

SEGURIDAD  
EMPRESAS  
**EDR**

**Claro**—  
empresas





## Contenido

**Introducción ..... 3**

**Bienvenido a Seguridad Empresas EDR ..... 3**

**Visión general del documento ..... 3**

**Acronis Cyber Protection ..... 4**

**Activación de la cuenta..... 4**

**Descargar agentes de cyber protection..... 7**

**Instalación de agentes .....10**

**Creación de un plan de protección con Seguridad Empresas EDR.....12**



# Introducción

## Bienvenido a Seguridad Empresas EDR

Cyber Protection es una solución de ciber protección todo en uno que integra la realización de copias de seguridad y recuperaciones, recuperación ante desastres, prevención del malware, controles de seguridad, asistencia remota, supervisión y creación de informes.

Protege toda su empresa y las compañías de sus clientes mediante un enfoque de protección por capas, una combinación innovadora de tecnologías de protección de datos proactivas, activas y reactivas.

- Las acciones proactivas, como la gestión de parches, la evaluación de vulnerabilidades o el análisis predictivo del estado de disco duro según tecnologías de aprendizaje automático, le permiten evitar todas las amenazas que afecten a sus equipos.
- Gracias a las acciones activas, como la protección antimalware o la autoprotección, puede detectar las amenazas que surjan.
- Las acciones reactivas, como las copias de seguridad y las recuperaciones (in situ y en la nube), así como la recuperación ante desastres (in situ y en la nube), le permiten actuar ante cualquier fallo.

Cyber Protection le ofrece un agente de protección, una consola de servicio sencilla de manejar y un plan de protección que abarca todos los aspectos relacionados con la seguridad y la protección de datos.

## Visión general del documento

Este documento consta de tres secciones:

- Cómo instalar el agente de Acronis Cyber Protect
- Cómo crear un plan de protección



# Acronis Cyber Protection

## Activación de la cuenta

Cuando el administrador le cree una cuenta, se le enviará un mensaje a su dirección de correo electrónico. El mensaje contiene la siguiente información:

- Sus credenciales de inicio de sesión. Este es el nombre de usuario que utiliza para iniciar sesión. Sus credenciales de inicio de sesión aparecen también en la página de activación de la cuenta.
- Enlace de activación. Asegúrese de que la contraseña tenga al menos nueve caracteres. Para obtener más información sobre la contraseña, consulte Requisitos de contraseña.

1. A su correo electrónico llegara mail de activación de la cuenta. Haga clic en el enlace de activación y establezca la contraseña de su cuenta.

Acronis Cyber Protect Cloud: Complete account activation



Este remitente es externo a la organización.

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

Haga clic aquí para descargar imágenes. Para ayudarle a proteger su confidencialidad, Outlook ha impedido la descarga automática de algunas imágenes en este mensaje.

Traducir mensaje a: Español | No traducir nunca del: Inglés | Preferencias de traducción

Responder | Responder a todos

### Complete account activation

Dear ,

Your Acronis Cyber Protect Cloud account was created.  
To activate it, click the **Complete activation** button below.

Login: AS  
Login URL: <https://acronis.clarobackup.com.ec>

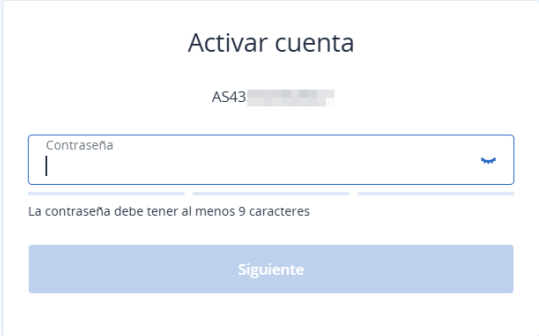
**Complete activation**

For future logins, visit <https://acronis.clarobackup.com.ec> and sign in with your new credentials.

