Módulo 3. Federación de identidades

CÓRDOBA CREA FUTURO

1. Gestión centralizada de identidades y accesos web. Keycloak.

2. Acceso a Red de Confianza Cero y mínimos privilegios.

Referencias

1. Gestión centralizada de identidades y accesos web. Keycloak.

Gestión centralizada de identidades y accesos (IAM) web. Keycloak (protocolos SAML y OpenID Connect (OIDC))[

En las arquitecturas digitales actuales, las organizaciones operan múltiples aplicaciones web, plataformas internas y servicios distribuidos. Cada uno de estos sistemas requiere mecanismos de autenticación y autorización para garantizar que las personas accedan únicamente a los recursos que les corresponden. Cuando cada aplicación gestiona sus propios usuarios, contraseñas y permisos, se generan entornos fragmentados que dificultan la administración de identidades, aumentan el riesgo de errores de configuración y amplían la superficie de exposición frente a ataques de suplantación o uso indebido de credenciales.

En ese contexto, la gestión centralizada de identidades y accesos —conocida como Identity and Access Management (IAM)— permite organizar el control de autenticación y

autorización desde un único punto de administración. Este enfoque facilita integrar múltiples aplicaciones bajo un mismo sistema de identidad, reducir la duplicación de usuarios, aplicar políticas de seguridad coherentes y registrar de manera sistemática los eventos de acceso. Dentro de estas soluciones, plataformas como Keycloak ofrecen herramientas para implementar autenticación federada y control de acceso en aplicaciones web mediante estándares ampliamente utilizados.

Los protocolos Security Assertion Markup Language (SAML) y OpenID Connect (OIDC) permiten que distintas aplicaciones confíen en un mismo proveedor de identidad para autenticar usuarios y transmitir información relevante sobre su perfil. A partir de esta lógica, una persona puede autenticarse una sola vez y acceder a múltiples servicios sin repetir el proceso en cada sistema, manteniendo al mismo tiempo controles centralizados sobre permisos, políticas de seguridad y mecanismos de autenticación.

En esta unidad abordaremos los componentes que estructuran un sistema de identidad centralizado basado en Keycloak. Analizaremos cómo se organizan los dominios de identidad o realms, los clientes que

representan aplicaciones conectadas y los flujos de autenticación que regulan el intercambio de credenciales y tokens. Luego se examinará la forma en que los atributos del usuario se traducen en claims y roles utilizados por las aplicaciones para autorizar acciones específicas. También se estudiarán los mecanismos de autenticación multifactor y las políticas de acceso que permiten reforzar la seguridad en función del contexto del usuario. Finalmente, se analizará el papel de los registros de eventos y auditoría como herramientas para monitorear accesos, detectar anomalías y sostener procesos de control dentro de la gestión de identidades.

Conjunto de recursos o dominio (Realms), clientes y flujos

La gestión centralizada de identidades en aplicaciones web requiere una estructura que permita organizar usuarios, aplicaciones y políticas de acceso dentro de un mismo sistema de autenticación. En plataformas de gestión de identidades como Keycloak, esta organización se construye mediante tres componentes principales: los dominios de identidad o realms, los clientes que representan aplicaciones y los flujos de autenticación que regulan el intercambio de

credenciales y tokens entre los distintos actores del sistema (Keycloak, 2024).

Un realm representa un dominio independiente de gestión de identidades. Dentro de él se almacenan usuarios, credenciales, roles, políticas de autenticación y configuraciones de seguridad. Cada realm funciona como un espacio aislado que permite administrar identidades sin interferir con otros entornos. Por ejemplo, una organización puede mantener un realm para empleados internos y otro para clientes externos, permitiendo aplicar políticas de autenticación y autorización distintas según el contexto de uso de la plataforma.

Este aislamiento lógico facilita la administración de identidades en entornos complejos donde múltiples aplicaciones comparten un mismo proveedor de identidad. Al agrupar los elementos de autenticación dentro de un dominio específico, el sistema puede aplicar reglas coherentes de acceso, mantener registros de actividad asociados a cada entorno y evitar conflictos entre configuraciones de seguridad.

Dentro de cada realm se registran los clientes, que representan las aplicaciones o servicios que delegan la autenticación en el sistema de identidad. Cuando una

aplicación web se integra con Keycloak mediante protocolos como Security Assertion Markup Language (SAML) u OpenID Connect (OIDC), se configura como un cliente dentro del dominio correspondiente. Esta configuración permite que la aplicación confíe en el proveedor de identidad para autenticar usuarios y recibir información sobre sus permisos o atributos (Okta, 2023).

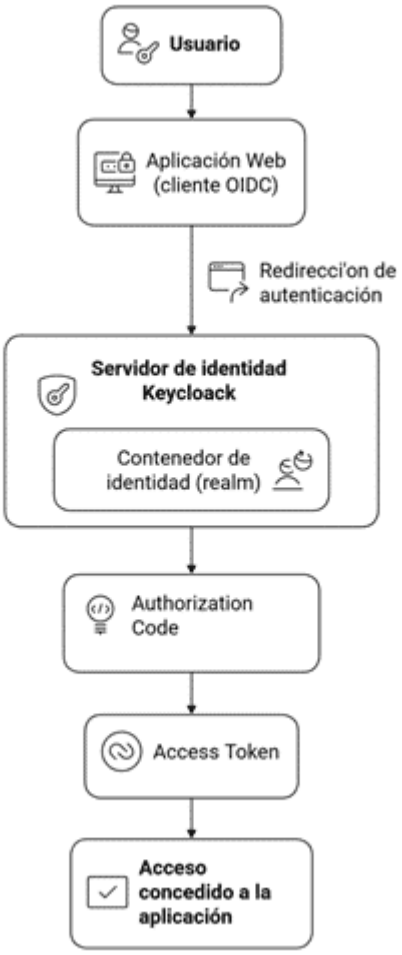
Cada cliente define parámetros que regulan cómo se produce la comunicación con el sistema de identidad. Entre estos parámetros se incluyen la dirección de redirección autorizada, los métodos de autenticación permitidos y los alcances de información que la aplicación puede recibir sobre el usuario. Estas configuraciones resultan fundamentales para evitar vulnerabilidades asociadas a redirecciones maliciosas o exposición innecesaria de información personal durante el proceso de autenticación.

