Seguridad Informática

Profesor: Pedro Pinacho Davidson

ppinacho@inf.udec.cl

Conceptos básicos

Dominios de Revisión

- Dom 1: Seguridad y Gestión de Riesgos
- Dom 2: Seguridad de Recursos
- Dom 3: Arquitectura de Seguridad e Ingeniería
- Dom 4: Comunicaciones y Seguridad de Red
- Dom 5: Identidad y Géstión de Acceso (IAM)
- Dom 6: Evaluación de Seguridad y Testing
- Dom 7: Operaciones de Seguridad
- Dom 8: Seguridad de Desarrollo de Software

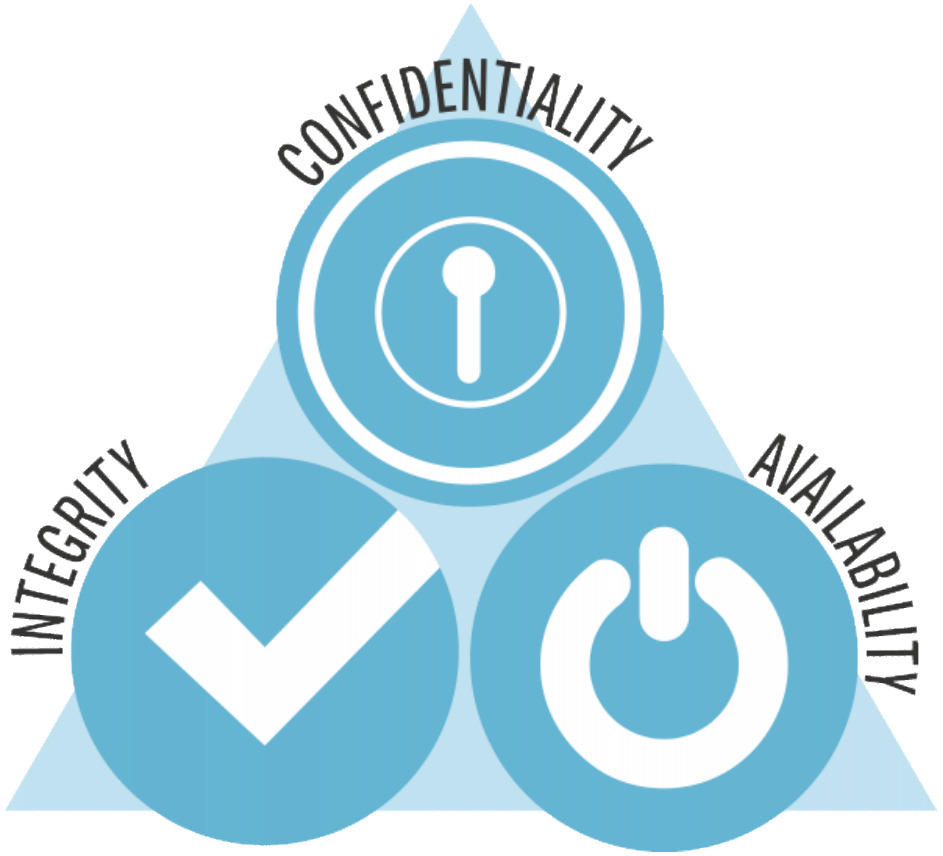
Security 101

A tener presente siempre..

- La Seguridad debe ser vista como un **elemento de gestión de negocios** más que un problema de TI.
- La Seguridad es una herramienta de gestión de negocios que asegura el funcionamiento adecuado de IT/IS. Existe para dar soporte a objetivos y misión de una organización.
- En la seguridad se conjugan elementos de evaluación, **protección costo-efectivo** y elementos legales
- **La seguridad es un camino no un destino.**

Modelos de Ciberseguridad

LA TRIADA CIA



JISSec
Journal of Information System Security

THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY

Spyridon Samonas
Virginia Commonwealth University, USA

David Coss
Virginia State University, USA

ssamonas@vcu.edu; dcoss@vsu.edu

Journal of Information System Security is a publication of the Information Institute. The JISSec mission is to significantly expand the domain of information system security research to a wide and eclectic audience of academics, consultants and executives who are involved in the management of security and generally maintaining the integrity of the business operations.

