sedian

Seguridad Digital
de Andalucía

Ficha técnica

Configuración Segura en Windows (edición 2)

Modalidad: presencial virtualizado

Fecha de celebración: 18 al 29 de mayo de 2020

Junta de Andalucía

Consejería de Economía, Conocimiento, Empresas y Universidad

ÍNDICE

1.Datos básicos de la acción formativa

Nombre de la acción formativa: Configuración Segura en Windows (edición 2)

Modalidad: presencial virtualizado

Público objetivo: Responsables de seguridad TIC de la Junta de Andalucía y profesionales TIC de la Junta de Andalucía

Fechas y lugar de celebración: 18 al 29 de mayo de 2020

Número de personas participantes: 30

2.Descripción

Los administradores de sistemas siguen prácticas generales a la hora de proteger los sistemas Windows. Si bien esta actividad es necesaria, hoy en día se torna insuficiente por dos razones:

- La administración de equipos Windows se realiza de la misma forma que en versiones previas y no se aprovechan las novedades de seguridad presentes en las últimas ediciones.
- El profesional de TI no tiene tiempo para investigar por su cuenta las buenas prácticas de seguridad de Windows, que se muchas y algunas complejas.

Por lo tanto, esta formación pretende ser muy concisa, concreta y avanzada, aportando los conocimientos que el profesional no tiene y cambiando prácticas

tradicionales que o bien ya no tienen sentido o han sido sustituidas por configuraciones modernas.

Descripción de los objetivos generales

- Repasar los aspectos de seguridad avanzados de Windows.
- Corregir prácticas antiguas que no tienen sentido hoy en día.
- Presentar nuevas tecnologías (como Windows Hello) que cambiarán de forma notable la manera de configurar la seguridad en los sistemas Windows.

3.Objetivos

- Aprender a gestionar la sincronización de hora en Windows.
- Conocer cómo funcionan y qué aportan los protocolos de VPN, DirectAccess y RDS.
- Conocer las posibilidades del Firewall de Windows.
- Aprender cómo defender a Windows frente al Malware.
- Determinar los servicios esenciales que debe correr un sistema Windows y cerrar el resto (Bastionado por líneas base de seguridad)
- Gestión correcta de las cuentas de usuarios locales y su interacción con las de dominio.
- Determinar si están desplegados convenientemente las configuraciones recomendadas de seguridad de Active Directory para proteger el dominio.
- Entender qué ocurre en un sistema Windows atendiendo a los eventos y la auditoría.
- Uso de bitlocker para proteger los dispositivos.
- Configuraciones avanzadas de la red WiFi en los dispositivos Windows.

4.Modelo metodológico

Número de participantes: 25

Metodología de evaluación

Se establece una metodología de evaluación basada en las evidencias de aprendizaje obtenidas mediante la **sesión presencial online** que se reflejarán a través de las actividades que los participantes desarrollarán fuera del tiempo de clase. Dichas evidencias de carácter principalmente aplicativo y práctico se obtendrán a través del trabajo de los participantes en el campus virtual gracias a los siguientes recursos:

- Actividades de aprendizaje de tipo aplicativo: Se trata de actividades que buscan que el participante ponga en práctica los conocimientos adquiridos en situaciones y escenarios cercanos a la realidad del curso sobre Configuración segura en Windows. Dichas actividades se solicitarán a los participantes al final de las tres sesiones online y deberán enviarlas a través de los buzones habilitados durante el tiempo dedicado a trabajo práctico.

- Pruebas de autocomprobación que los participantes realizarán en relación a los contenidos del curso. Dichas pruebas permiten conocer tanto al usuario acerca de su propio progreso, así como al docente para poder evaluar el nivel de adquisición de aprendizaje de los mismos. Son pruebas que irán incluyéndose durante la sesión presencial online, como medio para favorecer una formación activa, dinámica y colaborativa.

Control de los participantes

Gracias a las herramientas que se desplegarán para el desarrollo de la formación se podrá conocer tanto la asistencia, como la participación activa de cada uno de los participantes en la misma. Para ello, se recurren a las siguientes herramientas:

- **Informes** de acceso e interacción de los participantes con las herramientas del curso: Mediante dicho informe es posible conocer el nivel y recurrencia de acceso y participación de cada usuario con referencia al curso en sí, así como a las herramientas, actividades y dinámicas que se faciliten en el curso. Ejemplos de estas herramientas serán el foro del curso, las pruebas de autocomprobación o la asistencia y presencia en la sesión online organizada.