La interacción entre el usuario, la aplicación y el proveedor de identidad se organiza mediante flujos de autenticación. Un flujo describe la secuencia de pasos que el sistema ejecuta para verificar la identidad del usuario y emitir los tokens que permiten acceder al servicio solicitado. En el caso de OpenID Connect, uno de los flujos más utilizados es el Authorization Code Flow, que intercambia credenciales y tokens a través de una serie de redirecciones controladas entre el navegador

del usuario, el cliente y el proveedor de identidad (Auth0, 2023).

Durante este proceso, la aplicación redirige al usuario hacia el proveedor de identidad para realizar la autenticación. Una vez verificada la identidad, el sistema genera un código de autorización que posteriormente se intercambia por un token de acceso. Este token contiene información sobre el usuario autenticado y permite que la aplicación determine si el acceso solicitado debe ser autorizado.

Figura 1. Arquitectura básica de autenticación federada con Keycloak



Fuente: elaboración propia.

El uso de flujos estructurados de autenticación contribuye a reducir riesgos asociados a la exposición directa de credenciales o al intercambio inseguro de información entre aplicaciones. Al centralizar el proceso en un proveedor de identidad confiable, las aplicaciones pueden delegar la verificación de credenciales y concentrarse en la gestión de permisos dentro de su propio contexto operativo.

Además de mejorar la seguridad, este modelo facilita la implementación de Single Sign-On (SSO). Cuando múltiples aplicaciones confían en el mismo proveedor de identidad, un usuario autenticado puede acceder a distintos servicios sin repetir el proceso de inicio de sesión. Esta característica simplifica la experiencia de uso y reduce la necesidad de gestionar múltiples credenciales dentro de una organización.

Desde una perspectiva operativa, la combinación de realms, clientes y flujos permite estructurar la arquitectura de identidad de manera clara y escalable. Los dominios organizan los entornos de autenticación, los clientes representan las aplicaciones integradas y los flujos regulan el proceso de verificación de identidad y emisión de tokens. Esta estructura constituye la base sobre la cual se implementan mecanismos más avanzados de control de acceso, como la asignación de roles, las políticas de autenticación multifactor y los sistemas de auditoría de eventos.

Mapeo de claims y roles

En los sistemas de gestión de identidades federadas, la autenticación del usuario constituye sólo una parte del proceso de control de acceso. Una vez verificada la identidad, las aplicaciones necesitan información adicional que permita

determinar qué acciones puede realizar cada usuario dentro del sistema. Esta información se transmite mediante atributos incluidos en los tokens de autenticación y autorización. En entornos basados en *OpenID Connect* y *SAML*, estos atributos se conocen como *claims*.

Los *claims* representan afirmaciones sobre el usuario autenticado que el proveedor de identidad comunica a las aplicaciones cliente. Estas afirmaciones pueden incluir datos básicos, como el identificador del usuario, su dirección de correo electrónico o su nombre, pero también pueden contener información relevante para la autorización, como pertenencia a grupos, roles asignados o atributos organizacionales. En el contexto de OIDC, estos datos suelen enviarse dentro de un token JWT (JSON Web Token), que la aplicación puede interpretar para tomar decisiones de acceso (Okta, 2023).

Para que estas afirmaciones resulten útiles en el control de acceso, es necesario establecer una correspondencia entre los atributos presentes en el sistema de identidad y los permisos que las aplicaciones reconocen internamente. Este proceso se denomina **mapeo de *claims***. A través de este mecanismo, el proveedor de identidad transforma los datos almacenados en el sistema de usuarios en atributos

estructurados que las aplicaciones pueden interpretar durante el proceso de autorización.

En plataformas como Keycloak, el mapeo de *claims* se configura mediante componentes llamados *protocol mappers*. Estos elementos permiten seleccionar información almacenada en el perfil del usuario —por ejemplo, roles, grupos o atributos personalizados— y transformarla en campos específicos dentro del token emitido durante la autenticación. De esta forma, la aplicación cliente recibe información contextual sobre el usuario que puede utilizar para habilitar o restringir funcionalidades dentro del sistema (Keycloak, 2024).

El mapeo de roles constituye uno de los casos más frecuentes de utilización de *claims*. En este modelo, los permisos del usuario se definen en el proveedor de identidad mediante roles, que representan funciones o responsabilidades dentro de la organización. Durante el proceso de autenticación, estos roles se incorporan al token emitido por el sistema de identidad. La aplicación cliente puede entonces leer el contenido del token y verificar si el usuario posee los permisos necesarios para acceder a determinados recursos o ejecutar acciones específicas.

La separación entre autenticación y autorización que ofrecen los sistemas IAM resulta especialmente útil en arquitecturas distribuidas. En lugar de mantener bases de datos de usuarios y permisos en cada aplicación, el sistema de identidad centralizado gestiona los roles y transmite esa información a las aplicaciones mediante tokens firmados digitalmente. Este enfoque reduce la duplicación de datos, facilita la administración de permisos y mejora la coherencia en la aplicación de políticas de acceso.

Desde una perspectiva de seguridad, el uso de *claims* y roles también contribuye a implementar el principio de mínimo privilegio. Al definir roles específicos y transmitir únicamente la información necesaria en cada token, el sistema limita el acceso del usuario a las funciones estrictamente requeridas para su actividad. Este enfoque reduce la exposición a errores de configuración o a posibles abusos de privilegios dentro de la infraestructura digital.

En la práctica, el diseño del mapeo de *claims* requiere un análisis cuidadoso de los atributos que se compartirán con las aplicaciones. Incluir demasiada información en los tokens puede aumentar el riesgo de exposición de datos sensibles, mientras que un conjunto de atributos demasiado limitado puede impedir que las aplicaciones apliquen correctamente sus reglas de autorización. Por esta razón, los marcos de

diseño de identidad recomiendan definir *scopes* y atributos de forma explícita, asegurando que cada aplicación reciba únicamente la información necesaria para operar.

Otro aspecto relevante del mapeo de roles en sistemas como Keycloak es la posibilidad de utilizar **roles compuestos**. Este mecanismo permite agrupar múltiples permisos dentro de un rol de mayor nivel. Por ejemplo, un rol administrativo puede incluir automáticamente permisos de lectura, escritura y gestión de usuarios. Esta estructura jerárquica facilita la administración de permisos en entornos donde existen múltiples aplicaciones y niveles de acceso.

Finalmente, el mapeo de *claims* y roles constituye uno de los elementos fundamentales para integrar sistemas de identidad con arquitecturas de control de acceso basadas en contexto. Al transmitir información estructurada sobre el usuario, el proveedor de identidad permite que las aplicaciones y los sistemas de seguridad evalúen políticas dinámicas de autorización, que pueden considerar factores adicionales como el dispositivo utilizado, la ubicación de acceso o el nivel de riesgo de la sesión. De esta forma, los atributos incluidos en los tokens se convierten en una pieza clave para

implementar modelos modernos de control de acceso en entornos digitales.

