSFORMATION AND MANAGEMENT

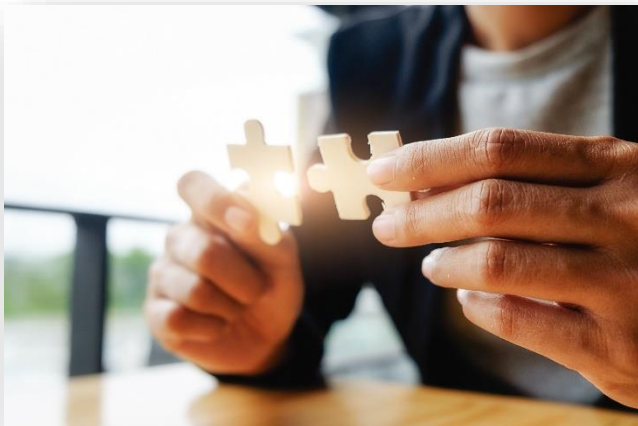
INTRODUCTION

ISOPH FIM, the solution you need to protect your files: adaptable to different needs, markets and that increases your organization's security against today's continuous threats.

- Monitors file integrity.
- Anticipates security breaches and identifies changes made to the system.
- Checks file properties such as permissions and document modification date.

THE NEED

Nowadays, one of the challenges for companies dedicated to Digital Transformation and Management is the implementation of a "File Integrity Monitoring" system (ISOHP FIM) in order to comply with different regulatory requirements, such as ISO27001 and PCI DSS.



THE CHALLENGE

With the implementation of the ISOHP FIM monitoring software, this company will secure all its systems and electronic files and thus comply with all the requirements of the international ISO 27001 and PCI-DSS standards.

THE TECHNOLOGY

ISOPH FIM (File Integrity Monitoring) is a cloud-based technology that continuously monitors files to see if they have undergone any unauthorized and unexpected changes. This integrity scanner works as a "fingerprint" of the files, since it compares them with each other and is thus able to know if changes have been made to the files.

ISOPH FIM is a state-of-the-art, fully customizable technology that monitors file integrity, helping to prevent and anticipate security incidents and identify errors that could expose an organization to cyber-attack. A solution that is adaptable to different needs, markets and increases security in the face of today's continuous threats.

In addition, it helps to comply with PCI-DSS requirements.

- Security, performance and functionality of your files.
- Activity logging.
- Integrity of the company's confidential files.
- Adaptable to different market needs.

METHODOLOGY

The methodology used by BOTECH is based on the continuous knowledge that our ISOHP FIM tool performs on its different installation environments, the logs and files obtained help us to continue researching, in order to improve our methodology of continuous analysis of vulnerabilities.

BENEFITS

The vertiginous increase of attacks to business infrastructures makes necessary the implementation of monitoring systems, as well as the management of change of permissions and attributes in files and applications.

ISOHP FIM, resolves 99.9% of this type of attacks, maintaining the integrity and availability of systems, analyzing the vulnerabilities present and offering a guarantee of security and customer satisfaction.

