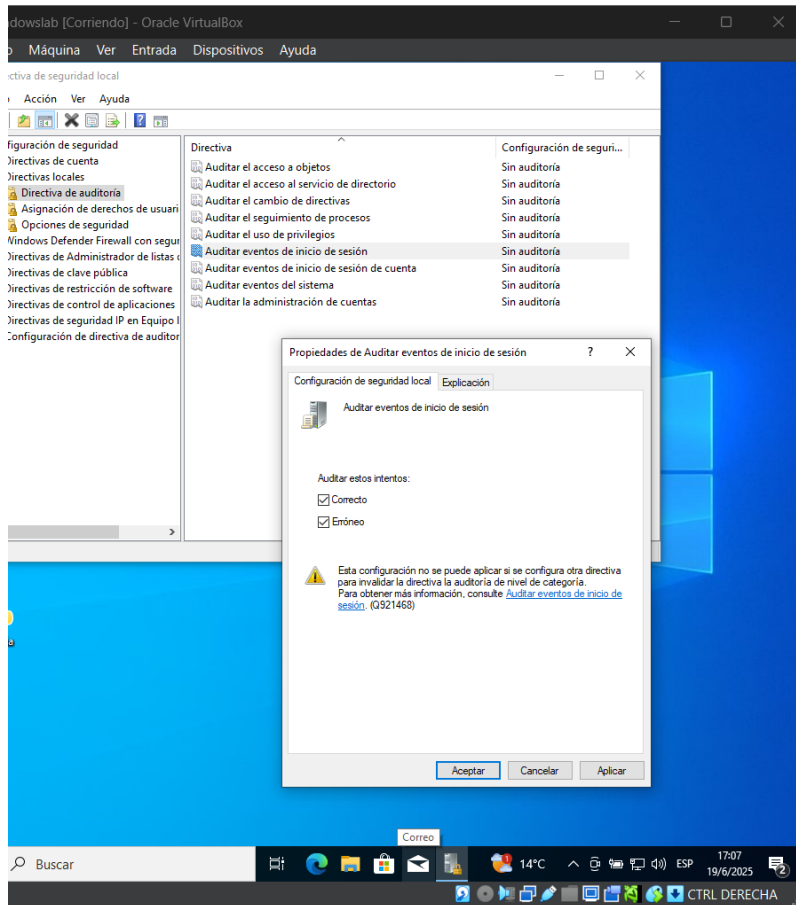


Laboratorio 4: Seguridad del sistema

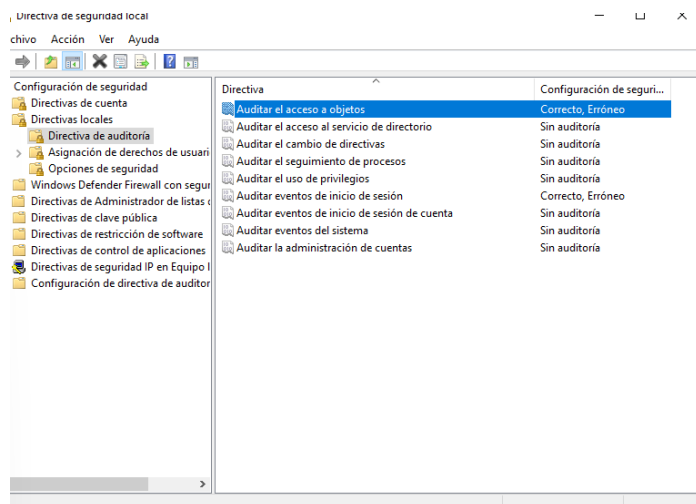
Auditoria de Seguridad

Para llegar mas rápido a las directiva locales, WIN+R, y en la ventana ejecutar gpedid.msc