**Tip:** Bookmark the link so it is easy to find next time.



2. Solicitará su nueva contraseña para la cuenta asignada.



Activar cuenta

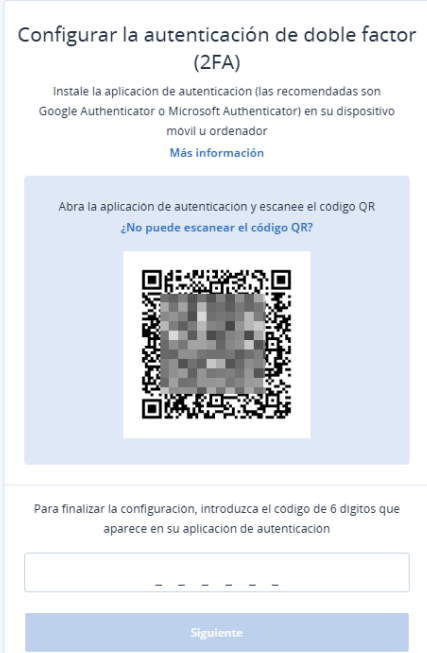
AS43 [redacted]

Contraseña

La contraseña debe tener al menos 9 caracteres

Siguiente

3. Posterior a la colocación de la contraseña, solicitará que se habilite el 2FA a la cuenta, proceda a escanear el código QR con su aplicación de Autenticación (Microsoft Authenticator o Google Authenticator)



Configurar la autenticación de doble factor (2FA)

Instale la aplicación de autenticación (las recomendadas son Google Authenticator o Microsoft Authenticator) en su dispositivo móvil u ordenador

[Más información](#)

Abra la aplicación de autenticación y escanee el código QR

¿No puede escanear el código QR?



Para finalizar la configuración, introduzca el código de 6 dígitos que aparece en su aplicación de autenticación

-----

Siguiente

[Seleccionar otro usuario](#)

#### 4. Le solicitara guardar las instrucciones de recuperación de 2FA

### Guardar las instrucciones de recuperación de 2FA

Iniciar sesión: AS43 [REDACTED]

Si pierde su dispositivo de autenticación, siga estos pasos para restaurar el acceso a su cuenta.

1. Instale una aplicación de autenticación en su dispositivo móvil u ordenador. Se recomienda Google Authenticator o Microsoft Authenticator.
2. Abra la aplicación de autenticación e introduzca el siguiente código de 32 dígitos para conectar la aplicación a su cuenta.

SPC [REDACTED]

Ahora puede usar el código de 2FA de 6 dígitos generado en la aplicación de autenticación para iniciar sesión en su cuenta.

[Guardar las instrucciones como PDF](#)

[Continuar sin guardar](#)

#### 5. Se le solicitara aceptar los términos y condiciones del producto

### Términos legales

Haga clic en "Aceptar" para confirmar que entiende y acepta los términos y condiciones.

☐ Acuerdo de licencia para el usuario final [Mas informacion](#)

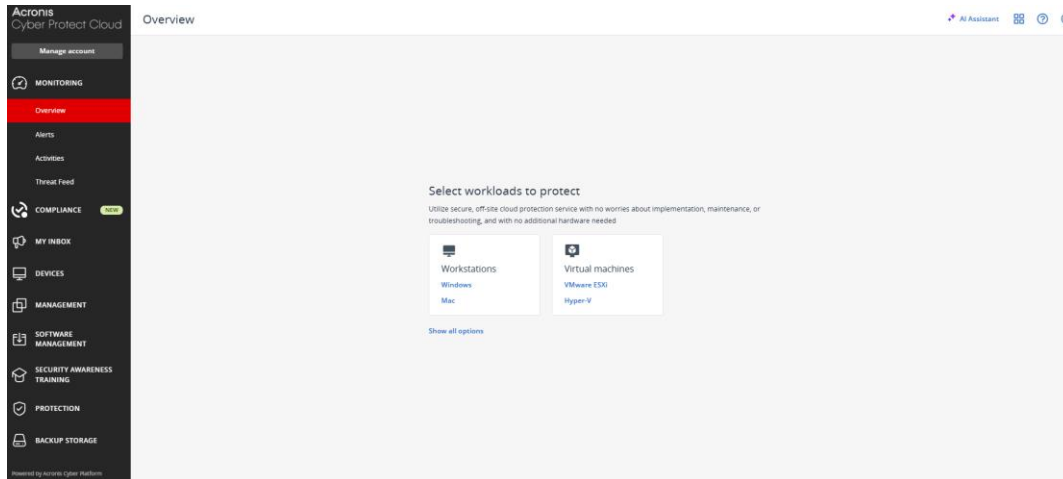
☐ Declaracion de privacidad [Mas informacion](#)

[Aceptar](#)

[Seleccionar otro usuario](#)

