

Laboratorio - 8: ¿Cómo crear Directivas en Intune?

Objetivo: El objetivo de este laboratorio es crear:

- 1. Directiva de cumplimiento en Intune.**
- 2. Perfiles de Configuración.**
- 3. Seguridad de dispositivo.**

Las Directivas que tenemos disponibles en el centro de administración de Endpoint Manager no sólo nos ayudan a **gestionar** diferentes tipos de dispositivos, tanto propiedad de la empresa como **dispositivos personales, tabletas y dispositivos con/sin usuarios**.

La forma más fácil de trabajar con estas directivas es crearlas y administralas en función de la plataforma que queramos gestionar.

Laboratorio – 8.1: Política de cumplimiento en Endpoint Protection Manager.

Objetivo: El objetivo de este laboratorio es. crear una: **Política de cumplimiento**.

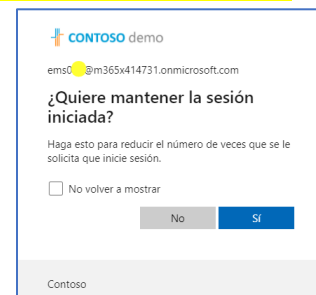
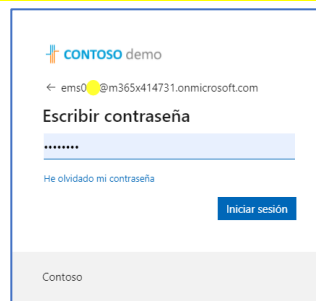
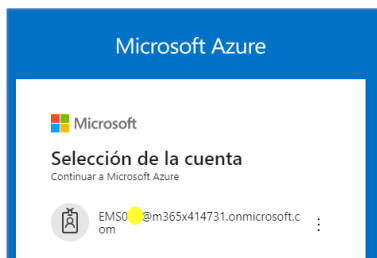
Las políticas de cumplimiento nos permiten especificar cuáles son los requerimientos mínimos que tienen que cumplir los dispositivos de nuestra empresa e informarnos de cuales no lo están cumpliendo para poder tomar medidas correctoras sobre ellos. En este **laboratorio**, nos ceñiremos a dispositivos móviles **iOS (Apple)**.

Prerrequisito: EMS Enterprise Mobility + Security E5.

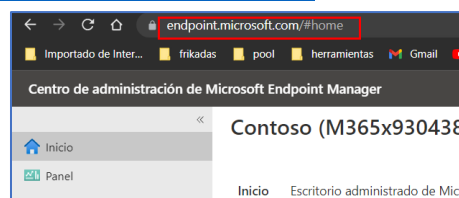
1. Logarnos con nuestras credenciales de admin al **Centro de administración de Microsoft Endpoint Manager**: <https://endpoint.microsoft.com/>.

Usuario: EMS0x@m365*****.onmicrosoft.com (la “x” es el usuario que os hemos dado al comienzo del curso).

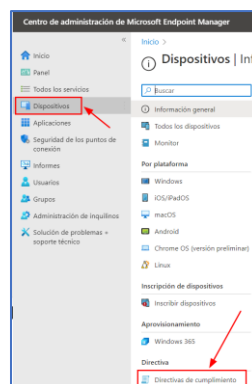
Contraseña: HolaMundo01 (o la contraseña que hayas puesto cuando el sistema te obligó a cambiarla)



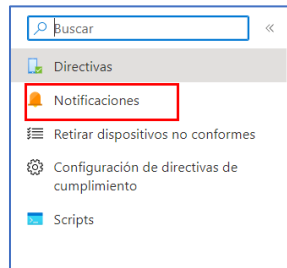
2. Aparecerá el **Centro de administración de Microsoft Endpoint Manager**, consola de gestión donde se ha integrado Intune. <https://endpoint.microsoft.com/>



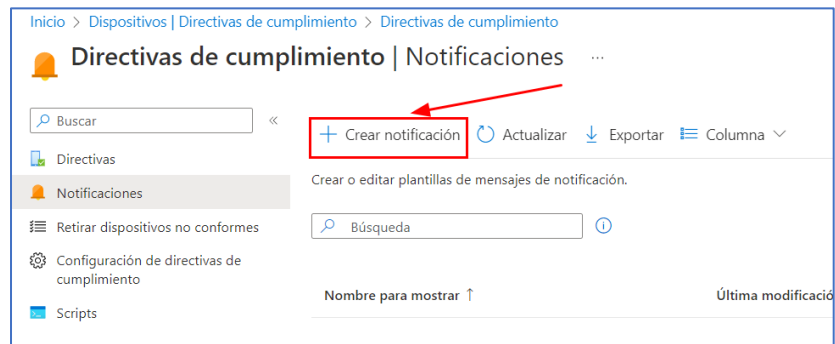
3. **Clic en Dispositivos** y después clic en la *sección Directiva* en la entrada **Directivas de cumplimiento**.



4. **Clic en la entrada del menú vertical: Notificaciones.** lo primero que nos vamos a crear es una **Plantillas de mensaje de notificación**. Para poder **enviar mensajes/notificaciones** tanto vía **email** como **notificaciones Push** a los **usuarios finales** los cuales sus dispositivos no tengan sus dispositivos en cumplimiento, como a **otros destinatarios adicionales**.



5. **Clic en el botón superior de la barra horizontal + Crear notificación.** Para crearnos una nueva.



6. **Aparecerá** en una nueva ventana el asistente de configuración de notificaciones. Este, está dividido en 2 pestaña: *Básico y Revisar y crear*.

a. En la **primera pestaña: Básico**. Tendremos que **rellenar** los **campos correspondientes** a la **notificación** que **recibirán nuestros usuarios**.

- Nombre: **NO conformidad GENERAL-EMSOx** (la "x" corresponde al nº de tu usuario admin).
- Encabezado de correo electrónico: incluir logotipo de la empresa. **Habilitar**.
- Pie de página de correo electrónico: incluir nombre de la empresa. **Habilitar**.
- Pie de página de correo electrónico: incluir información de contacto. **Habilitar**.
- Company Portal Website Link. **Deshabilitar**.

Clic en el botón: Siguiente para pasar a la **siguiente pestaña**.

b. En la **segunda pestaña: Plantilla de mensaje de notificación**: No cumplimiento normativo.

- Campo vertical Configuración re...**: En el desplegable seleccionar Español (España).
- Campo vertical Asunto**: Incumplimiento legal.
- Campo vertical Mensaje**: Copiar y pegar este texto o inventarnos el que nos parezca.
*Hola. Acabas de recibir este email porque no estás en cumplimiento con las normas especificadas en correos anteriores. Póngase en contacto con su responsable para solucionarlo o en un plazo de tiempo NO se le permitirá el acceso.
La empresa.*

iv. **Campo vertical Predeterminado**: **Clic en la casilla de selección**.

Clic en el botón Siguiente en la parte inferior izquierda de la ventana.

c. En la **tercera pestaña: Revisar y crear**. Clic en el **botón Crear**.

Inicio > Dispositivos | Directivas de cumplimiento > Directivas de cumplimiento | Notificaciones >

Crear notificación ...

✓ Básico ✓ Plantillas de mensaje de notificación 1 Revisar y crear

Resumen

Básico

Nombre NO conformidad GENERAL-EM509

Encabezado de correo electrónico: incluir logotipo de la empresa Habilitar

Pie de página de correo electrónico: incluir nombre de la empresa Habilitar

Pie de página de correo electrónico: incluir información de contacto Habilitar

Vínculo del sitio web de Portal de empresa Deshabilitar

Plantillas de mensaje de notificación

Configuración regio...	Asunto	Mensaje	Predeterminado
Español (España)	Incumplimiento legal	Hola. Acabas de recibir este email porque no e... true	

Anterior **Crear**

7. Clic en la entrada del menú vertical **Directivas**. Clic en el **botón + Crear Directiva**.

Inicio > Dispositivos | Directivas de cumplimiento >

Directivas de cumplimiento | Directivas ...

Buscar << + Crear directiva Actualizar Exportar

Directivas

Notificaciones

Retirar dispositivos no conformes

Configuración de directivas de

Nombre de directiva

8. Nos aparecerá el **asistente de creación de directiva de cumplimiento**. Dividida en pestañas

a. **Rellenamos los detalles**, como el **nombre** y la **descripción**.

i. **Clic en iOS/iPadOS** como **Plataforma** y **Clic en el botón Crear**.

Crear una directiva ×

Plataforma

iOS/iPadOS

Tipo de perfil

Directiva de cumplimiento de iOS

Crear

b. Aparecerá la **primera pestaña** de la ventana del **Asistente de configuración: Básico**.

