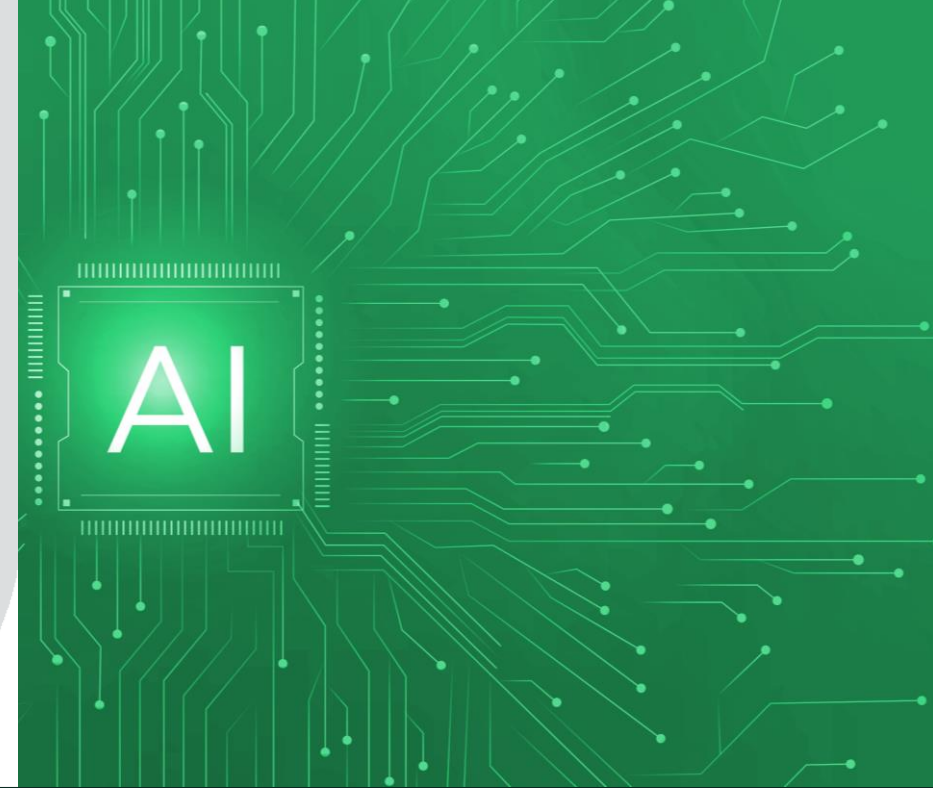# Artificial intelligence

AI

Challenges and Benefits to increase
the productivity of companies
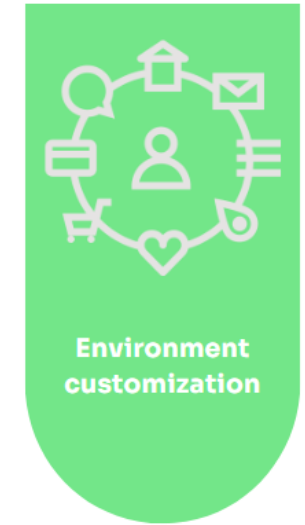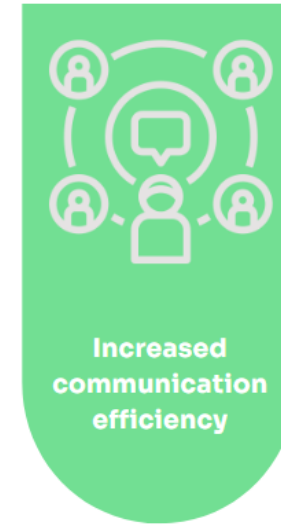
November 2023

ONESEC Microsoft

UN DIA EXTRA ONESEC.IA

Artificial
intelligence

To improve productivity in organizations, AI implements intelligent systems and algorithms that perform tasks and processes in an efficient, accurate and automated manner.

Task automation

Process optimization

Decision-making assistance

Increased communication efficiency

Environment customization
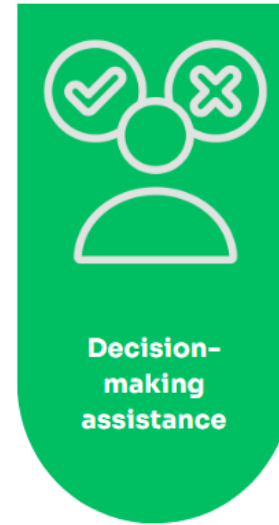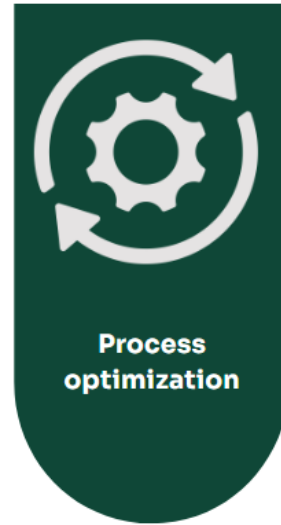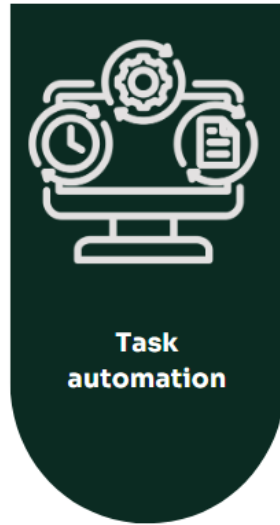
Artificial intelligence makes you more productive

ONESEC Microsoft

ONESEC.IA

M365
Copilot target

Microsoft 365 Copilot is an artificial intelligence tool that helps you create and improve your content in the Microsoft 365 apps you use every day

