

Duration: 3 hours

Prerequisites:

- No prior knowledge of cybersecurity required.
- Access to a computer with an Internet connection.

Teaching methods:

- Online training, asynchronous
- Training materials included

Skills acquired by the end of the course:

- Develop robust internal cybersecurity policies
- Oversee the management of access, backups and devices
- Build an action plan for incident response

Certificate: yes

DESCRIPTION

Designed specifically for leadership teams, this course focuses on the importance of putting robust internal cybersecurity policies in place. You will find that holding cybersecurity knowledge and adopting good online practices is essential — but insufficient if those practices are not shared and adopted across your teams. If you want to understand the risks associated with cyberattacks, and above all anticipate and neutralize them through clear policies and rigorous protocols, you are in the right place. Knowledge is power, but sharing that knowledge is what secures your organization for the long term.

PROGRAM:

General objective

- Proactively secure access to your data and embed lasting online habits across your teams.

Specific objectives

- Develop a regular maintenance schedule for all devices.
- Keep access rights up to date as roles change.
- Adopt sound backup practices.
- Establish criteria for creating strong passwords.
- Manage sent and received email properly.
- Maintain secure connections, particularly for remote work.
- Frame the internal use of artificial intelligence tools.
- Define clear guidelines for the use of personal devices in a professional setting.
- Ensure a secure handover when a team member leaves.
- Build a clear, practical action plan for handling cybersecurity incidents.

QUESTIONS/ANSWERS