sedian

Seguridad Digital
de Andalucía

Configuración Segura en Windows

- 3ª sesión -

Junta de Andalucía

Unidades didácticas

Sincronización de Hora
Acceso remoto con Direct Access.
Acceso remoto VPN tradicional.
Acceso remoto por medio de Servicios de Escritorio Remoto (RDS)
Windows Defender Firewall con seguridad avanzada.
Protección frente a malware.
Bastionado de sistemas Windows por medio de líneas base.
Protección de las cuentas locales.
El visor de eventos de Windows.
La auditoría de Windows.
Cifrado del almacenamiento secundario.
Implementación del acceso inalámbrico en Windows.

Bastionado de sistemas por medio de líneas bases

Todas las organizaciones se enfrentan amenazas de seguridad que son distintas para cada empresa.

Por ejemplo, puede que una compañía de comercio electrónico se centre en proteger sus aplicaciones web conectadas a Internet, mientras que puede que un hospital esté más interesado en proteger información confidencial del paciente.

Lo único que todas las organizaciones tienen en común es la necesidad de mantener sus aplicaciones y dispositivos seguros.

Estos dispositivos deben cumplir con los estándares de seguridad (o líneas base de seguridad) definidos por la organización.

Bastionado de sistemas por medio de líneas bases

Una línea base de seguridad es un grupo de opciones de configuración recomendadas por Microsoft.

Estas opciones de configuración se basan en comentarios de los equipos de ingeniería de seguridad de Microsoft, los grupos de productos, los partners y los clientes.

Hay más de 3000 opciones de configuración de directiva de grupo para Windows 10, sin incluir las más de 1800 opciones de configuración de Internet Explorer 11.

De estas 4800 opciones de configuración, solo algunas de ellas están relacionadas con la seguridad.

Tendrías que determinar por ti mismo el impacto en la seguridad de cada opción de configuración. A continuación, tendrás que determinar el valor adecuado de cada configuración.

Bastionado de sistemas por medio de líneas bases

¿Cómo puedes usar las líneas base de seguridad?

Asegúrate de que los valores de configuración de usuarios y dispositivos son conformes a la línea base.

Establecer opciones de configuración.

Puedes usar la Directiva de grupo, Microsoft Endpoint Configuration Manager o Microsoft Intune para configurar un dispositivo con los valores de configuración especificados en la línea base..

Bastionado de sistemas por medio de líneas bases

¿Dónde puedo obtener las líneas base de seguridad?

Puedes descargar las líneas base en https://www.microsoft.com/en-us/download/details.aspx?id=55319.

Las líneas base de seguridad se administran en **Security Compliance Manager**

En este video puedes ver como se aplican líneas base usando SCT:

https://www.youtube.com/watch?v=H8O67D3Heas

Cómo exportar e importar a GPO en GPMC una línea base: https://www.petri.com/create-gpos-using-security-compliance-manager-tool

Protección de las cuentas locales

Las cuentas de usuario predeterminadas son cuentas que aparecen por defecto al instalar Windows.

No se pueden quitar ni eliminar

Se usan para administrar el acceso a los recursos de la máquina local.

La cuenta de **administrador** local tiene el SID S-1-5-id del dominio-500, no se puede bloquear ni eliminar.

En Windows 10/2016 el programa de instalación deshabilita la cuenta de administrador integrada y crea otra cuenta local en es miembro del grupo administradores.

Protección de las cuentas locales

La cuenta de **invitado (guest)** está deshabilitada de forma predeterminada y tiene una contraseña en blanco.

La cuenta **help-assistant (asistente de ayuda)** se instala con una sesión de Asistencia Remota (no confundir con Escritorio Remoto)

Esta cuenta se deshabilita de forma automática cuando no hay solicitudes de Asistencia Remota.

El sistema operativo y los servicios usan la cuenta **System.** Hay muchos servicios que necesitan estar logados para que puedan funcionar.

La cuenta **System** no aparece en el administrador de usuarios y no se puede agregar a ningún grupo de seguridad.