Artificial intelligence that makes you more productive
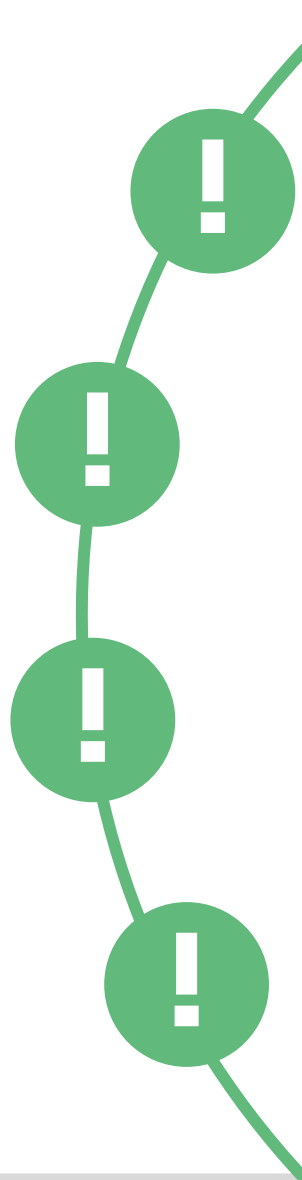
! **Reduce operating costs** — Companies using Copilot can save up to 2 hours per week per employee

! **Increase income and competitiveness** — Copilot helps you generate original content, create more innovative and attractive products and services

! **Activities optimization** — Copilot is between 25% and 35% faster , reduces 15% errors and generates 20% user satisfaction

! **Improve employee satisfaction and retention** — Copilot helps you develop your skills and knowledge by providing you with information and resources relevant to your topic.

ONESEC Microsoft ONESEC.IA

Companies need a **different approach** to face challenges:

Identity Governance and Information Governance

Understanding the benefit

Expedite adoption

Use cases that improve processes

Lack of experience and knowledge

Inefficient Collaboration
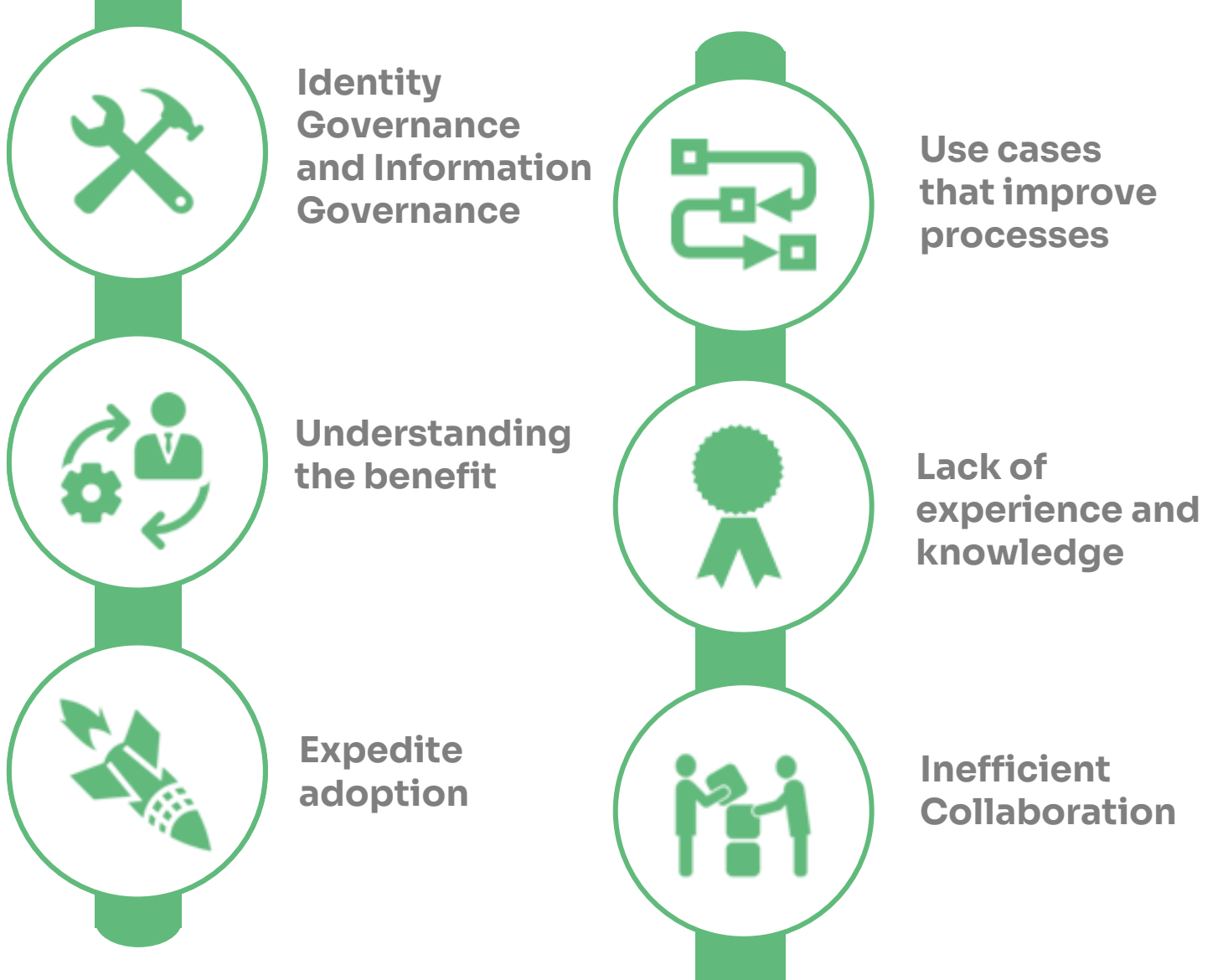
ONESEC.AI

What is
ONESEC.AI?

It is your ally in artificial intelligence to enhance productivity, innovation and efficiency in organizations.

Onesec.AI is distinguished by its 360 approach, ensuring effective and secure adoption of key technologies such as Microsoft's Copilot in a reliable and efficient cybersecurity environment.

