

**sedian**

Seguridad Digital  
de Andalucía



Ficha técnica  
**Bastionado de  
servidores Windows.**

Fecha: jueves, 31 de enero de 2019



© 2018 Junta de Andalucía. Consejería de Empleo, Empresa y Comercio. Este documento y, en su caso, cualquier documento anexo al mismo, contiene información de carácter confidencial exclusivamente dirigida a su destinatario o destinatarios. Queda prohibida su divulgación, copia o distribución a terceros sin la previa autorización escrita de "Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.". Si no es Ud. el destinatario del documento le ruego lo destruya sin hacer copia digital o física, comunicando a "Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A." vía e-mail o fax la recepción del presente documento. Toda declaración de voluntad contenida deberá ser tenida por no producida.

# ÍNDICE

1. Datos generales.....	2
2. Ponentes .....	3
3. Calendario y lugar de celebración.....	3
4. Objetivos.....	4
5. Contenido.....	4
6. Observaciones.....	5

# 1. Datos generales

**Título:**

Bastionado de servidores Windows.

**Modalidad:**

Webinar.

**Fecha:**

31 de enero

**Lugar de celebración:**

Plataforma Gotowebinar.

**Duración:**

1 hora.

**Horario:**

10:00 a 11:00.

**Dirigido a:**

TIC Junta de Andalucía.

## 2. Ponentes

### **Adrián Ramírez**

Adrián Ramírez es un profesional altamente especializado en ciberseguridad apostando claramente por el hacking ético y su implicación en la ingeniería social. Su especialidad abarca ámbitos como; arquitectura de servidores, ingeniería social, seguridad informática, análisis forense, robo de identidad. Hacking ético, virtualizaciones, recuperación de datos, destrucción de datos, anti forense, cyberinteligencia, vmware, kali, pentesting. OSINT y conocimientos de PNL.  
<https://www.linkedin.com/in/adriandolbuck/>

## 3. Calendario y lugar de celebración

Día 31 de enero de 2019 de 10:00h a 11:00h.

Webinar Online (GoToMeeting).

## 4. Objetivos

Mediante el webinar se determinarán las claves y procesos más críticos para proteger un Servidor en Windows con un último módulo explicando las técnicas más frecuentes de ataques para que el alumno conozca cómo se realizan y que rastro dejan en el servidor.

Objetivos:

- Identificar las mejores prácticas en seguridad para configurar sistemas Windows server.
- Conocer las técnicas de ataques más frecuentes.

## 5. Contenido

- 1.- La seguridad de la organización.
- 2.- Hardening, cuentas de usuario.
- 3.- Configuración de red.
- 4.- Opciones de registro.
- 5.- Políticas y directivas de seguridad.
- 6.- Protección de servicios.
- 7.- Gestión de logs.
- 8.- Protección y prevención frente a incidentes.
- 9.- Checklist de los puntos más críticos.
10. - Adecuación de los servidores al ENS
  - Despliegue de la herramienta Clara
  - Clara ENS, agente
  - Clara ENS, análisis independiente

11. –Recomendaciones de las guías Serie 800 de CCN-CERT aplicadas al bastionado y seguridad de Servidores en entorno Windows y demás recursos disponibles (cursos, material,etc) en CCN-CERT.

## 6. Observaciones

A la finalización de la sesión, los asistentes podrán elevar consultas y dudas al ponente mediante el chat del webinar.