Observación: se debe ejecutar como administrador

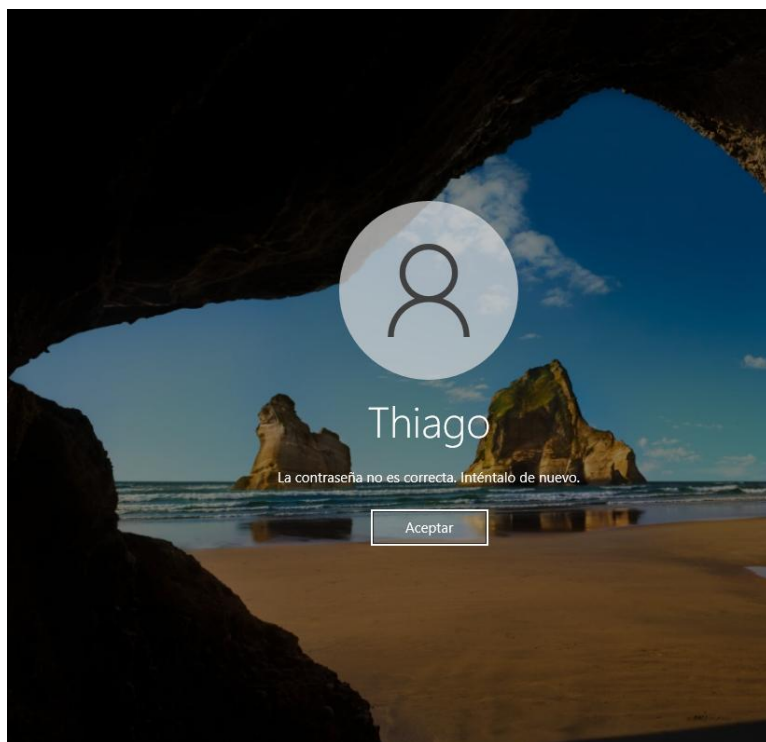


Nos dirigimos a directivas locales, directivas de auditoria, le damos a auditar eventos de inicio de sesión, marcamos las casillas, de correcto y erroneo, aplicamos. Lo mismo aplicamos auditar el acceso a objetos



INICIO DE SESION

Cerramos sesión y hacemos de forma intencional poniendo la contraseña mal



Como podemos visualizar, no aparece el mensaje “La contraseña no es correcta. Inténtalo de nuevo”

Lo realizamos dos veces, y luego ponemos bien la contraseña

Nos dirigimos a visor de eventos, llegamos de manera rápida, WIN+R seecpol.msc

Registro de Windows, Seguridad y se muestra esta tabla donde vemos los diferentes id de auditoria

Archivo Acción Ver Ayuda

visor de eventos (local)

- Vistas personalizadas
- Registros de Windows
 - Aplicación
 - Seguridad
 - Instalación
 - Sistema
 - Eventos reenviados
- Registros de aplicaciones y suscripciones

Seguridad Número de eventos: 4,776 (1) Nuevos eventos disponibles

Palabra...	Fecha y hora	Origen	Id. del ...	Catego...
Audi...	19/6/2025 17:08:53	Micros...	4656	SAM
Audi...	19/6/2025 17:08:53	Micros...	4798	User A...
Audi...	19/6/2025 17:08:53	Micros...	4658	Other ...
Audi...	19/6/2025 17:08:53	Micros...	4658	Other ...
Audi...	19/6/2025 17:08:53	Micros...	4656	SAM
Audi...	19/6/2025 17:08:53	Micros...	4656	SAM
Audi...	19/6/2025 17:08:53	Micros...	4658	Other ...
Audi...	19/6/2025 17:08:53	Micros...	4658	Other ...
Audi...	19/6/2025 17:08:53	Micros...	4656	SAM
Audi...	19/6/2025 17:08:53	Micros...	4656	SAM
Audi...	19/6/2025 17:08:53	Micros...	4658	Other ...
Audi...	19/6/2025 17:08:53	Micros...	4658	Other ...
Audi...	19/6/2025 17:08:53	Micros...	4656	SAM
Audi...	19/6/2025 17:08:53	Micros...	4672	Special...
Audi...	19/6/2025 17:08:53	Micros...	4672	Special...
Audi...	19/6/2025 17:08:53	Micros...	4627	Group ...
Audi...	19/6/2025 17:08:53	Micros...	4624	Logon
Audi...	19/6/2025 17:08:53	Micros...	4627	Group ...
Audi...	19/6/2025 17:08:53	Micros...	4624	Logon
Audi...	19/6/2025 17:08:53	Micros...	4648	Logon
Audi...	19/6/2025 17:08:53	Micros...	4627	Group ...

Evento 4648, Microsoft Windows security auditing.

General Detalles

Se intentó iniciar sesión con credenciales explícitas.