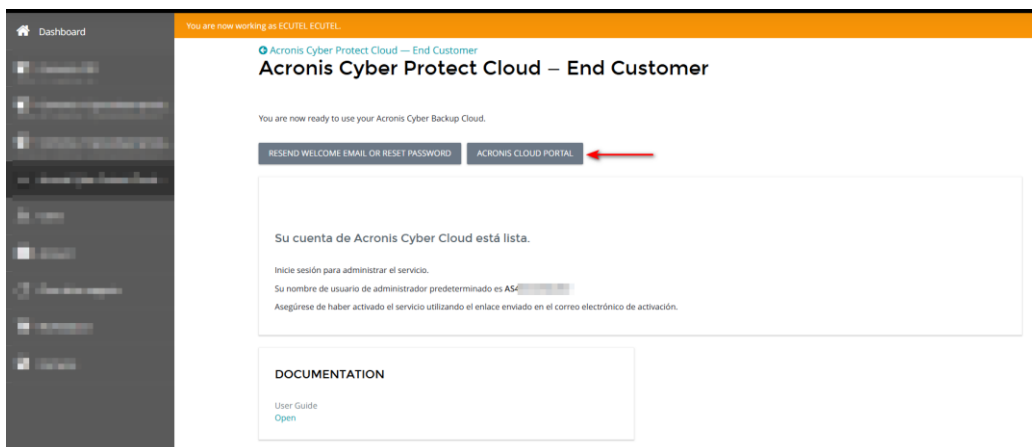
## 6. Ya su cuenta se encuentra Activada y lista para usar

**Importante:** Usará esta contraseña para registrar dispositivos más tarde.



## Descargar agentes de cyber protection

### 1. Inicie sesión en el portal de Claro Cloud y seleccionamos el producto que se adquirió.



## 2. Nos solicitara la contraseña de la cuenta previamente creada y activada



Introducir contraseña

< AS43

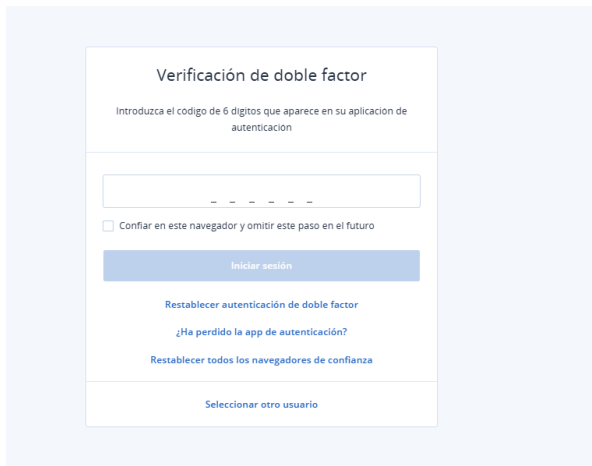
Contraseña

Siguiete

[¿Olvidó su contraseña?](#)

[Seleccionar otro usuario](#)

## 3. Ingresamos el código de nuestra aplicación de Autenticador



Verificación de doble factor

Introduzca el código de 6 dígitos que aparece en su aplicación de autenticación

— — — — —

☐ Confiar en este navegador y omitir este paso en el futuro

Iniciar sesión

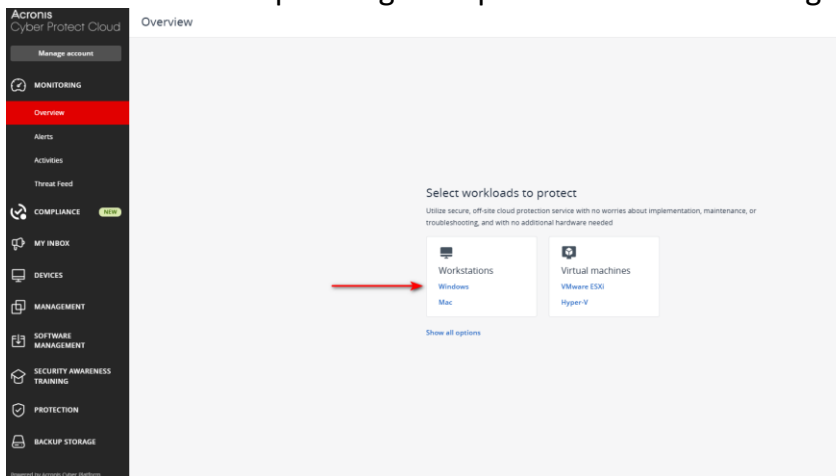
[Restablecer autenticación de doble factor](#)

[¿Ha perdido la app de autenticación?](#)

[Restablecer todos los navegadores de confianza](#)

[Seleccionar otro usuario](#)

## 4. Seleccionamos el tipo de agente que necesitamos descargar







5. Una vez descargado aparecerá esta ventana con los pasos indicados

Add Windows machine

×

1. Downloading

You are downloading the cyber protection agent installer. If your download has not started, [click here](#).