Protección de las cuentas locales

No debemos usar la cuenta de sistema al instalar servicios.

La cuenta **NetworkService (Servicio de red)** es una cuenta predefinida que se utiliza para presentar las credenciales del equipo en los servidores remotos.

La cuenta **LocalService (Servicio Local)** es una cuenta predefinida que usa el administrador de control de servicios. Tiene pocos privilegios (mínimos) y presenta credenciales anónimas en la red.

Para proteger las cuentas locales debemos usar el principio de menor privilegio (esto también es aplicable a cuentas de dominio) y utilizar el **Control de Cuentas de Usuario (UAC)** (ejecutar como administrador) para elevar los privilegios.

Para aprender a configurar UAC: https://docs.microsoft.com/es-es/Windows/security/identity-protection/user-account-control/user-account-control-overview

Protección de las cuentas locales

Respecto a las buenas prácticas de membresía a grupo locales para cuentas de dominio.

Administradores y **Usuarios** son dos grupo locales (hay más)

Una cuenta local que es miembro de uno de estos grupo determina las acciones que se pueden realizar con ella y activa UAC convenientemente.

Administradores del Dominio y **Usuarios del Dominio** son dos grupos del dominio (hay más)

El administrador del dominio (DOMAIN\administrador) pertenece al grupo Administradores del dominio.

Protección de las cuentas locales

Cuando unimos al dominio un equipo de Windows 10, ocurren muchas cosas, pero relacionadas con los grupos tenemos:

El grupo **Administradores del Dominio** es miembro del grupo **Administradores** local del equipo.

El grupo **Usuarios del Dominio** es miembro del grupo **Usuarios** local.

Por esta regla de tres, DOMAIN\Administrador es administrador local del equipo cuando inicia sesión.

¿Cómo podemos conseguir que un usuario del dominio que no pertenezca al grupo de administradores de dominio sea administrador local de la máquina en la que inicia sesión?

Protección de las cuentas locales

La respuesta está en el uso de la GPO de Grupos Restringidos de Active Directory.

Otro aspecto a verificar es comprobar si la instalación de algún servicio o aplicación en la máquina crea cuentas de usuarios con passwords conocidos. Una búsqueda en Google puede ayudar.

En seguridad informática, el **Movimiento lateral** es la técnica que usan los hackers para ir ganando presencia en la organización víctima.

El éxito de esta técnica depende en gran medida de que se utilice la misma combinación de usuario/password en las cuentas de administrador local. Si un equipo se ha visto comprometido y capturado la contraseña, se tiene acceso al resto de máquinas que la comparten. ¿Qué contramedidas aplicarías?

