



JMA
CYBER PROTECT

Indice

Contenido

INDICE.....	2
INFORME AUDITORIA INICIAL DE JMA CYBER PROTECT	3
INFORME DEL ESTADO DE LA CIBERSEGURIDAD EN EMPRESAS ESPAÑOLAS.....	4
INTRODUCCIÓN.....	4
SITUACIÓN ACTUAL	4
CONSECUENCIAS FRECUENTES	5
CONCLUSIÓN.....	5
ESTADO REAL DE LA EMPRESA Y POSIBILIDAD DE NUEVOS CIBERATAQUES	5
ESTADO REAL DE LA EMPRESA.....	5
POSIBILIDAD DE NUEVOS CIBERATAQUES.....	6
CONCLUSIÓN.....	6
A . ADMINISTRACIÓN DE USUARIOS Y PUESTOS DE TRABAJO	6
I . ALMACENAMIENTO CENTRAL	8
H . ESTRUCTURA DE DOMINIO	8
SEGURIDAD:.....	12
PRESIONAR CTRL + ALT + SUPR:.....	13
MENSAJE BIENVENIDA:.....	14
FONDO “DEPARTAMENTO”:.....	15
AUDITAR:	16
6 . UNIDAD DE RED COMPARTIDA:	17
TIEMPO DE INACTIVIDAD:.....	19
BLOQUEAR EJECUTAR:	20
BLOQUEAR PANEL DE CONTROL:	21
BLOQUEO SÍMBOLO DEL SISTEMA:.....	22
BLOQUEAR USB Y DERIVADOS:	23
FIREWALL SIEMPRE HABILITADO:.....	24
WINDOWS UPDATE:.....	25
INSTALACIÓN DE SOFTWARE:.....	25
N . ANÁLISIS DE LOG EN LOS EQUIPOS:	27

Informe auditoria inicial de JMA Cyber Protect

Estimado registradoresmadrid.com,

Tras habernos comunicado su problemática, hemos realizado una evaluación inicial de su infraestructura para identificar los riesgos dentro de su organización, con el objetivo de que una situación así no vuelva a ocurrir.

A continuación, paso a numerar y detallar las vulnerabilidades encontradas:

1. **Puertos abiertos a internet:** Encontramos accesos directos desde internet hacia su infraestructura interna, en concreto el escritorio remoto y el sistema de almacenamiento que tienen en la oficina que tiene un redireccionamiento para ser accesible desde fuera. Estas configuraciones se realizaron para facilitar el teletrabajo de los empleados, pero si no se protegen de forma adecuada es la entrada más común para sufrir ciberataques.
2. **Contraseñas débiles e información expuesta:** Tras revisar el entorno de trabajo de los empleados hemos detectado que se utilizan contraseñas comunes o incluso escritas en un post-it y pegadas en la pantalla, escritorios llenos de información y usuarios ausentes sin bloquear su escritorio. Todo esto facilita en gran parte a que alguien no autorizado acceda a los sistemas y datos que se encuentran en el equipo.
3. **Sistemas operativos obsoletos y sin actualizar:** Comprobando este apartado vemos que tanto el sistema operativo del NAS como los equipos de los empleados, están anticuados y sin actualizar. Al estar utilizando sistemas antiguos permite a los ciberatacantes aprovechar brechas de seguridad que tenían estos sistemas y colarse en la red.
4. **Falta de control interno básico:** Por último, observamos prácticas que aumentan el riesgo a ser atacados, usuarios con permisos de administrador, USB personales conectados a equipos, uso de programas pirateados, siendo este último el más problemático de todos ya que la gran mayoría de programas que no son legales tienden a tener un virus.

En resumen: Actualmente tienen una brecha de seguridad muy importante que os exponen a nuevos ciberataques, robo de datos o incluso una denuncia por uso ilegal de programas pirateados.

Recomendamos abordar estos puntos de forma inmediata, podemos realizar un plan de acción para corregir estas vulnerabilidades y fortalecer su infraestructura

Por último, respecto al tema de la nube, podemos evaluar que opciones podríamos ofrecerle para que se le adapte a su empresa de la mejor forma, pero nuestra recomendación sería:

1. **Actuar:** Corregir las vulnerabilidades actuales
2. **Evaluar opciones:** Podemos ayudaros a analizar:

- a. Cuánto costaría asegurar y modernizar la infraestructura actual para reducir los riesgos a un nivel aceptable
- b. Que servicios de la nube se os adaptarían mejor a vuestras necesidades, cuánto costaría y que beneficios reales os aportaría a nivel de seguridad y operatividad.

Atentamente,

El equipo de JMA Cyber Protect

INFORME DEL ESTADO DE LA CIBERSEGURIDAD EN EMPRESAS ESPAÑOLAS

Introducción

En los últimos años las empresas españolas se han convertido frecuentemente en objetivo de muchos ciberataques, principalmente por no contar con las medidas básicas de protección.

Este breve informe ofrece una visión clara sobre el estado actual de la ciberseguridad en las empresas españolas, con el objetivo de ayudar a entender por qué es urgente tomar medidas preventivas, incluso siendo una empresa pequeña.

Situación Actual

A día de hoy los ciberataques son cada vez más frecuentes, el ransomware que cifra la información y luego pide un rescate por esta, es uno de los ataques más utilizados.

Una gran parte de las empresas españolas carecen de personal especializado o de unos protocolos claros de seguridad.

Algunos de los errores más comunes son:

- Contraseñas débiles.
- Sistemas sin actualizar.
- Falta de copias de seguridad.
- Exposición innecesaria a Internet.
- Teletrabajo mal gestionado

Consecuencias Frecuentes

Algunas de las consecuencias por falta de seguridad de la información en las empresas son:

- Pérdida total o parcial de la información.
- Paradas en la actividad laboral diaria.
- Daños a la reputación de la empresa, lo que conlleva una pérdida de confianza en los clientes.
- Posibles pagos de rescate de información robada.

Conclusión

A día de hoy la ciberseguridad ya no es opcional, es una necesidad. No se debe pensar de “si” va a ocurrir un ataque, sino de “cuándo” va a ocurrir.

Las empresas que no se preparan están en desventajas frente a las ciberamenazas que están en una continua evolución.

Por suerte, existen medidas efectivas, adaptadas y económicamente viables para reducir la posibilidad de que ocurran estas amenazas.

ESTADO REAL DE LA EMPRESA Y POSIBILIDAD DE NUEVOS CIBERATAQUES

Estado Real de la Empresa

Actualmente la gestoría presenta un nivel muy bajo de ciberseguridad, con múltiples puntos débiles que explican porque fueron víctima del reciente ciberataque de ransomware.

Las principales vulnerabilidades detectadas son

- Malas prácticas por parte de los usuarios: Usuarios locales con permisos de administrador, contraseñas visibles pegadas con posit en los monitores, sesiones sin bloquear...
- Falta de medidas preventivas: Sin existencia de algún tipo de protección firewall o antivirus.
- Alta exposición a Internet: Puertos abiertos como el RDP y un NAS accesible desde fuera de la empresa con contraseñas débiles
- Infraestructura mal configurada: sistemas operativos sin actualizar, software pirateado
- Gestión de datos deficiente: cada usuario guarda la información en su propio equipo sin tener un sistema centralizado para copias de seguridad.
- Teletrabajo inseguro: puertos abiertos sin VPN ni autenticación segura.

Posibilidad de Nuevos Ciberataques

Con el estado actual de la gestoría las probabilidades de sufrir un nuevo ciberataque son muy altas, si no se corrigen las debilidades mencionadas anteriormente es solo cuestión de tiempo que vuelva a producirse un ciberataque.

Al no haber ninguna medida de detección ni sistemas de alerta se podría estar dando otro ciberataque en estos momentos y no detectarlo hasta que haya causado un daño significativo.

Conclusión

Mientras no se realice una actualización de seguridad completa a la infraestructura de la gestoría y se eduque a los usuarios en buenas prácticas, la posibilidad de un nuevo ciberataque es realmente alta.

Nuestra recomendación como empresa dedicada a la seguridad de la información es actuar de forma inmediata con un plan que permita mejorar la seguridad de su empresa sin interrumpir la actividad laboral.

A. Administración de usuarios y puestos de trabajo

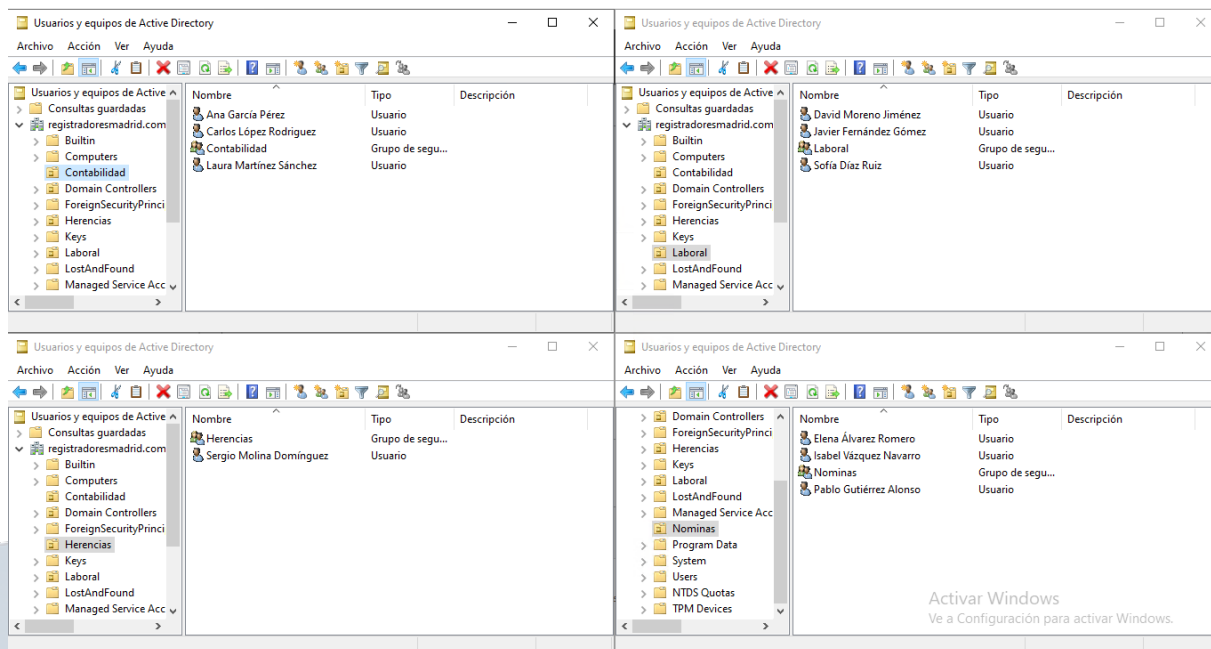
Se ha decidido optar por equipos con Windows 11, donde hemos creado los departamentos en el Active Directory de: Contabilidad, Laboral, Nominas y Herencias, dentro de cada grupo hemos asignado los usuarios que tienen que trabajar en cada departamento.