Descargable en:

http://www.proso.com/dl/Samonas.pdf

Controles de seguridad son evaluados según el soporte que dan a la protección de la Triada.
Vulnerabilidades y su riesgo son evaluadas en la forma que afectan a la Triada.

CONFIDENCIALIDAD

- DEFINICIÓN

Propiedad de un sistema que permite que la información **sólo sea accesible (visible)** por aquellas personas autorizadas.

LA TRIADA CIA

Contramedidas habituales

- Cifrado de datos
- Network Traffic Padding
- Control de Acceso estricto
- Procedimientos de autenticación rigurosos
- Clasificación de datos
- Entrenamiento de personal

INTEGRIDAD

- DEFINICIÓN

  - El conocimiento del sistema (construcción de información) **sólo podrá ser modificada** por personas debidamente autorizadas. Establece garantías de la exactitud y completitud de la información y el procesamiento de esta.

- Virus, bómbas lógicas, acceso no autorizado, errores en aplicaciones, modificaciones maliciosas, reemplazo intencional de aplicaciones, backdoors, error humano

Integridad contempla tres perspectivas:

Impedir que personas sin autorización hagan modificaciones.

Prevenir que personas autorizadas realicen modificaciones no autorizadas por ejemplo por error.

Mantener consistencia interna-externa de objetos de sistemas. Apunta a validez, consistencia y verificabilidad.

Contramedidas habituales

Control de acceso estricto

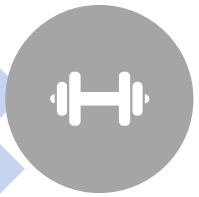
Procedimientos de autentificación rigurosos

Sistemas de detección de intrusos (IDS/IPS)

