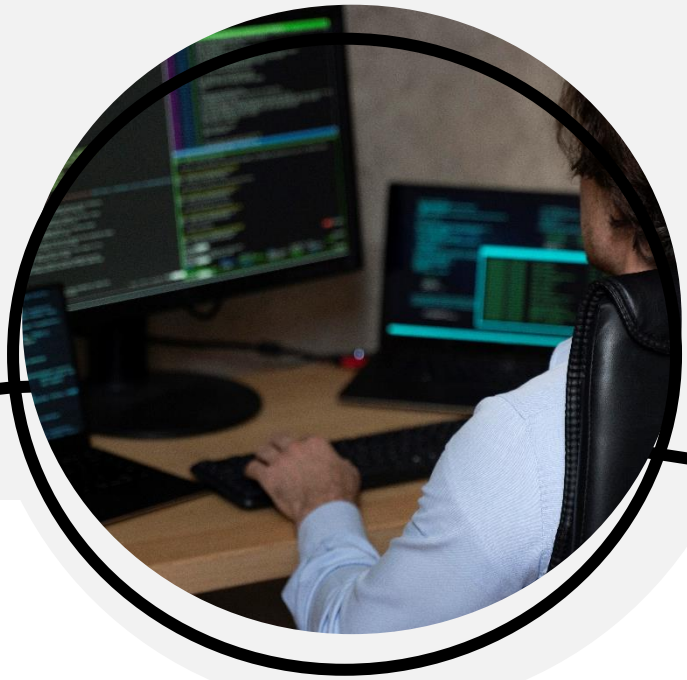
vuela | Junta de Andalucía

# Bastionado de sistemas operativos Microsoft y Linux



*Curso Blended* | *Nivel Avanzado* | *40h* | *15/03 al 29/04* | *De 25 a 45 plazas*

## ¿QUÉ VAS A APRENDER?

Este curso tiene como objetivo enseñar a los estudiantes la importancia del robustecimiento de los sistemas operativos. De esta forma se soluciona la mala práctica de instalar un sistema operativo y dejarlo en su configuración por defecto. Para ello el curso se divide en dos grandes bloques. El primero, presenta al alumno las configuraciones de seguridad del sistema operativo Windows que debe conocer e implementar. Para el segundo, los contenidos se centran en Linux, poniendo ejemplos de configuración para los sistemas operativos Ubuntu y CentOS.

## Parte eLearning → 20 horas

### OBJETIVOS:

Comprender los principios fundamentales de las aplicaciones web. Para ello es necesario tener un conocimiento profundo del funcionamiento del protocolo de transferencia de hipertexto (HTTP), además de cómo implementan la seguridad los navegadores modernos.

### CONTENIDOS:

**Módulo 1. Introducción al bastionado de sistemas operativos (2 horas)**

1. ¿Qué es el bastionado de sistemas operativos?
2. Cyber Kill Chain y las amenazas a las que se ve sometido un sistema operativo.
3. Vulnerabilidades y creación de malware.
4. Herramientas para detectar vulnerabilidades.
5. Malas prácticas de configuración conducentes al hackeo de sistemas.

**Actividad** → El alumno deberá desarrollar un resumen que explique las etiquetas HTML más importante.

## OBJETIVOS:

Conocer la importancia de la política Kerberos para la autenticación segura en un dominio.

Corregir la mala práctica de la configuración "la contraseña nunca caduca" en las credenciales usadas para las cuentas de servicio.

Corregir la mala práctica de usar la misma contraseña de administrador local en los equipos de los usuarios.