Autenticación multifactor (MFA) y políticas de acceso

En los sistemas modernos de gestión de identidades, verificar únicamente una contraseña resulta insuficiente para proteger el acceso a aplicaciones y recursos críticos. Las credenciales pueden verse comprometidas mediante ataques de phishing, reutilización de contraseñas o filtraciones de bases de datos. Para reducir estos riesgos, los sistemas de identidad incorporan mecanismos de autenticación multifactor (Multi-Factor Authentication, MFA), que exigen al usuario demostrar su identidad mediante más de un tipo de evidencia durante el proceso de autenticación.

La autenticación multifactor se basa en la combinación de distintos factores de verificación. Estos factores suelen clasificarse en tres categorías: algo que el usuario conoce (por ejemplo, una contraseña o PIN), algo que el usuario posee (como un dispositivo móvil, una llave de seguridad o un token físico) y algo que el usuario es (por ejemplo, una característica biométrica). Al exigir la presencia simultánea

de dos o más de estos factores, el sistema reduce significativamente la probabilidad de que un atacante pueda acceder a una cuenta incluso si ha obtenido una de las credenciales (SentinelOne, 2024).

En plataformas de gestión de identidades como Keycloak, el MFA se implementa mediante flujos de autenticación configurables que permiten añadir pasos adicionales de verificación durante el inicio de sesión. Estos pasos pueden incluir el envío de códigos temporales generados por aplicaciones autenticadoras, el uso de tokens basados en tiempo (Time-based One-Time Password, TOTP) o la validación mediante dispositivos registrados previamente por el usuario. La flexibilidad de estos flujos permite adaptar el proceso de autenticación a distintos niveles de seguridad según las necesidades de la organización (Keycloak, 2024).

La integración del MFA dentro de un sistema de identidad centralizado facilita aplicar políticas de seguridad consistentes en todas las aplicaciones que dependen del proveedor de identidad. En lugar de configurar mecanismos de verificación adicionales en cada aplicación de manera independiente, el sistema IAM gestiona el proceso de autenticación y transmite a las aplicaciones el resultado de la verificación mediante los tokens emitidos durante el proceso de autenticación federada.

Además de reforzar la verificación de identidad, los sistemas IAM permiten definir políticas de autenticación que determinan cuándo y cómo debe aplicarse el MFA. Estas políticas pueden basarse en distintos factores contextuales, como la dirección IP desde la cual se realiza el acceso, la ubicación geográfica del usuario, el dispositivo utilizado o el nivel de riesgo asociado a la sesión. Este enfoque permite ajustar el nivel de verificación requerido según el contexto operativo de cada acceso.

Por ejemplo, una organización puede permitir el acceso con un solo factor cuando el usuario se conecta desde la red corporativa, pero exigir MFA cuando el acceso se realiza desde una ubicación externa o desde un dispositivo no reconocido. Este tipo de configuración permite equilibrar seguridad y usabilidad, evitando que los mecanismos de protección generen fricciones innecesarias en entornos de trabajo habituales.

La aplicación de políticas dinámicas de autenticación constituye uno de los fundamentos de los modelos modernos de control de acceso basados en identidad. En estos modelos, el sistema de identidad evalúa continuamente distintos atributos asociados al usuario y a la sesión antes de conceder acceso a los recursos solicitados. Este enfoque resulta coherente con los principios de

arquitecturas de confianza cero (Zero Trust), donde cada solicitud de acceso debe verificarse de forma explícita en función del contexto y del nivel de riesgo asociado (NIST, 2020).

En entornos donde múltiples aplicaciones comparten un mismo proveedor de identidad, las políticas de autenticación también facilitan la administración centralizada de los mecanismos de seguridad. Los administradores pueden definir reglas de acceso que se aplican automáticamente a todas las aplicaciones integradas con el sistema IAM, lo que simplifica la gestión de seguridad y reduce la probabilidad de configuraciones inconsistentes entre servicios.

La implementación adecuada de MFA requiere, sin embargo, considerar ciertos aspectos operativos. Uno de los desafíos más comunes consiste en garantizar que los usuarios puedan recuperar el acceso a sus cuentas cuando pierden el dispositivo utilizado para el segundo factor de autenticación. Para abordar este problema, muchos sistemas incorporan mecanismos de recuperación controlada, como códigos de respaldo o procesos de verificación administrados por el equipo de soporte.

Otro aspecto importante es la protección frente a ataques dirigidos específicamente a los sistemas de autenticación

multifactor. En los últimos años se han documentado técnicas como la fatiga de notificaciones de autenticación, donde un atacante intenta forzar al usuario a aprobar repetidas solicitudes de acceso. Para mitigar estos escenarios, las organizaciones suelen complementar el MFA con controles adicionales, como limitaciones de intentos, detección de comportamientos anómalos y monitoreo de eventos de autenticación.

En conjunto, la autenticación multifactor y las políticas de acceso representan componentes fundamentales dentro de una arquitectura moderna de gestión de identidades. Al reforzar la verificación de identidad y permitir aplicar controles basados en contexto, estos mecanismos contribuyen a reducir el riesgo de compromisos de credenciales y fortalecen la seguridad del acceso a aplicaciones distribuidas en entornos digitales.

Logs y auditoría en sistemas de gestión de identidades

En los sistemas de gestión de identidades y accesos, la autenticación y la autorización representan únicamente una parte del control de seguridad. Para garantizar la integridad del sistema y detectar comportamientos anómalos, resulta necesario registrar de forma sistemática las actividades relacionadas con el acceso de los usuarios. Estos registros se conocen como logs de eventos y constituyen una fuente fundamental de información para el monitoreo de seguridad, la detección de incidentes y los procesos de auditoría.

Los sistemas IAM generan registros que documentan diferentes eventos asociados al ciclo de vida de la autenticación. Entre estos eventos se incluyen intentos de inicio de sesión exitosos y fallidos, emisión de tokens, cambios en la configuración de roles o políticas de acceso, y acciones administrativas realizadas dentro del sistema. Cada uno de estos registros contiene información contextual como la identidad del usuario, la dirección IP de origen, la aplicación involucrada y la marca temporal del evento (Keycloak, 2024).