También hemos creado una política de creación de usuarios interna, que se compone de la **inicial + apellido**, a continuación, detallo la lista de usuarios, con su departamento, nombre, usuario y correo asignado.

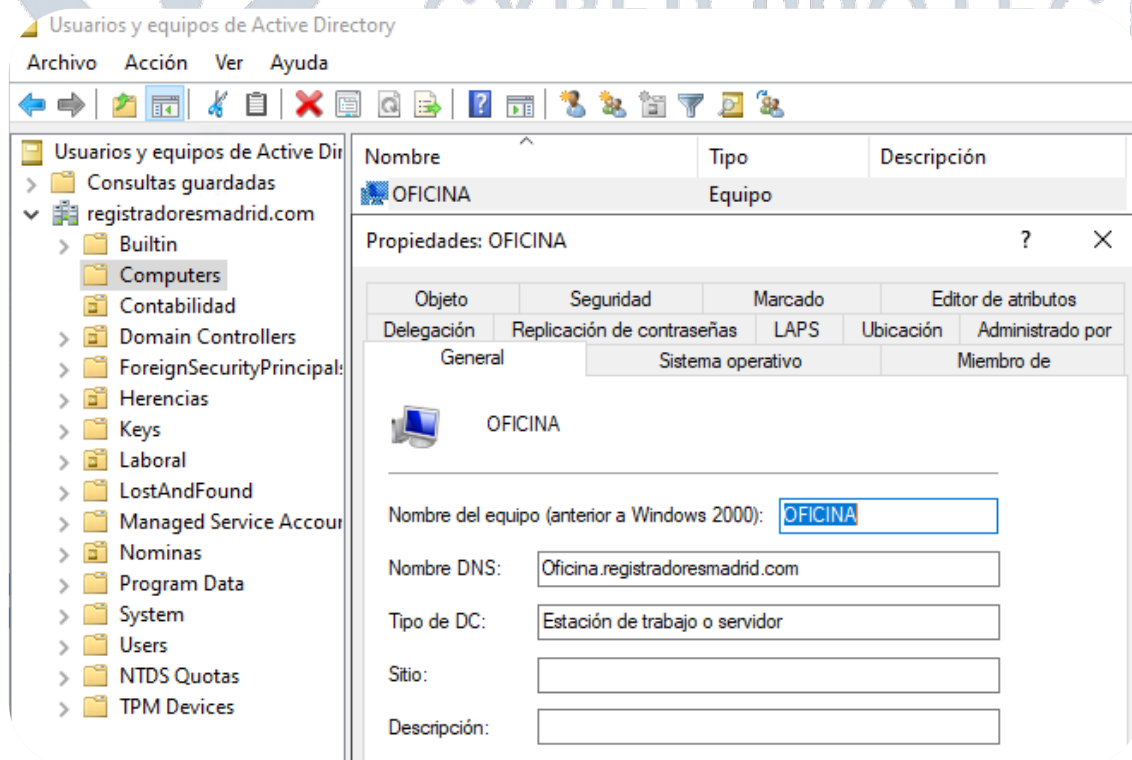
Departamento	Nombre	Usuario	Correo
Contabilidad	Ana García Pérez	agarcia	agarcia@registradoresmadrid.com
	Carlos López Rodríguez	clopez	clopez@registradoresmadrid.com
	Laura Martínez Sánchez	lmartinez	lmartinez@registradoresmadrid.com
Laboral	Javier Fernandez Gomez	jfernandez	jfernandez@registradoresmadrid.com
	Sofia Díaz Ruiz	sdiaz	sdiaz@registradoresmadrid.com
	David Moreno Jimenez	dmoreno	dmoreno@registradoresmadrid.com
Nominas	Elena Álvarez Romero	ealvarez	ealvarez@registradoresmadrid.com
	Pablo Gutiérrez Alonso	pgutierrez	pgutierrez@registradoresmadrid.com
	Isabel Vázquez Navarro	ivazquez	ivazquez@registradoresmadrid.com

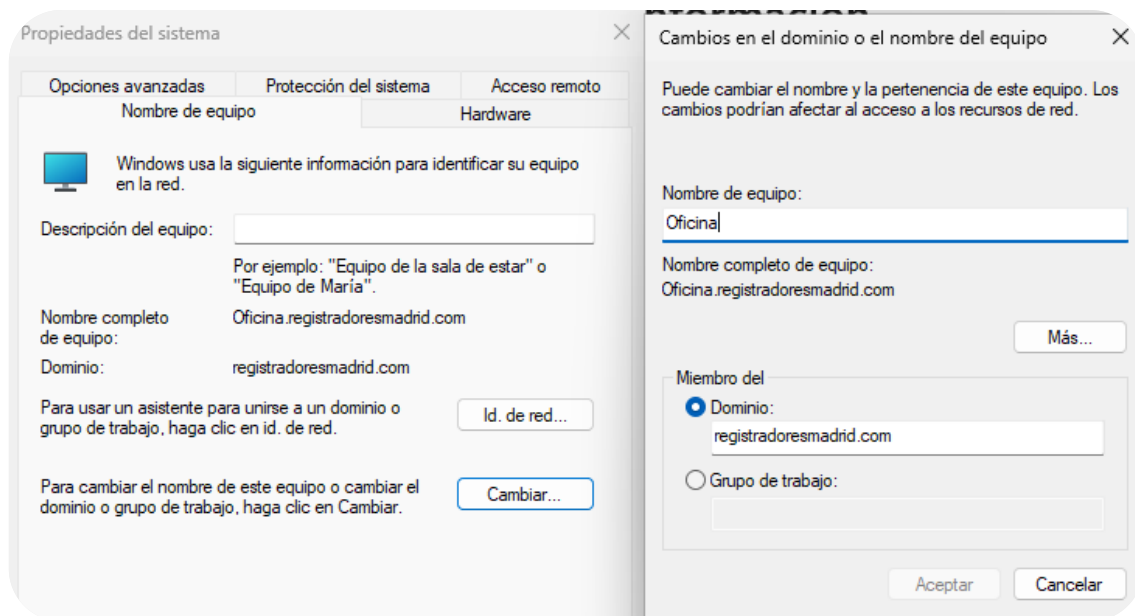
Herencias	Sergio Molina Domínguez	smolina	smolina@registradoresmadrid.com
-----------	-------------------------	---------	---------------------------------

Dentro del AD tiene la siguiente estructura



Hacemos una comprobación, de que el equipo está dentro del dominio, lo podemos ver tanto en el Windows Server como en el equipo destino



