




## Cuestionario de la segunda parte del ejercicio

Especialidad: A6 D4. Seguridad Informática.

Por favor, lea detenidamente antes de comenzar:

- **NO** abra el **CUESTIONARIO** ni empiece el examen hasta que se le indique.
- Para realizar este primer ejercicio se hace entrega de dos documentos:
  1. Cuadernillo con los **casos prácticos prácticos**, sobre las materias del programa de esta convocatoria.
  2. **Hoja de respuestas** donde se consignará la respuesta correcta a cada pregunta.
- Al finalizar la prueba se hará entrega de la hoja de respuestas.
- Sólo se calificará las respuestas desarrolladas en la **HOJA DE RESPUESTAS**
- Una vez abierto el cuestionario, compruebe que consta de todas las páginas y preguntas y que sea legible. En caso contrario solicite uno nuevo al personal del aula.
- Verifique que el número de la solapa donde se recogen sus **datos personales coincide con el número de la hoja** de examen donde se consignan las respuestas.
- El examen se realizará con bolígrafo azul o negro. Si no dispone de uno, solicítelo al Tribunal.
- El cuestionario consta de **2 casos** propuestos
- La persona candidata deberá **ELEGIR UNO de esos dos escenarios, haciéndolo contar en la hoja de respuesta** y, basándose en la afirmación aportada por el tribunal, construir justificadamente un caso específico y plantear las formas de abordar la situación, proponiendo vías de soluciones o mejoras e intervenciones a llevar a cabo, todo debidamente argumentado
- El **enunciado** del caso se entregará en **INGLÉS**. La **contestación** al mismo se desarrollará en **CASTELLANO**.
- Numera las hojas de respuesta en orden de lectura e indique los datos personales solicitadas en la misma.
- Se podrán pedir hojas en blanco para utilizar como borrador, pero estas **NO** serán calificadas.
- **NO Separe** ninguna de las copias de la **HOJA DE RESPUESTAS**. Una vez finalizado, el personal del aula le indicará los pasos a seguir.
- **Dispone de 120 minutos**, máximo, para realizar este ejercicio.

	<p>Proceso selectivo por el sistema de acceso libre para ingreso en la Escala de Tecnólogos de los Organismos Públicos de Investigación, convocado por resolución de 22 de diciembre de 2025 (BOE N°314 30 de diciembre) – OEP 2023-2024-2025</p> <p>Primer Ejercicio</p>	<p>Fecha: 10/05/2026</p> <p>Página: 2 de 5</p>
---	---	--

## **Estudio de CASO NÚMERO 1**

A public research centre uses its own and third-party information systems for its internal tasks and to provide public services (e-government). The centre has been processing files locally for years, previously by hand and now using its own computer system.

A connection to a central archive has recently been added to this computer system; this archive functions as a ‘historical memory’, allowing data to be retrieved and closed files to be retained. The latest development involves offering the centre’s own e-government service, through which users can carry out their administrative procedures online, using their tax identification number (NIF) as their login, along with a personal password. The same processing system is used locally by a civil servant who assists members of the public visiting the unit’s offices.

The head of the e-government project, alarmed by media reports regarding internet security, and aware that a service failure would seriously damage his unit’s reputation, takes on the role of project leader. In this role, he writes an internal report addressed to the unit director, in which he outlines: The IT resources currently in use and those to be installed. Incidents that have occurred since the unit was established. The uncertainties arising from the use of the Internet to deliver the service. Based on this report, he argues the case for launching a project.


Management, convinced of the need to take action before a disaster strikes, sets up a monitoring committee comprising the heads of the relevant departments: customer service, legal advice, IT services and physical security. It is decided that the scope of the project will cover electronic, in-person and remote processing services. This includes the following:

- An assessment of the security of the information handled: files.
- Equipment analysis: security equipment and the communications networks necessary for the protection of the service will be analysed.
- Study of relevant elements such as identification and authentication data for system users, the work areas of the staff handling them, the equipment room (data processing centre) and the people involved in the process.
- Security assessment of the subsidiary services used. The analysis is local, confined to the unit in question
- Architecture of security systems to protect the service, such as DMZ, IDS, SIEM, SOAR, etc.

The project is announced internally via a general communication to all staff in the unit and personal notification to those who will be directly affected. These communications identify the persons responsible for the project.

Summary:


- E-government.
- Research Centre providing administrative services to the public:
  - In person (counter).
  - By visiting the town hall premises.
  - Online service.
  - Via the Internet, at home or outside the city.

	<p>Proceso selectivo por el sistema de acceso libre para ingreso en la Escala de Tecnólogos de los Organismos Públicos de Investigación, convocado por resolución de 22 de diciembre de 2025 (BOE N°314 30 de diciembre) – OEP 2023-2024-2025</p> <p>Primer Ejercicio</p>	<p>Fecha: 10/05/2026</p> <p>Página: 3 de 5</p>
---	---	--

- Notifications are received by email.
- The information system manages administrative files.
- Files are stored locally whilst they are open.
  - There is a VPN connection to the provincial capital.
  - Files are downloaded when required.
  - Files are sent to the capital when they are closed.
  - Long-term availability is provided in the provincial capital.
- Email is used regularly.
  - Internal coordination.
  - Notifications to service users.
  - Messages are stored on the central server.
  - No messages are stored on PCs.

