Guía de Estudio en Español

CompTIA Security+ (SY0-701) — Capítulo 2

Understanding Identity and Access Management — Gestión de Identidad y Acceso

---

Este material es un **resumen conceptual elaborado con palabras propias**, pensado como guía de apoyo para estudiar junto al libro original en inglés. No es una traducción ni una reproducción del texto original; cubre los mismos temas, en el mismo orden, para facilitar el repaso en español.

Incluye: resumen por secciones, glosario de términos clave (inglés ↔ español) y preguntas de práctica originales para autoevaluación.

1. Autenticación, Autorización y Auditoría (AAA)

La gestión de identidad y acceso se apoya en cuatro conceptos que trabajan juntos: identificación, autenticación, autorización y auditoría (accounting). Entender estos cuatro pasos es la base de todo el capítulo.

- **Identificación:** el usuario afirma una identidad (ej. con un nombre de usuario o correo electrónico). Todavía no hay prueba de esa identidad.
- **Autenticación:** el usuario demuestra esa identidad con algún tipo de credencial (ej. una contraseña). Recién ahí el sistema confirma que sos quien decís ser.
- **Autorización:** una vez autenticado, el sistema decide qué recursos puede usar esa identidad (permisos).
- **Auditoría (accounting):** se registra la actividad del usuario en logs, generando un rastro de auditoría (audit trail) que permite reconstruir lo que pasó ante un incidente.

La autenticación no es exclusiva de personas: servicios, procesos, estaciones de trabajo, servidores y dispositivos de red también se autentican entre sí (por ejemplo, un servidor web presenta un certificado digital como prueba de su identidad).

2. Factores de Autenticación

CompTIA define cuatro factores de autenticación. Sin embargo, solo tres de ellos se consideran factores 'fuertes' capaces de probar identidad por sí solos; el cuarto (ubicación) casi siempre se usa como refuerzo adicional, no como prueba única.

Factor	Qué es	Ejemplos
Algo que sabés	Un secreto compartido.	Contraseña, PIN.
Algo que tenés	Un objeto físico o digital en tu poder.	Tarjeta inteligente, token, security key, teléfono.
Algo que sos	Una característica biológica (biometría).	Huella, iris, rostro, voz, marcha (gait).
Dónde estás	Tu ubicación geográfica o de red.	Geolocalización por IP, dirección MAC.

2.1 Algo que sabés — contraseñas

Las buenas prácticas actuales (según NIST SP 800-63B) recomiendan: exigir un mínimo de 8 caracteres, usar autenticación multifactor, no forzar cambios periódicos de contraseña, prohibir contraseñas comunes, no reutilizar la misma contraseña en varios sitios y permitir (sin exigir) caracteres especiales, incluidos espacios.

- **Longitud y complejidad:** cuanto más larga la contraseña, más combinaciones posibles. La complejidad exige mezclar mayúsculas, minúsculas, números y símbolos.

- **Expiración/antigüedad:** hoy se recomienda NO forzar cambios periódicos si ya se usa autenticación multifactor, porque los usuarios tienden a elegir contraseñas más débiles cuando deben cambiarlas seguido.
- **Historial de contraseñas:** impide reutilizar contraseñas anteriores (ej. las últimas 24). Se combina con una *edad mínima* para evitar que el usuario cambie la contraseña 24 veces seguidas solo para volver a la original.
- **Gestores de contraseñas (password managers/vaults):** guardan las credenciales cifradas para que el usuario solo deba recordar una contraseña maestra.
- **Autenticación basada en conocimiento (KBA):** preguntas de seguridad. La *estática* se define al crear la cuenta (ej. nombre de tu mascota); la *dinámica* se genera con datos públicos/privados en tiempo real para transacciones de alto riesgo. Se relaciona con el proceso de **identity proofing** (verificación de identidad de un usuario nuevo).
- **Bloqueo de cuentas (account lockout):** el *umbral* (threshold) define cuántos intentos fallidos se permiten; la *duración* define cuánto tiempo queda bloqueada la cuenta. Frena ataques de fuerza bruta y de diccionario.
- **Cambiar contraseñas por defecto:** práctica básica antes de poner en producción cualquier dispositivo o aplicación (ej. admin/admin en routers).