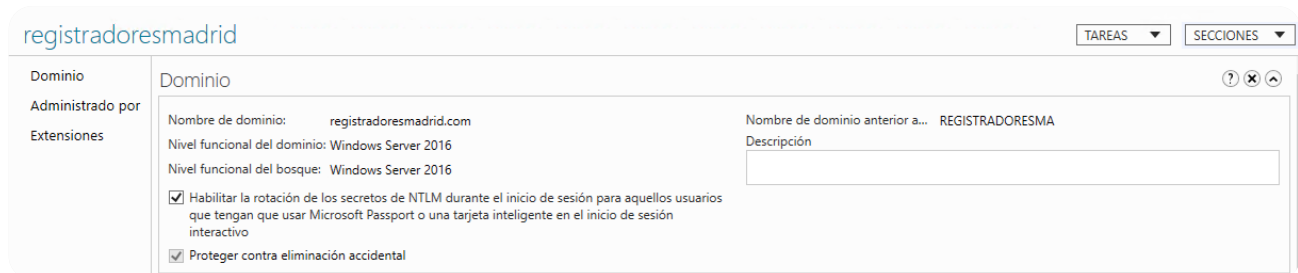


i . Almacenamiento central

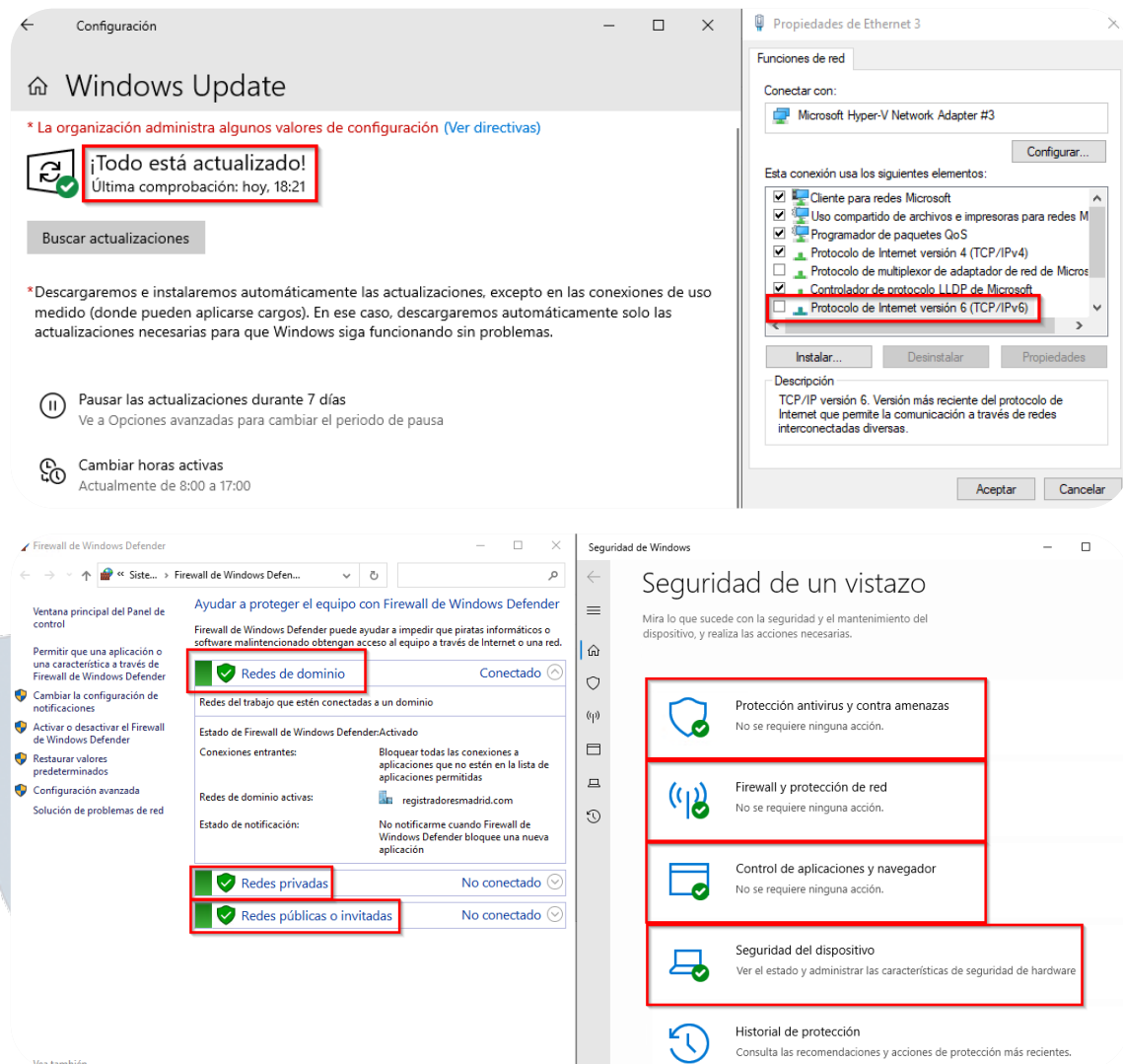
Hemos decidido montar un Proxmox y dentro de el se encontrará un Firewall Sophos y un Windows Server 2022 que se encargará de cumplir las funciones de directorio activo (AD), gestión de grupos, usuarios, de gestionar las directivas de grupo (GPO), albergar las aplicaciones de los trabajadores al igual que las unidades de red compartidas entre los diferentes departamentos.

h . Estructura de dominio

Dentro del Servidor Windows se crea un dominio con nombre **registradoresmadrid.com**



Se actualiza a la última versión, se desactiva el protocolo de IPv6, se comprueba que el firewall y el antivirus están operativos



Para comprobar que ambos equipos se encuentran el uno al otro, procedemos a hacer un PING y un tracert

```
Administrador: C:\Windows\system32\cmd.exe
C:\Users\Administrador.SERVIDORWIN22>whoami
registradoresma\administrador

C:\Users\Administrador.SERVIDORWIN22>ping 192.168.20.2

Haciendo ping a 192.168.20.2 con 32 bytes de datos:
Respuesta desde 192.168.20.2: bytes=32 tiempo=3ms TTL=127
Respuesta desde 192.168.20.2: bytes=32 tiempo<1m TTL=127
Respuesta desde 192.168.20.2: bytes=32 tiempo<1m TTL=127
Respuesta desde 192.168.20.2: bytes=32 tiempo<1m TTL=127

Estadísticas de ping para 192.168.20.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 3ms, Media = 0ms

C:\Users\Administrador.SERVIDORWIN22>tracert 192.168.20.2

Traza a 192.168.20.2 sobre caminos de 30 saltos como máximo.

  1    <1 ms    <1 ms    <1 ms  192.168.10.1
  2    <1 ms    <1 ms    <1 ms  192.168.20.2

Traza completa.

C:\Users\Administrador.SERVIDORWIN22>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet 3:

    Sufijo DNS específico para la conexión. . . :
    Dirección IPv4. . . . . : 192.168.10.2
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.10.1

C:\Users\Administrador.SERVIDORWIN22>

Simbolo del sistema
Microsoft Windows [Versión 10.0.26100.3915]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\agarcia>whoami
registradoresma\agarcia

C:\Users\agarcia>ping 192.168.10.2

Haciendo ping a 192.168.10.2 con 32 bytes de datos:
Respuesta desde 192.168.10.2: bytes=32 tiempo=1ms TTL=127
Respuesta desde 192.168.10.2: bytes=32 tiempo=1ms TTL=127
Respuesta desde 192.168.10.2: bytes=32 tiempo<1m TTL=127
Respuesta desde 192.168.10.2: bytes=32 tiempo<1m TTL=127

Estadísticas de ping para 192.168.10.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\agarcia>tracert 192.168.10.2

Traza a 192.168.10.2 sobre caminos de 30 saltos como máximo.

  1    <1 ms    <1 ms    <1 ms  192.168.20.1
  2    <1 ms    <1 ms    <1 ms  192.168.10.2

Traza completa.

C:\Users\agarcia>ipconfig

Configuración IP de Windows























Adaptador de Ethernet Ethernet 2:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::f5a1:2eca:86bc:fc39%14
    Dirección IPv4. . . . . : 192.168.20.2
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.20.1

C:\Users\agarcia>
```



Para maximizar la seguridad de la organización, se implantan políticas de seguridad en todos los departamentos, siguiendo la siguiente estructura.

Nombre	Estado de GPO
 Auditar	Habilitado
 Bloquear_Ejecutar	Habilitado
 Bloqueo_Panel_de_Control	Habilitado
 Bloqueo_simbolo_del_sistema	Habilitado
 Bloqueo_USB	Habilitado
 Default Domain Controllers Policy	Habilitado
 Default Domain Policy	Habilitado
 Firewall_siempre_habilitado	Habilitado
 Fondo_Contabilidad	Habilitado
 Fondo_Herencias	Habilitado
 Fondo_Laboral	Habilitado
 Fondo_Nominas	Habilitado
 Instalacion_Software	Habilitado
 Mensaje_bienvenida	Habilitado
 Presionar_ctrl+alt+supr	Habilitado
 Seguridad	Habilitado
 Tiempo_de_inactividad	Habilitado
 Unidad_Red_Contabilidad	Habilitado
 Unidad_Red_Herencias	Habilitado
 Unidad_Red_Laboral	Habilitado
 Unidad_Red_Nominas	Habilitado
 Windows_Update	Habilitado



JMA
CYBER PROTECT

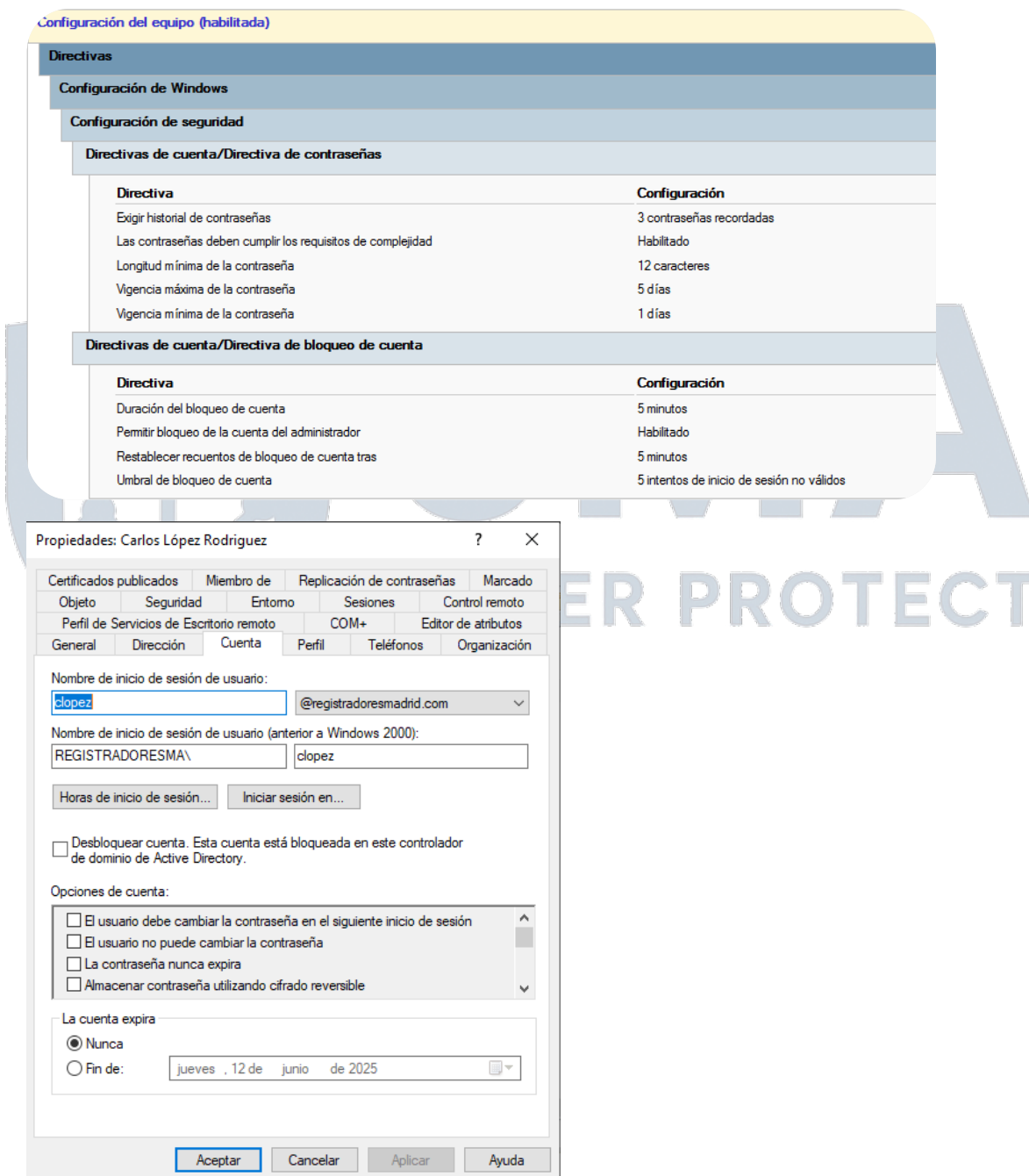
A continuación pasaremos a explicar todas las GPO's creadas en el servidor