Nombre de registro: Seguridad

Origen: Microsoft Windows security Registrado: 19/6/2025 17:08:53

Id. del: 4648 Categoría de tarea: Logon

Nivel: Información Palabras clave: Auditoría correcta

Usuario: No disponible Equipo: DESKTOP-06UVE05

Código de operación: Información

Más información: [Ayuda Registro de eventos](#)

Acciones

- Seguridad
- Abrir registro guard...
- Crear vista personali...
- Importar vista perso...
- Vaciar registro...
- Filtrar registro actual...
- Propiedades
- Buscar...
- Guardar todos los ev...
- Adjuntar tarea a este...
- Ver
- Actualizar
- Ayuda
- Evento 4648, Microsoft ...
- Propiedades de eve...
- Adjuntar tarea a este...
- Copiar
- Guardar eventos sel...
- Actualizar
- Ayuda

visor de eventos

Archivo Acción Ver Ayuda

visor de eventos (local)

- Vistas personalizadas
- Registros de Windows
 - Aplicación
 - Seguridad
 - Instalación
 - Sistema
 - Eventos reenviados
- Registros de aplicaciones y suscripciones

Seguridad Número de eventos: 4,776 (1) Nuevos eventos disponibles

Palabra...	Fecha y hora	Origen	Id. del ...	Catego...
Audi...	19/6/2025 17:10:26	Micros...	4658	Other ...
Audi...	19/6/2025 17:10:26	Micros...	4658	Other ...
Audi...	19/6/2025 17:10:26	Micros...	4656	SAM
Audi...	19/6/2025 17:10:26	Micros...	4656	SAM
Audi...	19/6/2025 17:10:26	Micros...	4656	SAM
Audi...	19/6/2025 17:10:26	Micros...	4658	Other ...
Audi...	19/6/2025 17:10:26	Micros...	4658	Other ...
Audi...	19/6/2025 17:10:26	Micros...	4656	SAM
Audi...	19/6/2025 17:10:26	Micros...	4656	SAM
Audi...	19/6/2025 17:10:26	Micros...	4656	SAM
Audi...	19/6/2025 17:10:24	Micros...	5379	User A...
Audi...	19/6/2025 17:10:24	Micros...	5379	User A...
Audi...	19/6/2025 17:10:24	Micros...	5379	User A...
Audi...	19/6/2025 17:10:24	Micros...	5379	User A...
Audi...	19/6/2025 17:10:24	Micros...	5379	User A...
Audi...	19/6/2025 17:10:24	Micros...	5379	User A...
Audi...	19/6/2025 17:10:24	Micros...	4672	Special...
Audi...	19/6/2025 17:10:24	Micros...	4627	Group ...
Audi...	19/6/2025 17:10:24	Micros...	4624	Logon
Error...	19/6/2025 17:10:24	Micros...	4656	File Sys...

Evento 4624, Microsoft Windows security auditing.

General Detalles

Se inició sesión correctamente en una cuenta.

Nombre de registro: Seguridad

Origen: Microsoft Windows security Registrado: 19/6/2025 17:10:24

Id. del: 4624 Categoría de tarea: Logon

Nivel: Información Palabras clave: Auditoría correcta

Usuario: No disponible Equipo: DESKTOP-06UVE05

Código de operación: Información

Más información: [Ayuda Registro de eventos](#)

Acciones

- Seguridad
- Abrir registro guard...
- Crear vista personali...
- Importar vista perso...
- Vaciar registro...
- Filtrar registro actual...
- Propiedades
- Buscar...
- Guardar todos los ev...
- Adjuntar tarea a este...
- Ver
- Actualizar
- Ayuda
- Evento 4624, Microsoft ...
- Propiedades de eve...
- Adjuntar tarea a este...
- Copiar
- Guardar eventos sel...
- Actualizar
- Ayuda