- i. **Nombre:** Directiva cumplimiento para iPhone/iPad-EMSOx (la "x" corresponde al nº de tu usuario admin).
- ii. **Descripción:** La dejamos en blanco.
- iii. **Plataforma:** Ya le hemos elegido, aparece sombreada y no podemos tocar.
- iv. **Tipo de perfil:** Ya lo hemos elegido, aparece sombreada y no podemos tocar.

v. **Clic en el botón** de la parte inferior de la pantalla: **Siguiente**.

c. **Segunda pestaña. Configuración de cumplimiento:**

- i. **Clic en el desplegable Seguridad del sistema.** Cambiar el valor del **deslizable Contraseña: Requerir**.

- ii. En la **sección: Inscripción de dispositivos e inscripción de dispositivos automatizada**. Podremos también, **configurar** las **opciones por defecto** que se **aplicarán** cuando se produzca la **inscripción vía Intune** e inscritos vía *Apple School Manager* o *Apple Business Manager*:

1. **Contraseñas sencillas.**
2. **Longitud mínima de la contraseña.**
3. **Tipo de contraseña requerida.**
4. **Número de caracteres no alfanuméricos en la contraseña.**

5. **Máximo de minutos tras bloqueo de pantalla antes de solicitar la contraseña.**
6. **Máximo de minutos de inactividad hasta que se bloquea la pantalla.**
7. **Expiración de la contraseña (días).**
8. **Número de contraseñas anteriores que no se pueden utilizar.**

Inicio > Dispositivos | Directivas de cumplimiento > Directivas de cumplimiento | Directivas >

Directiva de cumplimiento de iOS

iOS/iPadOS

desbloquear dispositivos móviles ⓘ

Inscripción de dispositivos e inscripción de dispositivos automatizada

Esta configuración funciona para los dispositivos que se inscribieron en Intune a través de la inscripción de dispositivos y para los dispositivos inscritos con Apple School Manager o Apple Business Manager con inscripción automatizada de dispositivos (anteriormente DEP).

Contraseñas sencillas ⓘ Bloquear Sin configurar

Longitud mínima de la contraseña ⓘ Especificar un número (de 4 a 14)

Tipo de contraseña requerida ⓘ Sin configurar

Número de caracteres no alfanuméricos en la contraseña ⓘ Sin configurar

Máximo de minutos tras bloqueo de pantalla antes de solicitar la contraseña ⓘ Sin configurar

Máximo de minutos de inactividad hasta que se bloquea la pantalla ⓘ Sin configurar

Expiración de la contraseña (días) ⓘ Especificar el número de días (de 1 a 65535)

Número de contraseñas anteriores que no se pueden reutilizar ⓘ Especificar un número (de 1 a 24)

- iii. En la **sección: Seguridad del dispositivo**. En la parte: **Aplicaciones restringidas**. Al no tener configurada la conexión con otros MDMs (Apple o Google Business) NO tendremos ninguna App restringida por defecto.

- iv. **Clic en el botón** de la parte inferior de la pantalla **Siguiente**.

Seguridad del dispositivo

Aplicaciones restringidas ⓘ Exportar

Nombre de aplicación Identificación de lote de aplicaciones

Anterior **Siguiente**

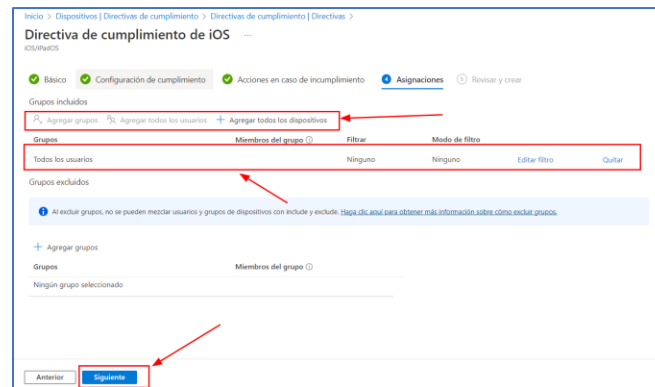
- d. **Tercera pestaña: Acciones en caso de incumplimiento.** Que pasará cuando no se cumplan la directiva de cumplimiento para la plataforma iOS.
- En la columna: Acción.** En del desplegable seleccionamos. **Enviar correo electrónico a usuario final.**
 - En la columna: Programar (días después del no cumplimiento).** Escribimos "1".

- En la columna: Plantilla de mensaje.** Clic en el enlace: **No se ha seleccionado ninguno.**

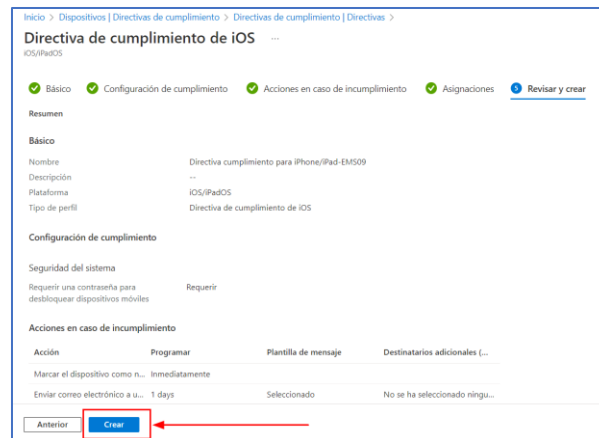
En la ventana lateral que aparecerá. Clic en el nombre de la notificación que nos creamos en el punto anterior y clic en el botón Seleccionar.

- En la columna: Destinatarios adicional... . NO haremos nada más.**
- Clic en el botón: Siguiente.**

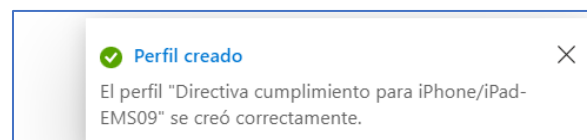
- e. **Cuarta pestaña: Asignaciones.** Esta pestaña está dividida en 2 partes.
- Grupos incluidos.** En el **desplegable asignar a:** **Clic** en el enlace **+ Seleccionar grupos a incluir** en la **sección Grupos incluidos** y **seleccionamos** el **grupo** de usuarios que **tenemos: EMS0** (la “x” corresponde al usuario que os hemos facilitado al comienzo del curso) o como en nuestro caso, **hemos elegido a todos los usuarios:** **Clic** en el botón **seleccionar** para volver a la ventana de configuración primaria.
 - Grupos excluidos.** **NO** seleccionamos ningún grupo desde el enlace **“Seleccionar grupos para excluir”**.
 - Clic** en el **botón Siguiente**. Para continuar con la siguiente pestaña.



- f. **Quinta pestaña: Revisar y crear.** Comprobamos las opciones que hemos seleccionado en las anteriores pestañas. **Clic** en el **botón Crear**.



9. Ahora podemos **ver** que se ha **creado el Perfil creado** y que también **aparecerá una notificación**.



Laboratorio – 8.2: Política de configuración del dispositivo.

Objetivo: El objetivo de este laboratorio es crear una: **Política de configuración del dispositivo**.

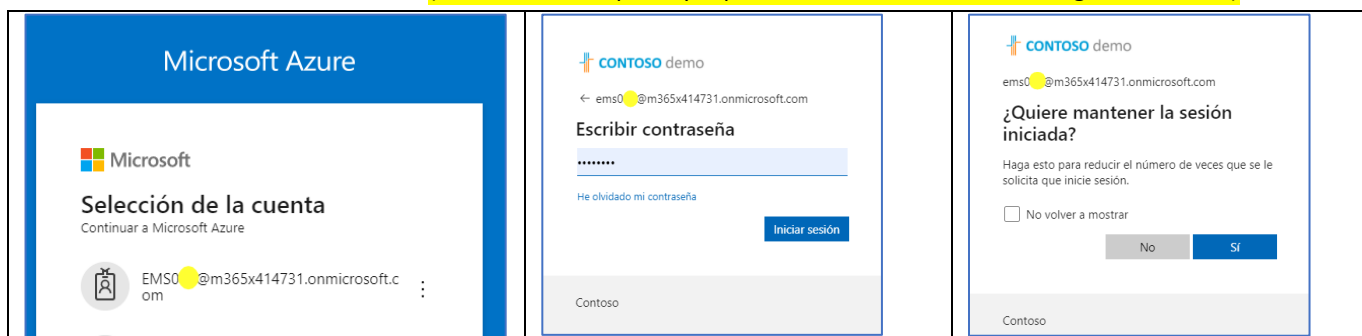
Las **políticas de configuración de dispositivos** nos **permiten** tanto **restringir** determinados **programas - funcionalidades** en los **dispositivos** como realizar la **administración** de estos, **asignándoles**, por ejemplo, la **WIFI** corporativa que deben utilizar, etc. Para este **laboratorio**, nos ceñiremos a la **plataforma: Windows 10**.