2.2 Algo que tenés

- **Tarjetas inteligentes (smart cards):** incluyen un certificado digital embebido que aporta autenticación, cifrado y firma digital. Suelen combinarse con un PIN (dos factores).
- **Security keys y hard tokens:** dispositivos físicos que generan o contienen información criptográfica para autenticarse.
- **Soft tokens:** apps (ej. Google Authenticator) que generan contraseñas de un solo uso, igual que un token físico.
- **HOTP vs. TOTP:** ambos son estándares abiertos para contraseñas de un solo uso. *HOTP* genera un código que no expira hasta que se usa (se genera con un botón, basado en un contador). *TOTP* genera un código que expira cada 30-60 segundos (basado en la hora actual).
- **SMS y notificaciones push:** el SMS envía un código por mensaje de texto (NIST desaconseja su uso por vulnerabilidades como el secuestro de número). Las notificaciones push simplemente piden aprobar o rechazar el acceso desde el teléfono, sin ingresar ningún código — más cómodas para el usuario.

2.3 Algo que sos — biometría

La biometría suele considerarse el factor más fuerte porque es lo más difícil de falsificar. Métodos comunes: huella dactilar, reconocimiento de venas de la palma, escaneo de retina, escaneo de iris, reconocimiento facial, reconocimiento de voz y análisis de marcha (gait analysis). El iris y la retina son los métodos más precisos; el iris se prefiere porque no requiere contacto físico ni revela datos médicos como la retina. El reconocimiento facial y el análisis de marcha pueden usarse de forma pasiva, sin un proceso formal de inscripción (enrollment).

Tasas de eficacia: Falso positivo/aceptación (FAR) = el sistema acepta a alguien que no debería. Falso negativo/rechazo (FRR) = el sistema rechaza a alguien válido. La **tasa de error cruzado (CER)** es el punto donde FAR y FRR se cruzan: cuanto más bajo el CER, más preciso el sistema.

2.4 Dónde estás

Usa la geolocalización (normalmente por dirección IP) para detectar inicios de sesión sospechosos, como un 'viaje imposible' (impossible travel) — cuando alguien inicia sesión desde dos lugares del mundo en un tiempo demasiado corto para haber viajado entre ellos. No es infalible: una VPN puede enmascarar la IP real.

2.5 Combinando factores

Usar dos métodos del *mismo* factor (ej. contraseña + PIN, ambos 'algo que sabés') sigue siendo autenticación de un solo factor. La autenticación de **dos factores (2FA)** combina dos factores distintos. La **multifactor** usa dos o más. La autenticación **sin contraseña (passwordless)** reemplaza la contraseña por otro factor, pero eso no la convierte automáticamente en multifactor.

3. Gestión de Cuentas

3.1 Tipos de cuenta y políticas de credenciales

- **Cuentas de usuario final:** la mayoría del personal; política de credenciales básica.
- **Cuentas de administrador/root:** privilegios elevados; requieren autenticación más fuerte (ej. MFA) y controles adicionales.
- **Cuentas de servicio:** usadas por aplicaciones (no por personas), ej. una base de datos. No deberían expirar, porque si la contraseña vence, el servicio deja de funcionar.
- **Cuentas de dispositivo:** equipos que se unen a un dominio también tienen cuenta propia.
- **Cuentas de terceros:** de proveedores externos con acceso a la red; requieren políticas de credenciales estrictas.
- **Cuenta invitado (Guest):** acceso limitado y temporal; suele estar deshabilitada por defecto.
- **Cuentas compartidas/genéricas:** desaconsejadas porque impiden identificar quién hizo qué (rompen la cadena de identificación-autenticación-autorización-auditoría).

