**Gestión de la Ciberseguridad**



**Presentado por:**

**My. Serrano Parra John Alexander**

**My. Suarez Rojas Yerson**

**My. Cubides Elkin**

**My. Aguilar Andres Camilo**

**Presentado a :**

**Jaider Ospina Navas**

**Escuela Superior de Guerra**

**Bogotá D.C**

**2025**

**Gestión de Identidad y Acceso (Identity and Access Management - IAM)**

La **Gestión de Identidad y Acceso (IAM)** es un conjunto de políticas, tecnologías y procesos diseñados para garantizar que las personas adecuadas tengan el acceso correcto a los recursos de una organización, en el momento adecuado y con el nivel de seguridad adecuado. Esto es fundamental para proteger la información crítica y minimizar los riesgos de accesos no autorizados.

**Principales Componentes de IAM**

1. **Provisioning/Deprovisioning (Aprovisionamiento y Desaprovisionamiento)**
   * Se refiere al proceso de creación, modificación y eliminación de cuentas de usuario en los sistemas de la organización.
   * **Aprovisionamiento**: Asignar credenciales y permisos a nuevos empleados o sistemas.
   * **Desaprovisionamiento**: Revocar accesos cuando un usuario deja la organización o cambia de rol, reduciendo riesgos de cuentas huérfanas.
2. **Single Sign-On (SSO) - Inicio de sesión único**
   * Permite a los usuarios autenticarse una sola vez y acceder a múltiples aplicaciones sin necesidad de ingresar credenciales repetidamente.
   * **Ventajas**: Mayor comodidad para los usuarios, reducción de la fatiga de contraseñas y menor carga de trabajo para el departamento de TI.
3. **Federated Single Sign-On (FSSO) - Inicio de sesión único federado**
   * Extiende el concepto de SSO permitiendo que los usuarios inicien sesión en múltiples organizaciones o sistemas sin necesidad de múltiples credenciales.
   * Utiliza protocolos como **SAML (Security Assertion Markup Language)** o **OAuth** para compartir autenticación entre distintas entidades.
4. **Multi-Factor Authentication (MFA) - Autenticación Multifactor**
   * Requiere que los usuarios se autentiquen con al menos dos factores diferentes para verificar su identidad:
     + **Algo que saben** (Contraseña o PIN)
     + **Algo que tienen** (Token físico o aplicación móvil)
     + **Algo que son** (Biometría como huella digital o reconocimiento facial)
   * **Objetivo**: Aumentar la seguridad y reducir el riesgo de accesos no autorizados.
5. **Role-Based Access Control (RBAC) - Control de Acceso Basado en Roles**
   * Asigna permisos a los usuarios en función de su rol dentro de la organización.
   * **Ejemplo**: Un empleado del área de Finanzas puede acceder a sistemas contables, pero no a los servidores de Desarrollo.
   * **Ventajas**: Centraliza la gestión de permisos y reduce errores humanos en la asignación de accesos.
6. **Identity Store (Almacén de Identidades)**
   * Bases de datos donde se almacenan las credenciales y permisos de los usuarios.
   * **Ejemplos**:
     + **LDAP (Lightweight Directory Access Protocol)**: Protocolo utilizado para consultar y modificar información en directorios centralizados.
     + **Active Directory (AD)**: Solución de Microsoft que permite gestionar identidades y accesos dentro de una red empresarial.

**Conclusión**

IAM es un pilar clave en la seguridad empresarial, asegurando que las personas adecuadas tengan acceso solo a la información y sistemas que necesitan. La implementación de **SSO, MFA y RBAC** permite equilibrar seguridad y usabilidad, reduciendo los riesgos de ataques cibernéticos y mejorando la eficiencia operativa.

**SOC**

**Self assessment -Autoevaluación**

**Monitoreo de Configuración, Evaluación de Vulnerabilidades, Pruebas de Penetración y Ejercicios de Seguridad**

Estos elementos son fundamentales dentro de la estrategia de seguridad de cualquier organización y del funcionamiento de un **Centro de Operaciones de Seguridad (SOC)**. Su propósito es garantizar la protección de los sistemas de información frente a amenazas cibernéticas, ataques y errores de configuración.

**1. Monitoreo de Configuración (Configuration Monitoring)**

El **monitoreo de configuración** es un proceso clave dentro de la seguridad de TI que permite garantizar que los sistemas operen dentro de los parámetros definidos y no presenten cambios inesperados que puedan ser aprovechados por atacantes.

**Principales actividades:**

✅ **CREAR BASELINES (Líneas Base)**

* Se establecen configuraciones seguras y óptimas para los sistemas y redes.
* Ejemplo: Definir reglas de firewall, permisos de usuarios y configuraciones de servidores.

✅ **IDENTIFICAR CAMBIOS DE CONFIGURACIÓN (Identify Configuration Changes)**

* Se monitorean las modificaciones en los sistemas y se detectan alteraciones sospechosas.
* Ejemplo: Un cambio en los permisos de acceso sin autorización podría indicar un ataque interno.

✅ **MANTENIMIENTO DE SISTEMAS (Maintain Systems)**

* Se aplican actualizaciones, parches y mejoras en la seguridad para evitar vulnerabilidades.
* Ejemplo: Actualizar el sistema operativo y reforzar configuraciones de seguridad.

**2. Evaluación de Vulnerabilidades (Vulnerability Assessment)**

Este proceso ayuda a detectar debilidades en los sistemas antes de que sean explotadas por atacantes.

**Principales actividades:**

✅ **IDENTIFICAR RIESGOS Y EXPOSICIÓN (Identify Risk and Exposure)**

* Se analizan los sistemas para encontrar posibles puntos débiles.
* Ejemplo: Detectar servidores expuestos sin cifrado o accesibles desde internet sin protección.