Prerrequisito: EMS Enterprise Mobility + Security E5.

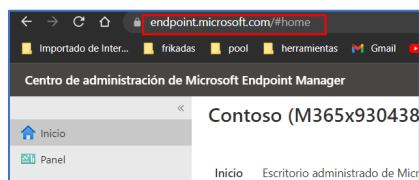
1. Logarnos con nuestras credenciales de admin al **Centro de administración de Microsoft Endpoint Manager**: <https://endpoint.microsoft.com/>.

Usuario: EMS0x@m365*****.onmicrosoft.com (la “x” es el usuario que os hemos dado al comienzo del curso).

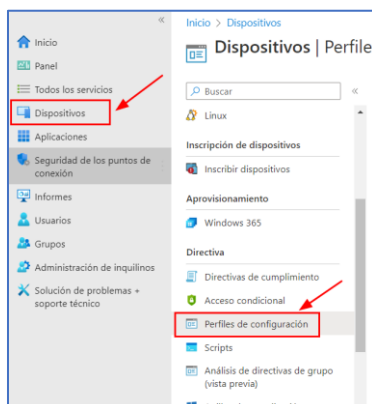
Contraseña: HolaMundo01 (o la contraseña que hayas puesto cuando el sistema te obligó a cambiarla)



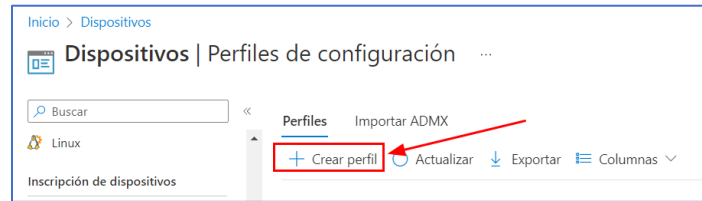
2. Aparecerá el **Centro de administración de Microsoft Endpoint Manager**, consola de gestión donde se ha integrado Intune. <https://endpoint.microsoft.com/>



3. Clic en **Dispositivos** y después clic en la **sección Directiva** en la **entrada: Perfiles de configuración**.

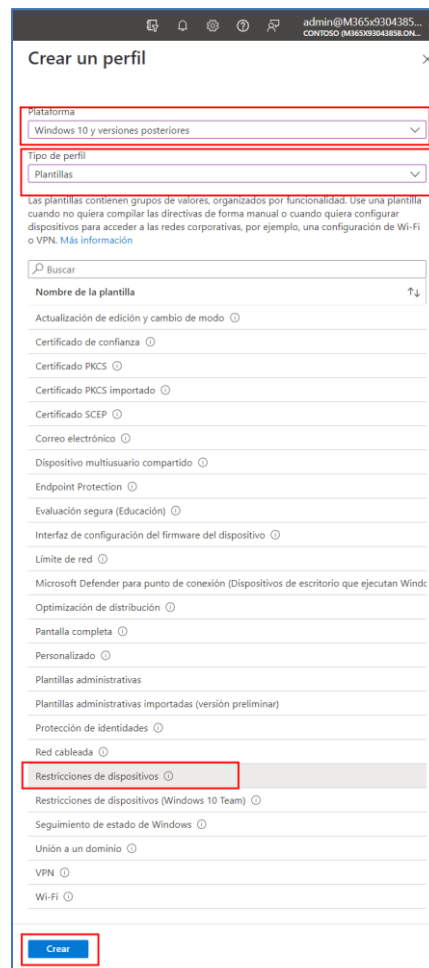


4. Clic en el **botón + Crear perfil**.



5. Aparecerá una nueva ventana donde podremos **seleccionar** tanto la **plataforma** como el **tipo de perfil** que vamos a aplicar. **CASO DE USO:** Vamos a crear un **perfil** de **MUY restrictivo** para los **equipos de sobremesa** de nuestra **empresa**, en el cual, vamos a intentar **evitar desconfiguraciones** por parte de los usuarios y vamos a **restringir al máximo** las **opciones disponibles** en sus equipos Windows 10. Nos crearemos, por tanto, un **perfil** de tipo **Restricciones de dispositivos**.

- En el *primer desplegable*: **Plataforma:** Clic en **Windows 10 y versiones posteriores**.
 - En el *segundo desplegable*: **Tipo de Perfil.** Plantillas.
 - En el *tercer desplegable*: **Clic en Restricciones de dispositivos.**
- Una vez seleccionados estas *desplegables*, clic en el **botón Crear**.



¿Cuáles son las plataformas a las que podemos establecer restricciones de dispositivos?:

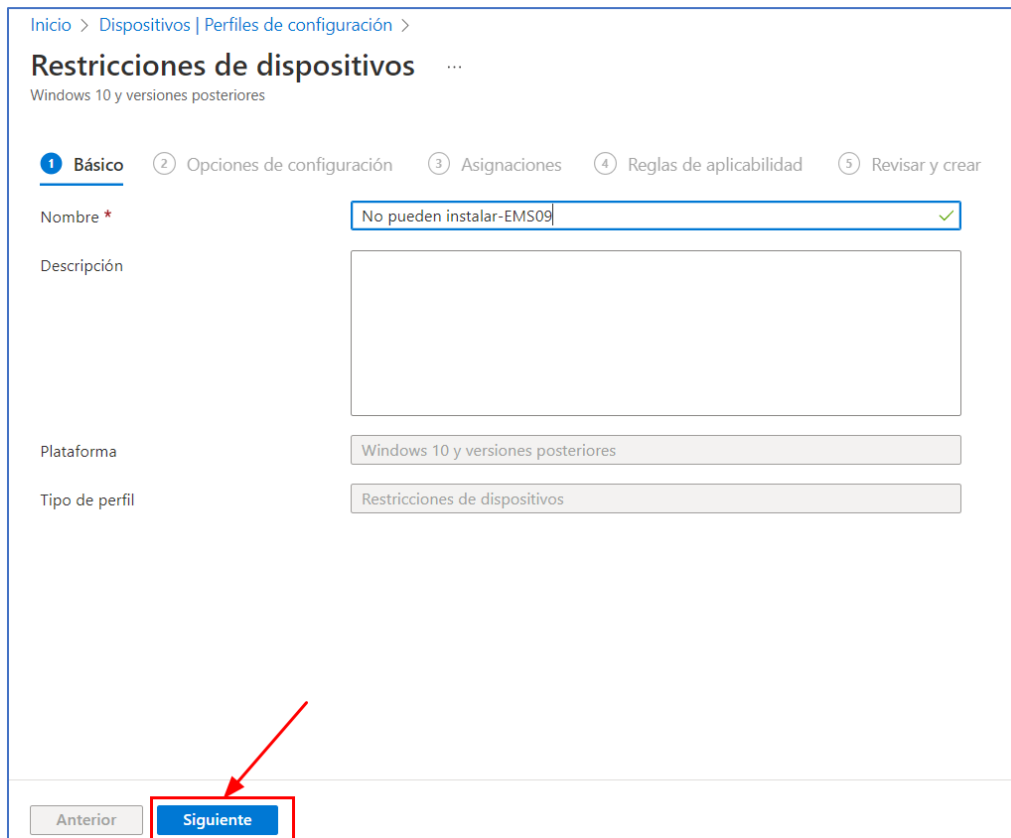
- Administrador de dispositivos Android.
- Android Enterprise.
- iOS/iPadOS.
- macOS.
- Windows 10 y versiones posteriores.
- Windows 8.1 y versiones posteriores.

+ info: <https://docs.microsoft.com/es-es/intune/configuration/device-restrictions-configure>

6. Nos aparecerá el asistente de creación de Configuración de dispositivos: Perfiles – Restricciones de dispositivos. Dividida en pestañas

a. Primera pestaña. Básico

- Nombre:** No pueden instalar-EMS0x (la "X" corresponde con tu usuario). El nombre lo más descriptivo posible.
- Descripción.** Podemos añadir o no una Descripción.
- Plataforma.** Ya seleccionada anteriormente, este campo esta sombreado y no es modificable.
- Tipo de perfil.** Ya seleccionada anteriormente, este campo esta sombreado y no es modificable. Clic en el botón de la parte inferior de la pantalla: **Siguiente**.



Inicio > Dispositivos | Perfiles de configuración >

Restricciones de dispositivos

Windows 10 y versiones posteriores

1 Básico 2 Opciones de configuración 3 Asignaciones 4 Reglas de aplicabilidad 5 Revisar y crear

Nombre * No pueden instalar-EMS09 ✓

Descripción

Plataforma Windows 10 y versiones posteriores

Tipo de perfil Restricciones de dispositivos

Anterior **Siguiente**

b. Segunda pestaña. Opciones de configuración:

i. Clic en el valor: Tienda de aplicaciones.