## CONTENIDOS:

**Módulo 2. Bastionado de sistemas operativos de Microsoft Windows. Parte I (5 horas)**

1. Robustece Windows por medio de la Directiva Kerberos, el grupo Protected Users, las Cuentas de Servicio Administrada de Grupo (gMSA) y los Password Setting Objects (PSO)
2. Asignación de Derechos de Usuario y configuración de seguridad en la directiva de grupo.
3. Buenas prácticas relacionadas con la auditoría de Windows.
4. Local Admin Password Solution (LAPS)
5. Credential Guard y Privileged Access Workstation (PAW)

**Actividad** → El alumno deberá desarrollar documento que explique cómo poder exigir a los administradores contraseñas de al menos 15 caracteres, mientras que al resto de usuarios solo se le exigen 8.

## OBJETIVOS:

Conocer la importancia de crear configuraciones de Firewall por medio de las GPOs.

Controlar las aplicaciones que puede ejecutar el usuario mediante el control de aplicación.

Automatizar la aplicación de la seguridad de los servidores por medio de las líneas base.

Conocer la STIC de Windows Server publicada por el Centro Criptológico Nacional y por extensión otras.

## CONTENIDOS:

**Módulo 3. Bastionado de sistemas operativos de Microsoft Windows. Parte II (4 horas)**

1. Windows Defender y Firewall con Seguridad Avanzada.
2. Configuración de Windows Defender por medio de GPO.
3. Uso de WSUS para la aplicación de parches de seguridad.
4. AppLocker y Windows Defender Application Control.
5. Líneas base de seguridad y Windows Server Security Compliance Toolkit
6. Limitar los permisos del administrador por medio de Just Enough Administration (JEA)
7. CCN-STIC 570A23 Guía de aplicación de perfilado de seguridad para Windows Server

**Actividad** → Crear un documento que resuma las configuraciones de seguridad recomendadas para Windows 10/11 según CCN.

## OBJETIVOS:

Conocer cómo proteger las cuentas de usuario en Linux.

Aprender a usar diferentes Firewalls en Linux.

Entender cómo se cifran las particiones de Linux.

Aprender a usar claves asimétricas para el acceso por SSH.

Saber para qué se usan los permisos SUID y SGID.

## CONTENIDOS:

**Módulo 4. Bastionado de sistemas operativos Linux. Parte I (4 horas)**

1. Proteger las cuentas de usuario.
2. Proteger al servidor por medio del firewall.
3. Encriptar las particiones con LUKS.
4. PKI en Linux.
5. Proteger el acceso por SSH.
6. Uso de los permisos SUID y SGID.

**Actividad:** →El alumno deberá desarrollar un documento que exponga un ejemplo de cuándo es importante usar SUID.

## OBJETIVOS:

Entender cómo se puede proteger un sistema Linux por medio de SELinux y perfiles de AppArmor.

Entender la importancia del aislamiento de procesos en Linux.

Conocer cómo se instala y usa un antivirus en Linux.

Conocer cómo debe configurarse el log desde el punto de vista de la seguridad.

Conocer la configuración de seguridad recomendada según el Centro Criptológico Nacional para los sistemas CentOS y, por extensión a otros.

## CONTENIDOS:

**Módulo 5. Bastionado de sistemas operativos de Linux. Parte II (5 horas)**

1. Robustecimiento de Linux por medio de SELinux y AppArmor.
2. Aislamiento de procesos y hardening del kernel.
3. Instalación de antivirus en Linux.
4. Configuración del log de seguridad.
5. Actualización en Linux.
6. IDS e IPS en Linux.
7. CCN-STIC 619B Implementación de seguridad sobre CentOS 8 (Cliente independiente)

**Actividad** → Crear un documento que resuma las configuraciones de seguridad recomendadas para CentOS 8 según CCN.

# Sesiones online en directo → 20 horas

## OBJETIVOS:

El principal objetivo de estas sesiones es que apliquen la parte elearning mediante ejercicios prácticos. Por ello, se usará la metodología flipped clasroom.

## CONTENIDOS:

**Sesión 1 Despliegue del laboratorio y primeras prácticas → 4 horas.**
(Relacionado contenidos del módulo 1)

- **Temática a tratar**: Despliegue del laboratorio para hacer las prácticas. Evaluación de herramientas para detectar vulnerabilidades.