- **Control** de acceso y participación de los usuarios en la Jornada presencial online que se organizará como la principal sesión en la que el formador proporcionará los conocimientos teórico-prácticos del curso. Esta formación propone una sesión de 6 horas de duración

Dinámicas de impartición

La metodología de impartición de esta formación está basada en un modelo de enseñanza que combina dos metodologías diferentes, pero que se coordinan entre sí. Por un lado, la formación se organiza en modalidad **blended learning**, es decir, enseñanza semipresencial que combina el trabajo offline que el participante realiza en plataforma fuera de las sesiones (pruebas, actividades, participación en foro, etc) y la presencia y actividad del participante en cada una de las sesiones presenciales online.

Por otro lado, aplicamos una metodología activa basada en el "**Aula invertida o Flipped Classroom**. Esta metodología trata de obtener el máximo provecho de las sesiones online en directo, dedicando el máximo tiempo a la aplicación y puesta en práctica de los contenidos teóricos. Dichos contenidos estarán presentes en el campus virtual en todo momento y accesibles para que los participantes puedan consultarlos en cualquier momento fuera de las sesiones online. Durante las sesiones online se dedicará un tiempo inicial a presentar y exponer dudas por parte de los participantes que el docente resolverá y pondrá en común con el grupo.

A lo largo de las sesiones presenciales online el docente facilitará los contenidos de aprendizaje integrando diversas dinámicas de tipo colaborativo y participativo. En este sentido, es pertinente el uso de dinámicas basadas en casos y escenarios fácilmente aplicables a la realidad de los participantes en referencia a los contenidos teóricos del curso. El objetivo de dichas dinámicas no son solamente ofrecer la teoría de los contenidos formativos, sino que los participantes logren ubicarlos en su entorno laboral a través de situaciones o escenarios posibles.

Distribución de las jornadas

El curso Configuración Segura en Windows se desarrollará en modalidad presencial-online con una duración global de 10 horas, distribuidas en tres días no consecutivos. Cada jornada presencial online tendrá una duración de 2 horas y se programarán dejando margen de un día entre una sesión y la próxima con el objetivo de que los participantes dispongan de tiempo para desarrollar el trabajo práctico solicitado por el formador en la sesión anterior.

Debido al carácter de esta formación, se organizará siguiendo la siguiente estructura:

Sesión 18 de mayo: Sesión presencial online con una duración de 2 horas, distribuyéndose de la siguiente manera:

- Primeros 30 minutos: Presentación del formador y presentación del curso: objetivos, contenidos, descripción de la plataforma y modalidad de formación. El docente explicará cómo se distribuirán las sesiones online y las actividades de carácter práctico que se desarrollarán fuera de clase.

- Siguientes 1,5 horas: Exposición por parte del formador de los contenidos teóricos. Dicha exposición servirá para, posteriormente, que los participantes puedan aplicarlos en las dinámicas participativas. Antes de finalizar la sesión, el formador describirá las actividades de aprendizaje prácticas que los participantes deberán desarrollar tras la sesión online. A lo largo de este tiempo se propondrá una o dos actividades prácticas a los asistentes para aplicar los conocimientos adquiridos durante la exposición

del formador. Se tratará de actividades de trabajo autónomo y/o colaborativo donde los participantes deberán diseñar o ejecutar dinámicas propuestas por el formador que, a su vez, representará la vía para evaluar a los asistentes. En el caso de aplicar actividades de tipo colaborativo se dividirá a los asistentes en grupos de máximo 3 personas y trabajarán en un espacio reservado para cada grupo. El formador, a través del foro, deberá asumir el papel de orientador, asistente y guía para que las actividades se ejecuten de forma óptima.

Cabe destacar que, como se ha mencionado anteriormente, entre las tres sesiones online presenciales se dejará un día de margen para que los participantes realicen las actividades prácticas propuestas por el formador.

Sesión 20 de mayo: Sesión presencial online con una duración de 2 horas, distribuyéndose de la siguiente manera:

- Primeros 30 minutos: Presentación y resumen de las actividades de aprendizaje que los asistentes desarrollaron a lo largo del día anterior. Durante esta media hora se expondrán los resultados derivados de dichas actividades y, además, se reservará un periodo de 10 minutos para la resolución de dudas o preguntas relacionadas con los contenidos.