En plataformas como Keycloak, el registro de eventos se gestiona mediante mecanismos de event logging que permiten capturar y almacenar información detallada sobre las operaciones realizadas dentro del sistema de identidad.

Estos eventos pueden clasificarse en diferentes categorías, como eventos de autenticación de usuarios, eventos administrativos o eventos relacionados con el funcionamiento interno del sistema. Esta clasificación facilita la organización de los registros y permite a los equipos de seguridad identificar rápidamente los eventos relevantes durante una investigación (Keycloak, 2024).

El análisis de los logs resulta especialmente importante para detectar patrones de comportamiento que puedan indicar intentos de compromiso de cuentas. Por ejemplo, múltiples intentos fallidos de autenticación desde una misma dirección IP pueden señalar un posible ataque de fuerza bruta. Del mismo modo, accesos realizados desde ubicaciones geográficas inusuales o desde dispositivos no registrados pueden indicar un posible uso indebido de credenciales. La disponibilidad de registros detallados permite identificar estas anomalías y activar mecanismos de respuesta temprana.

Además de su utilidad operativa para la detección de incidentes, los logs de autenticación cumplen una función relevante en los procesos de auditoría de seguridad. Muchas organizaciones deben demostrar que aplican controles adecuados sobre el acceso a sistemas críticos y datos sensibles. Los registros generados por el sistema de

identidad permiten reconstruir el historial de accesos, identificar qué usuarios accedieron a determinados recursos y verificar si las políticas de seguridad se aplicaron correctamente durante cada sesión.

Para que estos registros resulten útiles en auditorías y procesos de investigación, deben cumplir ciertos criterios de calidad. En primer lugar, los logs deben ser completos y contener suficiente información contextual para comprender el evento registrado. En segundo lugar, deben almacenarse de forma segura para evitar alteraciones o eliminaciones no autorizadas. Finalmente, deben mantenerse durante un período de tiempo definido por las políticas de seguridad o por los requisitos regulatorios de la organización.

En entornos empresariales, los registros generados por los sistemas IAM suelen integrarse con plataformas de monitoreo de seguridad, como sistemas SIEM (Security Information and Event Management). Esta integración permite correlacionar eventos provenientes de diferentes fuentes dentro de la infraestructura tecnológica, como servidores, aplicaciones y dispositivos de red. Al combinar estos registros, los equipos de seguridad pueden obtener una visión más completa de la actividad dentro del sistema y

detectar incidentes que podrían pasar desapercibidos si se analizaran los registros de forma aislada.

La integración con herramientas de análisis también facilita la generación de alertas automáticas ante determinados eventos. Por ejemplo, el sistema puede emitir una alerta cuando se detectan múltiples intentos fallidos de autenticación en un intervalo corto de tiempo o cuando un usuario intenta acceder a recursos para los cuales no posee permisos asignados. Estas alertas permiten a los equipos de seguridad actuar de manera preventiva antes de que un incidente evolucione hacia un compromiso mayor.

Otro aspecto importante en la gestión de logs de identidad es la trazabilidad de las acciones administrativas. Las modificaciones realizadas por administradores dentro del sistema IAM —como cambios en roles, políticas de acceso o configuraciones de autenticación— deben registrarse de manera detallada. Esta práctica permite identificar quién realizó cada cambio, cuándo se efectuó y qué impacto tuvo sobre la configuración del sistema.

En conjunto, los mecanismos de registro de eventos y auditoría constituyen un componente esencial dentro de la arquitectura de gestión de identidades. Al proporcionar visibilidad sobre las actividades de autenticación y

administración, los logs permiten detectar comportamientos anómalos, respaldar procesos de investigación de incidentes y demostrar el cumplimiento de políticas de seguridad organizacionales. En entornos donde múltiples aplicaciones dependen de un proveedor de identidad centralizado, la correcta gestión de estos registros resulta fundamental para mantener la confianza en el sistema de autenticación y proteger el acceso a los recursos digitales.

Los mecanismos de autenticación, gestión de roles y control de acceso analizados en la unidad anterior constituyen la base sobre la cual se construyen los modelos modernos de acceso a recursos en redes distribuidas. A partir de estos fundamentos, las arquitecturas de confianza cero utilizan la identidad como principal punto de control del acceso a aplicaciones y servicios.

CONTINUAR

2. Acceso a Red de Confianza Cero y mínimos privilegios.

Acceso a Red de Confianza Cero (o ZTNA, Zero Trust Network Access) y mínimos privilegios

En las infraestructuras digitales contemporáneas, las organizaciones operan aplicaciones, servicios en la nube y recursos internos accesibles desde múltiples redes y dispositivos. En este contexto, el modelo tradicional de seguridad basado en perímetros de red definidos pierde eficacia. Durante muchos años, los sistemas de seguridad se apoyaron en la idea de que los recursos ubicados dentro de la red corporativa podían considerarse confiables, mientras que el acceso desde el exterior requería controles más estrictos. Sin embargo, la expansión del trabajo remoto, la adopción de servicios en la nube y la interconexión entre plataformas han transformado este escenario, haciendo que los límites de la red resulten cada vez menos claros.

Frente a este cambio, los modelos de seguridad actuales se orientan hacia un enfoque donde la verificación de identidad y el contexto del acceso adquieren un papel central. En lugar de asumir confianza basada en la ubicación dentro de la red, los sistemas modernos evalúan cada solicitud de acceso de manera explícita, considerando factores como la identidad del usuario, el dispositivo utilizado, la ubicación desde la cual se realiza la conexión y el nivel de riesgo asociado a la sesión. Este enfoque se conoce como arquitectura de confianza cero o Zero Trust Architecture (NIST, 2020).

Dentro de este modelo, el acceso a recursos de red se gestiona mediante mecanismos denominados Zero Trust Network Access (ZTNA). Este enfoque permite establecer conexiones seguras entre usuarios y aplicaciones sin exponer directamente los sistemas internos a la red pública. En lugar de permitir acceso amplio a la infraestructura, cada solicitud se evalúa individualmente y se concede únicamente el acceso mínimo necesario para realizar una tarea específica.

El funcionamiento de ZTNA se apoya en sistemas de gestión de identidades y autenticación centralizada. Tal como se analizó en la unidad anterior, plataformas IAM permiten verificar la identidad del usuario, aplicar políticas de autenticación multifactor y transmitir información contextual mediante tokens de acceso. En el modelo de

confianza cero, estos mecanismos se combinan con controles adicionales que evalúan continuamente el contexto de la conexión antes de permitir el acceso a los recursos.