ONESEC · Microsoft

ONESEC.IA

Microsoft Copilot They are changing the way we work, making clients more efficient while unlocking new levels of creativity.

While these tools open the door to new possibilities, questions arise around the technology.

✓ How do I guarantee the privacy of my information?

✓ Where can I apply the use of artificial intelligence tools?

✓ Am I ready for artificial intelligence in my company?

Onesec has developed an offer where companies can adopt artificial intelligence tools in a safe environment and with the peace of mind that they comply with what is necessary in terms of identity and information protection.

Information Protection

Secure identity

Productivity and Collaboration

ONESEC . AI

How do we do it?

ONESEC Microsoft
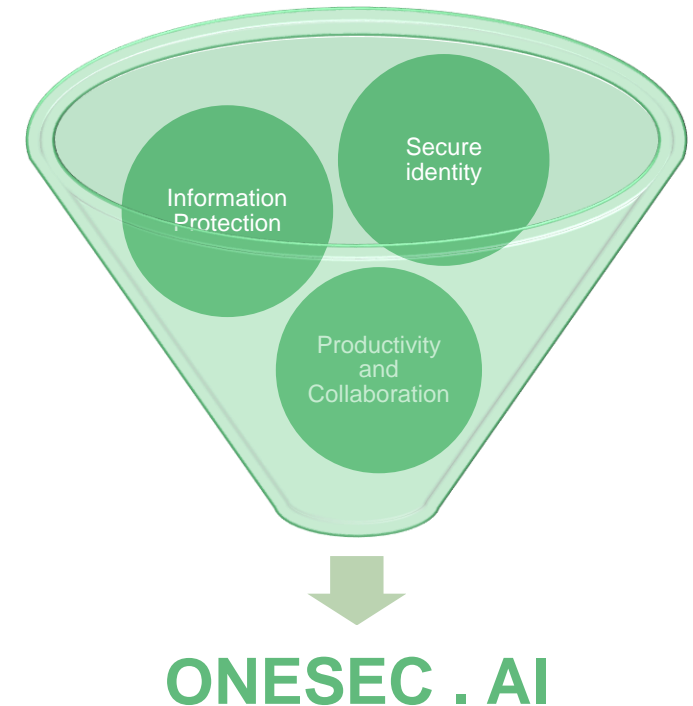
ONESEC.IA

Discover the power of **ONESEC.AI** for AI-powered success!

01A Requirement assessment
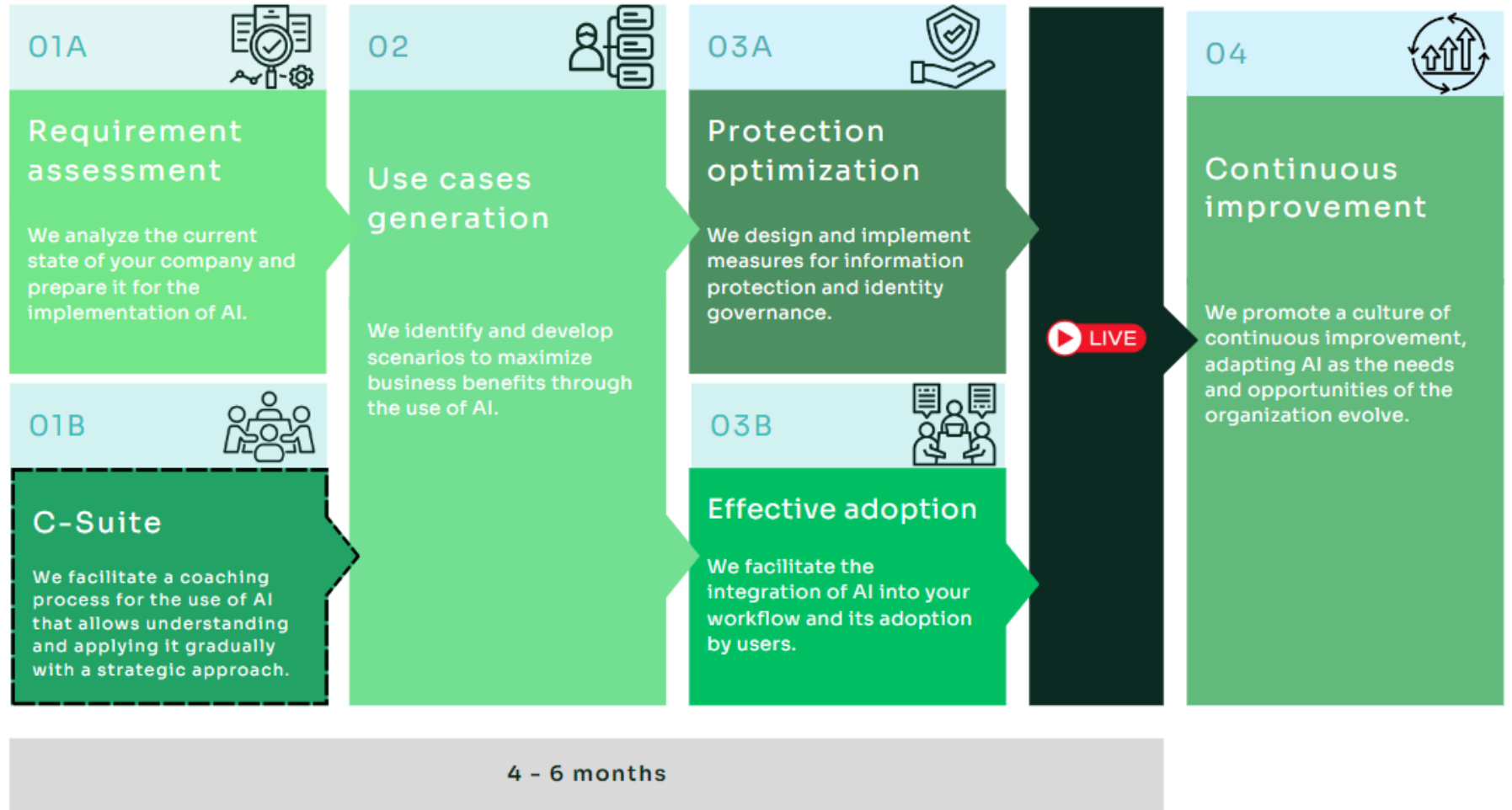
We analyze the current state of your company and prepare it for the implementation of AI.