- Siguientes 1,5 horas: El formador continuará exponiendo los contenidos teóricos que continúan a la sesión anterior. Dicha exposición servirá también para, posteriormente, que los participantes puedan aplicarlos en las actividades de aprendizaje que se propondrá para su realización fuera del tiempo de clase.

Sesión 22 de mayo: Sesión presencial online con una duración de 2 horas, distribuyéndose de la siguiente manera:

- Primeros 30 minutos: Presentación y resumen de las actividades de aprendizaje que los asistentes desarrollaron a lo largo del día anterior. Durante esta media hora se expondrán los resultados derivados de dichas

actividades y, además, se reservará un periodo de 10 minutos para la resolución de dudas o preguntas relacionadas con los contenidos.

- Siguientes 1,5 horas: El formador continuará exponiendo los contenidos teóricos que continúan a la sesión anterior. Dicha exposición servirá también para, posteriormente, que los participantes puedan aplicarlos en las actividades de aprendizaje que se propondrá para su realización fuera del tiempo de clase.

5.Contenidos

- Sincronización de Hora:
  - Cómo funciona el Servicio de Hora de Windows.
  - La misión del maestro de operaciones de emulación del PDC respecto a la sincronización de hora de los equipos miembros de un dominio de Active Directory.
  - Sincronización de hora con las herramientas del servicio de hora de Windows (cliente NTP).
- Acceso remoto con Direct Access.
  - Opciones de despliegue del servidor Direct Access.
  - Protocolos de túnel del servidor Direct Access.
  - Configuración del servidor de Direct Access por GPO.
- Acceso remoto VPN tradicional.
  - Escenarios de uso de servidores VPN.
  - Protocolos de túnel.
  - Tipos de autenticación para VPN.
  - Reconexión automática VPN (IKEv2)
  - Creación de perfiles de conexión de cliente con CMAK.
- Acceso remoto por medio de Servicios de Escritorio Remoto (RDS)
  - Ventajas e inconvenientes.
  - Configuración del acceso local y por GPO.
  - Configuración del acceso RDS usando una puerta de enlace (protección SSL)
  - Monitorización de los accesos remoto.
- Windows Defender Firewall con seguridad avanzada.
  - Perfiles de reglas.
  - Creación de reglas locales.
  - Creación de reglas por GPO.
  - Reglas de seguridad de la conexión IPSec con Firewall de Windows.
- Protección frente a malware.
  - Vectors de ataques prominentes (Spear phishing, USB como plataforma de ataque)
  - Recuperación frente a ransomware (Historial de archivos de Windows)
  - Soluciones centralizadas de antivirus.
  - Función del sandbox en un antivirus.
  - Defensa frente a malware de día cero.
  - Detección de vulnerabilidades presentes en Windows.

    - El reto de Windows como servicio (WaaS) el nuevo modelo de parcheo y actualización de Windows.
    - Configurar la actualización de Windows localmente.
    - Configurar la actualización de Windows por medio de WSUS/WaaS (Nuevas GPOs disponibles)
- Bastionado de sistemas Windows por medio de líneas base.
    - ¿Qué es Security Compliance Toolkit?
    - Minimizar la superficie de ataque con líneas base de seguridad.
    - El principio del menor privilegio.
    - Descargas de líneas base de configuración de seguridad recomendadas por Microsoft.
    - Análisis de las líneas base.
    - Creación de una GPO a partir de líneas base.
    - Aplicación masiva de las líneas base seguridad por medio de GPO.
- Protección de las cuentas locales.
    - Cuentas por defecto de usuario: La cuenta “Guest”, la cuenta “HelpAssistant”
    - Cuentas por defecto del sistema.
    - Cómo administrar las cuentas locales.
    - Restricción y protección de cuentas locales con derechos de administrador.
    - Pertenencia a grupos locales de identidades del dominio: Buenas prácticas.
    - La GPO de grupos restringidos.
    - Eliminar o cambiar contraseñas de cuentas locales que crean los servicios al instalarse.
    - Evitar ataques de movimiento lateral con cuentas locales.
    - Los grupos locales y los permisos para poder instalar programas en Windows.
    - Evitar que los usuarios cambien la configuración IP del dispositivo.
- Configuraciones de Active Directory para mejorar la seguridad.
    - ¿Qué es el TGT (Ticket Granting Ticket)
    - La política de Kerberos: Cómo evitar ataques del tipo “Replay”
    - La política de contraseña del directorio.
    - Conseguir diferentes esquemas de complejidad de contraseña por medio de objetos de ajuste de password (PSO objects)
    - La problemática del uso de una cuenta de usuario de AD para instalar servicios.
    - Minimizar la probabilidad del exito de ataques de fuerza bruta a servicios por medio de Cuentas de Servicio Administradas de Grupo (GSMA)
    - Activación de la Papelera de Reciclaje de Active Directory.