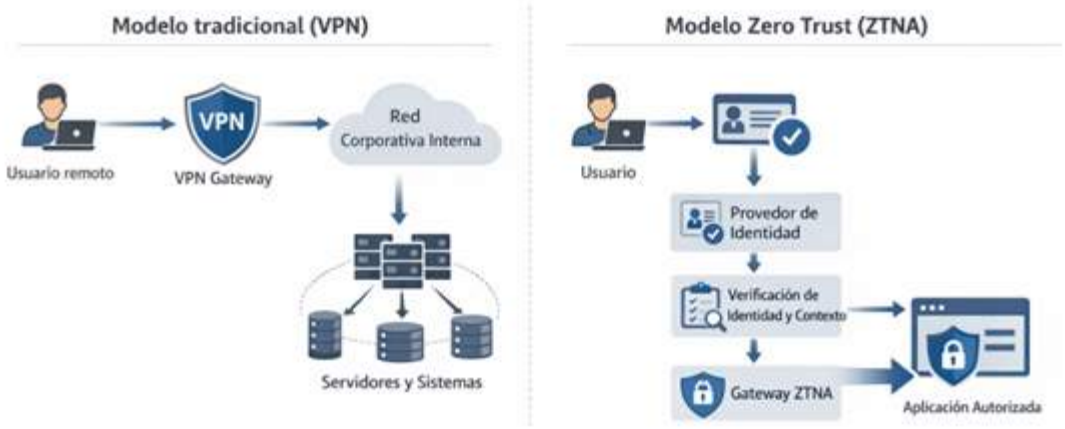
En esta unidad analizaremos los principios que estructuran las arquitecturas de confianza cero y los patrones utilizados para implementar control de acceso basado en identidad y contexto. También examinaremos mecanismos de acceso granular como el micro-bypass controlado y los métodos utilizados para medir la exposición de los sistemas frente a posibles accesos no autorizados. A través de estos conceptos se busca comprender cómo las organizaciones diseñan infraestructuras de acceso seguras en entornos donde la identidad se convierte en el principal punto de control del sistema.

Principios y patrones de Zero Trust

El modelo de confianza cero (Zero Trust) surge como respuesta a las limitaciones de los enfoques tradicionales de

seguridad de red basados en perímetros. En estos modelos clásicos, los sistemas ubicados dentro de la red corporativa eran considerados confiables, mientras que el acceso externo era tratado como potencialmente hostil. Sin embargo, la adopción de servicios en la nube, la movilidad de los usuarios y la interconexión entre plataformas han reducido la eficacia de este enfoque, ya que los recursos de una organización pueden encontrarse distribuidos en múltiples entornos tecnológicos. Frente a este escenario, la arquitectura de confianza cero propone un cambio conceptual: ningún acceso se considera confiable por defecto, independientemente de la ubicación desde la cual se origine (NIST, 2020).

Figura 2. Comparación entre modelo de acceso tradicional basado en perímetro y modelo Zero Trust (ZTNA)



Fuente: elaboración propia.

En lugar de confiar en la posición dentro de una red, el modelo Zero Trust establece que cada solicitud de acceso debe verificarse de manera explícita antes de conceder acceso a un recurso. Esta verificación se basa en múltiples atributos asociados al usuario, al dispositivo y al contexto de la sesión. De esta manera, el control de acceso deja de depender del perímetro de red y se centra en la identidad y en la evaluación continua de la confianza.

Uno de los principios fundamentales del modelo consiste en verificar siempre la identidad del solicitante. Esto implica que cada interacción con un recurso debe estar respaldada por mecanismos de autenticación robustos, como sistemas de autenticación multifactor o tokens de identidad emitidos por proveedores de identidad confiables. La verificación de identidad no ocurre únicamente al inicio de la sesión, sino que puede reevaluarse durante el acceso cuando cambian las condiciones de la conexión o el nivel de riesgo asociado a la actividad.

Otro principio clave es la aplicación del acceso con privilegios mínimos. Bajo este enfoque, los usuarios reciben

únicamente los permisos necesarios para realizar sus tareas específicas y solo durante el tiempo estrictamente requerido. Este principio reduce la superficie de exposición del sistema, ya que limita el alcance de posibles accesos indebidos o compromisos de credenciales. En entornos de confianza cero, la gestión de identidades y roles desempeña un papel central para garantizar que los permisos asignados reflejen las responsabilidades reales de cada usuario dentro de la organización.

El modelo Zero Trust también incorpora el principio de segmentación de recursos. En lugar de permitir acceso amplio a segmentos completos de la red, los recursos se organizan en unidades más pequeñas y controladas. Cada solicitud de acceso se evalúa individualmente y se concede únicamente hacia el recurso específico requerido. Este enfoque reduce la posibilidad de movimientos laterales dentro de la infraestructura en caso de que un atacante logre comprometer una cuenta o un sistema.

Además de verificar la identidad del usuario, el modelo evalúa el contexto de la conexión. Factores como la ubicación geográfica, el tipo de dispositivo, el estado de seguridad del sistema o el comportamiento previo del usuario pueden influir en la decisión de acceso. Esta evaluación contextual permite ajustar dinámicamente las

políticas de seguridad, aumentando los requisitos de verificación cuando se detectan condiciones que elevan el nivel de riesgo.

Desde una perspectiva arquitectónica, estos principios se materializan mediante patrones de implementación que organizan los componentes del sistema de seguridad. Uno de los patrones más comunes consiste en la utilización de puertas de acceso controladas por identidad, que actúan como intermediarios entre los usuarios y las aplicaciones. En lugar de permitir conexiones directas a los recursos internos, los usuarios se autentican primero ante un sistema de identidad que evalúa sus credenciales y el contexto del acceso antes de establecer la conexión.

Otro patrón relevante es el uso de túneles de acceso específicos para aplicaciones, característico de los sistemas de Zero Trust Network Access. En este modelo, el usuario no obtiene acceso general a la red corporativa, sino únicamente a la aplicación que necesita utilizar. La conexión se establece de forma directa entre el usuario autenticado y el recurso autorizado, evitando que otros sistemas de la red queden expuestos al mismo acceso.

La arquitectura Zero Trust también se apoya en sistemas de monitoreo continuo que analizan el comportamiento de los

accesos y generan alertas ante patrones anómalos. Este monitoreo permite detectar intentos de acceso inusuales, cambios en el comportamiento de los usuarios o posibles compromisos de credenciales. Al combinar controles de identidad, segmentación de recursos y monitoreo continuo, el sistema mantiene una evaluación permanente del nivel de confianza asociado a cada sesión.