Seguridad:

En esta política aplicaremos todo lo relacionado a política de contraseñas, se sigue la siguiente ruta para poder crearse

Configuración del equipo > Directivas > Configuración de seguridad > Directivas de cuenta / Directiva de contraseñas

Configuración del equipo > Directivas > Configuración de seguridad > Directivas de cuenta / Directiva de contraseñas



Presionar ctrl + alt + supr:

Para aumentar un poco más el grado de seguridad se ha implantado que para que se pueda entrar al inicio de sesión al arrancar el equipo se tenga que presionar las teclas de control + alt + suprimir a la vez, para crear dicha regla se sigue la siguiente ruta:

Configuración del equipo > Directivas > Configuración de seguridad > Directivas locales / Opciones de seguridad

Configuración del equipo (habilitada)	
Directivas	
Configuración de Windows	
Configuración de seguridad	
Directivas locales/Opciones de seguridad	
Inicio de sesión interactivo	
Directiva	Configuración
Inicio de sesión interactivo: no requerir Ctrl+Alt+Supr	Habilitado



JMA

CYBER PROTECT

Mensaje bienvenida:

Para que los usuarios sean conscientes de que están dentro del dominio, se les manda una alerta visual que tendrán que aceptar para que sean conscientes de que tienen que respetar una serie de normas, para crearla se sigue la siguiente ruta:

Configuración del equipo > Directivas > Configuración de seguridad > Directivas locales / Opciones de seguridad

Configuración del equipo (habilitada)		ocultar
Directivas		ocultar
Configuración de Windows		ocultar
Configuración de seguridad		ocultar
Directivas locales/Opciones de seguridad		ocultar
Inicio de sesión interactivo		ocultar
Directiva	Configuración	
Inicio de sesión interactivo: texto del mensaje para los usuarios que intentan iniciar una sesión	Bienvenido al dominio registradoresmadrid.com, este equipo queda sujeto a respetar las políticas de privacidad y seguridad de la empresa	
Inicio de sesión interactivo: título del mensaje para los usuarios que intentan iniciar una sesión	"AVISO IMPORTANTE"	

AVISO IMPORTANTE

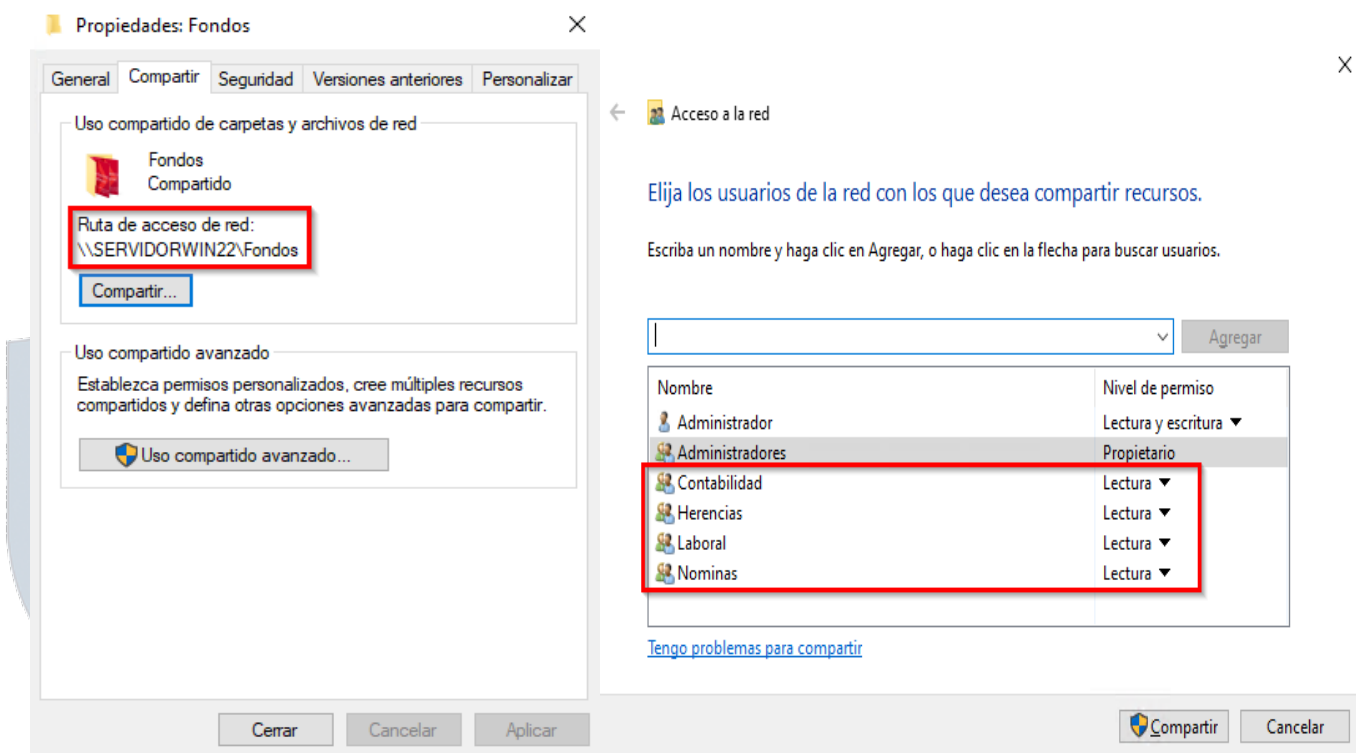
Bienvenido al dominio registradoresmadrid.com, este equipo queda sujeto a respetar las políticas de privacidad y seguridad de la empresa

Aceptar

Fondo “departamento”:

Se crea un fondo de escritorio para cada departamento, donde se coloca el color corporativo, el número de teléfono del soporte técnico y otro aviso indicando que tienen que cumplir con las políticas de privacidad de la empresa, para crearla hay que seguir los siguientes pasos:

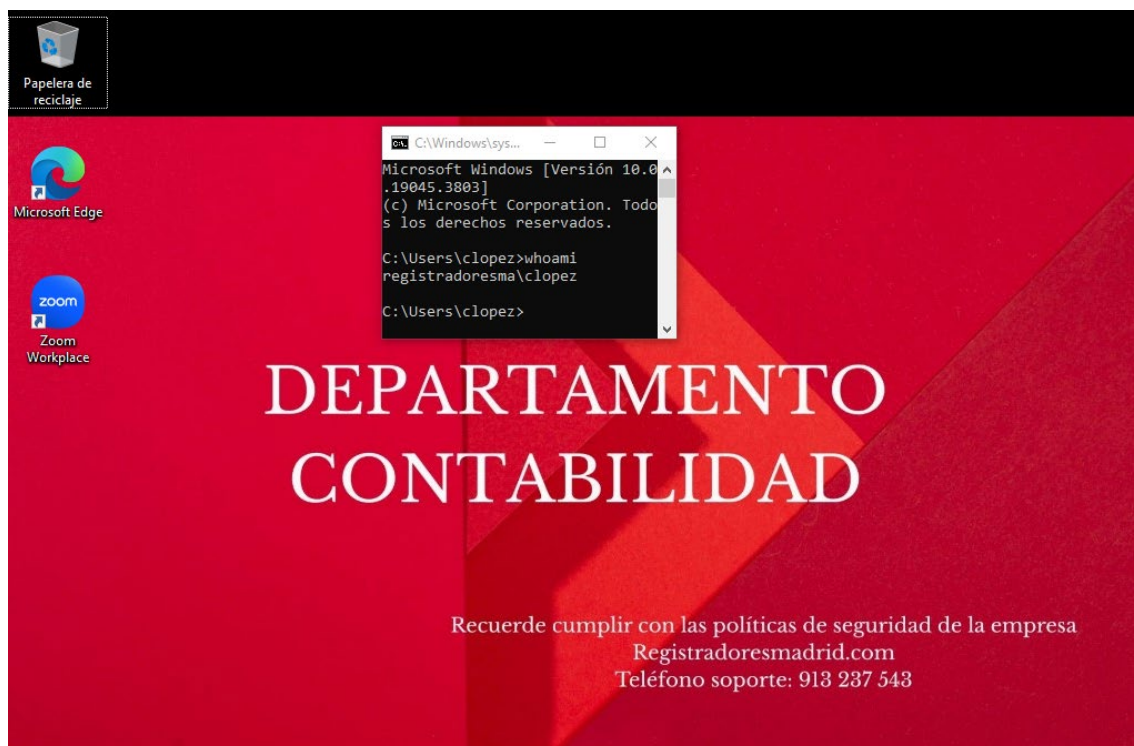
Se crea una carpeta donde meteremos los fondos de escritorio con un formato de imagen .jpg y se comparte la carpeta, dando permiso de lectura a los grupos de la organización, en el campo de Seguridad también le daremos permisos.



