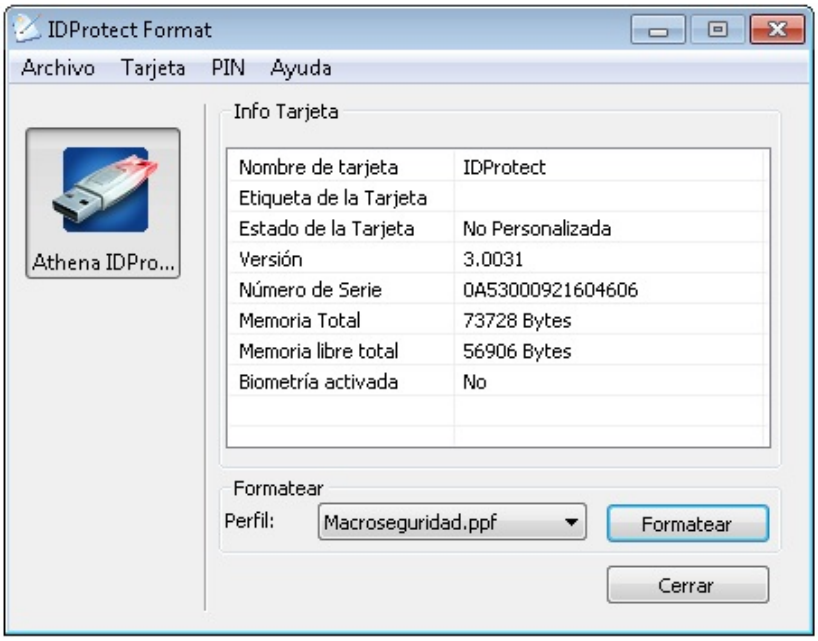
# Formateo de dispositivos criptográficos
# MS-IDProtect
# (Token USB o Smartcard)

**Requisitos:**
Tener instalado el middleware **versión 6.22.22** o superior.

Conectamos el MS-IDProtect (token usb o smartcard) e iniciamos **IDProtect Format** (*Inicio* | *Programas* | *IDProtect Client*) o (*Inicio* | *Programas* | *Macroseguridad.org*)

Para comenzar el proceso de formateo primero debemos seleccionar y editar el perfil de formateo de seguridad deseado que vamos a aplicar sobre el MS-IDProtect.




El perfil recomendado por Macroseguridad es "*Macroseguridad.ppf*" y lo puede encontrar dentro de la carpeta "Herramientas\Formateo\". Establece los siguientes parámetros de seguridad:

Pestaña **General**:
- ✓ Caducará en 356 Días
- ✓ Recordar los últimos 5 PINs

Pestaña **PIN de Usuario**

- ✓ Password del Usuario por defecto es **12345678.**
- ✓ El máximo número de intentos fallidos por defecto es 10.
- ✓ La cantidad de desbloqueos en caso de que se supere la cantidad de intentos fallidos es ilimitada. (en otras palabras el token puede volver a formatearse)
- ✓ La longitud mínima del PIN de Usuario es de 8 caracteres y la máxima de 16.