01B C-Suite

We facilitate a coaching process for the use of AI that allows understanding and applying it gradually with a strategic approach.

02 Use cases generation

We identify and develop scenarios to maximize business benefits through the use of AI.

03A Protection optimization

We design and implement measures for information protection and identity governance.

03B Effective adoption

We facilitate the integration of AI into your workflow and its adoption by users.

LIVE

04 Continuous improvement

We promote a culture of continuous improvement, adapting AI as the needs and opportunities of the organization evolve.

4 - 6 months

ONESEC   Microsoft   ONESEC.IA

We deliver a complete offer that allows companies to have a process that allows them to integrate artificial intelligence in an agile and safe way, identifying the benefits to their productivity, establishing use cases in accordance with business priorities, communicating appropriately to customers. collaborators and minimizing possible security risks.

The Onesec.IA offer is designed to support the organization by delivering value in the same solution that includes:

Analysis and evaluation : We identify the security risks that may arise in organizations derived from identity governance in their services and the governance of sensitive information and we deliver a personalized protection strategy for each client and industry.

Change management : We accompany organizations in the adoption, identification of use cases, aligning and improving their processes, accompanying end users in understanding and taking advantage of capabilities, as well as identifying the economic and strategic benefits of AI in their organization. .

Security remediation and technical deployment : Once we generate a business strategy and have a clear understanding of the security posture, we carry out the optimizations or remediations that minimize the risks in identity protection and information governance, thus guaranteeing a reliable deployment. of Microsoft 365 Copilot appropriate and aligned to the needs of the business.

ONESEC

Microsoft

ONESEC.IA

Adoption

Adoption Scope

Provide an adoption process focused on transforming digital habits and skills to **maximize the use of Microsoft 365 + Copilot** through new productive and safe scenarios.

Microsoft 365 Copilot

ONESEC.IA

Benefits

- **Accompaniment to leaders** with a gradual Microsoft Copilot coaching process.

- **Form an elite** adoption team.

- **Facilitate understanding of Microsoft Copilot** through effective communication.

- **Guide users in adopting new habits** using Microsoft Copilot.

- **Speed up learning prompts and best practices** that boost productivity using Microsoft Copilot.

ONESEC.IA

Services

The services we have for adoption

C-Suite adoption process

We facilitate **a coaching process for the use of Copilot** that allows you to unlock productivity and gradually integrate AI into your work experience.

Generation of use cases

We identify the area where **the adoption of Microsoft Copilot** and its use cases will have the greatest impact to drive productivity and meet the unique needs of the organization.

End User Adoption Process

We promote the process of adopting **new productive habits by streamlining tasks, automating workflows and improving collaboration** with Microsoft Copilot on Teams.

C-Suit
Adoption

C-Suite Adoption

This adoption service focuses on **increasing productivity and optimizing leaders' times to focus on the most important issues.**

★ The adoption of Microsoft Copilot is based on the best practices of the tool adapted to customer needs.

01 Learn what you can do with Microsoft Copilot

★ **02** Integrate Copilot into your daily activities

03 Speed up your learning about Microsoft Copilot

★ **04** Experience Copilot in your day

★ **05** Expand your horizons with Copilot

ONESEC ■ Microsoft

ONESEC.IA

INTERNAL USE INFORMATION ONESEC

How do we perform
C-Suite Adoption?

Microsoft Copilot adoption is based on tool best practices and customer needs

01.
Learn what you can do with Microsoft Copilot

Discover the best productivity practices with Microsoft Copilot through a workshop for managers.

02.
We integrate Copilot into your daily activities

You will have use cases where Copilot will be applied to eliminate manual tasks, facilitating use and saving time in the applications of :
– Office (Word, Excel, PowerPoint)
– Outlook,
– Teams, among others.

03.
Speed up your learning about Microsoft Copilot

You will have multimedia education materials and reference infographics to use Copilot in your use cases.

04.
Experience Copilot in your day

Integrate Microsoft Copilot into your work experience through a workshop focused on applying your use cases and discover step by step when and how to use your virtual assistant.

05.
Broaden your horizons with Copilot

Continue learning gradually and discovering new cases to apply Microsoft Copilot through **coaching support.**

ONESEC Microsoft

INTERNAL USE INFORMATION ONESEC

ONESEC.IA

Generation of Use Cases

Generation of Use Cases

Detect the area that will benefit most from Copilot	01	Analysis of the information RESULTS REPORT	02	Apply Copilot in use cases in the area

- We define the adoption objectives

- Identify the area that Copilot will take advantage of due to its impact on the business through an awareness and needs detection workshop.

- The use cases where to apply Copilot will be defined based on the needs of the area through the analysis of its main workflows.

- You will have graphic material of the use cases where you can identify the transformation of Copito's workflows and integration.

ONESEC Microsoft

ONESEC.IA

Apply Copilot
in use cases in the area

Effective adoption in your organization

This service favors the process of acceptance, integration and use of Microsoft Copilot in the flow of activities in the productivity of collaborators with more powerful productivity tools.

03 A
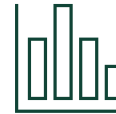
Has an effective communication process

04

Measure the adoption process

05

Strengthen use cases and explore new applications of Copilot

03 B

Facilitates and directs Copilot learning

COPILOT LEAD TRAINING
N1 | N2 | N3

How do we carry out Effective Adoption in your organization?

03A. Has a communication process
- **Guides users in understanding Copilot** with visual material and simple language.