A continuación, creamos la GPO correspondiente con la siguiente ruta:

Configuración del usuario > Directivas > Plantillas administrativas > Active Desktop

Configuración del usuario (habilitada)			ocultar
Directivas			ocultar
Plantillas administrativas			ocultar
Definiciones de directiva (archivos ADMX) recuperadas del equipo local.			
Active Desktop/Active Desktop			ocultar
Directiva	Configuración	Comentario	
Habilitar Active Desktop	Habilitado		
Permite papel tapiz JPEG y HTML			
Directiva	Configuración	Comentario	
No permitir cambios	Habilitado		
Tapiz del escritorio	Habilitado		
Nombre del papel tapiz: \\SERVIDORWIN22\Fondos\Contabilidad.jpg			
Ejemplo: con una ruta de acceso local: C:\windows\web\wallpaper\inicio.jpg			
Ejemplo: con una ruta de acceso UNC: \\Servidor\RecursoCompartido\Corp.jpg			
Estilo del papel tapiz:	Ajustar		



Auditar:

Para averiguar si podemos sufrir un ataque de fuerza bruta, se habilita las opciones de auditoría que tiene Windows Server para ver entre otros muchos valores, los inicios y cierres de sesión, para habilitarla seguiremos la siguiente ruta:

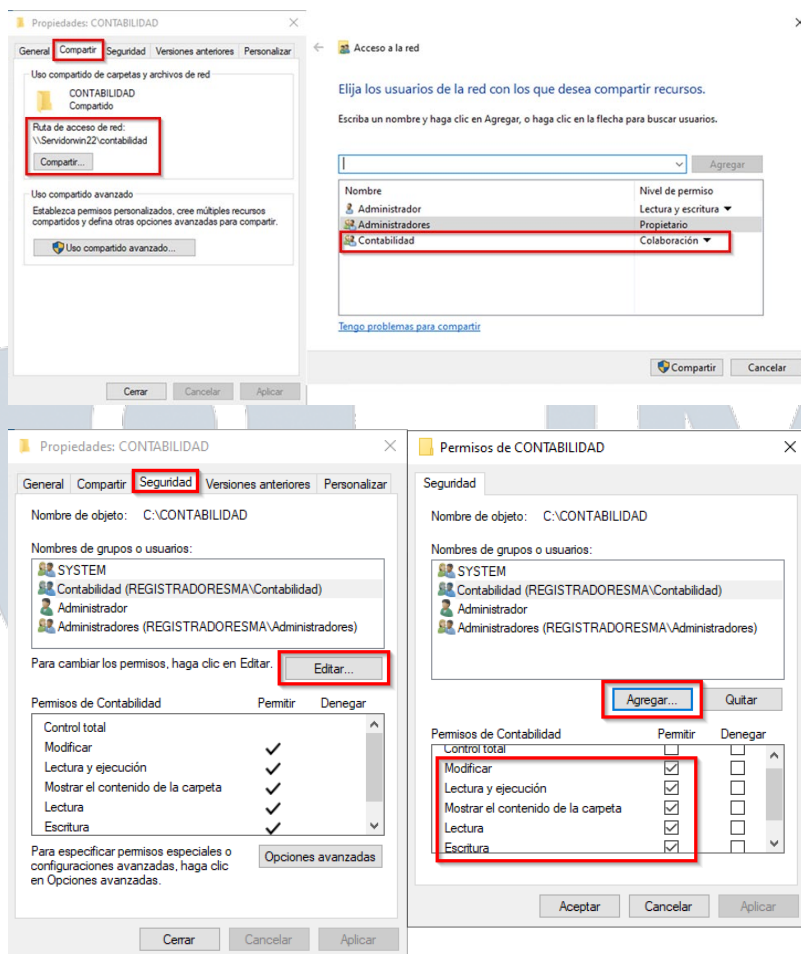
Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad > Configuración de auditoría avanzada > Inicio y cierre de sesión

Configuración del equipo (habilitada)		ocultar
Directivas		ocultar
Configuración de Windows		ocultar
Configuración de seguridad		ocultar
Configuración de auditoría avanzada		ocultar
Inicio y cierre de sesión		ocultar
Directiva	Configuración	
Auditar cierre de sesión	Aciertos, errores	
Auditar inicio de sesión	Aciertos, errores	

6 . Unidad de red compartida:

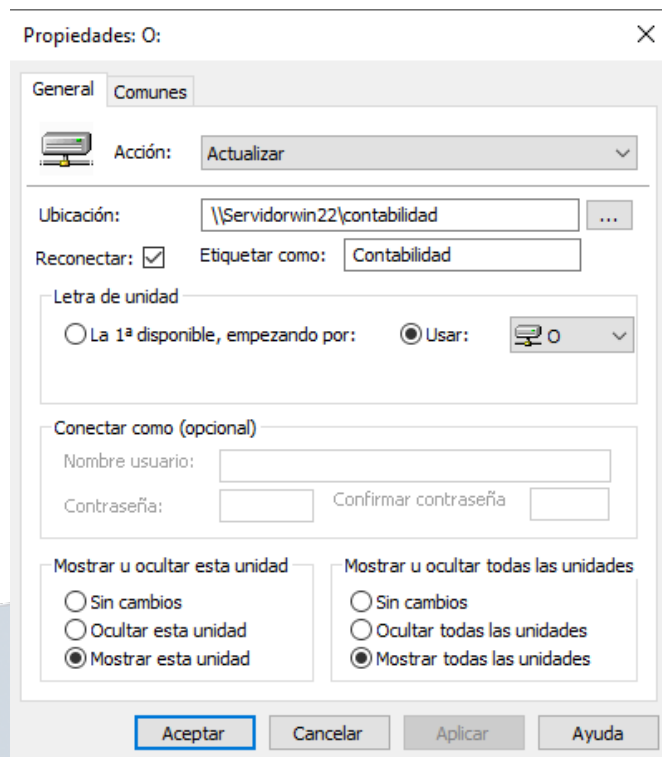
Para tener centralizado todos los recursos de los distintos departamentos se plantea la siguiente estructura y es que dentro del servidor albergue lo que serán en un futuro las unidades de red compartidas de cada uno de los equipos, para llevar a cabo esta tarea se realiza de la siguiente forma:

Se crea la carpeta del departamento, se comparte se le da permisos de lectura y escritura al equipo que corresponda y se hace lo mismo en el campo de seguridad, los cambios quedarían de la siguiente forma:



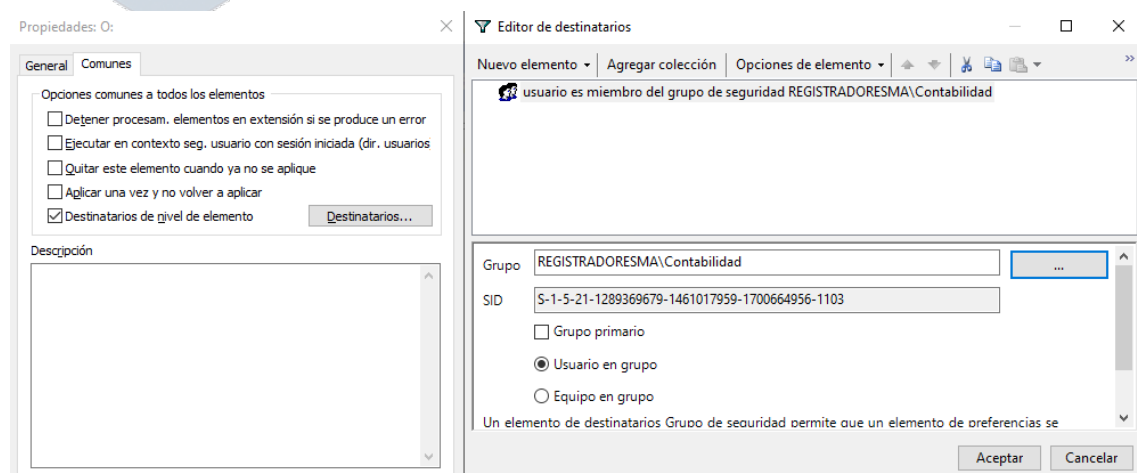
A continuación dentro de la GPO nos dirigimos a la siguiente ruta:

Configuración del usuario > Preferencias > Configuración de Windows > Asignación de unidades > botón derecho > nuevo



Rellenamos la información de ubicación: [\\servidor\carpeta_grupo](#)

A continuación, vamos a comunes y habilitamos el check de “Destinatarios de nivel de elemento” y una vez dentro seleccionamos nuevo elemento y grupo de seguridad, añadimos el grupo al que pertenece y aplicamos cambios



La GPO, quedaría así:

Configuración del usuario (habilitada) ocultar

Preferencias ocultar

Configuración de Windows ocultar

Asignaciones de unidades ocultar

Asignación de unidad (unidad: O) ocultar

O: (orden: 1) ocultar

General ocultar

Acción	Actualizar
Propiedades	
Letra	O
Ubicación	\\Servidorwin22\contabilidad
Volver a conectar	Habilitado
Etiquetar como	Contabilidad
Usar primera disponible	Deshabilitado
Mostrar u ocultar esta unidad	Mostrar
Mostrar u ocultar todas las unidades	Mostrar

Comunes ocultar

Opciones

Dejar de procesar elementos en esta extensión si se produce un error en este elemento	No
Ejecutar en el contexto de seguridad del usuario con sesión iniciada (opción de directiva de usuario)	No
Quitar este elemento cuando ya no se aplique	No
Aplicar una vez y no volver a aplicar	No

Destinatarios de nivel de elemento: grupo de seguridad

Atributo	Valor
bool	AND
not	0
name	REGISTRADORESMA\Contabilidad
sid	S-1-5-21-1289369679-1461017959-1700664956-1103
userContext	1
primaryGroup	0
localization	n

Activar Windows
Ve a Configuración para activar Windows.

Tiempo de inactividad:

Como uno de los problemas principales era que los usuarios se levantaban de sus puestos y no bloqueaban el escritorio, hemos habilitado que, si en 5 minutos no se hace ningún movimiento, se bloqueara automáticamente la pantalla y tendrán que ingresar nuevamente la contraseña, para poder habilitarla hay que seguir la siguiente ruta:

Configuración del usuario > Directivas > Plantillas administrativas > Panel de control / personalización

Configuración del usuario (habilitada) ocultar

Directivas ocultar

Plantillas administrativas ocultar

Definiciones de directiva (archivos ADMX) recuperadas del equipo local.