Otro patrón operativo asociado a Zero Trust es la integración con sistemas de gestión centralizada de identidades. Las plataformas IAM proporcionan los mecanismos necesarios para autenticar usuarios, gestionar roles y transmitir atributos de identidad a las aplicaciones. Esta integración permite que las decisiones de acceso se basen en información consistente sobre la identidad del usuario, evitando la fragmentación de controles de seguridad entre múltiples sistemas.

En conjunto, los principios y patrones del modelo Zero Trust redefinen la manera en que se gestiona el acceso a recursos en entornos digitales distribuidos. Al sustituir la confianza implícita en la red por una verificación continua basada en identidad y contexto, las organizaciones pueden construir infraestructuras más

resistentes frente a ataques que buscan explotar credenciales comprometidas o configuraciones de red permisivas. Este enfoque establece las bases para mecanismos más avanzados de control de acceso que analizaremos en los siguientes apartados de la unidad.

Acceso por identidad y contexto

En los modelos tradicionales de seguridad de red, las decisiones de acceso se basaban principalmente en la ubicación del usuario dentro de la infraestructura. Si un dispositivo se encontraba dentro de la red corporativa, se asumía que podía acceder a determinados recursos con un nivel relativamente amplio de confianza. Este enfoque dependía de la existencia de un perímetro de red claramente definido. Sin embargo, en entornos donde las aplicaciones, los usuarios y los dispositivos se distribuyen entre redes corporativas, servicios en la nube y conexiones remotas, este modelo resulta insuficiente para garantizar un control de acceso adecuado.

Las arquitecturas de confianza cero proponen un enfoque diferente, en el que el acceso a los recursos se determina a partir de l**a identidad del usuario y del contexto en el que**

se realiza la solicitud. En lugar de confiar en la ubicación dentro de la red, el sistema evalúa múltiples atributos asociados a cada intento de acceso antes de permitir la conexión. Este enfoque permite aplicar controles de seguridad más precisos y adaptables a entornos distribuidos (NIST, 2020).

El primer elemento que interviene en este modelo es la **identidad digital del usuario**. La identidad se valida mediante mecanismos de autenticación gestionados por sistemas de gestión de identidades, como los analizados en la unidad anterior. Estos sistemas verifican las credenciales del usuario y generan tokens que contienen información sobre su perfil, roles y atributos relevantes para el control de acceso. A partir de esta información, las aplicaciones pueden determinar si el usuario posee los permisos necesarios para acceder al recurso solicitado.

Sin embargo, la identidad por sí sola no resulta suficiente para evaluar el nivel de riesgo de una conexión. Por esta razón, los sistemas de acceso basados en confianza cero incorporan también información contextual sobre la sesión. Este contexto puede incluir elementos como el dispositivo desde el cual se realiza el acceso, la dirección IP de origen, la ubicación geográfica aproximada, el horario de conexión o el estado de seguridad del equipo utilizado. Al combinar estos

factores con la identidad del usuario, el sistema obtiene una visión más completa del intento de acceso.

La evaluación conjunta de identidad y contexto permite aplicar **políticas de acceso adaptativas.** Estas políticas establecen diferentes condiciones que deben cumplirse antes de permitir la conexión a un recurso determinado. Por ejemplo, un usuario autenticado puede acceder a una aplicación desde un dispositivo corporativo sin requisitos adicionales, pero si intenta conectarse desde una red externa o desde un equipo no registrado, el sistema puede exigir mecanismos adicionales de verificación, como autenticación multifactor.

Este tipo de políticas dinámicas contribuye a reducir el riesgo asociado a credenciales comprometidas. Si un atacante obtiene la contraseña de un usuario legítimo, el sistema puede detectar inconsistencias en el contexto de acceso —como una ubicación geográfica inusual o un dispositivo desconocido— y bloquear la conexión o solicitar verificaciones adicionales antes de permitir el acceso.

En los sistemas de Zero Trust Network Access, el acceso basado en identidad y contexto se implementa mediante intermediarios de autenticación que actúan como punto de control entre el usuario y las aplicaciones. Antes de

establecer la conexión, el sistema verifica la identidad del solicitante y evalúa las condiciones contextuales definidas en las políticas de seguridad. Solo después de superar estas verificaciones se establece un canal seguro hacia el recurso autorizado (Cloudflare, 2023).

Este mecanismo permite limitar la exposición directa de los sistemas internos. En lugar de permitir que los usuarios se conecten directamente a la red corporativa, el acceso se concede únicamente a aplicaciones específicas y solo cuando se cumplen las condiciones de seguridad definidas por la organización. De esta manera, el sistema reduce la superficie de ataque y dificulta que un actor malicioso utilice credenciales comprometidas para explorar otros recursos de la infraestructura.

Otro aspecto importante del acceso basado en identidad y contexto es la posibilidad de realizar **evaluaciones continuas de confianza** durante la sesión. En algunos sistemas de seguridad, las condiciones del acceso se revisan periódicamente mientras la conexión permanece activa. Si el sistema detecta cambios en el contexto —por ejemplo, una modificación en la dirección IP o en el estado del dispositivo — puede exigir una nueva verificación de identidad o incluso finalizar la sesión para prevenir accesos indebidos.

La incorporación de estas evaluaciones continuas transforma el control de acceso en un proceso dinámico. En lugar de depender únicamente de la autenticación inicial, el sistema mantiene un análisis permanente del nivel de confianza asociado a cada sesión. Este enfoque resulta especialmente relevante en entornos donde los usuarios acceden a recursos críticos desde dispositivos móviles o desde redes que pueden cambiar durante la sesión.

Además de mejorar la seguridad, el acceso basado en identidad y contexto facilita la integración entre sistemas de identidad y herramientas de monitoreo de seguridad. Los eventos generados durante el proceso de evaluación —como intentos de acceso bloqueados, cambios en el contexto de la sesión o activación de factores adicionales de autenticación — pueden registrarse y analizarse mediante plataformas de monitoreo. Esta información permite a los equipos de seguridad identificar patrones de comportamiento anómalos y ajustar las políticas de acceso cuando sea necesario.

En conjunto, el acceso basado en identidad y contexto constituye uno de los elementos centrales de las arquitecturas de confianza cero. Al combinar

verificación de identidad, evaluación contextual y control dinámico de las sesiones, las organizaciones pueden establecer mecanismos de acceso más adaptables y resistentes frente a amenazas que buscan explotar credenciales comprometidas o configuraciones de red excesivamente permisivas. Este enfoque sienta las bases para mecanismos de control más granulares que analizaremos en los siguientes apartados de la unidad.