✅ **ESCANEAR SISTEMAS EN BUSCA DE VULNERABILIDADES CONOCIDAS (Scan Systems for Known Vulnerabilities)**

* Se usan herramientas como **Nessus, OpenVAS o Qualys** para encontrar vulnerabilidades en sistemas, redes y aplicaciones.

✅ **EVALUACIÓN DEL IMPACTO DE NUEVAS VULNERABILIDADES (Impact of New Vulnerabilities)**

* Se revisan nuevas amenazas y cómo pueden afectar a la infraestructura de la organización.
* Ejemplo: La empresa debe evaluar cómo la aparición de una nueva vulnerabilidad crítica en Windows afecta sus servidores y tomar acciones inmediatas.

**3. Pruebas de Penetración (Penetration Testing)**

Las pruebas de penetración o **pentesting** simulan ataques cibernéticos con el fin de identificar vulnerabilidades explotables antes de que los atacantes reales lo hagan.

**Principales actividades:**

✅ **MODELO DE ESCENARIOS DE ATAQUE (Model Attacker Scenarios)**

* Se crean escenarios realistas basados en cómo actuaría un hacker.
* Ejemplo: Simular un ataque de phishing contra empleados para ver cuántos caen en la trampa.

✅ **EXPLOTACIÓN DE SISTEMAS (Exploit Systems)**

* Se ejecutan pruebas para verificar si es posible comprometer los sistemas mediante fallos de seguridad.
* Ejemplo: Un hacker ético intenta acceder a una base de datos sin autenticación para demostrar una vulnerabilidad.

✅ **RECONOCIMIENTO E INTELIGENCIA ORGANIZACIONAL (Reconnaissance, Organizational Intelligence)**

* Se recolecta información sobre la organización para identificar posibles puntos de ataque.
* Ejemplo: Buscar datos filtrados en la dark web que puedan ser utilizados para ataques.

✅ **DECONFLICCIÓN (Deconfliction)**

* Se coordinan las pruebas con el equipo de seguridad para evitar interrupciones o daños en la infraestructura.

**4. Ejercicios de Seguridad (Exercises)**

Los ejercicios de seguridad preparan a la organización para responder ante incidentes y mejorar la capacidad de reacción del equipo.

**Principales actividades:**

✅ **ESCENARIOS DE SIMULACIÓN (Tabletop Scenarios)**

* Se realizan reuniones para simular un ataque y discutir cómo responder sin afectar los sistemas reales.
* Ejemplo: Simular un ransomware y analizar la toma de decisiones.

✅ **MODELADO DE AMENAZAS Y EVENTOS (Model Threats and Events)**

* Se estudian diferentes amenazas potenciales y su impacto en la organización.

✅ **CAPACITACIÓN Y EVALUACIÓN DEL PERSONAL (Train and Assess Staff)**

* Se capacita a los empleados en manejo de incidentes y toma de decisiones bajo presión.

✅ **PLANES DE CONTINUIDAD Y RECUPERACIÓN ANTE DESASTRES (DR/BCP - Disaster Recovery/Business Continuity Planning)**

* Se establecen procedimientos para mantener la operación de la empresa tras un ataque o desastre.

**Conclusión**

Estos procesos son esenciales para garantizar que la seguridad de la organización sea **proactiva** en lugar de **reactiva**. El **monitoreo de configuración** asegura que los sistemas sean gestionados adecuadamente, la **evaluación de vulnerabilidades** identifica riesgos, las **pruebas de penetración** ayudan a validar la seguridad en la práctica y los **ejercicios de seguridad** fortalecen la preparación del equipo ante amenazas reales.

**Bibliografías**

SANS Institute. (2018). *CISO Mind Map & Security Operations Center (SOC) Essential Functions* [Poster]. SANS Cybersecurity Leadership. <https://www.sans.org/curricula/management>

**Gestión de Identidad y Accesos (IAM)**

NIST. (2020). *Digital Identity Guidelines* (NIST Special Publication 800-63-3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63-3

Sun, Y., Hahn, C., & Liu, Z. (2019). *Role-Based Access Control and Multi-Factor Authentication in Cloud Computing*. *Journal of Cyber Security and Mobility, 8*(2), 111-134. https://doi.org/10.13052/jcsm2245-1439.822

**Evaluación de Vulnerabilidades**

Scarfone, K., & Mell, P. (2007). *Guide to Vulnerability Scoring Systems* (NIST Special Publication 800-126). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-126

Peterson, G., & Axford, S. (2021). *Vulnerability Assessment and Management in Modern Cybersecurity*. *Cybersecurity Journal*, *15*(4), 55-72. https://cybersecjournal.com/vul-assessment

**Pruebas de Penetración (Pentesting)**

Mitropoulos, S., Spinellis, D., & Katsikas, S. (2017). *Penetration Testing and Ethical Hacking: A Systematic Review of the Literature*. *ACM Computing Surveys, 50*(2), 1-40. https://doi.org/10.1145/3057269

OWASP Foundation. (2023). *OWASP Penetration Testing Methodology Guide*. Open Web Application Security Project. https://owasp.org/www-project-penetration-testing/

**Ejercicios de Seguridad y Respuesta a Incidentes**

National Institute of Standards and Technology (NIST). (2018). *Computer Security Incident Handling Guide* (NIST Special Publication 800-61r2). https://doi.org/10.6028/NIST.SP.800-61r2

SANS Institute. (2021). *Incident Response Playbook: Enhancing Cyber Resilience through Tabletop Exercises*. SANS Security Awareness. https://www.sans.org/incident-response-tabletop