Panel de control/Personalización ocultar

Directiva	Configuración	Comentario
Habilitar protector de pantalla	Habilitado	
Proteger el protector de pantalla mediante contraseña	Habilitado	
Tiempo de espera del protector de pantalla	Habilitado	
Número de segundos de espera hasta que se active el protector de pantalla		
Segundos:	300	

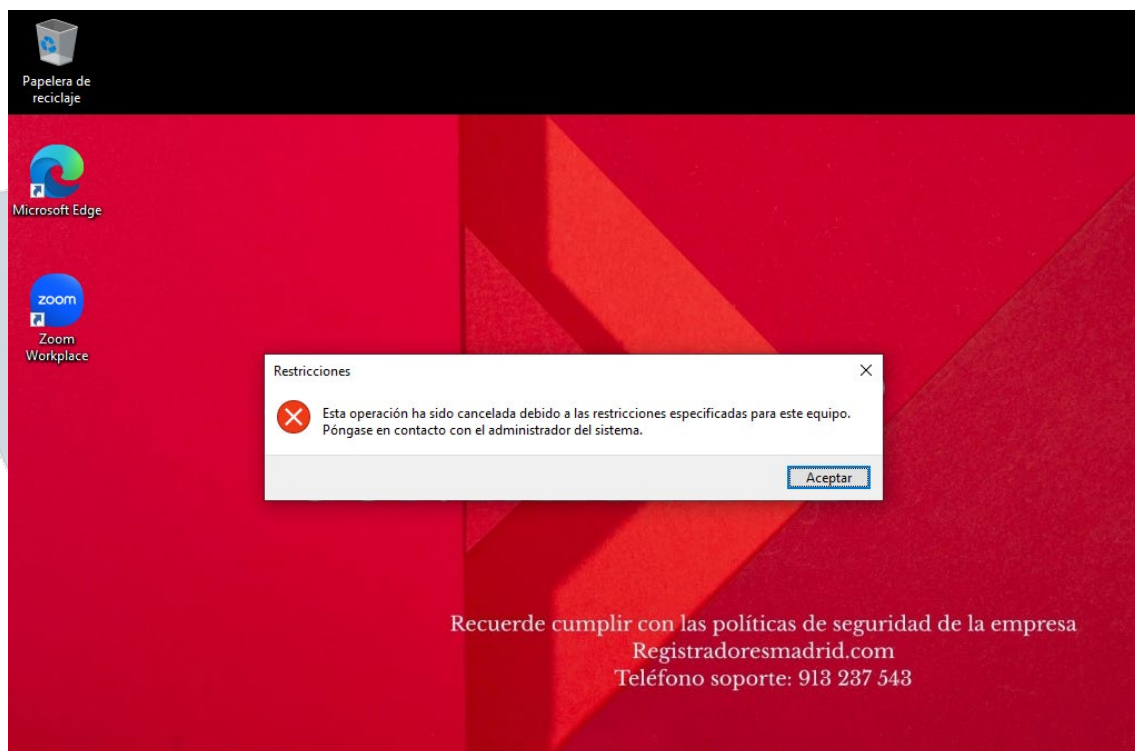
Activar Windows

Bloquear ejecutar:

Para evitar que pudieran hacer uso indebido del apartado “ejecutar”, para evitar ataques o para evitar que empleados accedan a partes del sistema mediante ese apartado, para poder habilitarlo hay que seguir la siguiente ruta:

Configuración del usuarios > Directivas > Plantillas administrativas > Menú Inicio y barra de tareas

Configuración del usuario (habilitada)			ocultar
Directivas			ocultar
Plantillas administrativas			ocultar
Definiciones de directiva (archivos ADMX) recuperadas del equipo local.			ocultar
Menú Inicio y barra de tareas			ocultar
Directiva	Configuración	Comentario	
Quitar el menú Ejecutar del menú Inicio	Habilitado		

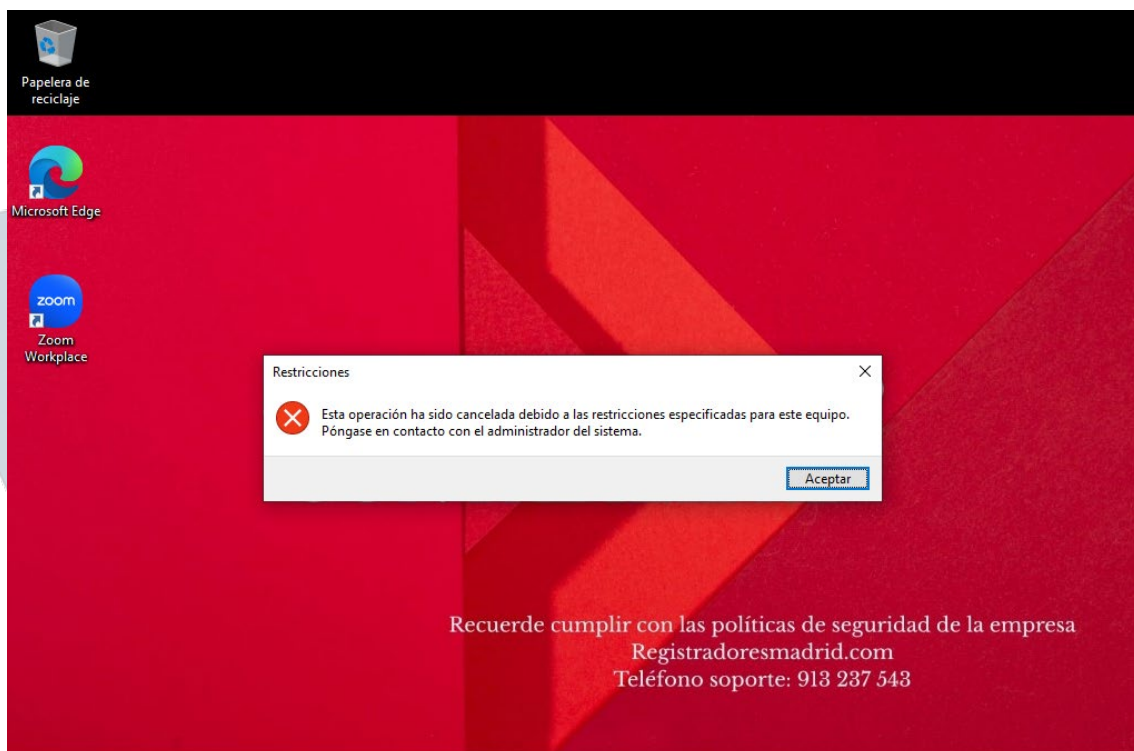


Bloquear panel de control:

Para que los usuarios no puedan acceder a ninguna modificación y así trastocar el buen funcionamiento del sistema, se habilitaría de la siguiente forma:

Configuración del usuario > Directivas > Plantillas administrativas > Panel de control

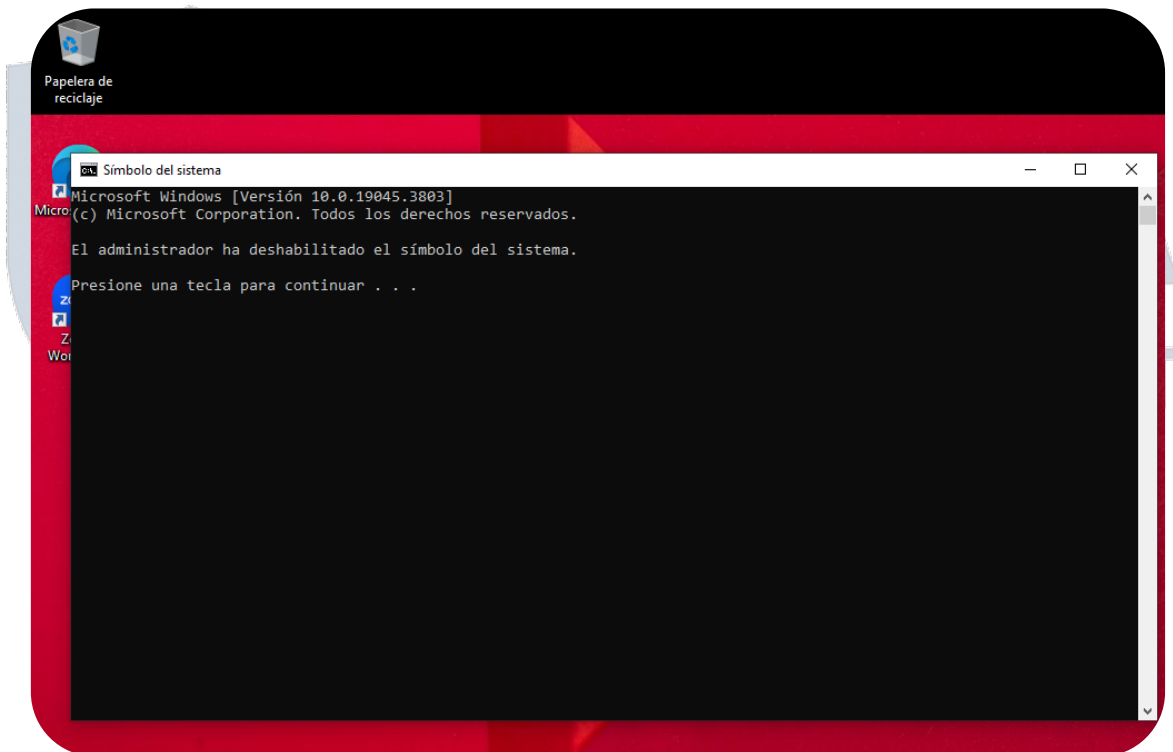
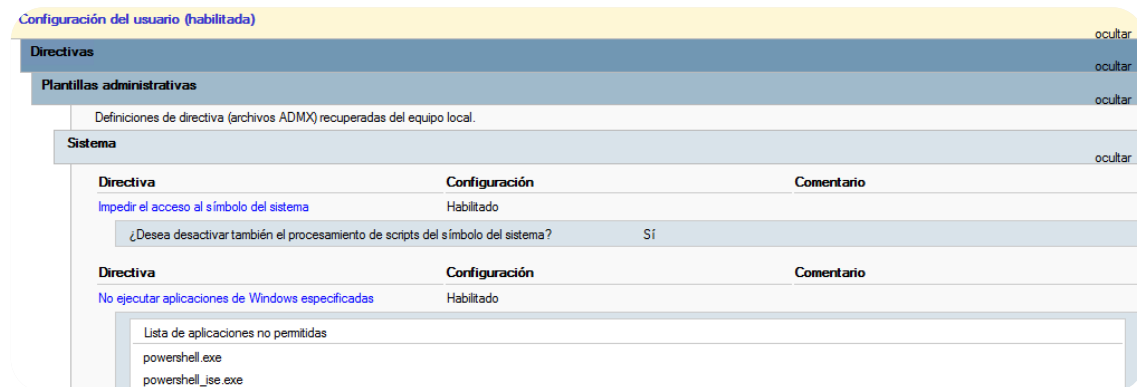
Configuración del usuario (habilitada)			ocultar
Directivas			ocultar
Plantillas administrativas			ocultar
Definiciones de directiva (archivos ADMX) recuperadas del equipo local.			ocultar
Panel de control			ocultar
Directiva	Configuración	Comentario	
Prohibir el acceso a Configuración de PC y a Panel de control	Habilitado		



Bloqueo símbolo del sistema:

Uno de los principales problemas que puede haber es que se ejecuten comandos y scripts maliciosos en el equipo, de esta forma hemos deshabilitado tanto el cmd como los powershell del sistema, para habilitarlo hay que seguir la siguiente ruta:

Configuración del usuario > Directivas > Plantillas administrativas > Sistema

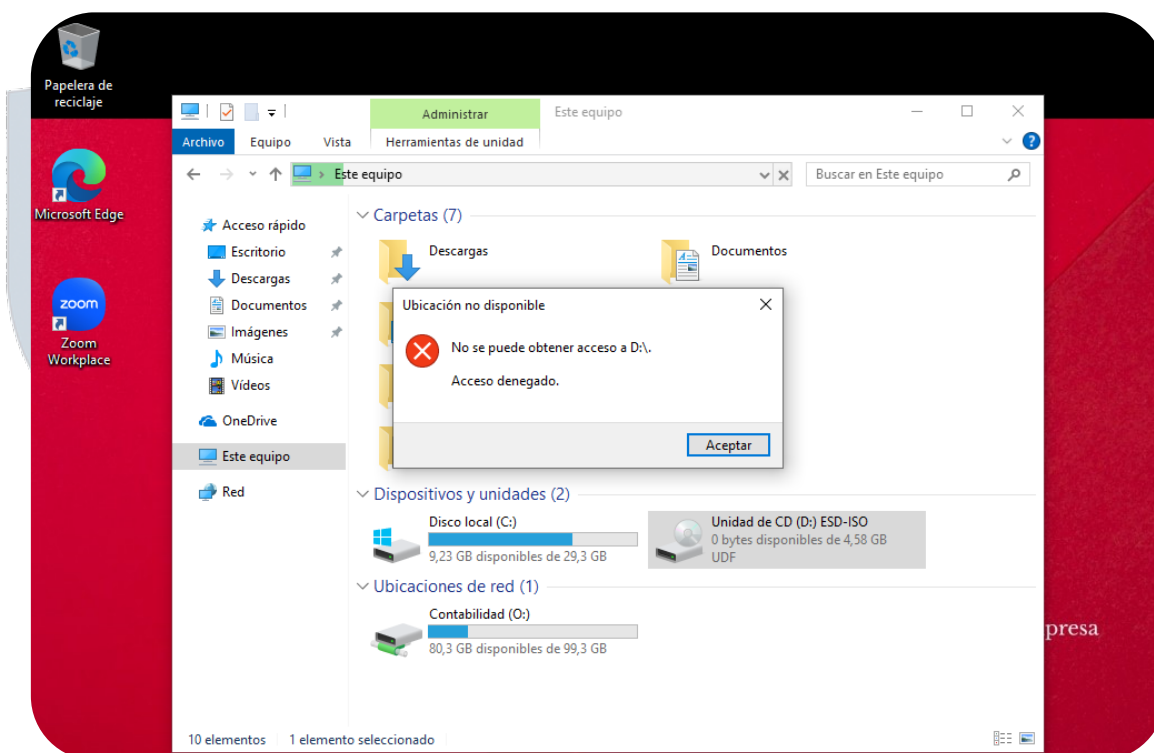


Bloquear USB y derivados:

Para respetar que las políticas de seguridad se respeten y no haya ningún problema de que se filtre o borre información, o se introduzca un archivo malicioso en la red por culpa de un almacenamiento externo, se ha decidido bloquear todos los elementos extraíbles que se quieran introducir en los equipos, para habilitar esta parte se ha seguido la siguiente ruta:

Configuración del usuario > Directivas > Plantillas administrativas > Sistema/Acceso de almacenamiento extraíble

Configuración del usuario (habilitada)			ocultar
Directivas			ocultar
Plantillas administrativas			ocultar
Definiciones de directiva (archivos ADMX) recuperadas del equipo local.			ocultar
Sistema/Acceso de almacenamiento extraíble			ocultar
Directiva	Configuración	Comentario	
Todas las clases de almacenamiento extraíble: denegar acceso a todo	Habilitado		



Firewall siempre habilitado:

Para evitar que los usuarios desactiven el firewall de Windows puesto que supondría una amenaza, se mantendrá una política de siempre habilitado, se habilita en la siguiente ruta:

Configuración del equipo > Configuración de Windows > Configuración de seguridad > Firewall de Windows con seguridad avanzada

Directivas		ocultar
Configuración de Windows		ocultar
Configuración de seguridad		ocultar
Firewall de Windows con seguridad avanzada		ocultar
Configuración global		mostrar
Configuración de perfil de dominio		ocultar
Directiva	Configuración	
Estado del firewall	Activado	
Conexiones entrantes	No configurado	
Conexiones salientes	No configurado	
Aplicar reglas de firewall local	No configurado	
Aplicar reglas de seguridad de conexión local	No configurado	
Mostrar notificaciones	No configurado	
Permitir respuestas de unidifusión	No configurado	
Registrar paquetes perdidos	No configurado	
Registrar conexiones correctas	No configurado	
Ruta de acceso del archivo de registro	No configurado	
Tamaño máximo del archivo de registro (KB)	No configurado	

Configuración del equipo > Plantillas administrativas > Red/Conexión de red/Firewall de Windows Defender/Perfil de dominio

Configuración del equipo (habilitada)			ocultar
Directivas			ocultar
Configuración de Windows			mostrar
Plantillas administrativas			ocultar
Definiciones de directiva (archivos ADMX) recuperadas del equipo local.			
Red/Conexiones de red/Firewall de Windows Defender/Perfil de dominio			ocultar
Directiva	Configuración	Comentario	
Firewall de Windows Defender: permitir excepciones de ICMP	Habilitado		
Permitir destino inalcanzable saliente	Habilitado		
Permitir paquete de control de flujo (source quench) saliente	Habilitado		
Permitir redirección	Habilitado		
Permitir petición eco entrante	Habilitado		
Permitir petición de enrutador entrante	Habilitado		
Permitir tiempo de salida excedido	Habilitado		
Permitir problema de parámetro saliente	Habilitado		
Permitir petición de marca de tiempo entrante	Habilitado		
Permitir petición de máscara entrante	Habilitado		
Permitir paquete saliente demasiado grande	Habilitado		
Directiva	Configuración	Comentario	
Firewall de Windows Defender: proteger todas las conexiones de red	Habilitado		

Windows update:

Para mantener una política de que todos los equipos estén actualizados a la última versión y con los últimos parches de seguridad instalados, se ha decidido habilitar la regla en la siguiente ruta:

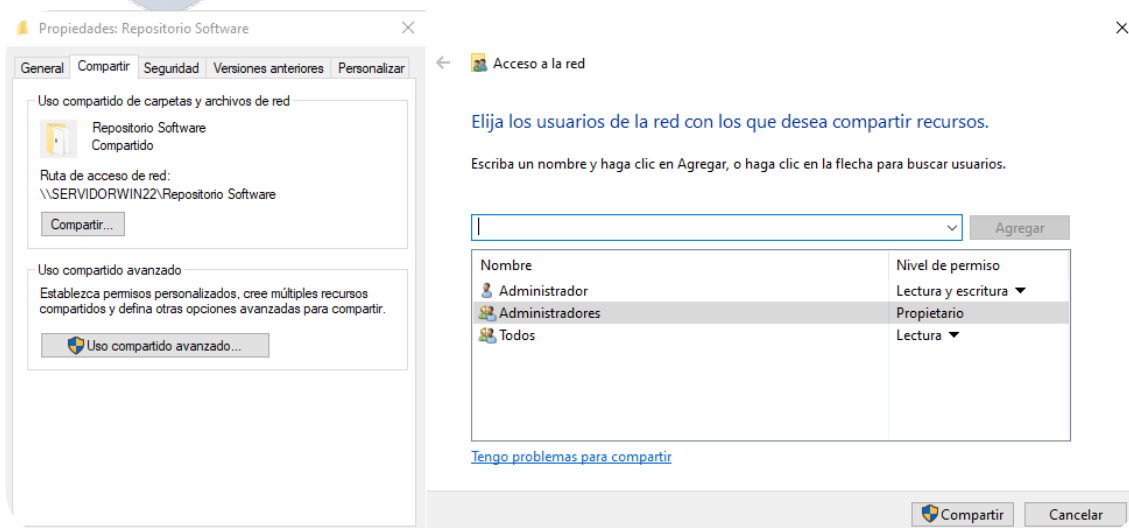
Configuración del equipo > Directivas > Plantillas administrativas > Componentes de Windows/Windows Update



Instalación de software:

Para que los usuarios puedan utilizar las aplicaciones y puedan trabajar.

Primero, se crea la carpeta en el servidor y se comparte con todos los usuarios con permisos de lectura:



A continuación se crea la GPO en la siguiente ruta:

Configuración del usuario > Directivas > Configuración del software > Aplicaciones asignadas > Botón derecho > Nuevo paquete > Se selecciona el archivo (.MSI)

A continuación: botón derecho sobre el paquete seleccionado > propiedades > implementación > “Instalar esta aplicación durante el inicio de sesión”

Configuración del usuario (habilitada)

Directivas

Configuración de software

Aplicaciones asignadas

7-Zip 24.09 (x64 edition)

Información del producto	
Información de implementación	

General	Configuración
Tipo de distribución	Asignada
Origen de implementación	\\SERVER\ORWIN22\Repositorio Software\7z2409-x64.msi
Opciones de la interfaz de usuario de instalación	Máximo
Desinstalar esta aplicación cuando esté fuera del ámbito de administración	Deshabilitado
No mostrar este paquete en Agregar o quitar programas en el Panel de control	Deshabilitado
Instalar esta aplicación durante el inicio de sesión	Habilitado

Opciones avanzadas de implementación	Configuración
Omitir el idioma al implementar este paquete	Deshabilitado
Hacer que esta aplicación x86 de 32 bits esté disponible en equipos de Win64	Habilitado
Incluir información de clase OLE y de producto	Habilitado

Información de diagnóstico	Configuración
Código de producto	{23170F69-40C1-2702-2409-000001000000}
Nº de implementaciones	0