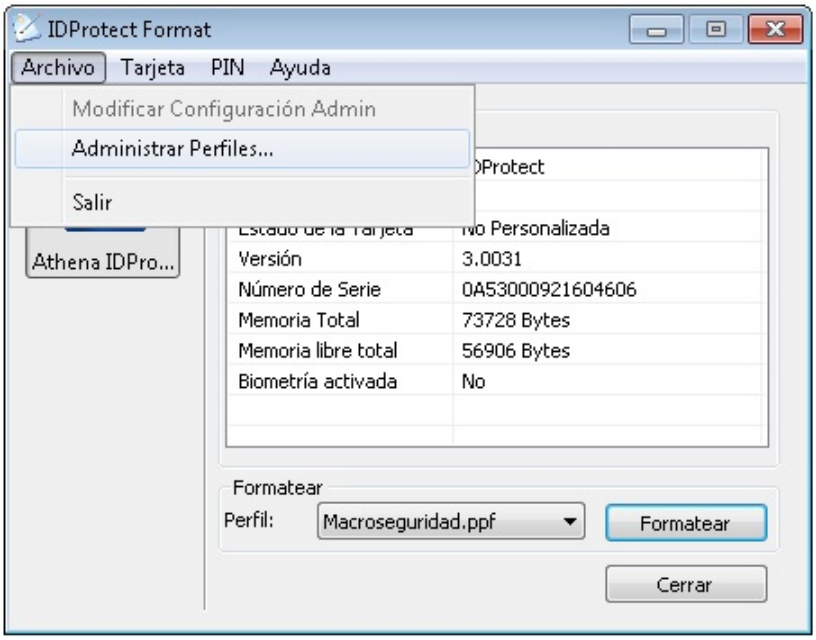
Pestaña **PIN Admin**

- ✓ Password del administrador por defecto es **12345678**.
- ✓ El máximo número de intentos fallidos por defecto es 5.
- ✓ La Longitud mínima del PIN de Administrador es de 8 y la máxima de 16,

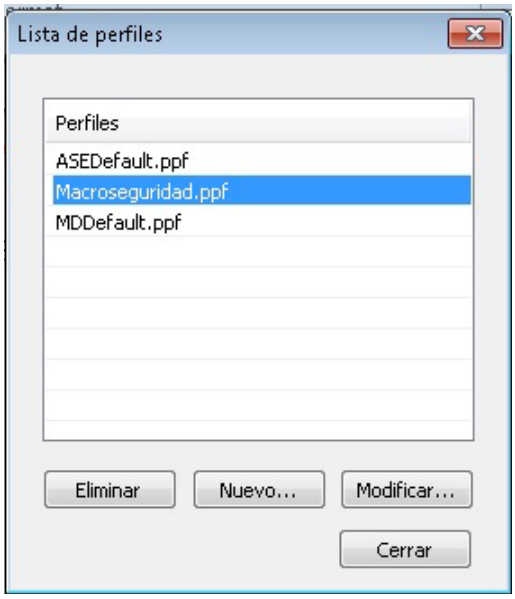
**IMPORTANTE:**
**Una vez bloqueado, el Admin PIN NO se puede desbloquear.**

MS-IDProtect posee una certificación FIPS 140-2 Level 3 y viene configurado de fábrica según los requisitos de este estándar.
Se entrega en modo FIPS por defecto.
Esta política de seguridad no puede ser modificada.

Si usted desea administrar sus perfiles (definir nuevas políticas) diríjase al menú (***Archivo | Administrar Perfiles…***).

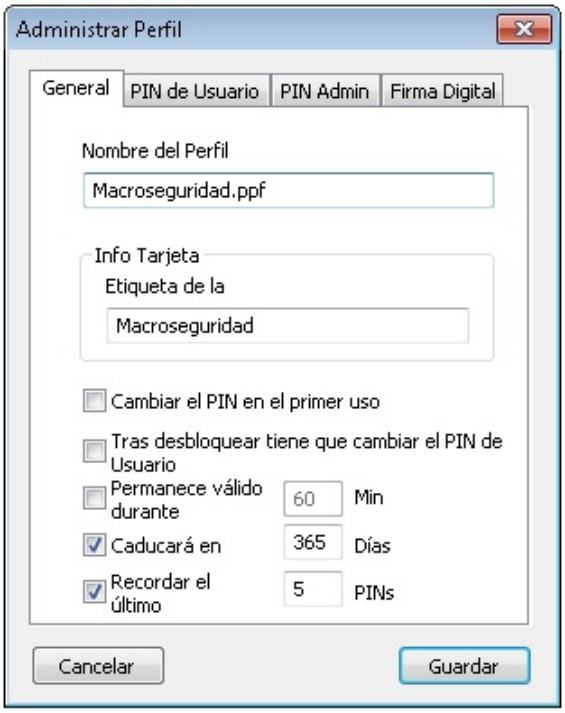


Si usted desea crear un perfil nuevo siga los siguientes pasos:




Haga click en "**Nuevo…**" para crear un nuevo perfil y completar las pestañas correspondientes con las configuraciones deseadas.

Los campos a completar en la pestaña "*General*" son:




"*Nombre*": Se establece el nombre deseado para el perfil.

"*Etiqueta*": Se establece el nombre por defecto del MS-IDProtect. Si no se establece un valor se utiliza el número de serie (smartcard ID) del MS-IDProtect.