    - Configurar mensaje de bienvenida (Disclaimer y política de acceso) al iniciar sesión en Active Directory.
    - Windows Hello para la Empresa: El nuevo paradigma de la autenticación Kerberos que evita ataques del tipo Rainbow Table.
    - Establecer MFA en Active Directory.
    - Cómo un CAPTCHA puede evitar ataques de denegación de servicio en la autenticación de usuarios.
- El visor de eventos de Windows.
    - Filtrado de eventos.
    - Acceso a logs operacionales (Avanzados) de Windows.
    - Recopilar los eventos remotos en el ordenador del técnico mediante la suscripción a eventos.
- Mantenimiento preventivo de sistemas Windows.
    - El log de Sistema y de Aplicación.
    - El Monitor de rendimiento.
    - Confirmar el correcto funcionamiento del sistema operativo por medio de Conjuntos Recopiladores de Datos.
    - Observar el degradado de un sistema Windows en el tiempo por medio del Monitor de Fiabilidad de Windows.
- La auditoría de Windows.
    - Elementos del sistema que se pueden auditar (inicios de sesión, cambio de credenciales, ...)
    - Habilitar la auditoría de acceso a objetos (archivos)
    - Configurar el registro circular del log de seguridad (auditoría)
    - Activar la auditoría en el sistema de archivos de Windows.
    - Consultar la auditoría.
    - Herramientas de terceros que mejorar la comprensión y la consulta del log de auditoría.
- Cifrado del almacenamiento secundario.
    - ¿Qué es Bitlocker?
    - La misión del módulo TPM (Trusted Platform Module) respecto a las claves de Bitlocker.
    - Emulación del TPM.
    - Exigir PIN o lectura biométrica para desbloqueo de TPM.
    - Configuraciones de bitlocker/TPM por directiva local/grupo.
    - Cifrar unidades de sistema y de datos.
    - Almacenar las claves de Bitlocker en Active Directory.
    - Recuperación de unidad Bitlocker.
- Implementación del acceso inalámbrico en Windows.
    - Despliegue y configuración de APs: Buenas prácticas.
    - Creación de grupos de seguridad de usuarios WiFi.
    - Políticas de configuración 802.11 en Windows.
    - Control centralizado de la autenticación de AP por medio de NPS.

- Consideraciones al unir al dominio un equipo desde la red WiFi.
- Asignación de perfil de firewall para conexiones WiFi.
- Configuración de redes de uso medido mediante directiva local.

6.Docente

Antonio Salazar Graván

Experto en Seguridad TIC y MCT de Microsoft.

Diplomado en Informática, especialidad de Sistemas Físicos. 1990-1994. Universidad de Cádiz
Certificado de Aptitud Pedagógica (CAP) Universidad de Cádiz (1997)
Microsoft Certified Trainer (MCT) (Microsoft 2013-Actualidad)
Train the Trainer (Microsoft Ibérica 2013)
Microsoft® Certified IT Professional (MCITP) Server Administrator on Windows Server® 2008 (Microsoft 2012)
Microsoft® Certified Solutions Associate (MCSA) Windows Server® 2008 (Microsoft 2012)
Microsoft® Certified Technology Specialist (MCTS) Windows Server® 2008 Network Infrastructure, Configuration. Windows Server® 2008 Active Directory, Configuration. (Microsoft 2012)
Microsoft® Certified Specialist (MCS) Administering Office 365 for Small Business Specialist (Microsoft 2013)
Ethical Hacking Foundation (EXIN 2016)
Secure Programming Foundation (EXIN (2017)
Microsoft® Certified Solutions Associate (MCSA) Windows Server® 2016 (Microsoft 2019)
Docker Certified Associate (Docker 2019)

LinkedIn: https://www.linkedin.com/in/antonio-salazar-grav%C3%A1n-8066214b/