3.2 Gestión de acceso privilegiado (PAM)

El PAM aplica controles más estrictos sobre cuentas con privilegios elevados. Su pieza clave es el concepto de **permisos justo a tiempo (just-in-time)**: el administrador no tiene privilegios elevados todo el tiempo, sino que los solicita cuando los necesita y el sistema se los revoca automáticamente después de un tiempo preestablecido. También permite:

- Acceder a la cuenta privilegiada sin conocer su contraseña (password vaulting).
- Cambiar automáticamente las contraseñas privilegiadas de forma periódica.
- Crear **cuentas temporales (temporal accounts)** con privilegios, válidas por un período corto y luego destruidas.
- Registrar (loggear) todo el uso de credenciales privilegiadas.

Buena práctica: los administradores deberían tener dos cuentas — una estándar para el trabajo diario y otra con privilegios solo para tareas administrativas. Esto reduce el riesgo de que malware escale privilegios si la cuenta estándar se ve comprometida mientras el usuario está lejos de su equipo.

3.3 Baja de cuentas (deprovisioning) y auditoría

- **Deshabilitar vs. eliminar:** ante la salida de un empleado, se prefiere *deshabilitar* la cuenta (no eliminarla), porque eliminarla también borra las claves de cifrado asociadas y los datos cifrados podrían quedar inaccesibles para siempre.
- **Restricciones por horario (time-of-day):** impiden iniciar sesión fuera de un horario permitido (no cierra sesiones ya abiertas, solo bloquea nuevas conexiones).
- **Auditoría de cuentas (account audit):** revisa los permisos otorgados contra los que realmente se necesitan, y detecta el **privilege creep** (acumulación de permisos innecesarios cuando alguien cambia de puesto pero conserva accesos anteriores).

- **Attestation (certificación de permisos):** proceso formal donde los gerentes revisan y certifican que los permisos de cada usuario siguen siendo necesarios.

4. Servicios de Autenticación

Estos servicios evitan que las credenciales viajen en texto plano por la red y permiten centralizar el inicio de sesión.

- **Single Sign-On (SSO):** el usuario se autentica una sola vez y accede a múltiples sistemas sin volver a iniciar sesión. Requiere autenticación fuerte, porque comprometer una sola credencial da acceso a todo.
- **LDAP:** protocolo usado para consultar información de un directorio centralizado de usuarios (ej. Active Directory); es un componente central de muchos sistemas SSO.
- **Federación (federation):** conecta mecanismos de autenticación de distintos entornos u organizaciones sin necesidad de unir sus redes. Una **identidad federada** vincula las credenciales de un usuario entre distintas redes, tratándolas como una sola.
- **SAML:** estándar basado en XML para intercambiar información de autenticación (y opcionalmente autorización) entre organizaciones, muy usado para SSO en aplicaciones web. Define tres roles: *principal* (el usuario), *proveedor de identidad (IdP)* (quien autentica) y *proveedor de servicio* (quien brinda el recurso).
- **OAuth:** estándar abierto de *autorización* (no de autenticación, pese al nombre similar a 'auth'). Permite que una aplicación acceda a información de otra (ej. tu calendario de Google) sin que le entregues tu contraseña.

5. Modelos de Control de Acceso (Autorización)

Una vez autenticado un **sujeto** (usuario/grupo/servicio), estos modelos determinan qué puede hacer sobre un **objeto** (archivo, carpeta, impresora, etc.).

Modelo	Cómo funciona	Dónde se usa
Role-BAC (basado en roles)	Se asignan permisos a roles/grupos según el puesto o función, no a usuarios individuales. Se documenta con una matriz de roles y permisos.	Grupos de seguridad de Windows, Active Directory.
Rule-BAC (basado en reglas)	Usa un conjunto de reglas aprobadas (ej. listas de control de acceso). Algunas reglas son dinámicas y se disparan ante un evento.	ACLs en routers y firewalls.
DAC (discrecional)	Cada objeto tiene un dueño, y el dueño decide quién accede. Muy flexible.	NTFS de Windows (usa DACL: lista de entradas ACE con SID + permiso).