03B. Makes learning Copilot easier
- **You will have multimedia education materials** and reference infographics to accelerate creative and productive processes with Copilot.
- **Integrate Microsoft Copilot into your work experience** through a workshop focused on applying the area's use cases.

04. Measure the adoption process
- **You will be able to track adoption** through Measurement Dashboards.
- **Collect the feelings and needs of users** through qualitative techniques.

05. Strengthen use cases and explore new Copilot applications
- **Resolve users' doubts in a timely manner** through sessions and visual FAQ material .
- **Reinforces the knowledge and use of Copilot** through gamification dynamics.

COPILOT LEAD TRAINING PROGRAM (on-site)

LEVEL 1
LEAD COPILOT
Introduction to Copilot and the role of a Lead Copilot

LEVEL 2
QUALIFIED LEAD
Detection of new use cases for Copilot , principles of *rapid engineering.
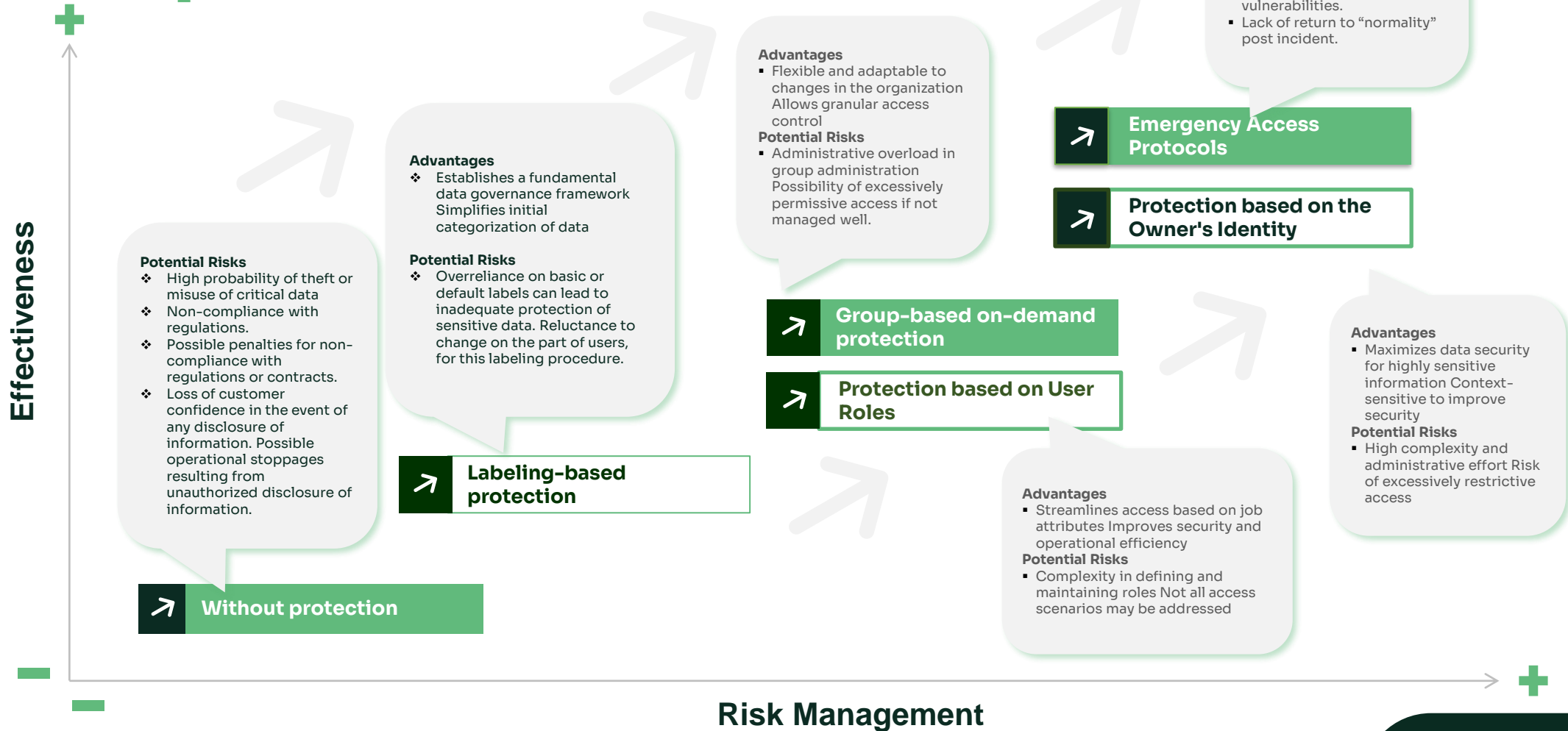
LEVEL 3
LEAD MASTER
Trainers of change agents for the adoption of Copilot in following areas and creation of clear and specific instructions for better results.

*Ability to know when and how to ask Copilot to do something for you.

ONESEC Microsoft

ONESEC.IA

Identity and data protection assessment

Advanced strategies for data protection

Effectiveness (vertical axis)

Risk Management (horizontal axis)

Without protection

Potential Risks
- ❖ High probability of theft or misuse of critical data
- ❖ Non-compliance with regulations.
- ❖ Possible penalties for non-compliance with regulations or contracts.
- ❖ Loss of customer confidence in the event of any disclosure of information. Possible operational stoppages resulting from unauthorized disclosure of information.

Labeling-based protection

Advantages
- ❖ Establishes a fundamental data governance framework Simplifies initial categorization of data

Potential Risks
- ❖ Overreliance on basic or default labels can lead to inadequate protection of sensitive data. Reluctance to change on the part of users, for this labeling procedure.

Group-based on-demand protection

Protection based on User Roles

Advantages
- Flexible and adaptable to changes in the organization Allows granular access control

Potential Risks
- Administrative overload in group administration Possibility of excessively permissive access if not managed well.