**Sesión 2 Prácticas de seguridad con Windows. Parte I → 4 horas.**
(Relacionado con contenidos del módulo 2)

- **Temática a tratar:**
  - Configuración segura de la Directiva Kerberos. Uso del grupo Protected Users. Mejorar la seguridad de los servicios con gMSA. Conseguir diferentes niveles de complejidad de contraseña con PSOs.
  - Cerrar el servidor configurando derechos de usuarios.
  - Configurar la auditoría del servidor.
  - Uso de LAPS para evitar movimiento lateral.
  - Habilitar Credential Guard.

**Sesión 3 Prácticas de seguridad con Windows. Parte II → 4 horas.**
(Relacionado con contenidos del módulo 3)

- **Temática a tratar:**
  - Configuración del Firewall de Windows y reglas de IPSec.
  - Configurar el antivirus por medio de GPO.
  - Despliegue de WSUS.
  - Proteger la ejecución de aplicaciones con AppLocker.
  - Robustecer el servidor por medio de las líneas base de seguridad publicadas por Microsoft.
  - Estudiar la STIC de Windows Server.

**Sesión 4 Prácticas de seguridad con Linux. Parte I → 4 horas.**
(Relacionado con contenidos del módulo 4)

- **Temática a tratar:**
  - Asignar permisos con visudo. Cambiar el temporizador de sudo.
  - El comando adduser. Configurar la complejidad de la contraseña. Configurar la caducidad de la cuenta de usuario. Proteger al servidor frente a ataques de diccionario a la contraseña.
    Cómo usar iptables, Uncomplicated firewall, NFtables y firewalld.
  - GNU Privacy Guard. LUKS.
  - Creación de una Autoridad de Certificación en Linux.
  - Robustecer el acceso por SSH.
  - Buenas prácticas en el uso de SUID y SGID.

**Sesión 5 Prácticas de seguridad con Linux. Parte II → 4 horas.**
(Relacionado contenidos del módulo 5)

- **Temática a tratar:**
  - Políticas SELinux.
  - Perfile AppArmor.
  - Seguridad en Docker.
  - Protección del kernel.
  - Uso de un antivirus.
  - Configuración de logs.
  - Uso de Snort.
  - Estudiar la STIC de CentOS.

La impartición de esta acción formativa se realizará mediante la modalidad flipped classroom más online en directo de la siguiente forma:

- El **contenido interactivo** estará **disponible** en la **plataforma** online, de manera que será de **libre consulta** para el alumnado y este deberá haberse organizado de manera autónoma bajo las recomendaciones que se le marquen para haber consultado la lección o módulo correspondiente.
    - Con ello lo que se busca es un mayor protagonismo en el proceso de E-A y que el alumnado se involucre más en el mismo, mejorando su trabajo individual.
- Posteriormente, en la **sesión online**, se tratará el caso de uso de lo que ya el estudiante ha visto y leído, por lo que su participación y motivación será mucho más activa.
    - El objetivo de esto es fomentar un aprendizaje más profundo y significativo de manera que son ellos los que buscan construir sus conocimientos, a la par que esto permitirá mejorar el trabajo colectivo mediante los proyectos que compartan.

**Valor añadido → Permite atender a la diversidad del aula**

Los alumnos visionan los contenidos tantas veces como quieran y tienen las tutorías del profesor para resolver sus dudas de manera individualizada.

## ¿A QUIÉN ESTÁ DIRIGIDO?

- Profesionales del sector TIC en Andalucía.
- Perfiles TIC de empresas de Andalucía.