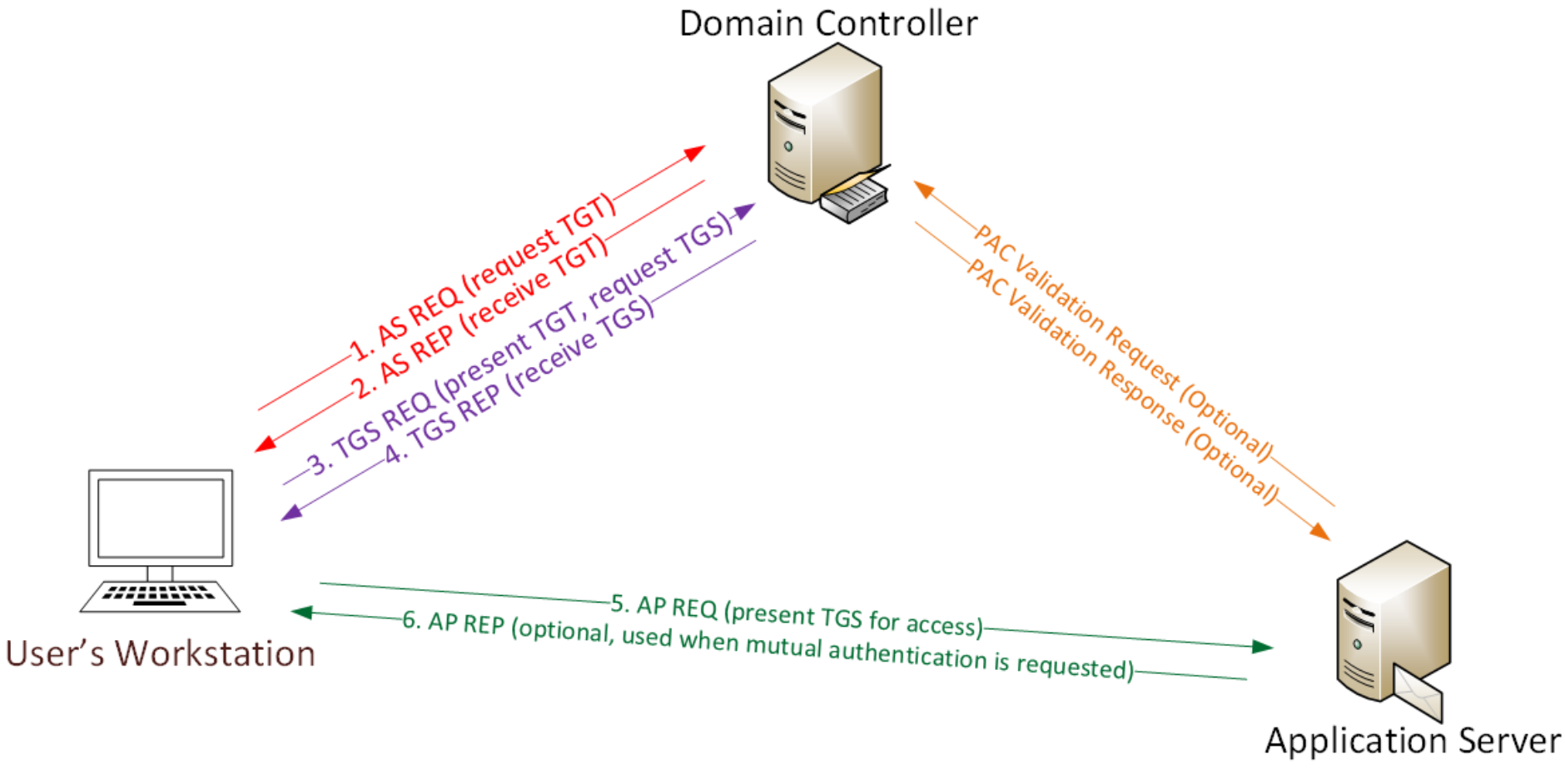
Protección de las cuentas locales

Para aprender más:

https://docs.microsoft.com/es-es/Windows/security/identity-protection/access-control/security-identifiers
https://docs.microsoft.com/es-es/Windows/security/identity-protection/access-control/security-principals
https://docs.microsoft.com/es-es/Windows/security/identity-protection/access-control/active-directory-accounts
https://docs.microsoft.com/es-es/Windows/security/identity-protection/access-control/service-accounts
https://docs.microsoft.com/es-es/Windows/security/identity-protection/access-control/active-directory-security-groups

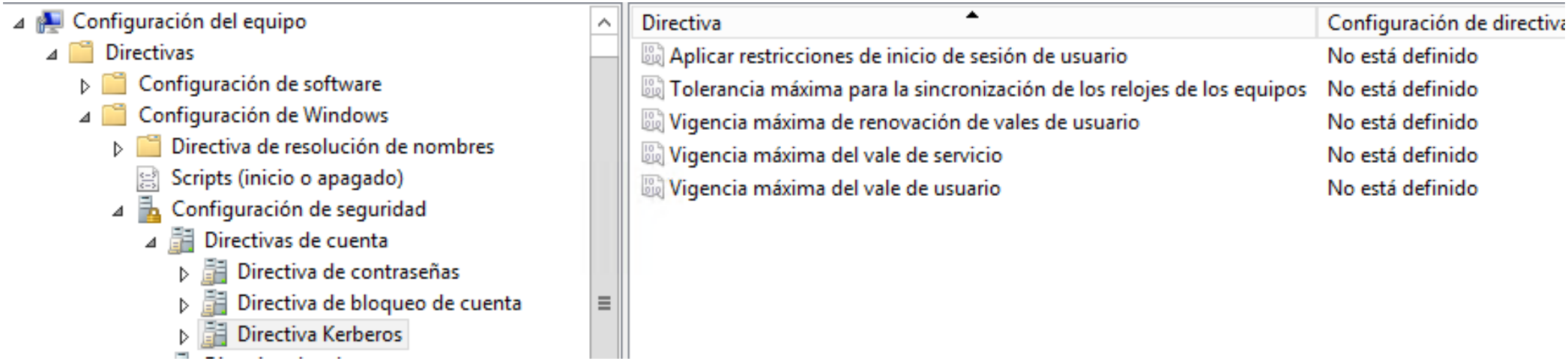
Configuraciones de Active Directory para mejorar la seguridad