Advantages
- Streamlines access based on job attributes Improves security and operational efficiency

Potential Risks
- Complexity in defining and maintaining roles Not all access scenarios may be addressed

Emergency Access Protocols

Protection based on the Owner's Identity

Advantages
- Enables rapid response in critical situations Ensures business continuity in emergency situations

Risks
- Risk of abuse or misuse Possible security vulnerabilities.
- Lack of return to "normality" post incident.

Advantages
- Maximizes data security for highly sensitive information Context-sensitive to improve security

Potential Risks
- High complexity and administrative effort Risk of excessively restrictive access

ONESEC   Microsoft

ONESEC.IA

Advanced strategies for data protection

Effectiveness

Risk Management

Activities
- ❖ Advisory analysis to determine what information should be protected.
- ❖ Review of current labeling and generation of improvement points or creation of a new labeling scheme.
- ❖ Identification of possible financial, operational, reputational and/or legal risks.
- ❖ Determination of treatment of each data label to provide better protection.

Activities
- ❖ Procedures for requesting and approving repositories and groups
- ❖ Help Desk Interface

Activities
- ❖ Define process for Incident Management
- ❖ Definition of emergency protocols
- ❖ Development of procedures for Help Desk

Activities
- ❖ Group request procedures
- ❖ Procedures for creating repositories

Activities
- ❖ Identity and Data Protection Assessment

Activities
- ❖ Analysis of populations, groups and identities
- ❖ Analysis of permissions in repositories and documents by infotype
- ❖ Design of the model for organization of information and groups and access assignment
- ❖ Change management

↗ **Emergency Access Protocols**

↗ **Protection based on the Owner's Identity**

↗ **Group-based on-demand protection**

↗ **Protection based on User Roles**

↗ **Labeling-based protection**

↗ **Without protection**

ꓵNESEC ▦ Microsoft

INTERNAL USE INFORMATION ONESEC

ONESEC.IA

Requirements Assessment

The implementation of AI requires clearly understanding and implementing the information protection policy and its use cases, to avoid unwanted leaks.

- Access Control Policy
- Procurement processes
- Populations
- Geographies, Departments and Positions
- Groups
- Authentication Policy
- Existing accesses
- Behavior (Teams, Networks, Schedules, etc.)
- Access Tools
- Accessed Repositories and Databases
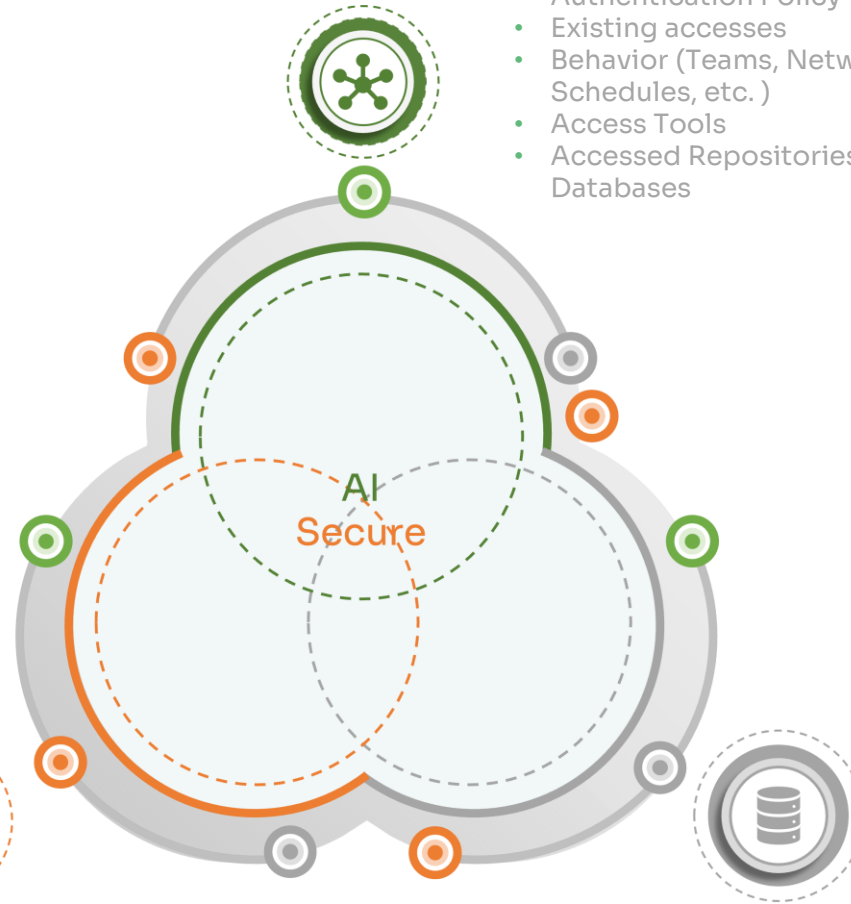
Identities Safe
Global Assessment of Identity Controls in Azure AD

Unstructured Data
Global Assessment of Controls for Information Protection

Data Structured
Global Assessment of Controls for Database Protection

AI Secure

- Information Classification Policy
- Infotypes
- Tags
- Files/Repositories
- Permissions
- Protection and Safeguarding Measures

- Information Classification Policy
- Infotypes
- Tags
- Databases and tables
- Information Quality
- Users, Roles and Permissions
- Database Configuration
- Protection and Safeguarding Measures

ONESEC Microsoft

ONESEC.IA

Evaluation of Government and Access Management

01 Analysis of populations, groups and identities

This phase involves gaining a detailed understanding of the organization's current landscape of populations, groups, and identities, identifying and understanding the criteria for identity management and access allocation processes.

- Identification of populations, life cycle and attributes
- Document the life cycle
- Evaluation of access to information policies
- Document processes for requesting and authorizing access
- AD and AAD group structure review

02 Analysis of permissions in repositories and documents by infotype

Understanding the current repository organization, information distribution, and assigned permissions

- Information Discovery by departments, locations, positions, repositories and infotypes
- Analysis of current permits

03 Design of the model for organization of information and groups and access assignment

It focuses on implementing secure information distribution and allocation processes to prevent accidental exposure or loss of sensitive data.