4624ID: Se inicio sesión correctamente

4648ID:Se intento iniciar sesión

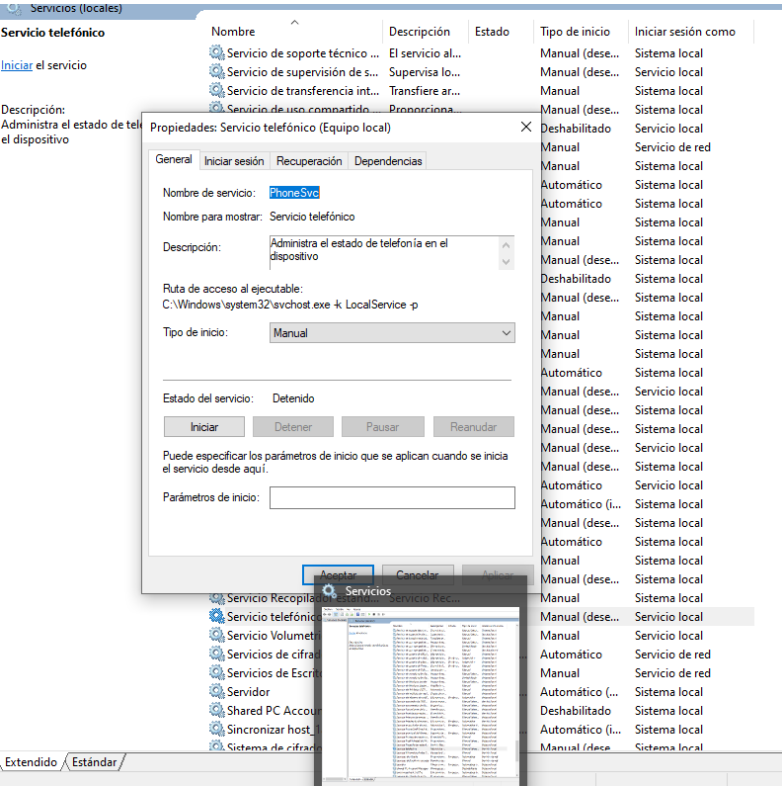
4625ID: Error de cuenta(primer intento fallido)

Análisis de vulnerabilidades

Desactivación de servicios innecesarios

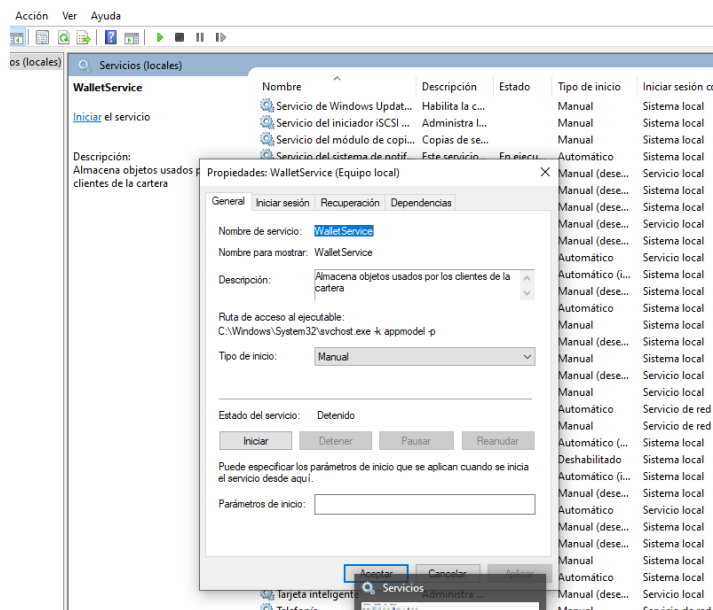
Buscamos el programa servicios de Windows

Encontramos el servicio de telefonía, procedemos a desactivarlo



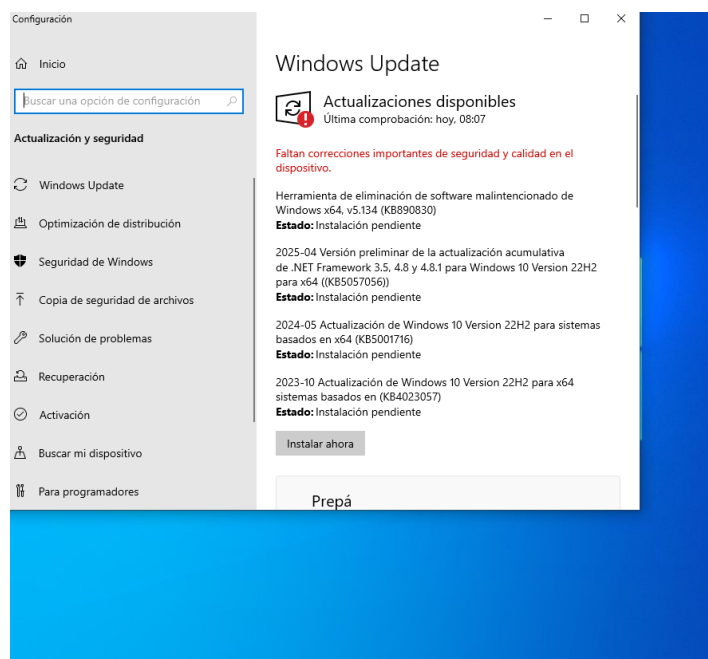
Servicio de telefonía: Proporciona la interfaz para realizar y recibir llamadas, enviar mensajes de texto y gestionar las opciones de configuración.