## Questions

1. Given the 'opacity' of the external central archive, how should the centre guarantee the integrity of files sent via VPN? **(2 points)**
2. Citizen Authentication: Assess the robustness of the 'NIF + password' method for an e-government service in accordance with the National Security Framework. **(2 points)**
3. Communications Security: The scenario mentions a VPN with the capital and the use of email. Which protocols would ensure the confidentiality of these data flows? **(2 points)**
4. Availability and Resilience: How does reliance on the central archive affect the centre's business continuity in the event of a VPN failure? **(2 points)**
5. Privacy and GDPR: Is a Data Protection Impact Assessment (DPIA) required for the new web-based processing? **(2 points)**
6. Network Architecture and Segmentation: Justify the need to implement a DMZ and an IDS system in this scenario, detailing how they protect the local database from web users. **(3 points)**
7. Security Operations: Explain the synergy between SIEM and SOAR in detecting and responding to a data exfiltration detected on the web portal. Where in the architecture would you place these systems? **(3 points)**
8. Design a SIEM correlation rule to detect a port scan. **(4 points)**
9. Design a playbook for the scenario where a user clicks on a phishing link and enters their corporate credentials on a malicious website. The Email Security Gateway (SEG) or Threat Intelligence reports a hash of a malicious link that has been accessed by the organisation. Your objective will be to validate the risk, verify whether the user has authenticated after clicking, isolate the compromised account and notify the team automatically. **(5 points)**

	Proceso selectivo por el sistema de acceso libre para ingreso en la Escala de Tecnólogos de los Organismos Públicos de Investigación, convocado por resolución de 22 de diciembre de 2025 (BOE N°314 30 de diciembre) – OEP 2023-2024-2025 Primer Ejercicio	Fecha: 10/05/2026 Página: 4 de 5
---	--	--

## **Estudio de CASO NÚMERO 2**

The "Centro Nacional de Energía y Física Nuclear (CNEFN)" has a mixed infrastructure: researchers' workstations (*Windows/Linux/macOS*), an HPC cluster, and storage servers. They recently deployed an EDR solution, but researchers complain that it "blocks legitimate simulation tools".

An attacker exploits a vulnerability in a misconfigured VPN and manages to compromise the endpoint of a theoretical physicist. The EDR detects a suspicious *PowerShell* execution but does not automatically block it because it was configured in "Learning Mode" to avoid false positives in the scientific environment. The attacker uses this time to disable the local EDR agent, exfiltrate nuclear reactor data, and finally deploy ransomware.

### **Questions**

**(In all responses, whenever possible, refer to specific controls of the National Security Scheme (ENS) -Annex II. Security Measures- that are involved)**

1. Explain why scientific software (customized compilers, Python scripts, data analysis tools) typically generates "malicious behavior" alerts in a standard EDR. **(1.5 points)**
2. The center's EDR was kept in 'learning mode' to avoid false positives that would abort long-running computational processes, which allowed the attacker's lateral movement. Given this operational limitation, argue for a technical solution that combines network restructuring through a Data DMZ and internal segmentation. How would this design allow the EDR to operate in strict 'blocking mode' at the perimeter while maintaining a 'controlled exclusion' environment in the research core, and in what way does this segmentation facilitate compliance with the National Security Framework (ENS) -Annex II. Security Measures- information flow protection measures? **(4 points)**
3. Research centers often have legacy hardware (sensor controllers) where an EDR agent cannot be installed. How would you cover this security "blind spot"? **(1.5 points)**
4. The attacker managed to disable the local EDR agent. What technical features should an EDR have to prevent a user with administrator privileges from stopping it? **(2 points)**
5. If the EDR logged telemetry before being disabled, what type of artifacts (e.g., unusual network connections, service creation) would you look for to reconstruct the attack timeline? Analyze the response from the perspective of the National Security Scheme (ENS). **(3 points)**
6. Explain why an EDR is insufficient when the attack originates from the network (misconfigured VPN) or uses identity services (*Active Directory*) before reaching the endpoint. Evaluate the limitations of an EDR in accordance with the National Security Scheme (ENS). **(2.5 points)**
7. How does XDR differ from EDR, and how would the integration of firewall and email logs have helped stop the attack at the VPN phase? **(2 points)**



Proceso selectivo por el sistema de acceso libre para ingreso en la Escala de Tecnólogos de los Organismos Públicos de Investigación, convocado por resolución de 22 de diciembre de 2025 (BOE N°314 30 de diciembre) – OEP 2023-2024-2025  
Primer Ejercicio

Fecha:  
10/05/2026  
Página: 5 de 5

8. In an XDR scenario, if the firewall detects a connection to a command and control (C2) IP and the EDR detects a registry change on a server, how does XDR help automatically connect these dots? **(2 points)**
9. The attack entered via VPN. Propose how the ZTNA model would have limited the damage by verifying "device health" (EDR posture) before allowing connection to the tunnel. **(2.5 points)**
10. For this research center, would you recommend investing first in improving the current EDR deployment or jumping directly to an XDR platform? Justify based on the complexity of its assets. **(4 points)**