- Specifying the distribution of information by departments, locations, positions, repositories, and infotypes
- Specification of rules for group assignment (fixed and dynamic)
- Design and construction of processes for creating groups and assigning permissions on demand
- Implementation of group and repository structure (if required)

04 Change management.

Training and change management to support the adoption of this operating model regarding information access

- Help desk training
- Training for administrators
- Training and change management for end users

ONESEC Microsoft

ONESEC.IA

Initial assessment of customer security data protection posture

01 — Know your data.

This phase involves gaining a detailed understanding of the organization's current critical data landscape, identifying and understanding the nature and location of the data.

- In-depth interviews are conducted with leaders from 3 departments to understand how critical data is collected, stored and used.
- Identify and understand the types of data in the selected departments.
- Assessment of current data management and protection practices.

02 — Protect your data.

Focused on the development and application of protection measures for identified data, ensuring its confidentiality and integrity.

- Development of specific data protection policies for departments.
- Implementation of controls and sensitivity labels.

03 — Leak Prevention.

Focuses on implementing controls and policies to prevent accidental exposure or loss of sensitive data.

- Pilot tests to validate the implemented policies.
- Adjustments based on test

04 — Results.

Results Delivery provides a report with key insights and a roadmap to assess the viability of implementing Microsoft Copilot . This approach allows customers to visualize the added value of the entire package, improving the security and governance of their data using Microsoft Copilot .

- Preparation of a detailed report that includes findings, recommendations and a roadmap for full-scale implementation.
- This report will allow the client to understand the benefits and needs before proceeding with the full service.

ONESEC   Microsoft

ONESEC.IA

Process of ONESEC.IA

1. Know your data.

This phase involves gaining a detailed understanding of the organization's current critical data landscape, identifying and understanding the nature and location of the data.

- In-depth interviews are conducted with department leaders to understand how critical data is collected, stored, and used.
- Applicable regulations and current data protection policies are reviewed to identify any gaps or needs for updates.
- Analysis is carried out on existing data definitions, including dictionaries and regular expressions, to evaluate their accuracy and relevance; If they do not exist, they are documented and defined together with the client's designated personnel.

2. Protect your data.

Focused on the development and application of protection measures for identified data, ensuring its confidentiality and integrity.

- Improvements or additions to the rules and restrictions of data flows and repositories are recommended, based on the analysis of the previous phase.
- Sensitivity labels and data protection policies are implemented using Microsoft Purview to ensure proper handling of sensitive data.

3. Leak Prevention.

Focuses on implementing controls and policies to prevent accidental exposure or loss of sensitive data.

- Pilot tests are conducted in selected departments to test the effectiveness of new policies and controls.
- Adjustments are made to data protection policies and controls based on feedback and pilot test results.
- The organizational structure is analyzed to establish clear notification and escalation protocols in the event of data security incidents.

4. Data governance.

Dedicated to the implementation and management of policies at an organizational level, ensuring alignment with regulations and best practices.

- Clear SLAs are defined for compliance alerts and data monitoring, ensuring response times and actions are appropriate.
- Data governance policies and tools will be implemented throughout the organization in lockdown mode, accompanied by ongoing auditing and monitoring processes to ensure compliance and effectiveness.

ONESEC   Microsoft

INTERNAL USE INFORMATION ONESEC

ONESEC.IA

Methodology
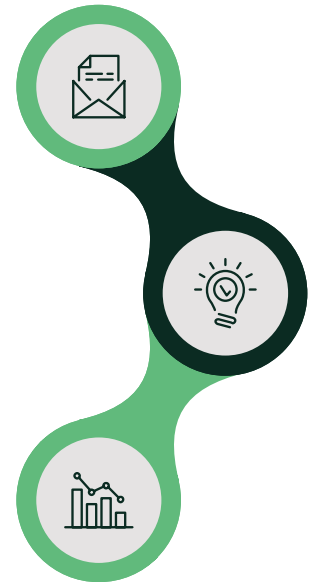
5. Implementation of Microsoft 365 solutions

- Our experts review and adapt the technical configurations and integrations to design the Compliance architecture in Microsoft 365, addressing the specific needs of each department previously identified.
- A session is organized to explain how these technological solutions satisfy the operational needs of the areas and Information Protection technologies are configured, Insider Risk Management and Discovery.
- After implementing and optimizing these configurations in a pilot group of 10 users per area, an awareness and change management campaign is executed, focusing on tools such as MIP and DLP. This phase includes explaining business information use policies and performing functionality tests with a select group of users.

6. Documentation and transfer of knowledge of the implemented services.

- After completing the necessary implementations and testing, we prepare a detailed technical report that describes the configurations in each solution covered in the project.
- Subsequently, we carry out a knowledge transfer about the tools and solutions implemented. This process ensures a deep understanding and facilitates the effective adoption of new technologies by the organization's team.

7. Activation of Microsoft Copilot.

- After completing the necessary implementations and tests, Microsoft Copilot will be activated, functionality and security tests will be carried out regarding the search for information.
- Subsequently, we carried out knowledge transfer and adoption of Microsoft Copilot. This process ensures deep understanding and facilitates effective adoption.

ONESEC   Microsoft

ONESEC.IA

How much does it cost?