"*Cambiar el PIN en el Primer uso*": En esta instancia se fija la política de cambio compulsivo del PIN por defecto. El usuario DEBERÁ cambiar obligatoriamente el PIN (fijado por los administradores al momento de formateo). No se permitirá ninguna clase de uso hasta que no se cambie el PIN.

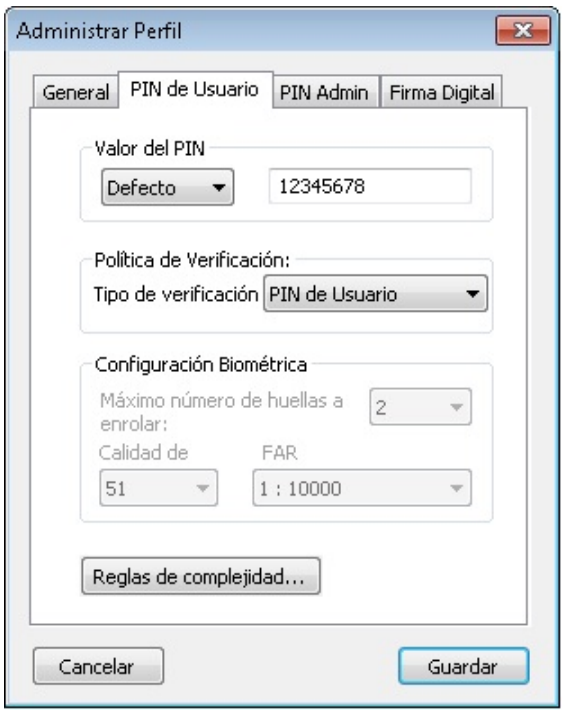
"*Tras desbloquear tiene que cambiar el PIN de Usuario*": Obliga al usuario a cambiar su PIN luego de que el mismo haya sido desbloqueado por un administrador.

"*Permanece valido durante*": En esta instancia se fija la política de tiempo que durará una sesión válida entre una aplicación que se ha autenticado al dispositivo Token USB de Macroseguridad. Pasado este tiempo, se requerirá que el usuario se autentique nuevamente al mismo.

"*Caducará en*": Se le obligará al usuario a cambiar el PIN cada *N* días.

"*Recordar el último*": En esta instancia se fija la política de Administración de PIN históricos. Para mayor seguridad, los Tokens USB de Macroseguridad no permitirán que se reutilicen PINs ya ingresados recientemente por un usuario. Aquí puede setearse la cantidad de PINs (passwords) anteriores que no se podrán reutilizar. Por ejemplo, si se asigna 1, no se podrá cambiar el PIN actual por el mismo PIN. Si se setea 2, no se podrá cambiar el PIN actual por el mismo, ni por el usado anteriormente.

Los campos a completar en la pestaña "*PIN de Usuario*" son:



"*Valor del PIN*": Se fija el PIN del Usuario por defecto. El mismo puede ser ingresado por "*Defecto*" (se utilizará el mismo en cada formateo), "*Manual*" (se deberá ingresar manualmente durante el formateo el PIN de usuario deseado), "*Aleatorio*" (se generará de manera aleatoria el PIN de Usuario. El mismo se mostrará durante el formateo").

"*Tipo de verificación*": Se establece el modo en que el usuario se autenticará al dispositivo. Las opciones son "*PIN de Usuario*", "*Biometría*", "*Biometría o PIN*" o "*Biometría y PIN*".

"*Máximo numero de huellas a enrolar*": Establece la cantidad de huellas que el usuario debe registrar durante el formateo.

"*Calidad de*": Establece la calidad del témplate de la huella (minucia).

"*FAR (False acceptance rate)*": Establece la cantidad de falso positivos probables.

"*Reglas de complejidad…*": Para establecer la complejidad y seguridad del PIN (tanto el PIN de Usuario como el PIN de Admin) deberá hacer click en "**Reglas de complejidad…**" en la respectiva pestaña de PIN.