Seleccionar en los campos deslizables las opciones tal y como aparecen en la siguiente imagen. Con esta configuración estamos restringiendo completamente la instalación de Apps por el usuario.

ii. Clic en el valor: Red de telefonía móvil y conectividad. Seleccionar en los campos deslizables las opciones tal y como aparecen en la siguiente imagen. De esta forma, Bloqueamos el bluetooth e impedimos la configuración manual WIFI por parte de los usuarios.

- iii. **Clic en el valor: Nube y almacenamiento. Seleccionar en los campos deslizables las opciones tal y como aparecen en la siguiente imagen. No permitimos que el usuario dé de alta su cuenta de Outlook personal en el equipo ni sincronice ficheros.**

- iv. **Clic en el valor: Panel de control y Configuración. Seleccionar en los campos deslizables las opciones tal y como aparecen en la siguiente imagen. Bloqueamos el acceso de los usuarios al Panel de control de Windows 10 en sus equipos.**

- v. **Clic en el valor: General. Seleccionar en los campos deslizables las opciones tal y como aparecen en la siguiente imagen. Bloqueamos el uso de la cámara, sincronización de archivos de OneDrive, cualquier tipo de almacenamiento extraíble y Cortana.**

General

- Captura de pantalla (solo móviles) ☐ Bloquear ☐ Sin configurar
- Copiar y pegar (solo móvil) ☐ Bloquear ☐ Sin configurar
- Cancelación manual de la suscripción ☐ Bloquear ☐ Sin configurar
- Instalación manual del certificado raíz (solo móviles) ☐ Bloquear ☐ Sin configurar
- Cámara ☐ **Bloquear** ☐ Sin configurar
- Sincronización de archivos de OneDrive ☐ **Bloquear** ☐ Sin configurar
- Almacenamiento extraíble ☐ **Bloquear** ☐ Sin configurar
- Geolocalización ☐ Bloquear ☐ Sin configurar
- Conexión compartida ☐ Bloquear ☐ Sin configurar
- Restablecimiento del teléfono ☐ Bloquear ☐ Sin configurar
- Conexión USB ☐ Bloquear ☐ Sin configurar
- Modo antirrob (solo móviles) ☐ Bloquear ☐ Sin configurar
- Cortana ☐ **Bloquear** ☐ Sin configurar
- Grabación de voz (solo móviles) ☐ Bloquear ☐ Sin configurar
- Modificación del nombre del dispositivo (solo móvil) ☐ Bloquear ☐ Sin configurar
- Agregar paquetes de aprovisionamiento ☐ Bloquear ☐ Sin configurar
- Quitar paquetes de aprovisionamiento ☐ Bloquear ☐ Sin configurar
- Detección de dispositivos ☐ Bloquear ☐ Sin configurar
- Cambio de tarea (solo móviles) ☐ Bloquear ☐ Sin configurar
- Cuadro de diálogo de error de tarjeta SIM (solo móviles) ☐ Bloquear ☐ Sin configurar
- Área de trabajo de Ink ☐ Sin configurar
- Restablecimiento con AutoPilot ☐ Permitir ☐ Sin configurar
- Exigir que los usuarios se conecten a la red durante la configuración del dispositivo ☐ Requerir ☐ Sin configurar
- Acceso directo a memoria ☐ Sin configurar
- Finalizar procesos desde el Administrador de tareas ☐ Bloquear ☐ Sin configurar

- vi. **Clic en el valor: Experiencia de pantalla de bloqueo. Seleccionar en los campos deslizables las opciones tal y como aparecen en la siguiente imagen. Bloqueamos las notificaciones, Cortana, cuando el equipo está bloqueado.**

Experiencia de pantalla de bloqueo

- Notificaciones del centro de actividades (solo móviles) ☐ **Bloquear** ☐ Sin configurar
- URL de imagen de pantalla de bloqueo (solo equipos de escritorio)
- Tiempo de espera de la pantalla configurable por el usuario (solo dispositivos móviles) ☐ Permitir ☐ Sin configurar
- Cortana en pantalla bloqueada (solo escritorio) ☐ **Bloquear** ☐ Sin configurar
- Notificaciones del sistema en pantalla bloqueada ☐ **Bloquear** ☐ Sin configurar
- Tiempo de espera de la pantalla (solo dispositivos móviles)
- Activar aplicaciones por voz desde la pantalla bloqueada ☐ Sin configurar

- vii. **Clic en el valor: Mensajería. Seleccionar en los campos deslizables las opciones tal y como aparecen en la siguiente imagen.**

- viii. **Clic en el valor: Explorador Microsoft Edge. Aquí solamente le definiremos nuestra web de Intranet de la empresa como página de Inicio. El resto de los valores no los modificaremos. Por favor, revisarlos para ver todas las opciones de configuración de Microsoft Edge, que tenemos disponibles.**

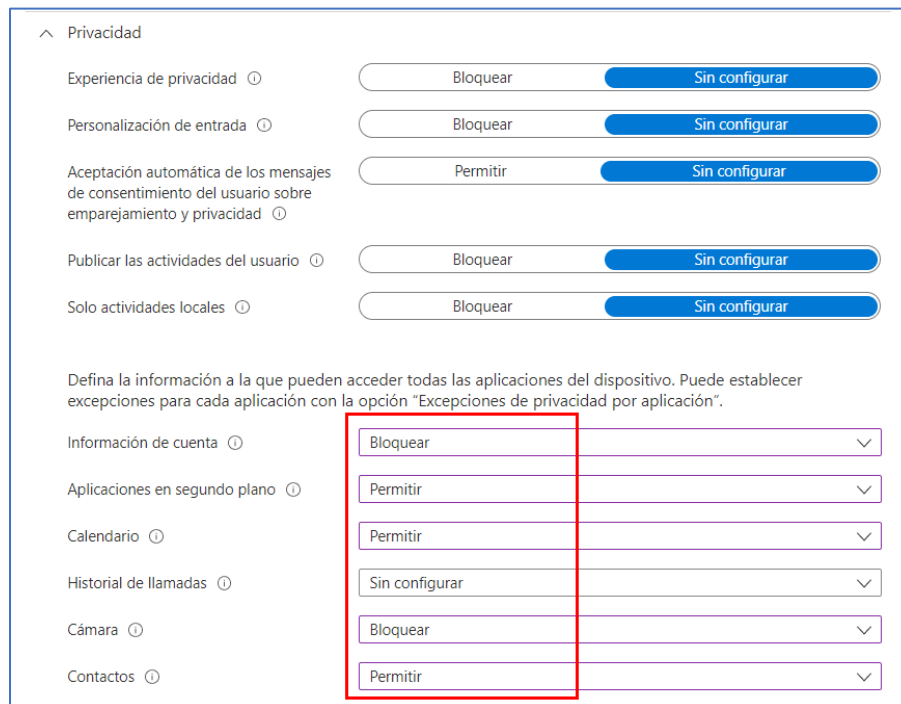
- ix. **Clic en el valor: Proxy de red. Seleccionar en los campos deslizables las opciones tal y como aparecen en la siguiente imagen. Bloqueamos la utilización de otros Proxies de red y grabamos la configuración de nuestro Proxy en los equipos.**

- x. en el **valor: Contraseña**. Seleccionar en los **campos deslizables** las **opciones tal y como aparecen** en la **siguiente imagen**. **Requerimos y obligamos el uso de contraseñas** según queramos.


- xi. **Clic en el valor: Personalización**. Podemos **establecer** un **fondo de pantalla corporativo** en los equipos de la empresa. En nuestro caso **NO** lo configuramos.


- xii. **Clic en el valor: Impresora**. Seleccionar en los **campos deslizables** las **opciones tal y como aparecen** en la **siguiente imagen**. **Bloqueamos** que se puedan **agregar otras impresoras que nos sean las de nuestra oficina a través de su nombre DNS**.


- xiii. **Clic en el valor: Privacidad.** Seleccionar en los campos deslizables las opciones tal y como aparecen en la siguiente imagen.





Privacidad

Experiencia de privacidad  Bloquear Sin configurar


Personalización de entrada  Bloquear Sin configurar


Aceptación automática de los mensajes de consentimiento del usuario sobre emparejamiento y privacidad  Permitir Sin configurar


Publicar las actividades del usuario  Bloquear Sin configurar


Solo actividades locales  Bloquear Sin configurar


Defina la información a la que pueden acceder todas las aplicaciones del dispositivo. Puede establecer excepciones para cada aplicación con la opción "Excepciones de privacidad por aplicación".


