# Tecnologías de control de acceso

## 1. Introducción

Gran número de organizaciones dentro del sector público se encuentran en la actualidad en un proceso de transformación digital. Se habla de tecnologías disruptivas que traen consigo un cambio de paradigma en el cual se diluye el concepto tradicional de seguridad basada en la protección de perímetro de sistemas o redes, debido a que las capacidades tecnológicas actuales permiten a los usuarios acceder a recursos de la organización en cualquier parte, en cualquier momento y desde cualquier dispositivo.

Si bien es cierto que para muchas organizaciones, como por ejemplo aquellas que manejan información clasificada, esta flexibilización puede no ser viable desde el punto de vista de seguridad, o al menos no en toda su extensión, la mayor parte se enfrentan al desafío de poder aprovechar la potencia tecnológica actual sin que ello suponga un detrimento de la seguridad de sus sistemas.

Así, actualmente, cualquier responsable de seguridad debe hacer frente, por una parte, al incremento en la amenaza que supone la hiperconectividad, movilidad y heterogeneidad de los sistemas TIC actuales y, por otra, al endurecimiento de las nuevas normativas de obligado cumplimiento (ej: ENS, RGPD).

En este contexto, cobran especial importancia aspectos relacionados con el control de acceso de usuarios a los sistemas o a los datos de un sistema, lo que ha propiciado un impulso en el desarrollo de tecnologías centradas en el control de acceso o en los subprocesos de identificación, autenticación y/o autorización.

## 2. Definición de tecnologías actuales de control de acceso

En este apartado nos centraremos principalmente en dos tipos de productos:

| NAC | ESM |
|---|---|
| (*Network Access Control*). | (*Enterprise Security Management*). |

## 3. Productos NAC (Network Access Control)

Un producto NAC (*Network Access Control*) es el que permite controlar el acceso de un dispositivo a la red de la organización en función de las políticas de seguridad configuradas.

Estas políticas que determinan si el dispositivo puede acceder o no, se pueden basar en autenticación (de usuario y/o dispositivo), en el chequeo de la postura de seguridad del dispositivo (política de pre-admisión), en la identidad o rol del usuario, etc.

También permiten aplicar políticas de post-admisión una vez que el dispositivo se ha conectado, y normalmente se basan en la integración con otros productos de seguridad de la organización. Por

ejemplo, el NAC podría imponer una política de contención del EndPoint en base a alguna alerta generada por un SIEM.

Las capacidades de un producto NAC suelen ser las siguientes:

| |
|---|
| *Profiling*: permiten descubrir, identificar y monitorizar los dispositivos conectados a la red. |
| Permiten bloquear el acceso a la red, o enviar los dispositivos a una VLAN de cuarentena. |
| Control de acceso granulado: permiten restringir el acceso a la red únicamente a los dispositivos autorizados y solo a los recursos necesarios. |
| Chequeo de la postura de seguridad de los dispositivos (actualización del antivirus, etc.). |
| Gestión de invitados (portal cautivo). |
| Integración bidireccional con otros productos de seguridad. |

## 4. Productos ESM (Enterprise Security Management)

Esta categoría de productos se divide en tres familias:

| PAM | IM | AM |
|---|---|---|
| (*Privileged Access Management*), | (*Identity Management*) | (*Access Management*) |

### 4.1. PAM – Privileged Access Management

Los productos PAM gestionan el acceso de los usuarios a cuentas privilegiadas en sistemas. Proporcionan un almacén seguro de credenciales. El producto, de forma automática, puede generar, mantener y actualizar las credenciales periódicamente, tanto en el almacén como en los propios sistemas, cumpliendo las políticas de la organización.

A través del producto, el usuario puede conectarse a un sistema sin necesidad de conocer las credenciales, ya que el producto las presentará al sistema en nombre del usuario. También graban y almacenan lo que han hecho los usuarios durante su sesión y detectan cuentas privilegiadas en sistemas.

### 4.2. IM – Identity Management

La función principal de estos productos es generar una identidad única para cada usuario, de forma que se le pueda identificar de forma unívoca, y contra la que asociar el resto de atributos, para la autenticación (credenciales), autorización (permisos) y otros atributos de usuario definidos por la Organización.

Cuando un usuario solicita el alta en el producto de gestión de identidades, a este proceso se le llama *enrollment* y consiste en la asignación a este usuario de su identificador único, la generación y emisión de sus credenciales, la definición del resto de atributos asociados al usuario, y la

propagación de todos estos datos al resto de sistemas de la organización que lo necesiten, a través de canales de comunicación seguros.

Estos productos suelen proporcionar:

| |
|---|
| *Provisioning* de usuarios: poder suministrar nuevos usuarios con sus atributos, a un repositorio corporativo, así como asociar o quitar atributos a los usuarios. |
| Generar, emitir y mantener credenciales asociadas a identidades de usuarios. |
| Publicar y mantener el "estado" operativo de las credenciales (activas, suspendidas o finalizadas). |
| Establecer canales de comunicación seguros con servidores de autenticación, auditoría, con el gestor de políticas y con cualquier sistema al que deba enviar datos y atributos de identidad. |

### 4.3. AM – Access Management

Los productos AM tienen como función principal proporcionar un punto de identificación, autenticación y autorización único al usuario, para los sistemas y aplicaciones corporativos (*Single-Sign-On*, SSO). Deben soportar múltiples tipos de autenticación, y deben proporcionar *Identity Federation* a través de protocolos estándar como SAML, etc.

Estos productos actúan como PDP (*Policy Decission Point*), tomando la decisión de si la acción solicitada por el usuario está permitida o no;y como PEP, (*Policy Enforcement Point*) ejecutando la decisión tomada y permitiendo o rechazando la petición del usuario.

**Contacto**

| | |
|---|---|
| **Correo electrónico CCN-PYTEC** | **ccn-pytec@cni.es** |
| **Twitter** | **@CCNPYTEC** |
| **LinkedIn** | **https://www.linkedin.com/company/CCN-PYTEC** |
| **Catálogo CPSTIC** | **Enlace web** |