El corazón de Kerberos: **TGT (Ticket Granting Ticket) y el ticket de sesión.**



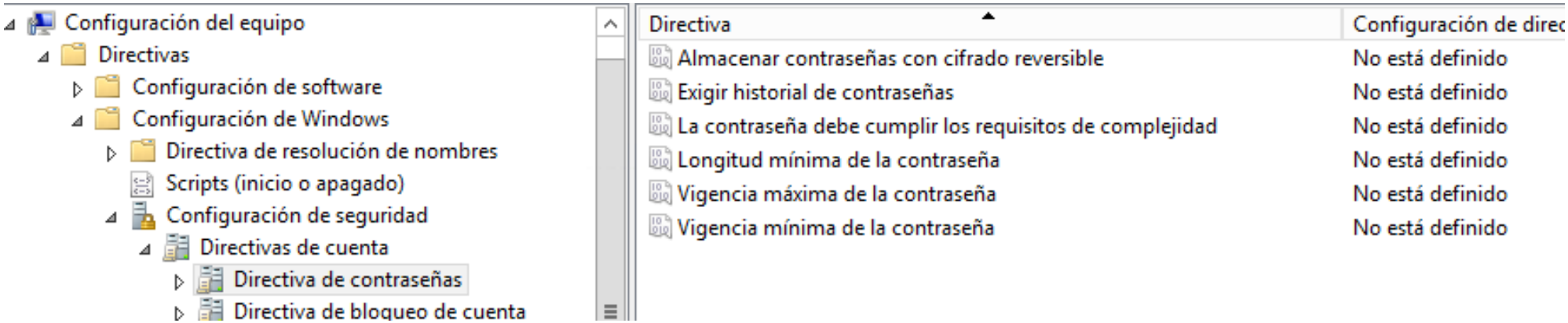
Configuraciones de Active Directory para mejorar la seguridad

Cómo gestionar TGT y TGS con la política Kerberos de AD.



Configuraciones de Active Directory para mejorar la seguridad

Consideraciones de la política de contraseñas del directorio.



Configuraciones de Active Directory para mejorar la seguridad

¿Y si queremos que diferentes grupos de usuarios tengan distintas longitudes en las contraseñas?

No se pueden crear distintas GPOs.

Para esto hay que utilizar **PSOs (Password Setting Objects)** y asignarlos a grupos de seguridad, no unidades organizativas.

Cómo crearlas: https://techclub.tajamar.es/crear-y-aplicar-una-pso-a-un-grupo-de-usuariogui/

¿y que decimos sobre la caducidad de contraseña para las cuentas de AD que usamos para los servicios? ¿Que nunca caducan?

Configuraciones de Active Directory para mejorar la seguridad

Active Directory permite que las máquinas donde corren los servicios puedan actualizar el password de ciertas cuentas de AD, es lo que se conoce como **Cuentas de Servicio Administradas de Grupo (GSMA)**

Esta tecnología elimina la amenaza de ataques de fuerza bruta al password.

Deben crearse con Powershell.