Procedemos a la desactivación



Wallet service: almacena de forma segura todos los datos que ya está acostumbrado a usar en Edge

Luego, en el buscador de Windows buscamos actualizaciones disponibles



Nos percatamos de que el sistema no está en su última versión y hay actualizaciones pendientes, le damos a instalar ahora. Para poder tener la última versión de nuestro sistema operativo.

Usamos además la herramienta de escaneo, del Microsoft, vemos que el resultado del escaneo nos dio el diagnostico que el sistema no tiene amenazas

Amenazas permitidas

Las amenazas permitidas son elementos identificados como amenazas, que permites que se ejecuten en el dispositivo.

¿Tienes alguna pregunta?

[Obtener ayuda](#)

No hay amenazas.

[Historial de protección](#)

Ayudar a mejorar la seguridad de Windows

[Envíanos tus comentarios](#)

Cambiar la configuración de privacidad

Consulta y cambia la configuración de privacidad del dispositivo Windows 10.

[Configuración de privacidad](#)

[Panel de privacidad](#)

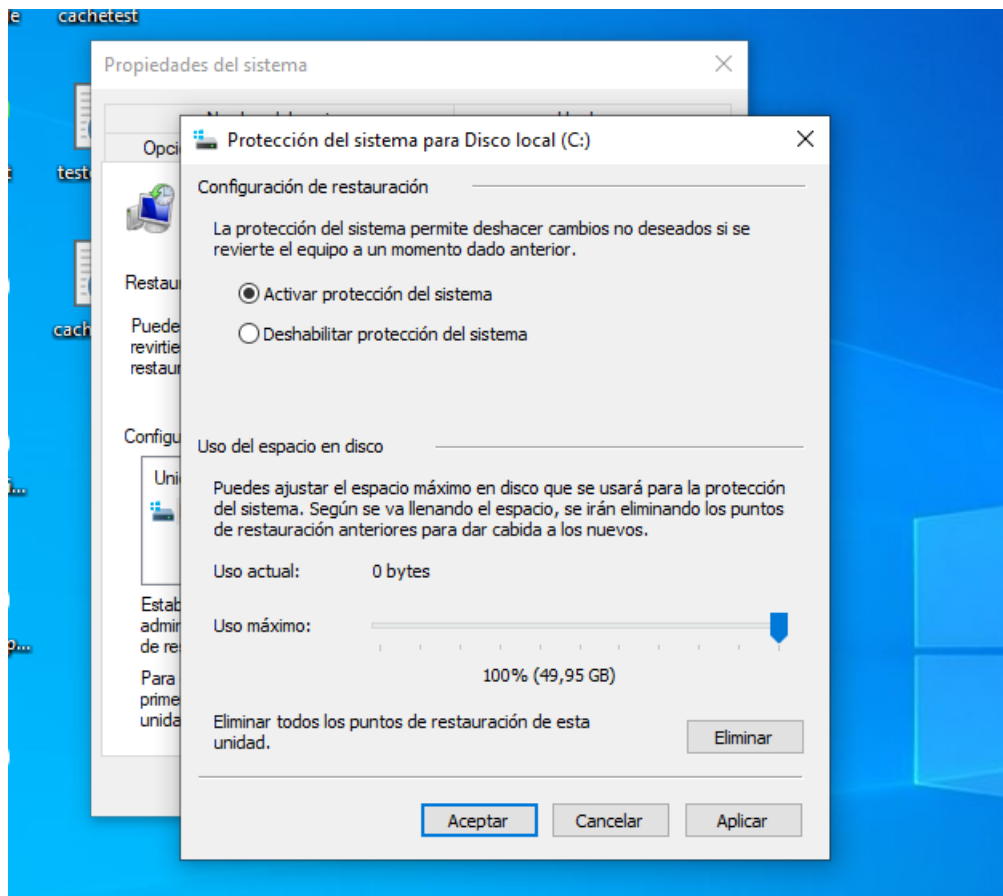
[Declaración de privacidad](#)