MAC (obligatorio)	Usa etiquetas de sensibilidad (ej. 'Secreto', 'Alto Secreto') tanto para sujetos como para objetos. Solo accede si las etiquetas coinciden y hay necesidad de saber ('need to know'). Poco flexible: solo un administrador puede cambiar los accesos según directivas de un nivel superior.	SELinux (modos: enforcing, permissive, disabled). Entornos milita res/gubernamentales.
ABAC (basado en atributos)	Evalúa atributos del sujeto, objeto, acción y entorno mediante políticas en lenguaje natural. Muy flexible; puede imitar tanto DAC como MAC.	Redes definidas por software (SDN).

Nota sobre MAC: el término 'MAC' tiene tres significados distintos en el temario de Security+: control de acceso obligatorio (Mandatory Access Control), dirección física de red (Media Access Control) y código de autenticación de mensaje (Message Authentication Code). Prestá atención al contexto.

6. Indicadores de Actividad Maliciosa en Autenticación

Al revisar logs de autenticación, estos son los patrones que deberías investigar:

- **Bloqueos de cuenta:** múltiples fallos de inicio de sesión que terminan bloqueando la cuenta.
- **Uso de sesiones concurrentes:** el mismo usuario conectado desde varios lugares al mismo tiempo — posible cuenta compartida o robada.
- **Viaje imposible (impossible travel):** inicios de sesión desde ubicaciones geográficas que no podrían alcanzarse en el tiempo transcurrido.
- **Contenido bloqueado:** niveles inusuales de código malicioso detectado por filtros de contenido.
- **Consumo de recursos:** uso excesivo e inexplicado de CPU, memoria o almacenamiento.
- **Inaccesibilidad de recursos:** servicios que caen repentinamente.
- **Anomalías en los logs:** entradas fuera de horario habitual o logs faltantes.

7. Glosario de Términos Clave (Inglés ↔ Español)

Inglés	Español	Definición breve
AAA	AAA	Authentication, Authorization, Accounting — autenticación, autorización y auditoría.
Identification	Identificación	El usuario afirma una identidad (ej. usuario).
Authentication	Autenticación	El usuario prueba su identidad (ej. contraseña).
Authorization	Autorización	Se define qué recursos puede usar el usuario autenticado.
Accounting	Auditoría / registro	Se registra la actividad del usuario en logs.
Something you know/have/are	Algo que sabés/tenés/sos	Los tres factores fuertes de autenticación.
Password manager / vault	Gestor de contraseñas	Almacena credenciales cifradas.
Account lockout	Bloqueo de cuenta	Bloquea la cuenta tras varios intentos fallidos.
HOTP / TOTP	HOTP / TOTP	Contraseñas de un solo uso basadas en contador / en tiempo.
Push notification	Notificación push	Aprobación de acceso desde el teléfono, sin código.
Biometrics	Biometría	Autenticación con características físicas.
FAR / FRR / CER	FAR / FRR / CER	Tasa de falsa aceptación / falso rechazo / error cruzado.
Privileged access management (PAM)	Gestión de acceso privilegiado	Controles estrictos para cuentas con privilegios elevados.
Just-in-time permissions	Permisos justo a tiempo	Privilegios otorgados solo cuando se necesitan.
Deprovisioning	Baja de cuenta	Proceso de deshabilitar una cuenta al salir un empleado.
Privilege creep	Acumulación de privilegios	Permisos innecesarios que quedan tras cambios de puesto.
Attestation	Certificación de permisos	Revisión formal de permisos por parte de un gerente.