La siguiente ventana se desplegará:

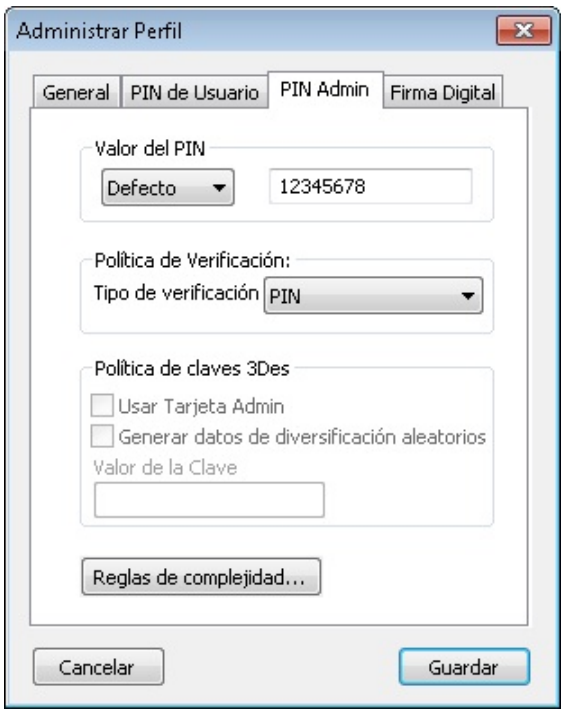
Reglas del PIN:

"*Max intentos*": Máxima cantidad de intentos fallidos consecutivos.
"*Max*": Máxima cantidad de desbloqueos del PIN (esta opción no está disponible para el Admin PIN).
"*Min car.*": La mínima cantidad de caracteres que debe tener el PIN.
"*Max car.*": La máxima cantidad de caracteres que debe tener el PIN.

Complejidad:

"*No Alfanumérica*": Establece la cantidad de caracteres no alfanuméricos que debe tener el PIN
"*Alfabética*": Establece la cantidad de caracteres alfabéticos que debe tener el PIN.
"*Mayúsculas*": Establece la cantidad de mayúsculas que debe tener el PIN.
"*Numérica*": Establece la cantidad de caracteres numéricos que debe tener el PIN.

Los campos a completar en la pestaña "*PIN Admin*" son:




"*Valor del PIN*": Se fija el PIN del Usuario por defecto. El mismo puede ser ingresado por "*Defecto*" (se utilizará el mismo en cada formateo), "*Manual*" (se deberá ingresar manualmente durante el formateo el PIN de usuario deseado), "*Aleatorio*" (se generará de manera aleatoria el PIN de Usuario. El mismo se mostrará durante el formateo").

"*Tipo de verificación*": Se establece el modo en que el usuario se autenticará al dispositivo. Las opciones son "*PIN*" o "*Clave 3DES*".

"Política de claves 3Des": Se establece si la clave 3DES se encuentra almacenada dentro de una "Tarjeta Admin" o si la misma es ingresada manualmente.

"*Reglas de Complejidad…*": Para establecer la complejidad y seguridad del PIN (tanto el PIN de Usuario como el PIN de Admin) deberá hacer click en "**Reglas de complejidad…**" en la respectiva pestaña de PIN.

La siguiente ventana se desplegará:


Reglas del PIN:

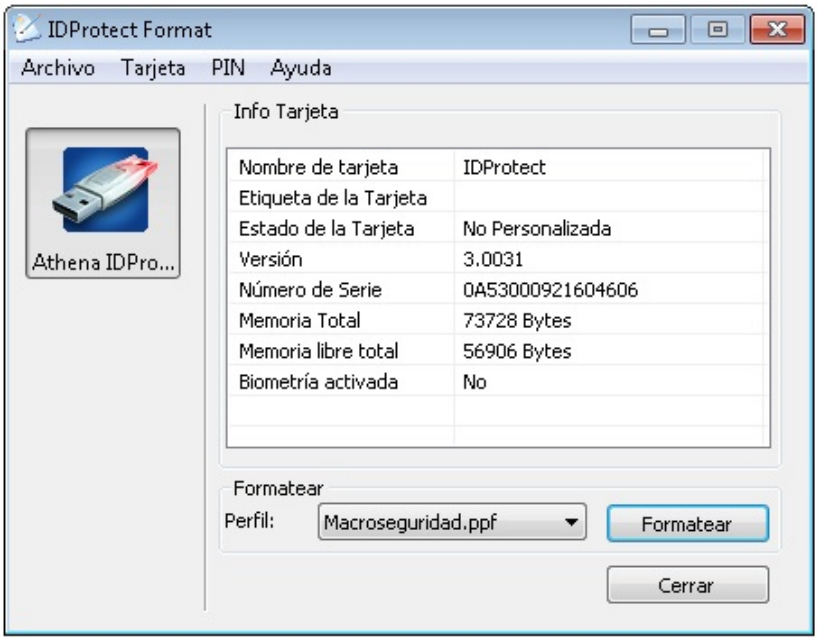
"*Max intentos*": Máxima cantidad de intentos fallidos consecutivos.
"*Max*": **Esta opción viene deshabilitada ya que el PIN de Administrador no se puede desbloquear.**
"*Min car.*": La mínima cantidad de caracteres que debe tener el PIN.
"*Max car.*": La máxima cantidad de caracteres que debe tener el PIN.

