centro criptológico nacional

Incident Prevention Measures

Audit

Activate perimeter access systems audtis. You must know who is connecting, at what time and from which IP address.

Surveillance

Proactively and continuously monitor the security of your remote working infrastructure.

Access

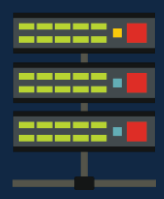
Limit teleworking access to known locations. If you're not based in Asia, no one should be able to connect from there.

Redundancy

Reinforce the availability of your teleworking infrastructure. Implement redundancy.

Patches

Update all your systems and client equipment with the latest security patches, especially those exposed to the Internet and those used in teleworking.



Backup

Review your backup plans and perform full-service recovery tests.

Contingency

Design a contingency and business continuity plan in case of a serious security incident.

Bandwidth

Increase bandwidth to ensure concurrent teleworking connections.

MFA

Implement Multi-Factor Authentication to users who are working from home.

ENS

Apply the necessary security measures taking the National Security Framework as a reference and installing EDRs both in the equipment that connects and in the one that is connected.

centro criptológico nacional