Identity governance assessment

Information protection assessment

Coaching C-Suite

AI adoption

Optimization of information and identity protection

Generation of use cases
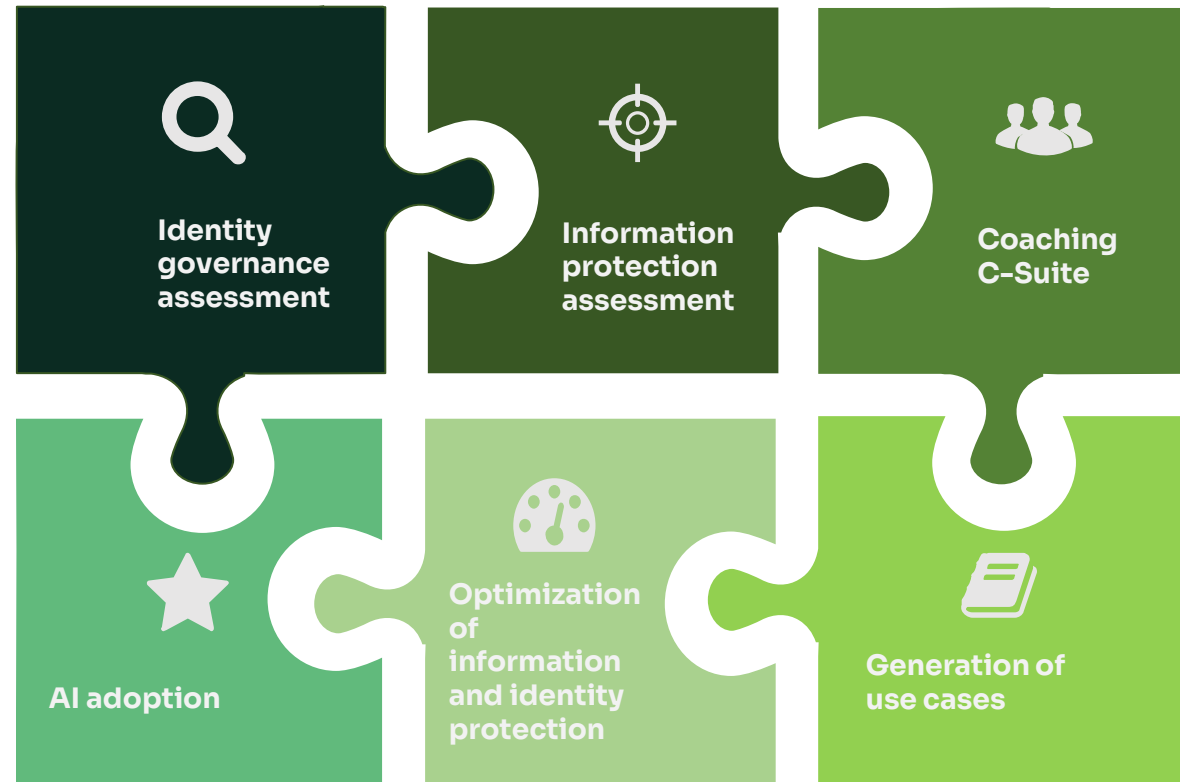
¿Why
ONESEC?

ONESEC + Un día extra

Secure change management

Joint collaboration allows us to offer a full range of skills and specialties, thus maximizing the value proposition for our clients.

Onesec

- Consulting and technical portfolio
- Partner of the Year 2023 Security Compliance
- +60 security specialists
- Cybersec
- Onesec member of all Microsoft security programs

Un Día Extra

- Certification in Change Management by APMG International.
- First company in Latin America certified to train in Change Management
- Focus on key high-value behaviors to drive technology adoption.
- Promote transformation and continuous improvement without neglecting the operation

UN DIA EXTRA + ONESEC

ONESEC + Un día extra

Secure change management

Joint collaboration allows us to offer a full range of skills and specialties, thus maximizing the value proposition for our clients.

UN DIA EXTRA

- Certification in change management by APMG international
- First company in Latin America certified to provide change management training
- Focus on high-value key behaviors to forter technology adoption.
- Drive transformation and continuous improvement without neglecting operations

ONESEC.IA

ᚷNESEC

- We meet Microsoft designations and specializations.
- Member of all Microsoft security programs.
- Consultative and technical portfolio.
- Security compliance partner of the year 2023.
- +60 security specialists.
- 110 Microsoft and cybersec security certifications

ᚷNESEC Microsoft

ONESEC.IA

WHY ONESEC? – MICROSOFT PROFILE
"Better Together"

One of our main advantages is the synergy we have with great allies.

Access our profile and locate us with the company name * **Secure Nextgen Systems**
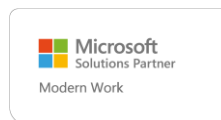
MAICPP – Microsoft AI Cloud Partner Program

Microsoft Cloud Partner Designations:

Advanced Specializations:

- o Security: Identity and Access Management
- o Security: Information Protection and Governance
- o Security: Threat Protection
- o Modern Work: Modernize Endpoints

Member of the specialized programs::

- o FastTrack Ready Partner liga
- o CSI (antes MSSP) Partner (Managed Security Service Provider) liga
- o MISA Partner (Microsoft Intelligent Security Association) liga
- o Microsoft Elite Security Partner
- o FY24 Programs:
  - o ECIF Ready Partner | México and Colombia
  - o Microsoft FY24 Secure Productivity
  - o Microsoft Sentinel Migration and Modernization Investment

Awards:

2023-2024: Microsoft Security Partner of the Year – LATAM & Caribbean
2022-2023: Microsoft Country Partner of the Year – MEXICO Microsoft Compliance Partner of the Year – LATAM

Microsoft Solutions Partner — Security

Microsoft Solutions Partner — Infraestructura Azure

Microsoft Solutions Partner — Modern Work

Microsoft Solutions Partner — Digital & App Innovation Azure

Microsoft Intelligent Security Association — Microsoft Security — Microsoft Verified Managed XDR Solution

ONESEC   Microsoft   ONESEC.IA

WHY ONESEC? – CERTIFIED EXPERIENCE AND TALENT

Cybersecurity challenges require specialized personnel to guarantee the success and expected value of the projects. Considering the above, ONESEC has formed a team supported by international certifications and organizations , thus guaranteeing the achievement of our clients' objectives.

Top Practices

Defensive

Offensives