2. Installation

Run the installer on your Windows machine.



3. Protection

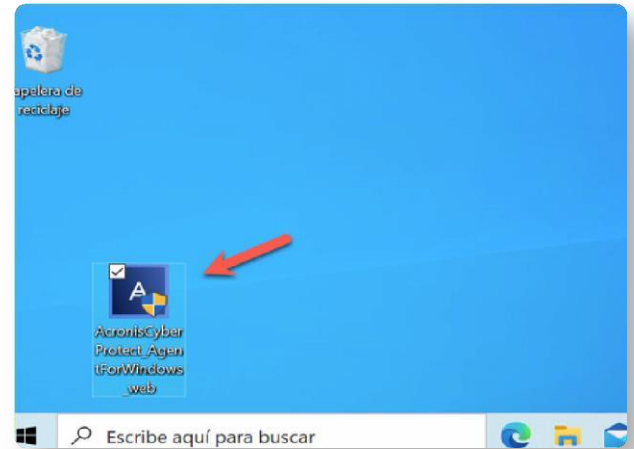
Once the installation is complete, enable protection plans on the taskbar or in the web interface.



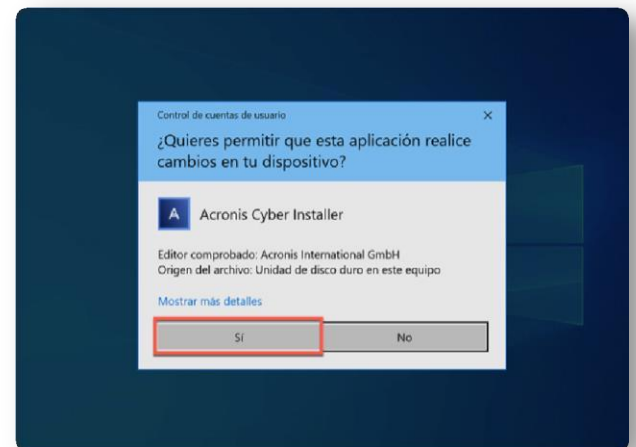


## Instalación de agentes

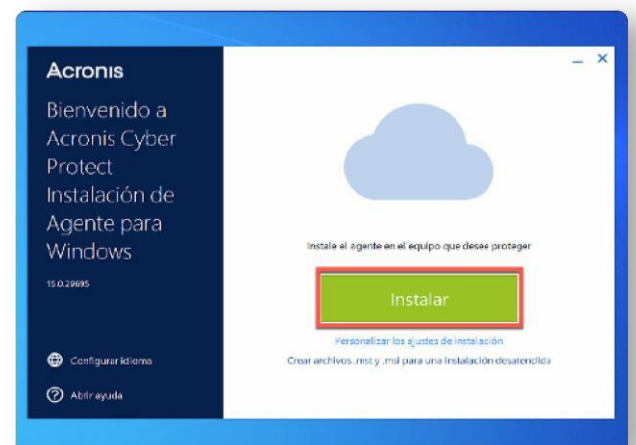
1. Asegúrese de que el equipo está conectado a Internet.
2. Inicie sesión como administrador e inicie el programa de instalación descargado previamente.



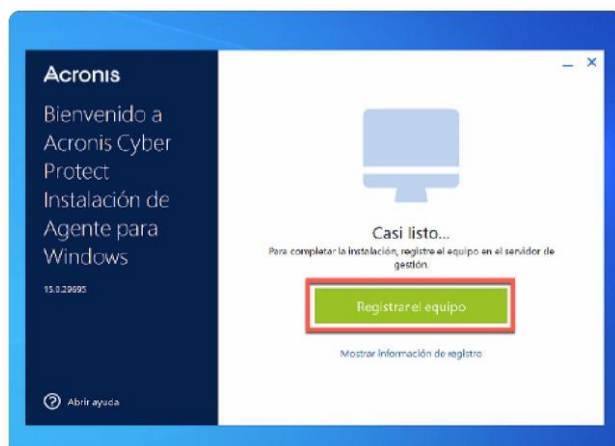
3. Haga click en **Sí**.