Tabla 1. Relación entre componentes de gestión de identidad y control de acceso en arquitecturas Zero Trust

Componente	Función en el sistema IAM	Papel dentro del modelo Zero Trust
Realm	Dominio de gestión de identidades que agrupa usuarios, roles y políticas	Permite separar contextos de autenticación y aplicar políticas específicas de acceso
Cliente (Application Client)	Aplicación que delega autenticación	Punto de acceso controlado a recursos protegidos

	en el proveedor de identidad	
Claims	Atributos del usuario incluidos en el token de autenticación	Proporcionan información contextual utilizada para evaluar políticas de acceso
Roles	Permisos asignados a usuarios o grupos	Permiten aplicar el principio de privilegio mínimo
MFA	Verificación adicional de identidad mediante múltiples factores	Reduce el riesgo asociado a credenciales comprometidas
Logs de identidad	Registro de eventos de autenticación y administración	Permiten monitorear accesos y detectar comportamientos anómalos
Evaluación de contexto	Análisis del dispositivo, ubicación o estado de la sesión	Permite aplicar políticas dinámicas de acceso
ZTNA Gateway	Punto de control entre usuario y aplicación	Autoriza conexiones específicas sin exponer la red interna

Fuente: elaboración propia con base en NIST (2020), Keycloak (2024) y CISA (2023).

Micro-bypass controlado.

En las arquitecturas de confianza cero, el acceso a los recursos se concede de forma estrictamente controlada y limitada a las necesidades específicas del usuario o del servicio que realiza la solicitud. Este enfoque reduce la superficie de exposición del sistema y dificulta que un actor malicioso pueda moverse lateralmente dentro de la infraestructura. Sin embargo, en entornos operativos reales existen situaciones donde ciertas actividades administrativas, procesos de mantenimiento o integraciones entre sistemas requieren mecanismos de acceso temporales o excepcionales. En este contexto aparece el concepto de micro-bypass controlado.

El micro-bypass controlado puede entenderse como un mecanismo que permite habilitar accesos específicos, temporales y altamente restringidos dentro de un entorno que opera bajo principios de confianza cero. A diferencia de los modelos tradicionales de excepción de seguridad —donde se abrían segmentos completos de red o se

otorgaban permisos amplios para facilitar tareas operativas —, el micro-bypass busca mantener el control granular del acceso incluso cuando se requiere permitir una excepción.

En este modelo, las excepciones de acceso se aplican únicamente a un recurso determinado, durante un período de tiempo limitado y bajo condiciones claramente definidas. De esta forma, el sistema evita introducir vulnerabilidades estructurales en la arquitectura de seguridad. El acceso se habilita exclusivamente para la tarea necesaria y se revoca automáticamente una vez finalizada la operación.

El uso de micro-bypass controlado resulta especialmente relevante en tareas administrativas o de mantenimiento. Por ejemplo, un administrador puede necesitar acceso temporal a un servidor específico para realizar una actualización de software o para revisar un incidente de seguridad. En lugar de otorgar acceso amplio a la red interna, el sistema de control de acceso puede generar una autorización temporal que permita conectarse únicamente a ese servidor y solo durante el tiempo requerido para realizar la tarea.

En arquitecturas de confianza cero, este tipo de acceso temporal suele gestionarse mediante sistemas de identidad y control de privilegios. Las solicitudes de acceso se autentican utilizando los mecanismos de identidad

existentes —como autenticación multifactor o tokens de identidad— y posteriormente se evalúan las políticas que determinan si el acceso excepcional puede concederse. Este proceso permite mantener la coherencia del modelo de seguridad incluso cuando se requieren permisos adicionales para tareas específicas.

El micro-bypass controlado también se relaciona con los principios de acceso con privilegios mínimos y privilegios temporales, ampliamente utilizados en sistemas de gestión de identidades y control de acceso privilegiado. Bajo este enfoque, los permisos administrativos no se asignan de manera permanente, sino que se activan únicamente cuando el usuario necesita realizar una tarea concreta. Una vez finalizada la actividad, el sistema revoca automáticamente los privilegios adicionales.

Este mecanismo contribuye a reducir el riesgo asociado a cuentas con privilegios elevados. En los modelos tradicionales de seguridad, las cuentas administrativas permanentes representan uno de los objetivos principales para los atacantes, ya que permiten acceder a múltiples recursos dentro de la infraestructura. Al limitar la duración y el alcance de los permisos administrativos, el micro-bypass reduce significativamente el impacto potencial de un compromiso de credenciales.

Además del control temporal del acceso, los sistemas que implementan micro-bypass suelen incorporar mecanismos de registro y monitoreo de las actividades realizadas durante el acceso excepcional. Cada solicitud de bypass, el momento en que se concede el permiso y las acciones ejecutadas durante la sesión quedan registradas dentro del sistema de auditoría. Estos registros permiten verificar que los accesos excepcionales se utilicen únicamente para los fines autorizados y facilitan la investigación de incidentes cuando resulta necesario.

Otro aspecto importante es que el micro-bypass controlado se aplica generalmente a niveles muy específicos de la infraestructura, como aplicaciones individuales, servicios concretos o interfaces administrativas particulares. Este enfoque evita que la excepción afecte a segmentos amplios de la red o a múltiples sistemas al mismo tiempo. Al limitar el alcance del acceso, la arquitectura de seguridad mantiene el principio de segmentación que caracteriza a los modelos de confianza cero.

En entornos donde las organizaciones utilizan herramientas de automatización y orquestación de seguridad, los micro-bypass también pueden gestionarse mediante flujos de aprobación automatizados. Un sistema puede requerir que la solicitud de acceso excepcional sea aprobada por un

supervisor o por un sistema de políticas antes de habilitar el permiso temporal. Este proceso refuerza la gobernanza del acceso privilegiado y permite mantener un registro claro de las decisiones de autorización.

En conjunto, el micro-bypass controlado constituye una estrategia que permite equilibrar seguridad y operatividad dentro de las arquitecturas de confianza cero. Mientras que el modelo Zero Trust restringe el acceso por defecto, los mecanismos de bypass controlado ofrecen una forma segura de habilitar excepciones cuando las operaciones del sistema lo requieren. Al limitar el alcance, la duración y las condiciones del acceso excepcional, este enfoque mantiene la coherencia del modelo de seguridad y reduce los riesgos asociados a configuraciones de acceso excesivamente permisivas.

