





Manage and secure your devices, applications and users

Highlights about the workshop

 **Improve** your Microsoft Secure Score with Enpoint Manager

 Learn how to create **management** policies that protect your users, company data and devices.

 **Gain insight** into user endpoints and compliance with IT policies

 Determine the best way to give users access to the **applications they need on the devices.**

"Modern device management covers a wide range of areas including user protection, device addition or removal, managed applications, end-user support and deployment of new capabilities."

-Forrester's Microsoft 365 Enterprise Total Economic Impact Study 2020

How do you manage your mobile devices, laptops and other user endpoints? Do you know if your users' devices comply with your IT policies?

Enable users to be productive, on any device, without compromising IT security

Today's users are looking for more ways to stay productive while working on any device. 95% of organizations allow personal devices in the workspace. All of these devices add additional risks, when you consider that 70 million smartphones are lost each year.

As users demand more ways to work the way they want to work, this workshop will show you how to manage both company-owned and user-chosen devices in the cloud.



Why you should attend

Experience the power of modern device management within your own environment.

This workshop will show you how to leverage intelligent security, risk-based controls, zero-touch provisioning, advanced analytics, and deep integration with the Microsoft products you already use. By attending, you will be able to:

Learn how to improve your management skills with Microsoft Enpoint

Discover and protect your endpoints by enforcing policies and implementing security tools.

Protect your users' identities with multifactor authentication and conditional access from any device

Enabling your users to be productive with the applications they need on the organization's devices

What to expect:



During this workshop we will look at how to manage the security of your organization's devices. We will give you the ability to protect the identities of your authorized users so you can authenticate credentials and manage access while giving users the freedom to collaborate with others.

- **Get** an executive immersion in remote deployment, management and security of devices in your organization.
- **Show** the best ways to manage endpoints at the enterprise level.
- **Provide** the ability to protect the identities of your authorized users so you can authenticate credentials and manage access while still giving users the freedom to collaborate.

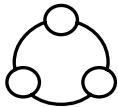
We will work with you to:

- **Enhance** your management capabilities with Microsoft Endpoint Manager.
- **Discover** and protect your endpoints by enforcing policies and deploying security tools.
- **Protect** your identities with multi-factor authentication and conditional access from any device.
- **Enable** your users to be productive with the applications they need on the devices they want.

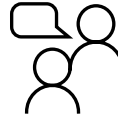
We customize the workshop according to the needs of your organization:

Establishment of the commitment:

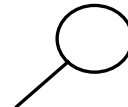
Microsoft Endpoint Manager
Basic security
Device configuration and management.



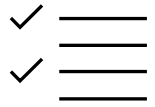
Design and Planning



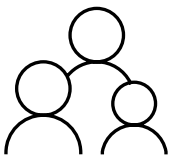
Customer value conversation



Endpoint discovery session



Presentation of recommendations and next steps



Who should attend

The workshop is aimed at security decision makers, such as:

- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)
- Chief Security Officer (CSO)
- Endpoint and device management owners and managers
- Application business owners.
- IT security, IT compliance and/or IT operations.
- Security architect
- Security engineers

Why Overcast?

When it comes to compliance, you need an experienced partner.

We want to be your technology partner

¡Contáctanos hoy para comenzar!