Complejidad:

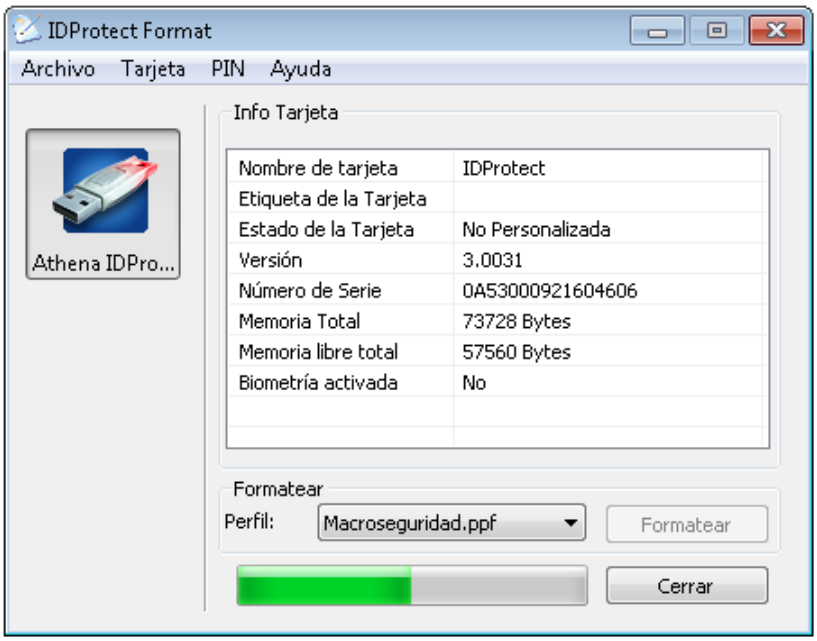
"*No Alfanumérica*": Establece la cantidad de caracteres no alfanuméricos que debe tener el PIN
"*Alfabética*": Establece la cantidad de caracteres alfabéticos que debe tener el PIN.
"*Mayúsculas*": Establece la cantidad de mayúsculas que debe tener el PIN.
"*Numérica*": Establece la cantidad de caracteres numéricos que debe tener el PIN.

**IMPORTANTE:**
**Una vez bloqueado, el Admin PIN NO se puede desbloquear.**

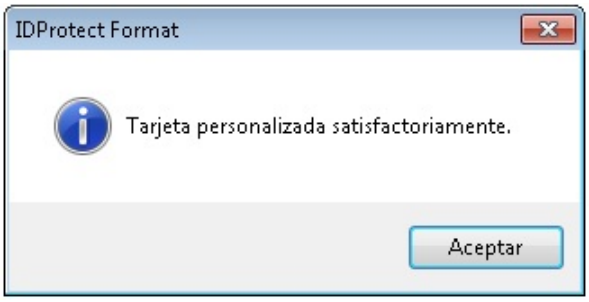
Una vez seleccionado el perfil deseado haga click en "**Formatear**". Si el MS-IDProtect (token usb o smartcard) ya estaba siendo utilizado por alguna persona, se necesitará ingresar el PIN de Administrador para formatearlo.




Espere mientras su MS-IDProtect Token USB es formateado.
No desconecte su dispositivo.




Una vez finalizado el formateo, el siguiente mensaje se mostrará.
Haga click en "*Aceptar*"




Este mensaje indica que el formateo del producto ha finalizado, tanto sea un token usb de Macroseguridad como una de las smartcards provistas.