Respaldo y Recuperación

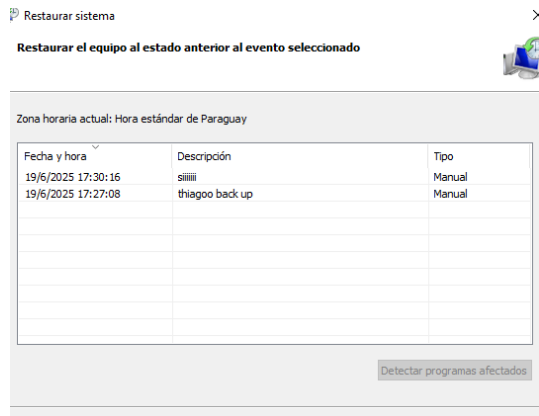
El respaldo y la recuperación de datos son estrategias y procedimientos para proteger la base de datos contra la pérdida de información y reconstruirla después de cualquier pérdida. Algunas mejores prácticas incluyen copias de seguridad periódicas y almacenamiento externo. Los beneficios incluyen protección contra virus y malware, y recuperación de datos eliminados accidentalmente

Primer paso buscamos en la barra de búsqueda de Windows crear punto de restauración

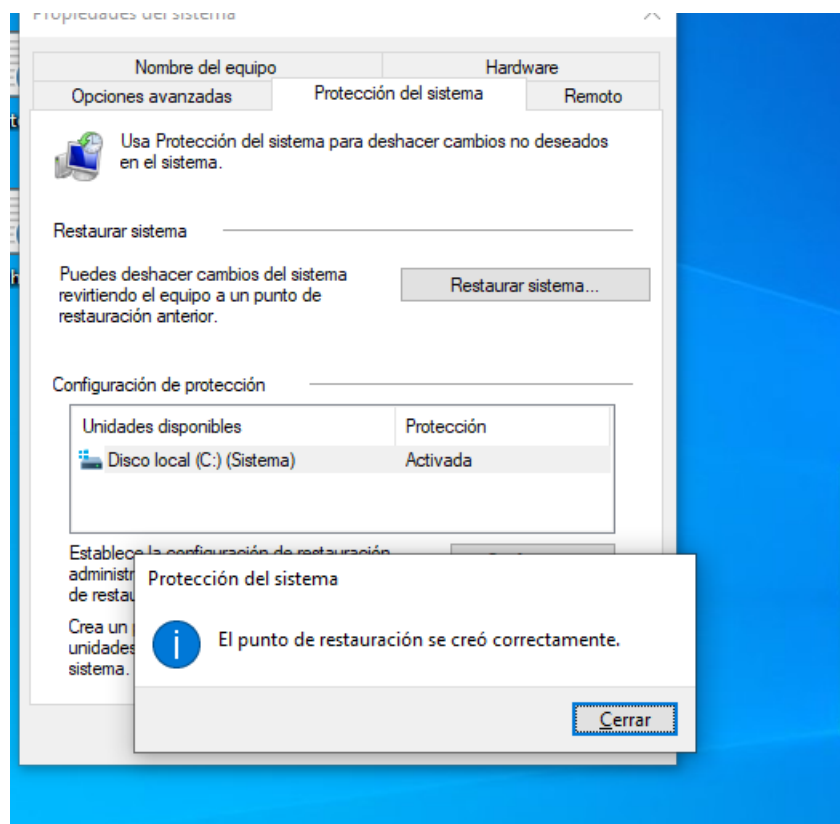
Tocamos la viñeta de protección del sistema



Le damos a la pestaña, de protección de sistema, le damos a la opción de activar el protección del sistema, le damos la cantidad que queremos respaldar aplicamos y aceptamos



Le damos un nombre, eso mismo nos muestra, que fecha queremos volver a la hora de restaurar el sistema, volverá todo a como era en ese momento de recuperación



Restauración y verificación

Se realizó la restauración del sistema, en el punto creado anteriormente. La acción fue exitosa, aproximadamente duró 15 minutos, el sistema volvió a su forma original sin pérdida de datos o archivos