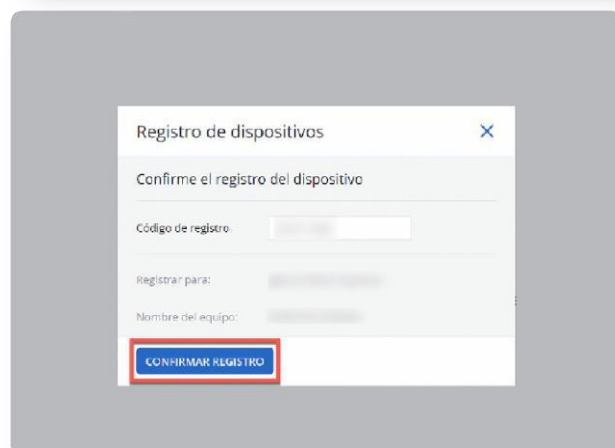
4. Haga clic en **Instalar** y espere que termine la instalación.



- Haga clic en **Registrar el equipo**. En la ventana del explorador que se abrirá, inicie sesión en la consola de servicio. Use la contraseña creada previamente en la página 7.



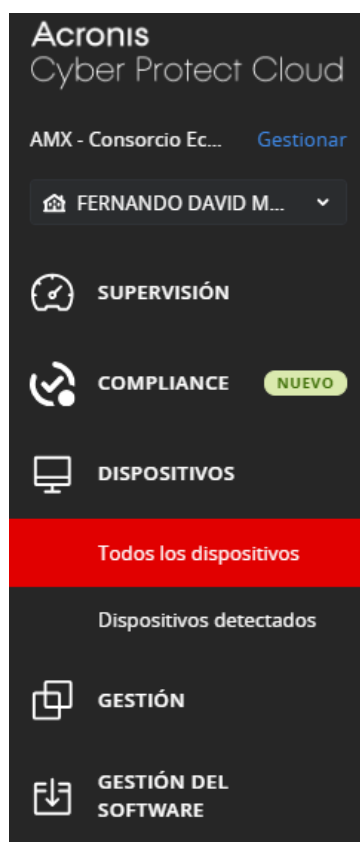
- Revise los detalles de registro y haga clic en **Confirmar registro**.



## Creación de un plan de protección con Seguridad Empresas EDR

Seguridad Empresas EDR ayuda a mantener sus dispositivos seguros bloqueando virus, ransomware y otras amenazas antes de que causen daño. Si ocurre algo sospechoso, rápidamente muestra qué salió mal y le permite solucionarlo con un solo clic, incluso restaurando su sistema a un estado limpio.

1. En la consola de Claro Backup, vaya a **Dispositivos > Todos los dispositivos**.





2. Seleccione el dispositivo que desea proteger.
3. En el menú **Acciones**, haga clic en **Proteger**.



4. [Si ya hay planes aplicados] Haga clic en **Agregar plan**.
5. Haga clic en **Crear plan > Protección**.  
Haga clic en **Crear plan** y, a continuación, en **Protección**.



6. [Opcional] Para cambiar el nombre del plan de protección, haga clic en el icono del lápiz y luego introduzca el nuevo nombre.
7. En la barra lateral del plan de protección, active el interruptor de **Seguridad Empresas EDR**.

New protection plan [✎](#) Cancel Save

---

**Backup** 🔴 [>](#)  
Entire machine to Cloud storage, Monday to Friday at 13:00 (Always incremental)

---

**Endpoint Detection and Response (EDR)** 📶 🔴 [>](#)  
Enabled

---

**Antivirus & Antimalware protection** 🔴 [>](#)  
Self-protection on, Real-time protection on

---

**URL filtering** 📶 🔴 [>](#)  
0 denied, 44 allowed

---

**Microsoft Defender Antivirus** 📶 🔴 [>](#)  
Full scan, Real-time protection on, at 12:00, only on Friday

8. En el cuadro de diálogo, haga clic en **Habilitar**.

## Endpoint Detection and Response



Endpoint Detection and Response (EDR) detects suspicious or malicious activity on the workload, generating incidents upon detection. When enabling EDR, we also recommend you enable the modules listed below to ensure the best possible detection coverage.

- ☒ Antivirus & Antimalware protection ⓘ
  - ☒ Real-time protection ⓘ
  - ☒ Behavior engine ⓘ
  - ☒ Exploit prevention ⓘ
  - ☒ Potentially unwanted application ⓘ
  - ☒ Active Protection ⓘ
  - ☒ Network folder protection ⓘ
  - ☒ Cryptomining process detection ⓘ
- ☒ URL Filtering ⓘ
- ☐ Microsoft Defender Antivirus ⓘ

CancelEnable

**¡Todo está listo!**



Todo se Conecta