Procedimiento: http://www.rebeladmin.com/2018/02/step-step-guide-work-group-managed-service-accounts-gmsa-powershell-guide/

Y si lo ponemos todo junto (GSMA + PSO)

Procedimiento: https://www.avante.es/como-securizar-despliegues-de-active-directory/

Configuraciones de Active Directory para mejorar la seguridad

El procedimiento para recuperar un objeto (p.e. usuario) eliminado de Active Directory es complejo y pasa por realizar una **restauración autoritativa** del objeto.

La solución es la **Papelera de Reciclaje de Active Directory**. Puede defendernos de errores del administrador o de malware específico de AD.

Existen aspectos muy sencillos de configurar que deben estar presentes en toda organización para advertir del intento no autorizado de los recursos. La GPO ofrece configuraciones para estos disclaimers.

https://www.prajwaldesai.com/how-to-configure-legal-notices-on-domain-computers-using-group-policy/

Windows Hello y Windows Hello para la Empresa

Nueva tecnología para robustecer los inicios de sesión de Kerberos.

No es lo mismo el producto **Windows Hello** que **Windows Hello para la Empresa.**

Introduce en el modelo de autenticación módulos TPM, claves de 48 caracteres y factores adicionales de autenticación basado el lecturas biométricas (requiere hardware especial)

https://docs.microsoft.com/es-es/Windows/security/identity-protection/hello-for-business/hello-how-it-works

El Visor de eventos de Windows

Es el gran conocido/desconocido.

Entre las posibilidades menos usadas tenemos:

- **Suscripción** a eventos.
- **Logs operacionales** (por ejemplo el cliente de GPO)

Mantenimiento preventivo de Windows

Los logs de **Sistema** y de **Aplicación** son bastantes conocidos y usados.

Además tenemos el **Monitor de rendimiento** con el que podemos realizar testeos del sistema operativo con los **conjuntos recopiladores de datos**.

El **Historial de confiabilidad** muestra la “degradación” del equipo a lo largo del tiempo.

La auditoría de Windows

La auditoría es una de las herramientas más poderosas que podemos utilizar para determinar qué ha pasado en un sistema.

Sirve para identificar ataques o intentos del mismo sobre el dispositivo y para demostrar las posibles actuaciones de un insider.

La auditoría de Windows se divide en dos grandes bloques:

- La auditoría tradicional o básica.
- La auditoría avanzada.

Las políticas de auditoría pueden establecerse por medio de la directiva local de la máquina o la de grupo.

La auditoría de Windows

La auditoría de seguridad básica.

Una política de auditoría básica especifica las categorías de eventos de seguridad que se auditan. Estas son:

- Eventos de logon de cuenta.
- Administración de cuentas.
- Acceso al servicio de directorio.
- Eventos de logon.
- Acceso a objetos
- Cambio en las políticas de auditoría.
- Uso de privilegios.
- Seguimiento de procesos
- Eventos de sistema.

La auditoría de Windows

La auditoría de seguridad Avanzada.

Los ajustes se encuentran en **Security Settings\Advanced Audit Policy Configuration\System Audit Policies**.

Parece que realiza funciones similares a la auditoria básica, pero difiere de ella en que los ajustes son más detallados y específicos.

Cómo se aplican los ajustes de auditoria de seguridad avanzada: https://docs.microsoft.com/es-es/Windows/security/threat-protection/auditing/planning-and-deploying-advanced-security-audit-policies

FAQ sobre auditoría: https://docs.microsoft.com/es-es/Windows/security/threat-protection/auditing/advanced-security-auditing-faq

La auditoría de Windows

La auditoría de seguridad básica.

