UNIVERSIDAD SERGIO ARBOLEDA | Colsubsidio

Diplomado de Ciberseguridad y Gestión de Seguridad de la Información

Módulo 5:

Gestión de Identidades y Seguridad en Dispositivos y Redes

Sesión 1:

Fundamentos de la gestión de identidades y autenticación

OBJETIVO DE LA SESIÓN:

Al finalizar la sesión, el estudiante estará en capacidad de comprender los fundamentos de la gestión de identidades digitales, diferenciar los conceptos de autenticación y autorización, identificar los métodos de autenticación más comunes, y aplicar buenas prácticas básicas para proteger su identidad en entornos digitales personales y organizacionales.

¿Qué es la identidad digital?

La identidad digital es el conjunto de atributos y datos que permiten identificar a una persona o entidad en entornos digitales. Incluye información como tu nombre de usuario, correo electrónico, número de teléfono, credenciales de acceso, certificados digitales y hasta tus comportamientos en línea (por ejemplo, tus patrones de navegación o publicaciones en redes sociales).

Ejemplo simple:

Tu cuenta de Google, con tu nombre, correo, contraseña, foto de perfil y configuración de seguridad, **es una forma de tu identidad digital**. Al igual que en la vida real usas una cédula o pasaporte, en el mundo digital usas cuentas y claves.

Importancia

Es la “llave” para acceder a servicios digitales como correo, redes sociales, banca en línea, plataformas educativas.

Si alguien suplanta tu identidad digital, **puede acceder a tu información, estafarte o cometer delitos en tu nombre.**

Diferencia entre Autenticación y Autorización

Concepto	¿Qué es?	Ejemplo
Autenticación	El proceso de demostrar que eres quien dices ser.	Ingresar usuario y contraseña en Gmail.
Autorización	El proceso que determina a qué recursos puedes acceder una vez autenticado.	Acceder a tu bandeja de entrada, pero no a la de otra persona.

Analogía:
Piensa en un edificio de oficinas:

- Mostrar tu cédula en la entrada es autenticación.
- Que te dejen entrar solo al piso 3 y no al 5 es autorización.

Métodos de autenticación

Los métodos de autenticación se clasifican por el tipo de “prueba” que se presenta para verificar tu identidad. Estas pruebas se agrupan en tres categorías:

Categoría	Método	Ejemplo
Algo que sabes	Contraseña, PIN, preguntas de seguridad	Tu contraseña del correo electrónico
Algo que tienes	Token físico, celular, tarjeta con chip	Código que recibes por SMS
Algo que eres	Huella digital, reconocimiento facial, iris	Desbloqueo con huella en el celular

Autenticación Multifactor (MFA)

Es un proceso de registro en varios pasos que requiere que los usuarios ingresen algo más de información que simplemente una contraseña. Por ejemplo, junto con la contraseña, los usuarios deberán ingresar un código que se envía a su correo electrónico, responder a una pregunta secreta o escanear una huella dactilar.

Ejemplo práctico:

- Escribir tu contraseña (algo que sabes)
- Recibir un código en tu celular (algo que tienes)

Importancia

El uso de MFA reduce drásticamente el riesgo de accesos no autorizados. Incluso si tu contraseña es robada, **el atacante no podrá acceder sin el segundo factor.**

¿En qué servicios personales/organizacionales debería ser obligatorio el uso de MFA?

Beneficios MFA

Mejora la respuesta de seguridad
Las compañías pueden configurar un sistema de autenticación multifactor para enviar de manera activa una alerta en cuanto se detecten intentos de inicio de sesión sospechosos. Esto ayuda tanto a compañías como a individuos a responder más rápido a ciberataques, lo que reduce cualquier daño potencial.

Permite iniciativas digitales
Las organizaciones pueden llevar a cabo iniciativas digitales con confianza. Las empresas utilizan autenticación multifactor para ayudar a proteger los datos de la organización y de los usuarios, de modo que puedan realizar interacciones y transacciones en línea de manera segura.