Inglés	Español	Definición breve
Single sign-on (SSO)	Inicio de sesión único	Autenticarse una vez y acceder a varios sistemas.
Federation	Federación	Vincula identidades entre organizaciones distintas.
SAML	SAML	Estándar XML para SSO e intercambio de autenticación/autorización.
OAuth	OAuth	Estándar abierto de autorización (no de autenticación).
Role-BAC / Rule-BAC	Control por roles / por reglas	Modelos de autorización basados en roles o en reglas.
DAC	Control de acceso discrecional	El dueño del objeto controla el acceso.
MAC	Control de acceso obligatorio	Usa etiquetas de sensibilidad y necesidad de saber.
ABAC	Control de acceso por atributos	Usa políticas basadas en atributos de sujeto/objeto/entorno.
Impossible travel	Viaje imposible	Indicador de posible cuenta comprometida.

8. Preguntas de Práctica (Autoevaluación)

Preguntas de elaboración propia, en español, para repasar los conceptos del capítulo 2. Las respuestas están al final.

1. Un empleado ingresa su usuario y contraseña, y el sistema además le pide un PIN adicional que solo él conoce, sin usar ningún dispositivo extra. ¿Es esto autenticación de uno, dos o múltiples factores?

2. Una empresa detecta que un empleado inició sesión en Buenos Aires y, cuatro minutos después, alguien inició sesión con la misma cuenta desde Tokio. ¿Qué indicador de actividad maliciosa describe esta situación?

3. Un token físico muestra un código que cambia automáticamente cada 30 segundos sin que el usuario presione ningún botón. ¿Qué algoritmo está usando, HOTP o TOTP?

4. Un administrador de sistemas necesita realizar tareas administrativas ocasionales, pero usa una cuenta estándar para el trabajo diario. ¿Qué buena práctica de gestión de cuentas está aplicando?

5. El sistema de una fábrica otorga acceso a una carpeta 'Inspectores' a cualquier cuenta que tenga los atributos 'empleado', 'inspector' y 'certificado nuclear', sin importar el rol formal del usuario. ¿Qué modelo de control de acceso es este?

6. En Windows, un usuario crea una carpeta y decide manualmente quién más puede acceder a ella. ¿Qué modelo de control de acceso está usando el sistema operativo?

7. Una organización usa etiquetas de 'Secreto' y 'Alto Secreto' tanto para los empleados como para los documentos, y solo permite el acceso cuando las etiquetas coinciden y existe necesidad de saber. ¿Qué modelo de control de acceso es?

8. Una aplicación de terceros pide permiso para acceder a tu calendario de Google sin pedirte la contraseña de tu cuenta de Google. ¿Qué protocolo está usando?

9. Dos organizaciones distintas permiten que sus empleados inicien sesión una sola vez y accedan a aplicaciones web de ambas usando mensajes XML para intercambiar la autenticación. ¿Qué estándar es?

10. Un empleado deja la empresa. El administrador prefiere deshabilitar su cuenta en vez de eliminarla inmediatamente. ¿Por qué es esto una buena práctica?

Respuestas

1. Un solo factor — el PIN y la contraseña son ambos 'algo que sabés', por lo tanto siguen en el mismo factor.

2. Viaje imposible (impossible travel) — dos inicios de sesión geográficamente incompatibles en muy poco tiempo.

3. TOTP (Time-based One-Time Password) — el código cambia automáticamente según el tiempo, sin intervención del usuario.

4. Requerir dos cuentas separadas para administradores: una estándar y otra con privilegios elevados, para reducir el riesgo de escalamiento de privilegios.

5. Control de acceso basado en atributos (ABAC) — la decisión se basa en atributos combinados, no en un rol único.

6. Control de acceso discrecional (DAC) — el dueño del objeto decide el acceso; NTFS usa este modelo.

7. Control de acceso obligatorio (MAC) — usa etiquetas de sensibilidad y necesidad de saber.

8. OAuth — estándar de autorización que da acceso limitado sin compartir la contraseña.

9. SAML (Security Assertion Markup Language) — estándar XML usado para SSO federado en aplicaciones web.

10. Porque eliminar la cuenta también elimina las claves de cifrado asociadas, y los datos cifrados por esa cuenta podrían quedar inaccesibles para siempre.