Cómo activar la auditoría: https://docs.microsoft.com/es-es/Windows/security/threat-protection/auditing/create-a-basic-audit-policy-settings-for-an-event-category

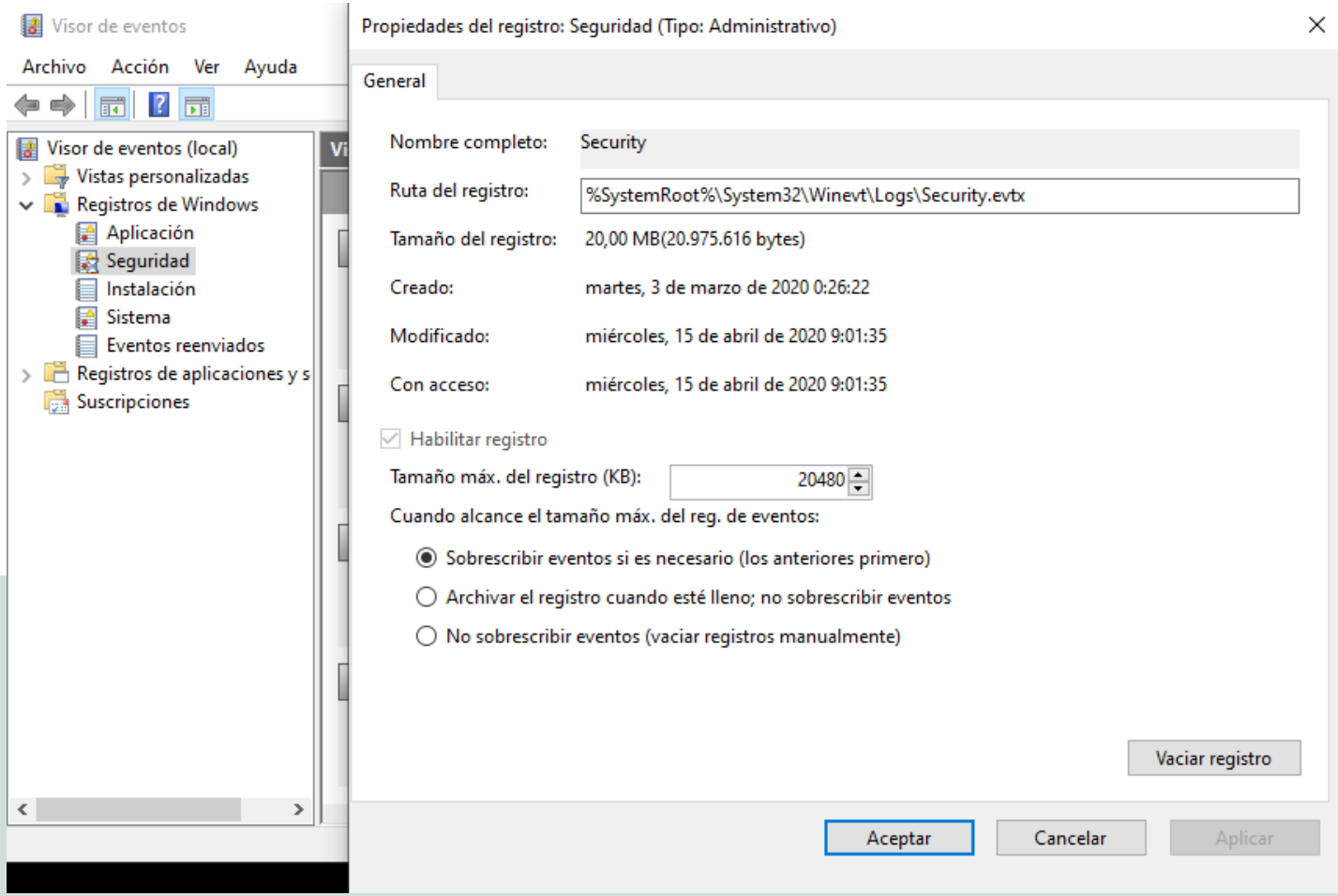
Aplicar auditoría el los archivos: https://docs.microsoft.com/es-es/Windows/security/threat-protection/auditing/apply-a-basic-audit-policy-on-a-file-or-folder

El resultado de los eventos que se auditan pueden verse en el log de **Seguridad**.

La auditoría de Windows

La auditoría de seguridad básica.

Es importante controlar el espacio que tenemos disponible para el almacenamiento de la auditoría.



La auditoría de Windows

La auditoría de seguridad básica.