Cifrado de datos y verificación con hash

Restricciones de interfaces

Checkeo de funciones de input



Entrenamiento de personal

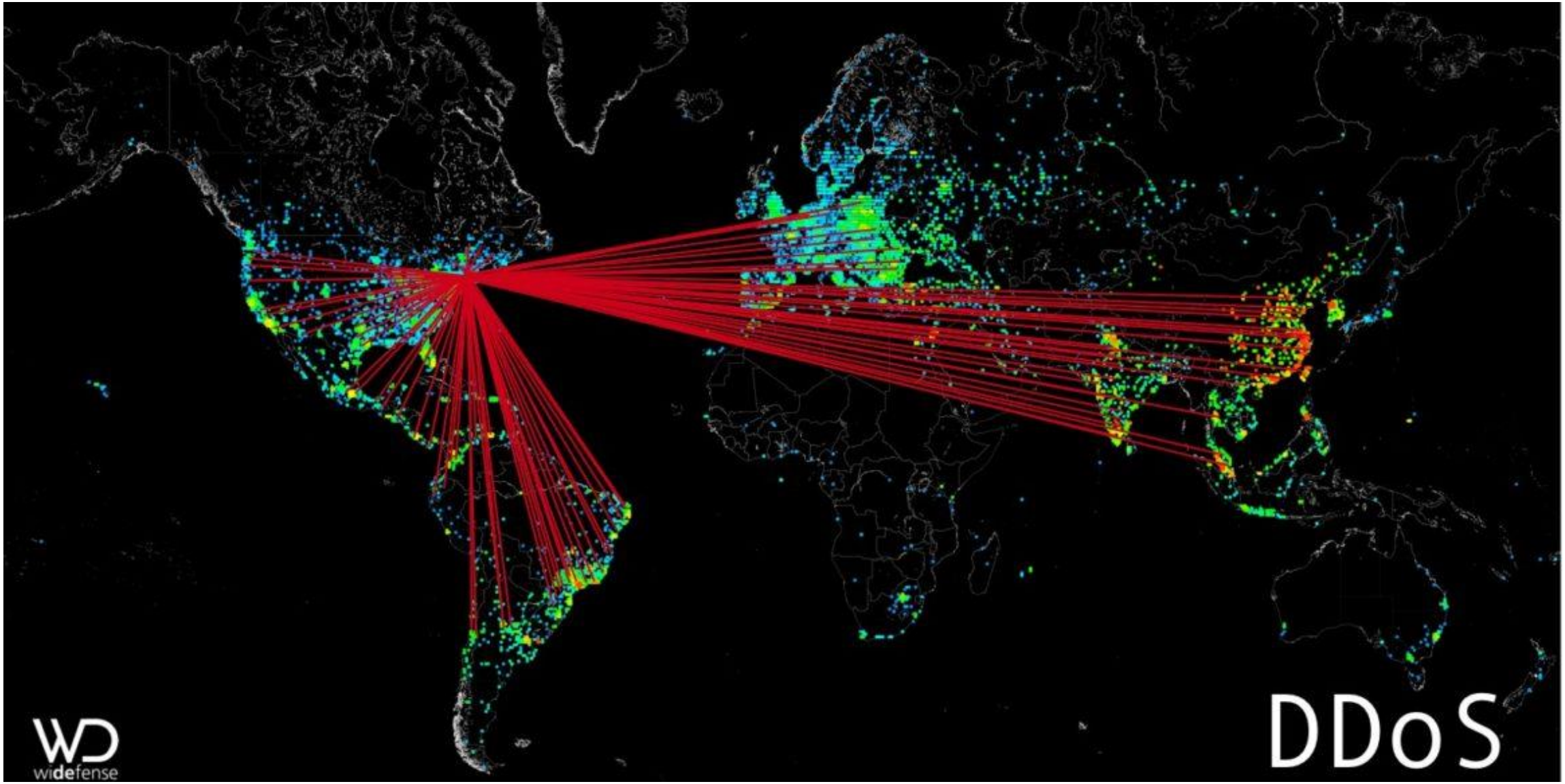
DISPONIBILIDAD

- DEFINICIÓN

Asegurarse que los usuarios autorizados **tengan acceso a sus recursos** de información y procesamiento cuando lo requieran (*)

(*) Debe considerarse la declaración de disponibilidad temporal del sistema.

- Fallas de dispositivos, errores de software, problemas ambientales
- (calor, electricidad estática, inundaciones, pérdidas de poder…).
- Ataques DoS, DDoS, destrucción de objetos, interrupción de comunicaciones


widefense
DDoS

Contramedidas habituales

- Diseño adecuado de sistema de entrega.
- Control efectivo de acceso
- Monitoreo de performance y tráfico de red
- Cortafuegos para prevenir DoS
- Implementación de redundancia de sistemas críticos
- Mantener y probar backups