Información de cuenta  Bloquear

Aplicaciones en segundo plano  Permitir

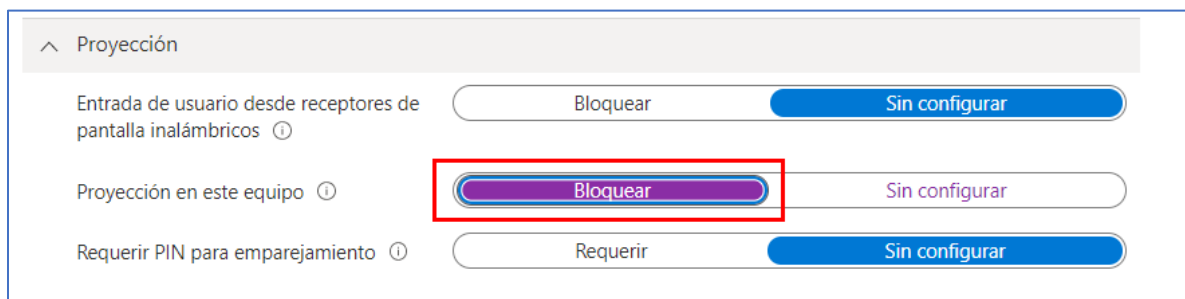
Calendario  Permitir

Historial de llamadas  Sin configurar


Cámara  Bloquear


Contactos  Permitir


- xiv. **Clic en el valor: Proyección.** Seleccionar en los campos deslizables las opciones tal y como aparecen en la siguiente imagen. Bloqueamos la proyección en estos equipos.



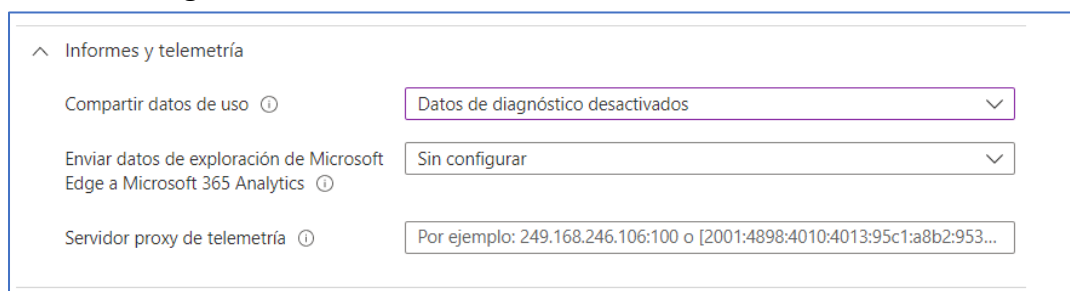
Proyección

Entrada de usuario desde receptores de pantalla inalámbricos  Bloquear Sin configurar


Proyección en este equipo  Bloquear Sin configurar


Requerir PIN para emparejamiento  Requerir Sin configurar


- xv. **Clic en el valor: Informes y telemetría.** Seleccionar en los campos deslizables las opciones tal y como aparecen en la siguiente imagen. Permitimos compartir únicamente los datos de seguridad.



Informes y telemetría

Compartir datos de uso  Datos de diagnóstico desactivados

Enviar datos de exploración de Microsoft Edge a Microsoft 365 Analytics  Sin configurar

Servidor proxy de telemetría  Por ejemplo: 249.168.246.106:100 o [2001:4898:4010:4013:95c1:a8b2:953...

- xvi. **Clic en el valor: Buscar. Seleccionar en los campos deslizables las opciones tal y como aparecen en la siguiente imagen. Bloqueamos la ubicación de búsqueda.**

^

Buscar

Búsqueda segura (solo móvil) ⓘ

Definido por el usuario

Mostrar los resultados de los sitios web en la búsqueda ⓘ

Bloquear

Sin configurar

Diacríticos ⓘ

Bloquear

Sin configurar

Detección automática del idioma ⓘ

Bloquear

Sin configurar

Ubicación de la búsqueda ⓘ

Bloquear

Sin configurar

Retroceso del indexador ⓘ

Bloquear

Sin configurar

Indexación de unidad extraíble ⓘ

Bloquear

Sin configurar

Indexación con espacio en disco insuficiente ⓘ

Habilitar

Sin configurar

Consultas remotas ⓘ

Habilitar

Sin configurar

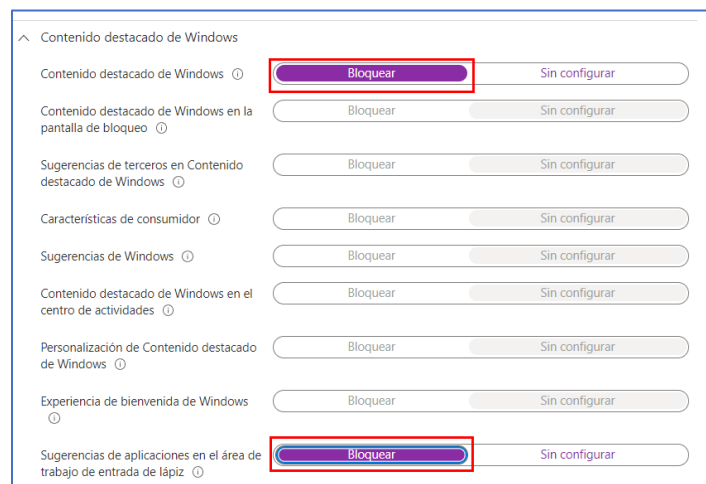
- xvii. **Clic en el valor: Inicio. Seleccionar en los campos deslizables las opciones tal y como aparecen en la siguiente imagen. Personalizamos el botón “Inicio” de Windows en cada uno de los equipos. No permitimos cambios tampoco suspender y cambiar cuenta**

[illegible]

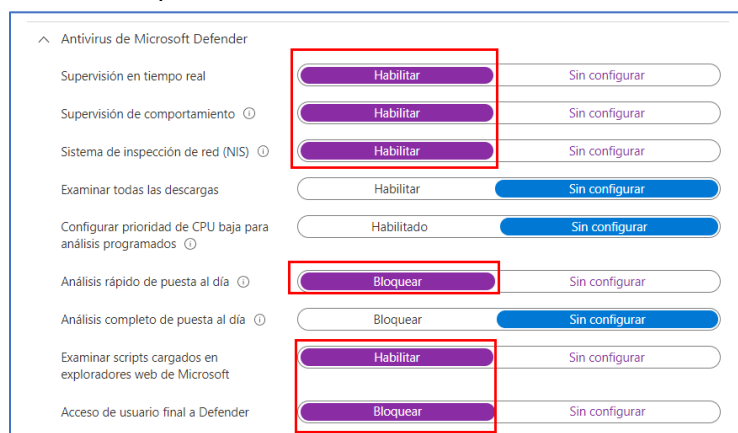
- xviii. En el **campo Configuración**. Clic en el valor: **SmartScreen de Microsoft Defender**. **Seleccionar** en los **campos deslizables** tal y como aparecen en la imagen. **Forzamos la protección de SmartScreen**.



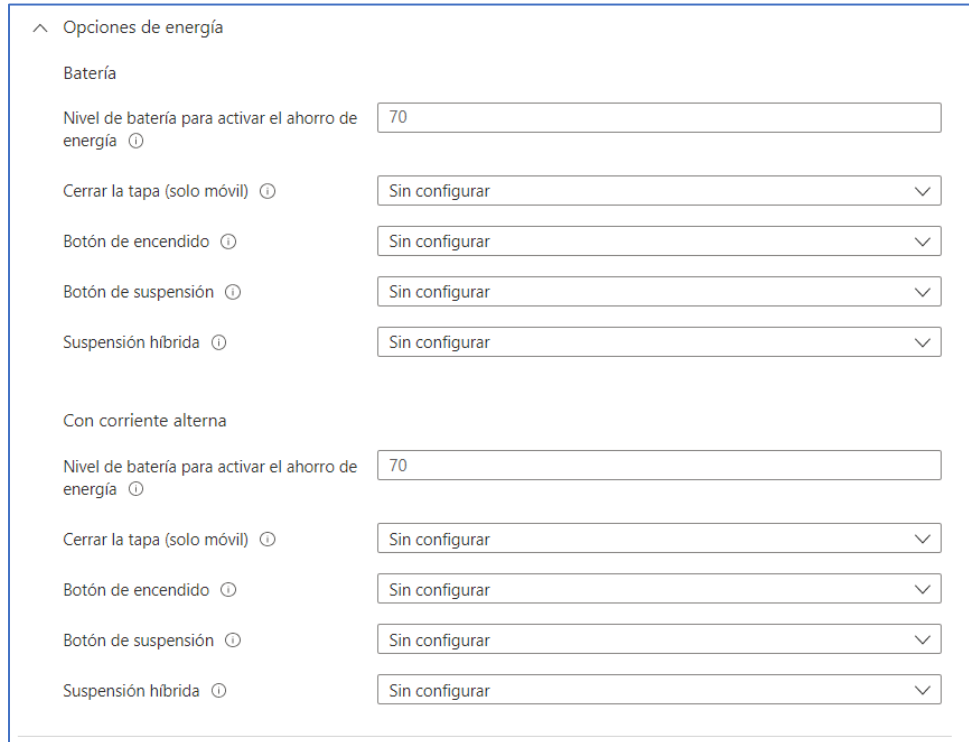
- xix. **Clic en el valor: Contenido destacado de Windows**. Tal y como aparece en la imagen. **Lo bloqueamos todo**.