Leer el log de seguridad es una labor tediosa y compleja.

Recomendamos utilizar algún software que lea la auditoria de Windows y presente los resultados de forma simple, permita activar alertas y generar informes.

En el mercado hay infinidad de aplicaciones que hacen esto, de software libre y de pago

Por ejemplo: https://www.quest.com/mx-es/products/change-auditor-for-windows-file-servers/

Cifrado de almacenamiento secundario

¿Qué es Bitlocker?

Proporciona protección adicional al sistema operativo y a los datos que se almacenan,

Asegura que los datos almacenados permanecen encriptados, evitando el acceso a los mismos al montar los discos duros en otros equipos.

Encripta todos los datos almacenados en el volumen de sistema y en los volúmenes de datos que se configuren.

También encripta los archivos de paginación y de paginación.

Por defecto usa TPM, para asegurar que no se han comprometido de los componentes de inicio temprano (BIOS, sector de arranque, administrador de arranque)

Cifrado de almacenamiento secundario

¿Qué es Bitlocker?

Una vez que el TPM ha verificado que no ha habido cambios, entrega la clave de desencriptación al cargador del sistema operativo Windows.

Si TPM ha detectado cambios entonces bloquea los volúmenes protegidos

Si el equipo no dispone de módulo TPM entonces Bitlocker no funciona, a menos que se emule (por GPO): https://www.howtogeek.com/howto/6229/how-to-use-bitlocker-on-drives-without-tpm/

Ajustes de Bitlocker por directiva: https://docs.microsoft.com/es-es/Windows/security/information-protection/bitlocker/bitlocker-group-policy-settings

Implementación del acceso inalámbrico en Windows

En el mercado existen soluciones propietarias para el despliegue de APs.

Cuando se despliegan múltiples Aps en una ubicación, debemos configurarlos para que utilicen un único canal (frecuencia) para reducir las interferencias.

El procedimiento concreto de cómo realizarlo dependerá del fabricante/producto, pero todos deben seguir las siguientes buenas prácticas:

https://docs.microsoft.com/es-es/windows-server/networking/core-network-guide/cncg/wireless/e-wireless-access-deployment#deploy-and-configure-wireless-aps

Implementación del acceso inalámbrico en Windows

Para conseguir que un equipo se conecte a los APs que deseemos (proporcionando una lista de preferencias) independientemente de la cobertura, debemos usar **Grupos de Seguridad para usuarios Wireless** y **Configurar las políticas de red inalámbrica.**

Cómo hacerlo: https://docs.microsoft.com/es-es/windows-server/networking/core-network-guide/cncg/wireless/e-wireless-access-deployment#bkmk_groups

Adicionalmente podemos delegar la autenticación del punto de acceso a un servidor RADIUS, convirtiendo los puntos de acceso en clientes de RADIUS.

El servidor RADIUS puede implementarse con el rol **Network Policy Server (NPS)** de Windows Server y usar Active Directory como origen de identidades. https://docs.microsoft.com/es-es/windows-server/networking/core-network-guide/cncg/wireless/e-wireless-access-deployment#configure-your-npss

Implementación del acceso inalámbrico en Windows

Para dispositivos móviles o portátiles con Windows 10, es importante conocer cómo se configura las redes de **uso medido**: https://www.redeszone.net/2019/06/13/ver-controlar-limitar-uso-datos-windows-10/

En ocasiones al conectar a una red WiFi, Windows 10 asigna un perfil de firewall que no es correcto. En Windows 7 podíamos cambiarlo con un clic, ahora hay que hacerlo con PowerShell.

https://www.solvetic.com/tutoriales/article/4406-cambiar-perfil-de-red-publico-privado-dominio-en-powershell/

Implementación del acceso inalámbrico en Windows

Por último, consideraciones para unir equipos al dominio cuando sólo está disponible la conexión WiFi:

https://docs.microsoft.com/es-es/windows-server/networking/core-network-guide/cncg/wireless/e-wireless-access-deployment#join-new-wireless-computers-to-the-domain

sedian Seguridad Digital de Andalucía