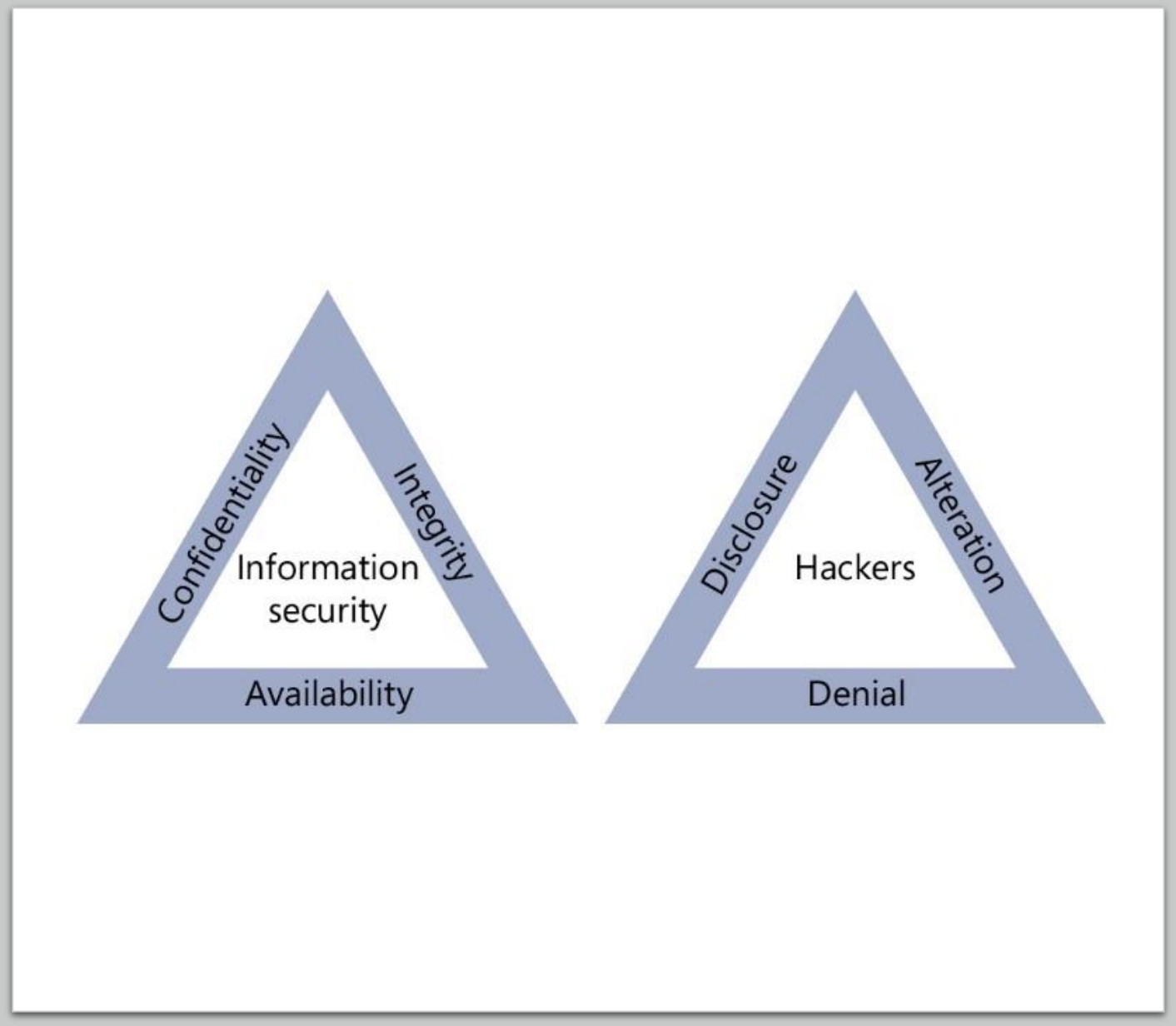
Conceptos, condiciones y aspectos de Disponibilidad

- **Usabilidad:** estado de ser fácil de aprender, entender y ser controlado por un sujeto
- **Accesibilidad:** Asegurarse que un amplio rango de sujetos puede interactuar con los recursos sin limitaciones.
- **Oportunidad (Timeliness):** estar a tiempo, disponible con baja latencia.

Complementemos la Triada CIA

- Otra visión es la Triada DAD
  - Disclosure
  - Alteration
  - Destruction

- Representa las fallas de protección de la Triada CIA



Sociotechnical Safety Evaluation of Generative AI Systems

Laura Weidinger[1], Maribeth Rauh[1], Nahema Marchal[1], Arianna Manzini[1], Lisa Anne Hendricks[1], Juan Mateos-Garcia[1], Stevie Bergman[1], Jackie Kay[1], Conor Griffin[1], Ben Bariach[1], Iason Gabriel[1], Verena Rieser[1] and William Isaac[1]