- xx. **Clic en el valor: Antivirus de Microsoft Defender**. **Seleccionar** en los **campos deslizables** las **opciones** tal y como aparecen en la siguiente imagen. **Configuramos la protección de Microsoft Defender** definiendo su *comportamiento*. *Por favor, revisar todas las opciones que tenemos disponibles*.



- xxi. **Clic en el valor: Opciones de energía. Seleccionar en los campos deslizables las opciones tal y como aparecen en la siguiente imagen.** Definimos el **comportamiento** que queremos para los *botones* del equipo *basado en el nivel de batería*.



- xxii. **Clic en el botón: Siguiente.** Para pasar a la **tercera pestaña de configuración**.



- c. **Tercera pestaña. Asignaciones.** Asignaremos esta **directiva** al **grupo** que tenemos: **EMS0**.
- Clic** en el **enlace Agregar todos los usuarios**. **Clic** en el **botón Seleccionar**.
 - Grupos excluidos. No seleccionar ninguno.**
 - Clic** en el **botón Siguiente**. Para pasar a la siguiente pestaña de configuración.

Inicio > Dispositivos | Perfiles de configuración >

Restricciones de dispositivos

Windows 10 y versiones posteriores

☒ Básico
 ☒ Opciones de configuración
 ☒ **Asignaciones**
☐ Reglas de aplicabilidad
 ☐ Revisar y crear

Grupos incluidos

Grupos	Miembros del grupo ⓘ	Filtrar	Modo de filtro	
Todos los usuarios		Ninguno	Ninguno	Editar filtro Quitar

Grupos excluidos

Grupos

Miembros del grupo ⓘ

Ningún grupo seleccionado

7. **Cuarta pestaña. Reglas de aplicabilidad.** Aquí **creamos** las **reglas** en las que se van a **aplicar** todas las opciones que hemos definido en los puntos anteriores.

Clic en las **columnas**:

- Regla:** En el desplegable seleccionamos: **Asignar perfi si**.
- Propiedad:** En el desplegable seleccionamos: **Edición del sistema operativo**.
- Valor:** En el desplegable seleccionamos: *Windows 10 Enterprise y Windows 10 Professional*.

Restricciones de dispositivos

Windows 10 y versiones posteriores

✓ Básico
✓ Opciones de configuración
✓ Asignaciones
4 Reglas de aplicabilidad
5 Revisar y crear

Especifique cómo aplicar este perfil en un grupo asignado. Intune solo aplicará el perfil a los dispositivos que cumplan los criterios combinados de estas reglas.

Regla	Propiedad	Valor
Asignar perfil si	Edición del sistema operativo	Windows 10/11 Enterprise y ...

d. Clic en el **botón: Siguiente** para continuar con la siguiente pestaña del asistente de configuración.

Anterior

Siguiente

8. **Quinta pestaña: Revisar y crear.** Podremos **revisar** toda la **configuración** que acabamos de realizar y haremos clic en el **botón: Crear**.

Inicio > Dispositivos | Perfiles de configuración >

Restricciones de dispositivos

Windows 10 y versiones posteriores

✓ Básico
✓ Opciones de configuración
✓ Asignaciones
✓ Reglas de aplicabilidad
5 Revisar y crear

Resumen

Básico

Nombre	No pueden instalar-EMS09
Descripción	--
Plataforma	Windows 10 y versiones posteriores
Tipo de perfil	Restricciones de dispositivos

Opciones de configuración

Tienda de aplicaciones

Tienda de aplicaciones (solo móvil)	Bloquear
Actualizar automáticamente las aplicaciones de la tienda	Bloquear
Instalación de aplicaciones de confianza	Bloquear
Desbloqueo de desarrollador	Bloquear
Usar solo una tienda privada	Permitir
Game DVR (solo escritorio)	Bloquear
Solo aplicaciones de la tienda	Solo Store

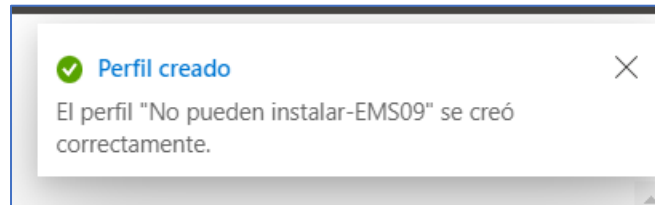
Red de telefonía móvil y conectividad

Conectar automáticamente a zonas Wi-Fi	Bloquear
--	----------

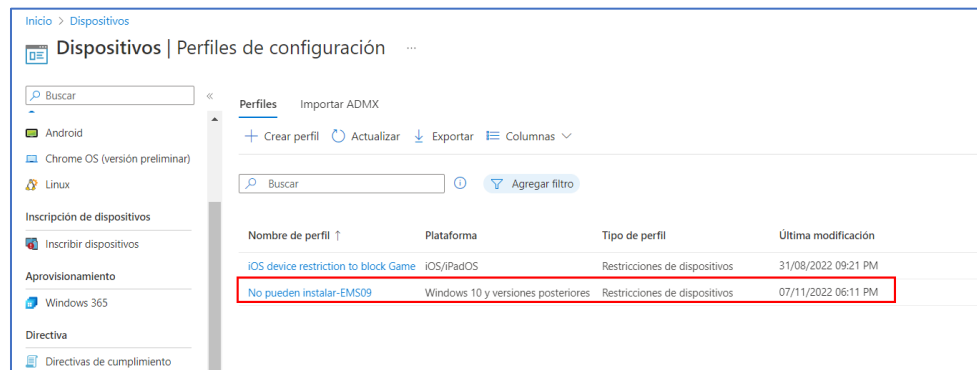
Anterior

Crear

9. Nos aparecerá la ventana informativa en el lado superior derecho de la ventana.



10. Nos **aparecerá** el **perfil** que nos acabamos de crear.



Laboratorio – 8.3: Política de Seguridad del dispositivo.

Objetivo: El objetivo de este laboratorio es. crear una: **Política de seguridad del dispositivo**.

Las políticas de seguridad de dispositivos no permiten configurar funcionalidades en los dispositivos a nivel de seguridad y comportamiento que queramos que tengan nuestras estaciones de trabajo, portátil y resto de dispositivos empresariales con **Windows 10**.

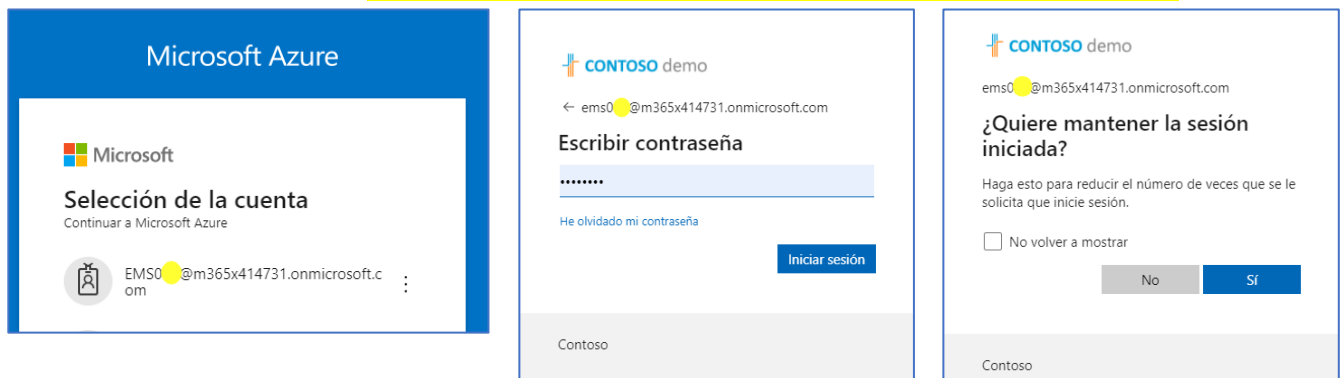
En este laboratorio vamos a revisar las opciones de seguridad que tenemos disponibles, comprobaremos que son muchas las que podremos asignar a nuestros equipos.

Prerrequisito: EMS Enterprise Mobility + Security E5.