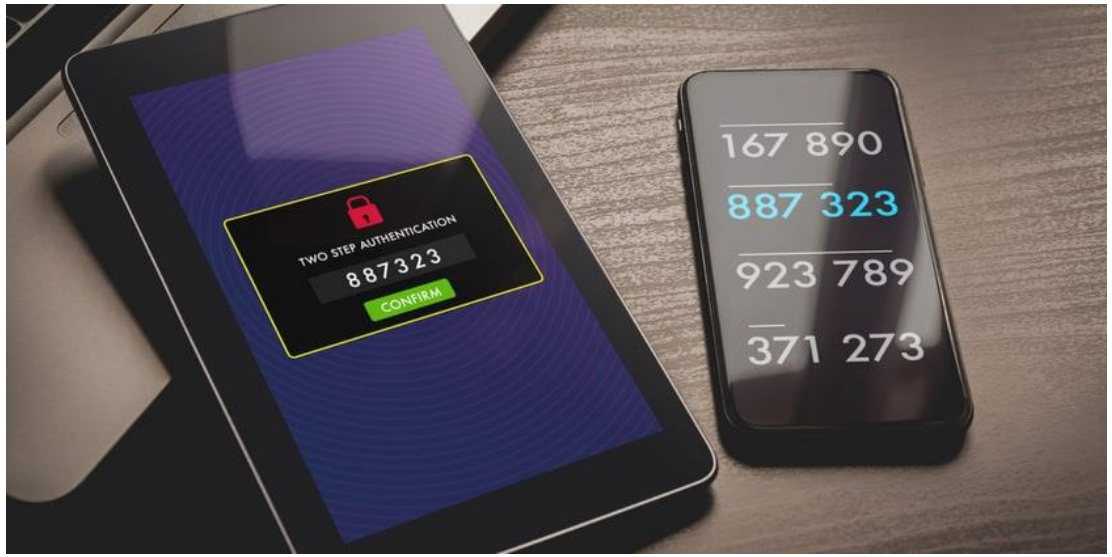
Reduce el riesgo de seguridad
La autenticación multifactor reduce los riesgos derivados de errores humanos, contraseñas extraviadas y dispositivos perdidos.

Autenticación Multifactor Adaptativa

Utiliza reglas empresariales e información sobre el usuario para determinar qué factores de autenticación deberían aplicarse. Las empresas utilizan autenticación adaptativa para equilibrar los requisitos de seguridad con la experiencia del usuario.

Las soluciones de autenticación adaptativa pueden aumentar o disminuir los pasos de autenticación de manera dinámica mediante el uso de información del usuario contextual, por ejemplo:

- Número de intentos erróneos de inicio de sesión
- Ubicación geográfica del usuario
- Geovelocidad o distancia física entre intentos de inicio de sesión consecutivos
- Dispositivo utilizado para el inicio de sesión
- Día y hora del intento de inicio de sesión
- Sistema operativo
- Dirección IP de origen
- Rol del usuario



Algo que tienes: Token celular

Algo que eres: Huella digital

Buenas prácticas de gestión de identidades

Las siguientes prácticas ayudan a reducir el riesgo de suplantación, robo de credenciales y accesos no autorizados:

a) Uso de contraseñas seguras

- Mínimo 12 caracteres
- Combina letras, números y símbolos
- Evita datos personales (fechas, nombres)

Ejemplo de contraseña débil: juan123
Ejemplo de contraseña segura: J!mp0rtaN7e_2024%

b) No repetir contraseñas

Usar la misma contraseña para varias cuentas expone todos tus servicios si una de ellas es comprometida.
Recomendación: Usa un gestor de contraseñas, como Bitwarden o KeePass.

c) Activar MFA

Siempre que un servicio lo permita (correo, redes, banca), activa la autenticación en dos pasos. Es la defensa más efectiva para evitar accesos no autorizados.

d) Eliminar cuentas inactivas

Las cuentas antiguas o abandonadas son vulnerables. Si ya no usas una cuenta o red social, elimínala o cambia su contraseña y activa MFA.

e) Revisar actividad de inicio de sesión

Muchos servicios muestran registros de acceso. Si ves inicios de sesión desde lugares extraños, cambia inmediatamente tu contraseña.

Ejercicio 1: Diagnóstico de la propia identidad digital

Completar la tabla listando sus cuentas digitales, métodos de autenticación usados, deficiencias identificadas y Recomendación de mejora.

Método de autenticación: escribe si usas solo contraseña, contraseña + MFA, biometría, etc.
Deficiencias identificadas: identifica riesgos (contraseñas débiles, sin MFA, misma contraseña en varios sitios, etc.).