Activar Windows

Papelera de reciclaje

Microsoft Edge

Zoom Workplace

7-Zip File Manager

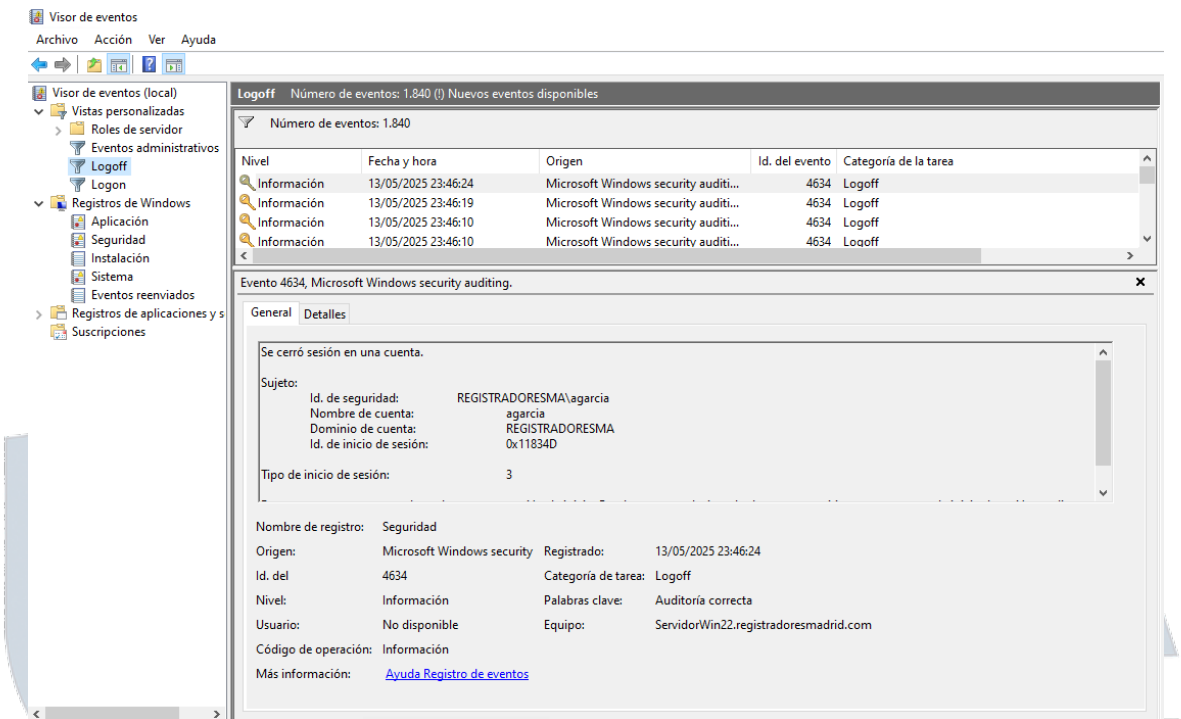
DEPARTAMENTO CONTABILIDAD

Recuerde cumplir con las políticas de seguridad de la empresa
 Registradoresmadrid.com
 Teléfono soporte: 913 237 543

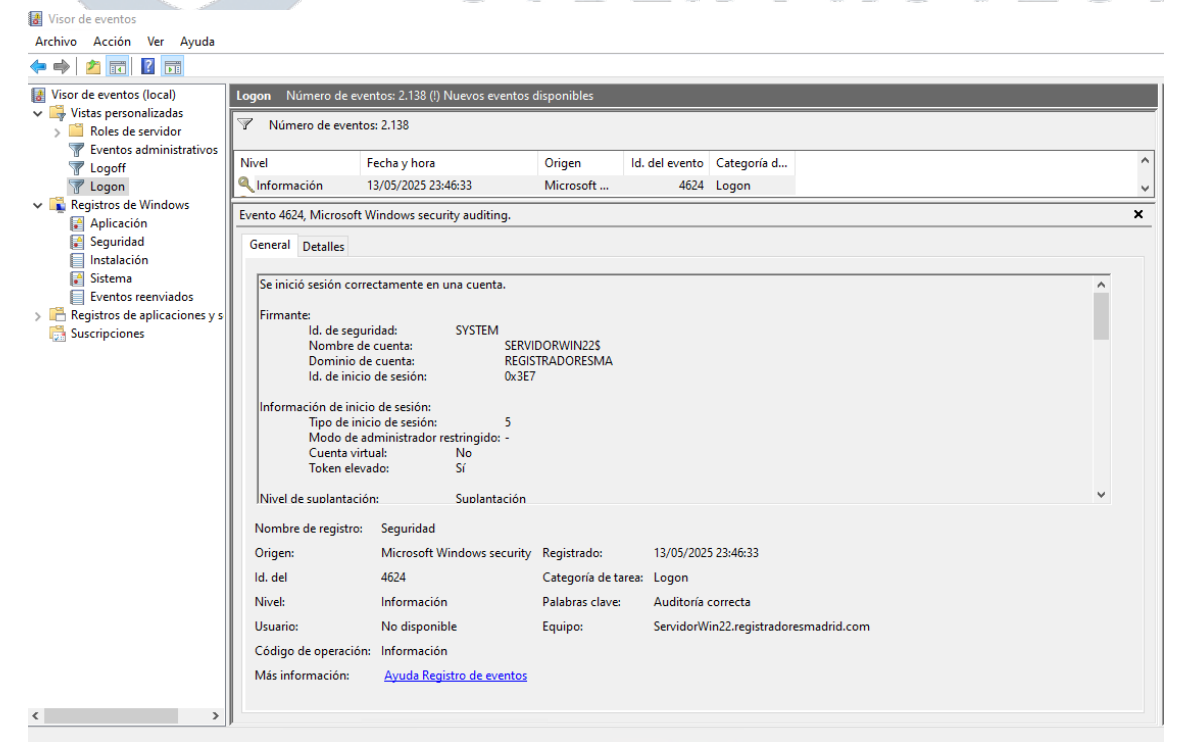
N . Análisis de log en los equipos:

Hemos decidido utilizar el visor de eventos de Windows que tiene integrado para la recolección de registros, los más importantes a tener en cuenta son los siguientes:

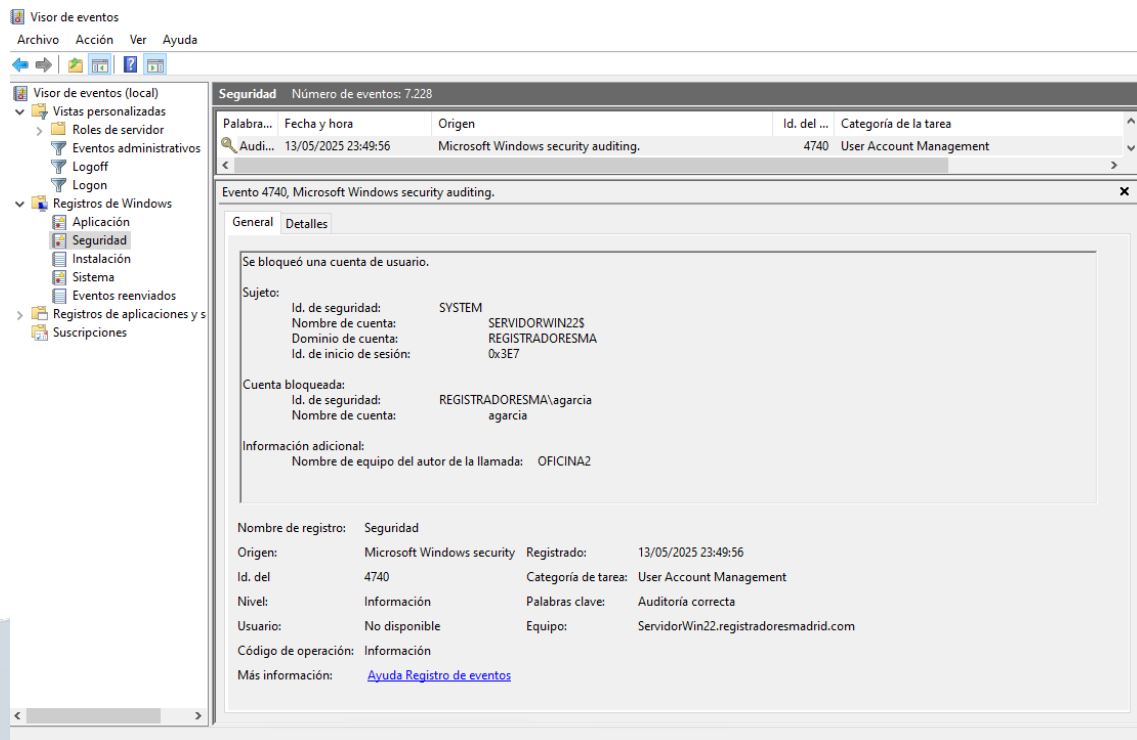
4634 – Cierre de sesión:



4624 – Inicio de sesión:



4740 – Bloqueo de usuario:



Estos otros ejemplos son los considerados como más importantes a la hora de hacer una auditoría del visor de eventos:

Ejemplos de ID de eventos y sus descripciones:

4624: Indica un inicio de sesión exitoso en un equipo local.

4625: Indica un intento de inicio de sesión fallido.

4738: Indica que una cuenta de usuario ha sido modificada.

4737: Indica que un grupo global con seguridad habilitada ha sido modificado.

513: Indica que Windows se está apagando.

3090: Indica que un archivo se ejecutó debido a ISG o instalador administrado.

4801: Indica que el equipo ha sido desbloqueado.

4616: Indica que la hora del sistema ha sido modificada.

5024: Indica que el servicio de Firewall se ha iniciado correctamente.

1019: Indica que una actualización se quitó correctamente.

1020: Indica que una actualización no se pudo quitar.

1022: Indica que una actualización se instaló correctamente.

1001: Indica un informe de errores de Windows.

672: Indica una falla en la autenticación de un usuario.

4673: Indica el uso de privilegios confidenciales.

4674: Indica una autorización de servicio.

4698: Indica una modificación de usuario.

51: Indica información de la sección de datos de un mensaje de evento.

1076: Indica un apagado o reinicio inesperado.

104: Indica que el registro de eventos se borró.

1100: Indica que el servicio del registro de eventos se apagó.

640: Indica eventos relacionados con el registro del sistema.

41, 42, 43, 44: Eventos de Microsoft Defender para punto de conexión.

658, 659: Eventos relacionados con la modificación de grupos.

528, 540: Eventos de inicio de sesión correctos en versiones anteriores de Windows.

1102: Indica que el registro de eventos fue borrado.



JMA
CYBER PROTECT