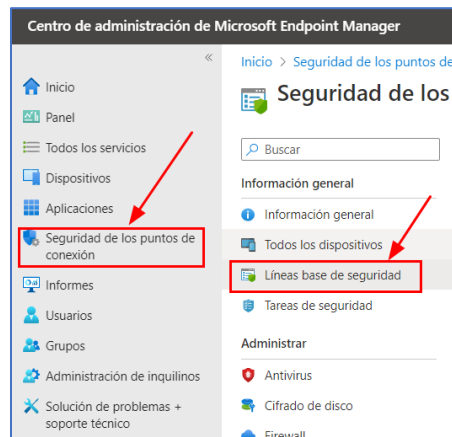
1. Logarnos con nuestras credenciales de admin al **Centro de administración de Microsoft Endpoint Manager**: <https://endpoint.microsoft.com/>.

Usuario: EMS0x@m365*****.onmicrosoft.com (la “x” es el usuario que os hemos dado al comienzo del curso).

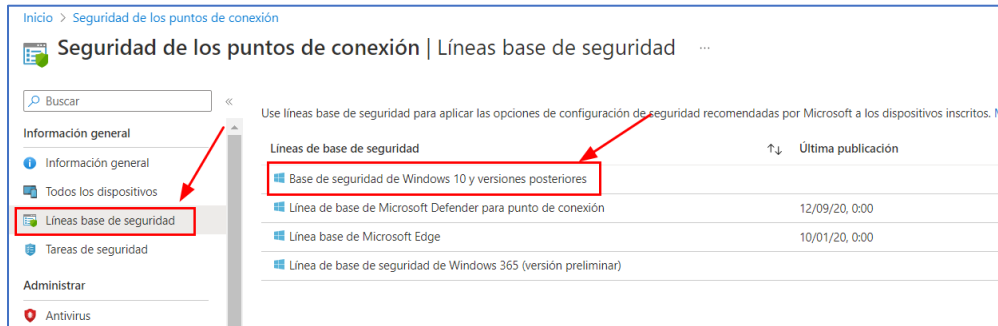
Contraseña: HolaMundo01 (o la contraseña que hayas puesto cuando el sistema te obligó a cambiarla)



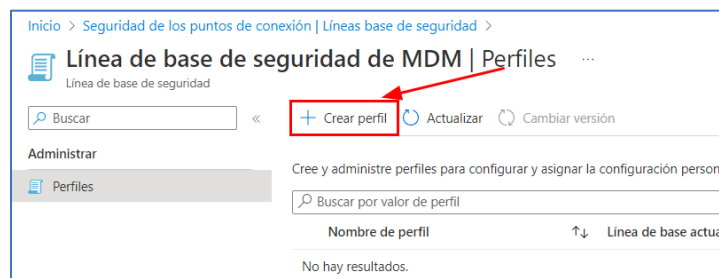
2. **Aparecerá** el Centro de administración de Microsoft Endpoint Manager. **Clic** en el menú vertical izquierdo, en la entrada **Seguridad de los puntos de conexión**. **Clic** en la entrada **Líneas base de seguridad**.



3. Clic en la entrada **Líneas de base de seguridad de Windows 10**.



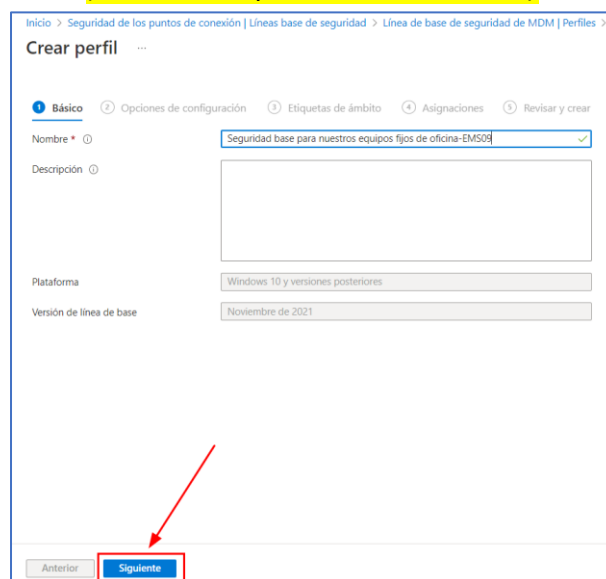
4. Clic en el botón: **+ Crear perfil** del menú horizontal superior.



5. Nos aparece el **asistente de creación de perfiles de líneas base**. Dividido en varias pestañas.

a. **Primera pestaña: Básico.**

Escribimos un **nombre descriptivo** para esta **directiva**: **Seguridad base para nuestros equipos fijos de oficina-EMS0x** (la "X" corresponde con tu usuario).



Como en los casos anteriores, nos aparecerán los campos **Plataforma** y **Versión de línea base**, **sombreados SIN poder modificarlos**. Clic en el botón **Siguiente** para continuar.

- b. **pestaña: Opciones de configuración.** Dentro de la **pestaña: Opciones de configuración** ponemos ir **seleccionando**, haciendo **scroll** para abajo. **Vamos a revisar todas y cada una de las opciones de seguridad que tenemos disponibles en EMS.**

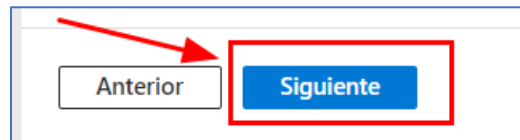
i. *Administración de aplicaciones y Administración remota.*

ii. *Administrador de conexiones de Windows, Área de trabajo de Windows Ink, Asistencia remota y Bitlocker.*

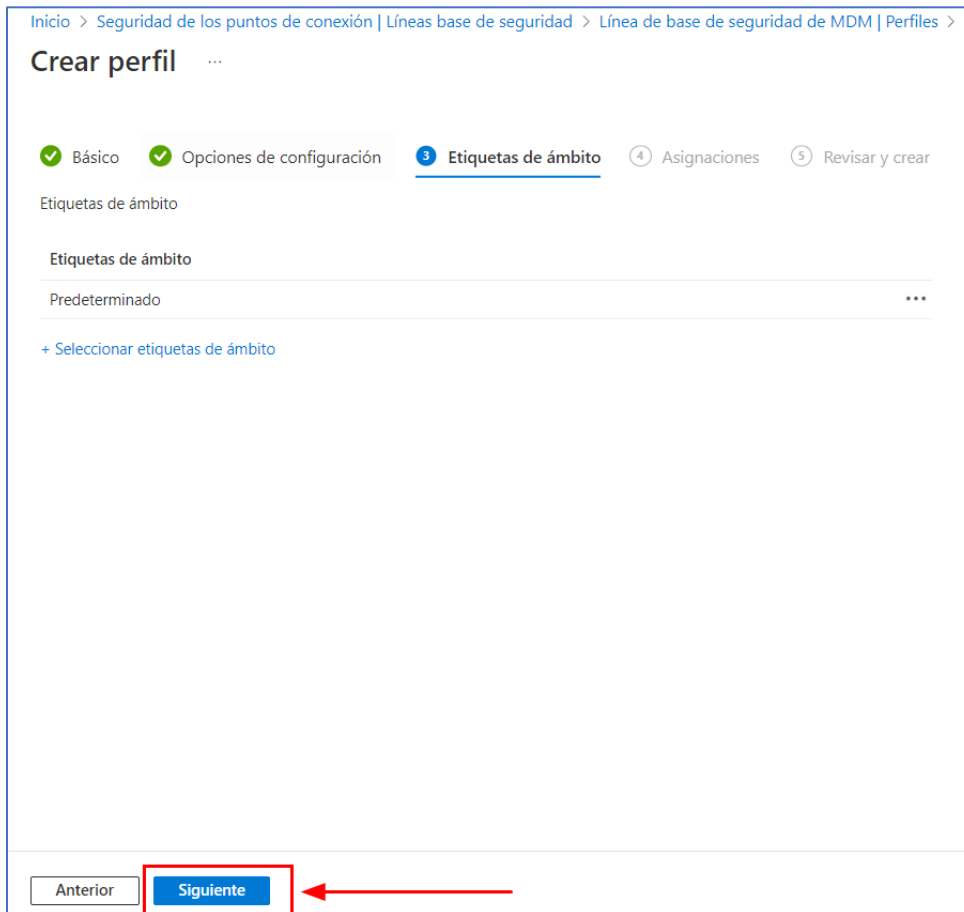
iii. *Bloqueo del dispositivo. Si requerimos o no que el usuario tenga que escribir un PIN o una contraseña cuando el dispositivo se reanuda desde un estado de inactividad y en que condiciones tendrá que realizarlo.*