Este control granular del acceso excepcional se complementa con los mecanismos de monitoreo y evaluación continua que analizaremos en el siguiente apartado, donde abordaremos cómo las organizaciones miden la exposición de sus sistemas frente a posibles accesos no autorizados.

Medición de exposición.

Las arquitecturas de confianza cero no se limitan a establecer controles de acceso basados en identidad y contexto. También requieren mecanismos que permitan evaluar de forma continua el nivel de exposición del sistema frente a posibles accesos no autorizados. La medición de exposición consiste en analizar qué recursos están accesibles, bajo qué condiciones se concede el acceso y qué riesgos pueden derivarse de configuraciones de permisos o de la interacción entre distintos componentes del sistema.

En los modelos tradicionales de seguridad, la exposición de la infraestructura se evaluaba principalmente mediante el análisis del perímetro de red. Las organizaciones se concentraban en proteger puntos de entrada específicos, como firewalls o gateways, bajo la premisa de que los recursos internos permanecían protegidos detrás de esas barreras. En entornos distribuidos y basados en servicios, esta lógica resulta insuficiente, ya que los recursos pueden estar accesibles desde múltiples entornos y las decisiones de acceso dependen de sistemas de identidad y políticas dinámicas.

Dentro del enfoque Zero Trust, la medición de exposición se centra en comprender qué identidades pueden acceder a qué recursos y bajo qué condiciones. Esta evaluación permite identificar configuraciones de acceso excesivamente amplias, permisos innecesarios o combinaciones de roles que podrían habilitar accesos no previstos. Analizar estas relaciones resulta fundamental para mantener el principio de privilegio mínimo y reducir la superficie de ataque de la infraestructura.

Una forma común de analizar la exposición consiste en mapear las relaciones entre usuarios, roles, aplicaciones y recursos dentro del sistema. Este análisis permite identificar rutas de acceso potenciales que podrían aprovecharse en caso de que una cuenta se vea comprometida. Por ejemplo, si un usuario posee permisos que permiten acceder a múltiples servicios críticos, el compromiso de esa cuenta podría generar un impacto significativo dentro de la infraestructura.

Los marcos de implementación de Zero Trust recomiendan mantener una visibilidad continua de los accesos y de los flujos de comunicación entre componentes del sistema. Esta visibilidad se logra mediante la integración de registros de actividad, sistemas de monitoreo y herramientas de análisis de seguridad que permiten observar cómo interactúan los

usuarios con las aplicaciones y servicios dentro de la infraestructura (CISA, 2023).

La medición de exposición también permite identificar posibles vectores de movimiento lateral dentro del sistema. Cuando un atacante logra acceder a una cuenta o a un dispositivo, su objetivo suele ser ampliar gradualmente el acceso hacia otros recursos. Analizar las relaciones de acceso existentes permite anticipar estos escenarios y ajustar las políticas de seguridad para limitar la propagación de accesos indebidos.

Otro aspecto relevante en la medición de exposición es la evaluación del estado de seguridad de los dispositivos que acceden a los recursos. En arquitecturas de confianza cero, el dispositivo utilizado por el usuario puede influir en la decisión de acceso. Sistemas que analizan la postura de seguridad del dispositivo —como la presencia de actualizaciones de seguridad o configuraciones de protección activas— pueden reducir el nivel de exposición al restringir el acceso desde equipos que no cumplen con los requisitos definidos por la organización.

Las organizaciones también utilizan métricas para evaluar el nivel de exposición de sus sistemas. Estas métricas pueden incluir indicadores como el número de cuentas con

privilegios elevados, la cantidad de accesos a recursos críticos desde redes externas o la frecuencia de intentos de autenticación fallidos. El análisis de estos indicadores permite identificar tendencias de riesgo y ajustar las políticas de seguridad cuando se detectan desviaciones respecto del comportamiento esperado.

En entornos empresariales, la medición de exposición suele integrarse con modelos de madurez de seguridad que permiten evaluar el estado de implementación de los principios de confianza cero. El modelo de madurez de Zero Trust propuesto por la Agencia de Seguridad de Infraestructura y Ciberseguridad de los Estados Unidos (CISA) establece diferentes niveles de capacidad relacionados con la visibilidad, la analítica y la automatización de los controles de seguridad. Estos niveles permiten a las organizaciones evaluar el grado en que sus sistemas pueden detectar y responder a cambios en la exposición de la infraestructura (CISA, 2023).

La combinación de monitoreo continuo, análisis de accesos y evaluación de métricas permite construir una visión dinámica del riesgo asociado al acceso a los recursos. En lugar de depender únicamente de configuraciones estáticas de seguridad, las organizaciones pueden ajustar sus políticas de acceso en función de la información obtenida a partir del

análisis de exposición. Este enfoque facilita la identificación temprana de configuraciones inseguras y permite reforzar los controles antes de que puedan ser explotados por actores maliciosos.

En conjunto, la medición de exposición constituye un componente fundamental para sostener la efectividad de las arquitecturas de confianza cero. Al analizar continuamente las relaciones de acceso, el comportamiento de los usuarios y el estado de los dispositivos, las organizaciones pueden mantener un control más preciso sobre quién accede a sus recursos y bajo qué condiciones. Esta capacidad de observación y ajuste permanente permite reducir la superficie de ataque y fortalecer la seguridad de los entornos digitales distribuidos.

CONTINUAR

Referencias

Auth0. (2023). *Authorization code flow*. https://auth0.com/docs/get-started/authentication-and-authorization-flow/authorization-code-flow

Cloudflare. (2023). *What is Zero Trust Network Access (ZTNA)?* https://www.cloudflare.com/learning/access-management/what-is-ztna/

Cybersecurity and Infrastructure Security Agency (CISA). (2023). *Zero Trust maturity model*. https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model

Keycloak. (2024). *Keycloak server administration guide*. https://www.keycloak.org/docs/latest/server_admin/

National Institute of Standards and Technology (NIST). (2020). *Zero trust architecture (NIST Special Publication 800-207).* https://doi.org/10.6028/NIST.SP.800-207

Okta. (2023). *Understanding SAML vs OAuth vs OpenID Connect.* https://www.okta.com/identity-101/saml-vs-oauth/

SentinelOne. (2024). *What is multi-factor authentication (MFA)?* https://www.sentinelone.com/cybersecurity-101/identity-security/what-is-multi-factor-authentication-mfa/

CONTINUAR