Cuenta digital	Método de autenticación actual	Deficiencias identificadas	Recomendación de mejora

Cuenta digital	Método de autenticación actual	Deficiencias identificadas	Recomendación de mejora
Correo personal	Contraseña única + notificación celular (algo que tienes)	Contraseña sin cambio en 2 años	Cambiar contraseña cada 6 meses
Banco en línea	Contraseña + Token app (algo que tienes)	Token por SMS es vulnerable a robo	Proteger el teléfono con la app con contraseña
Redes sociales (IG)	Solo Contraseña	Contraseña repetida en otra cuenta, No tiene MFA	Usar contraseña única, activar alertas de acceso y activar MFA
HBO	Solo contraseña	Contraseña compartida con amigos, no tiene MFA	No compartir credenciales, activar MFA si disponible
Universidad (Campus)	Contraseña + Captcha + MFA	Contraseña fácil de adivinar	Crear contraseña robusta

¿Cuál cuenta identificaste como la más vulnerable?

¿Qué mejoras aplicarías esta semana?

¿Qué cuentas deberían tener obligatoriamente MFA?

Ejercicio 2: Simulación de ataque por suplantación de identidad

Juan, un estudiante universitario, recibe un correo que aparentemente proviene de su institución. En el mensaje se le informa que debe verificar su cuenta para evitar que se bloquee. El enlace lo dirige a una página visualmente idéntica al portal real, donde introduce su usuario y contraseña. A las pocas horas, su correo y redes sociales han sido comprometidas

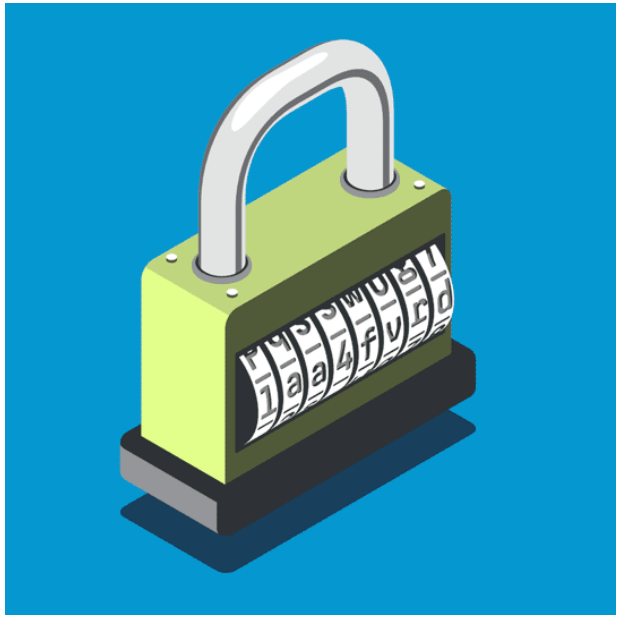
¿Qué señales de alerta tenía el correo que Juan recibió?
¿Qué activo(s) de información se vieron comprometidos?
¿Qué vulnerabilidad permitió el ataque?

¿Qué impacto puede tener en la vida académica y personal de Juan?
¿Qué acciones inmediatas debería tomar Juan tras darse cuenta?
¿Qué controles o medidas preventivas hubiera evitado el incidente?

Elemento	Respuesta
Activo comprometido	Correo institucional, redes sociales
Amenaza	Phishing (suplantación de identidad)
Vulnerabilidad	Falta de verificación de enlace, falta de MFA
Impacto	Alto (pérdida de control de cuentas, riesgo reputacional, robo de datos)
Acción inmediata	Cambiar contraseñas, avisar a soporte TI, habilitar MFA
Medida preventiva futura	Capacitación en phishing, filtros de correo, autenticación multifactor

Descifrar una contraseña con Fuerza Bruta

Simular cómo los atacantes prueban contraseñas mediante diferentes escenarios de fuerza bruta.



Instrucciones:

1. El usuario ingresa:
   - Su nombre
   - Su fecha de nacimiento
   - Una contraseña realista (a descifrar).
2. El programa intentará descifrarla en 3 escenarios:
   - Caso 1: Letras minúsculas + números.
   - Caso 2: Mayúsculas + minúsculas + números.
   - Caso 3: Mayúsculas + minúsculas + números + caracteres especiales.

3. El programa también probará con una lista de contraseñas comunes y con combinaciones basadas en el nombre y fecha de nacimiento.

Referencias

1. Bishop, M. (2003). *Computer Security.*
2. Briceño, E. (2021). *Seguridad De La Información*
3. Kremer, E. Et al. (2019). *Ciberseguridad*
4. Ozkaya, E. (2019). *Cybersecurity: The Beginner's Guide: A comprehensive guide to getting started in cybersecurity*
5. AWS. *(s/f). ¿Qué es la autenticación multifactor (MFA)? Amazon.com. Recuperado el 28 de agosto de 2025, de* https://aws.amazon.com/es/what-is/mfa/