- iv. *Buscar, Conectividad y Delegación de credenciales. Lo dejamos por defecto. Lo dejamos por defecto*
- v. *Device Guard y entorno de ejecución. Lo dejamos por defecto*
- vi. *Experiencia y Explorador. Lo dejamos por defecto*
- vii. *Explorador de archivos. Lo dejamos por defecto*
- viii. *Firewall. Lo dejamos por defecto*
- ix. *Guías de seguridad de MS y Heredado de MSS. Lo dejamos por defecto*
- x. *Instalación de dispositivos e Interfaz de usuario de credenciales. Lo dejamos por defecto*
- xi. *Internet Explorer. Lo dejamos por defecto*
- xii. *Llamada a procedimiento remoto y Microsoft Defender. Lo dejamos por defecto*
- xiii. *Opciones de seguridad de directivas locales. Lo dejamos por defecto*
- xiv. *Potencial y Protección contra vulnerabilidades de seguridad. Lo dejamos por defecto*
- xv. *Protección de datos, protección de DMA y Reproducción automática. Lo dejamos por defecto*
- xvi. *Servicio de registro de eventos y Servicios de Escritorio remoto. Lo dejamos por defecto*
- xvii. *Sistema y SmartScreen. Lo dejamos por defecto*
- xviii. *Sobre bloqueo, Wi-Fi, Windows Hello para empresas y Windows PowerShell. Lo dejamos por defecto*

Clic en el botón: Siguiente. Para pasar a la **siguiente pestaña de Etiquetas de ámbito.**



- c. **Tercera pestaña: Etiquetas de ámbito.** En Intune, podemos usar **tanto RBAC como etiquetas de ámbito** para asegurarnos de que los administradores adecuados tienen el acceso y la visibilidad correctos a los objetos de Intune que queremos. Los **roles** determinan **qué acceso** tienen los **administradores a qué objetos** y las **etiquetas de ámbito determinan qué objetos** pueden ver los **administradores**. En nuestro caso, lo dejaremos en **Predeterminado** (*por defecto*). **Clic en el botón Siguiente.**



+ Info (crearlas, etc): <https://docs.microsoft.com/es-es/mem/intune/fundamentals/scope-tags>

d. **Cuarta pestaña: Asignaciones.** Aquí **seleccionaremos** tanto los **grupos incluidos** para esta configuración de línea base de seguridad como los **excluidos**.

i. En el **desplegable: Grupos incluidos**. Campo **Asignar a**. Podremos seleccionar:

1. Todos los usuarios.
2. Todos los dispositivos.
3. Todos los usuarios y dispositivos.

ii. **Clic en Agregar todos los usuarios.** **Clic en el botón Siguiente.** Para **pasar a la última pestaña: Revisar y crear**.

11. En la **pestaña: Revisar y crear**. **Clic en el botón: Crear**. Podremos **revisar** toda la **configuración** que acabamos de realizar y haremos **clic en el botón: Crear**.

6. Ya nos **aparecerá** la **directiva** que **nos acabamos de crear: Seguridad base para nuestros Windows.**

Inicio > Seguridad de los puntos de conexión | Líneas base de seguridad >

Línea de base de seguridad de MDM | Perfiles ...

Línea de base de seguridad

Buscar << + Crear perfil Actualizar Cambiar versión

Administrar

Perfiles

Cree y administre perfiles para configurar y asignar la configuración personalizada a los grupos de su organización.

Buscar por valor de perfil

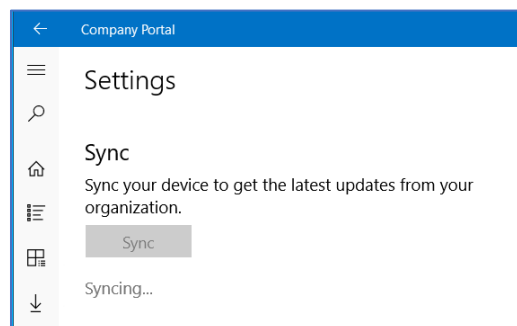
Nombre de perfil	↑↓ Línea de base actual	↑↓ Asignado	↑↓ Última modificación
<input type="checkbox"/> Seguridad base para nuestros equipos fijos de	Noviembre de 2021	Sí	07/11/22, 18:44

7. **EN ESTE PUNTO.** Tendríamos que **sincronizar** las **directivas** que **nos acabamos de crear** en cada uno de los **equipos** a los que se las **hemos asignado**.

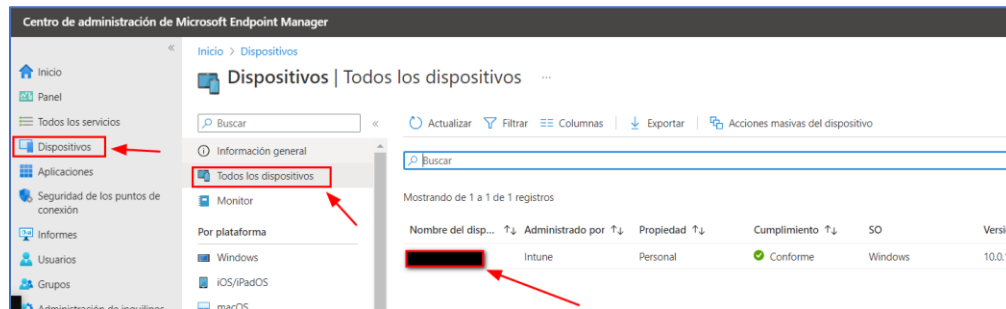
- a. **Sincronización Manual.** Para comprobar que funciona **es la recomendable para este laboratorio, NO para producción.**

Podemos ir a nuestro **Windows 10 (Máquina Virtual de laboratorio)**. **Abrir la App: Portal de Compañía** y hacer **click** en el **botón Sync** o **sincronizar**. Para forzar la sincronización en esta máquina.

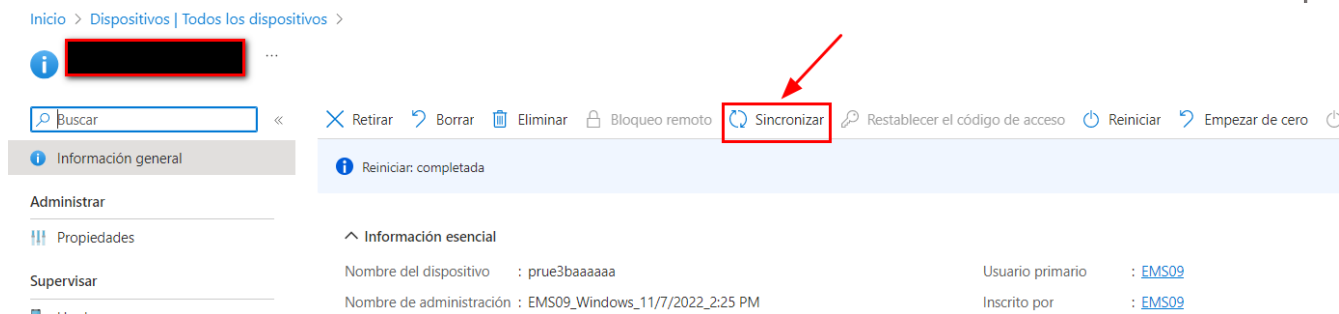
- i. Ahora, abrimos la App: **Portal de Empresa que instalamos antes**, en nuestra máquina de laboratorio, para comprobar que la App que acabamos de crear **no está disponible**.
- ii. **Forzamos la sincronización de forma manual**, para ello, seleccionamos la **rueda dentada** dentro del **Portal de Empresa**.
- iii. **Clic** en el **botón Sincronizar** para que aparezca transcurrido unos minutos, el proceso se puede retardar un poco por temas de sincronización cliente-plataforma.



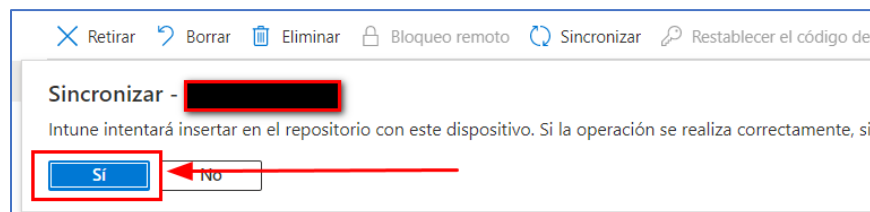
- b. En entorno de producción, generalmente no tenemos acceso físico a las máquinas, podemos forzar la sincronización. Dentro de la **consola de Centro de administración de Microsoft Endpoint Manager**. Clic en el **menú izquierdo vertical de la pantalla** en la entrada: **Dispositivos**. Clic en **Todos los dispositivos**. Veremos los dispositivos que se han inscrito en el servicio vía Portal de empresa. Clic en el **dispositivo/s que queramos que sincronicen**, en este ejemplo sólo marcamos **EMS-xxxxx**.



- c. Clic en el botón: **Sincronizar**.



- d. Clic en el botón **Sí**.



- e. Aparecerá la **ventana informativa** correspondiente a esta **tarea de sincronización de dispositivos**.