## REQUISITOS DE ACCESO:

- Podrán participar trabajadores con perfil TIC de empresas andaluzas. Por perfil TIC se entiende un titulado universitario en informática, ingenierías, matemáticas, estadística, física o FP superior en la Familia de Informática y Comunicaciones.
- Los criterios de valoración para aceptación de la persona participante en esta acción formativa serán:
  - Que sea un perfil TIC trabajando en sector TIC o en otro sector.
  - Estricto orden de llegada hasta completar plazas.

## CONOCIMIENTOS MÍNIMOS REQUERIDOS POR PARTE DEL ALUMNADO:

- Acceso a Internet
- Conocer algún lenguaje de programación.
- Conocimientos de ciberseguridad a nivel básico/medio.

## REQUISITOS PARA REALIZAR LA PARTE DE LAS CLASES EN DIRECTO DE MANERA ÓPTIMA

- El alumno deberá disponer de un equipo con VirtualBox instalado. con un mínimo de 16GB de RAM y 4 cores.
- Previo al inicio de la parte online en directo, que se descarguen las VMs.
- La configuración del laboratorio se hará el primer día del online en directo.

## EQUIPO DOCENTE

### Antonio Salazar Graván

Ingeniero Técnico Informático por la Universidad de Cádiz, MCT de Microsoft desde 2012.

Especialista en Ciberseguridad e infraestructuras con más de 20 años de experiencia en formación y consultoría

https://www.linkedin.com/in/antonio-salazar-gravan/

## CALENDARIO:

- **Fecha inicio del curso:**
  15/03/2024
- **Fecha impartición sesiones online en directo:**
- 11 al 15 de marzo de 9 a 13 horas.
- **Fecha fin del curso:**
  29/04/2024

## EVALUACIÓN:

**Obligatorio para obtener el certificado:**

- **[20%] La asistencia a las clases** o su visionado posterior. Estos vídeos se subirán a la plataforma y se establecerán los mecanismos para verificar que el alumnado que no asistió sí que visualizó el vídeo de manera asíncrona.
  - El mínimo de vídeos o asistencia a las clases para la titulación es de 4.
- **[30%] Visualización de contenido formativo.** Por medio de la lectura del SCORM.
  - Deberán ver al menos el 75% del contenido o lo que equivale a 4 módulos.
- **[30%] Realización de pruebas de conocimientos.** Que se colgarán mediante una batería de preguntas en la plataforma con orden aleatorio.
  - Deberán sacar un mínimo de un 5 al menos en 4 de los 5 módulos.

**No es obligatorio, pero sí muy recomendable:**

- **[20%] Actividades.** Serán de carácter no evaluable, pero servirá de preparación para las sesiones online en directo y además se ofrecerá retroalimentación.

## CERTIFICADO

Una vez superadas todas las evaluaciones de los módulos del curso y habiendo asistido al número mínimo de clases exigido, podrás obtener la certificación.

El certificado se emitirá digitalmente en formato pdf incluyendo la siguiente información:

- Datos del alumno.
- Datos del curso: título, fecha de impartición, duración, contenidos impartidos.
- Sello y firma digitalizada de la empresa impartidora del curso. El certificado no lleva firma digital ni sello/firma de la Junta de Andalucía

Ten en cuenta que estos cursos no tienen validez académica ni acreditación de créditos universitarios.

## OTRAS CUESTIONES DE INTERÉS DE ESTA ACCIÓN FORMATIVA:

Una posible orientación al tiempo dedicado al estudio, lectura y visualización del contenido sería la siguiente:

- Tiempo de consulta de contenidos y vídeos: 15 horas.
- Tiempo de realización de actividades: 1,5 horas.
- Tiempo de realización de exámenes: 2 horas.
- Tiempo de consulta en foros e interacción con los compañeros: 1,5 horas.
- Asistencia a las sesiones online en directo: 20 horas.

De todas formas y al tratarse de un curso abierto y parcialmente en línea, cada alumno podrá seguir su propio ritmo de aprendizaje siempre y cuando cumpla con los criterios mínimos de evaluación para la obtención del certificado de formación.