[1]Google DeepMind, London N1C 4DN, United Kingdom

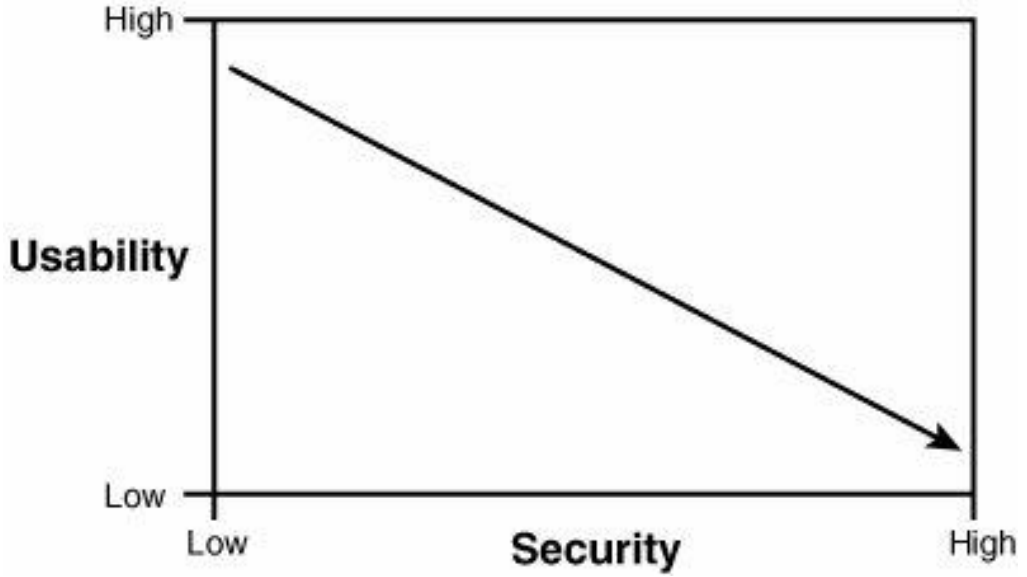
Generative AI systems produce a range of risks. To ensure the safety of generative AI systems, these risks must be evaluated. In this paper, we make two main contributions toward establishing such evaluations. First, we propose a three-layered framework that takes a structured, sociotechnical approach to evaluating these risks. This framework encompasses capability evaluations, which are the main current approach to safety evaluation. It then reaches further by building on system safety principles, particularly the insight that context determines whether a given capability may cause harm. To account for relevant context, our framework adds human interaction and systemic impacts as additional layers of evaluation. Second, we survey the current state of safety evaluation of generative AI systems and create a repository of existing evaluations. Three salient evaluation gaps emerge from this analysis. We propose ways forward to closing these gaps, outlining practical steps as well as roles and responsibilities for different actors. Sociotechnical safety evaluation is a tractable approach to the robust and comprehensive safety evaluation of generative AI systems.

Keywords: Evaluation, Sociotechnical, Generative AI, Multimodal

Necesitamos modelos distintos

El problema de la sobreprotección

- Aumento de Confidencialidad disminuye disponibilidad
- Aumento de Integridad disminuye disponibilidad
- Aumento de Disponibilidad disminuye confidencialidad e integridad



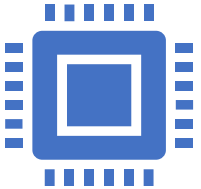
Otras propiedades importantes

Autenticidad:

Referente a fuente confiable

No repudiación:

Un sujeto que causa un evento nunca puede negar haberlo realizado



AAA Services:

Son el núcleo de mecanismos de seguridad para todos los entornos

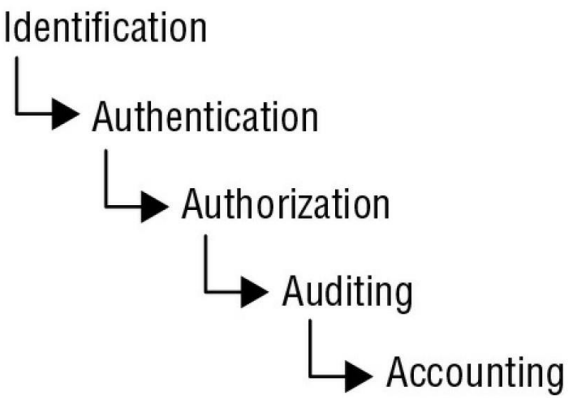
Authentication, Authorization, Accounting

Actualmente se entienden 5 elementos relevantes:

- Identification, authentication, authorization, auditing and accounting

AAA Services

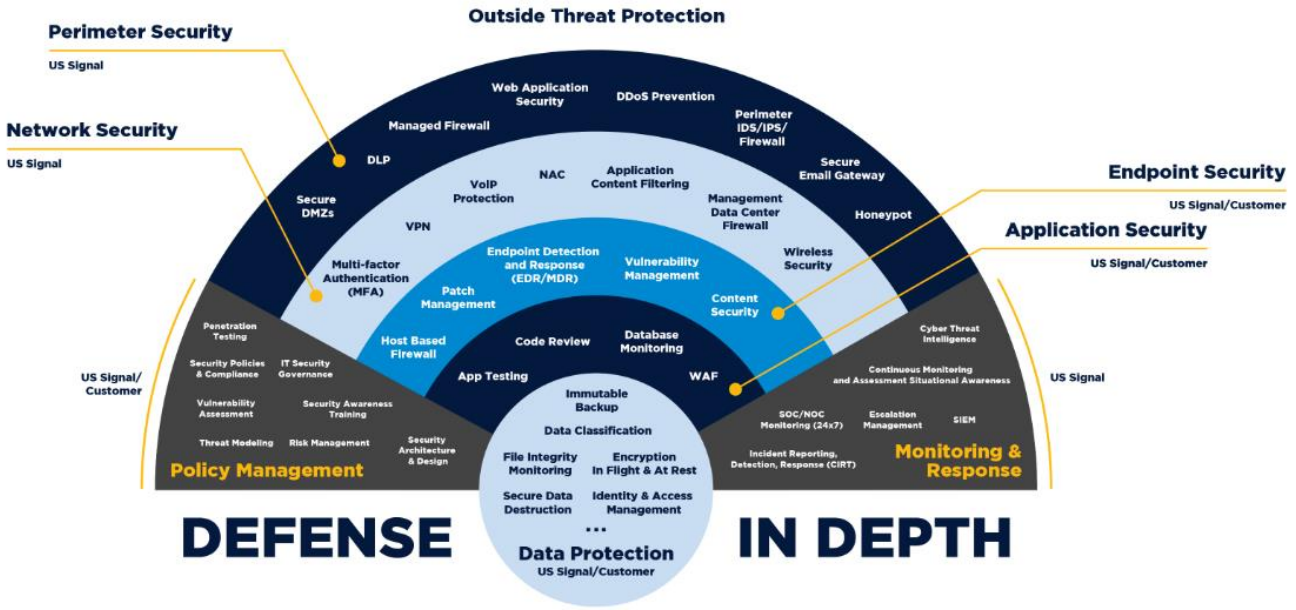
- **Identificación:** es declarar tu identidad
- **Autenticación:** probar tu identidad
- **Autorización:** asociar permisos de acceso a recursos asociados a su identidad.
- **Auditar:** registrar las actividades realizadas por sujetos en el sistema
- **Accounting:** revisar la información auditable buscando irregularidades



Mecanismos de Protección

Defense in Depth

- También conocido como Layering.
- Múltiples controles en una serie
- Diseño por capas para evitar exposición por simple falla.
- Se privilegia la serialidad y no el paralelismo de los controles



Abstraction

- Objetivo facilitar el orden y eficiencia
- Poner elementos similares en grupos, clases, roles que asocian controles de seguridad, restricciones o permisos como colectivo

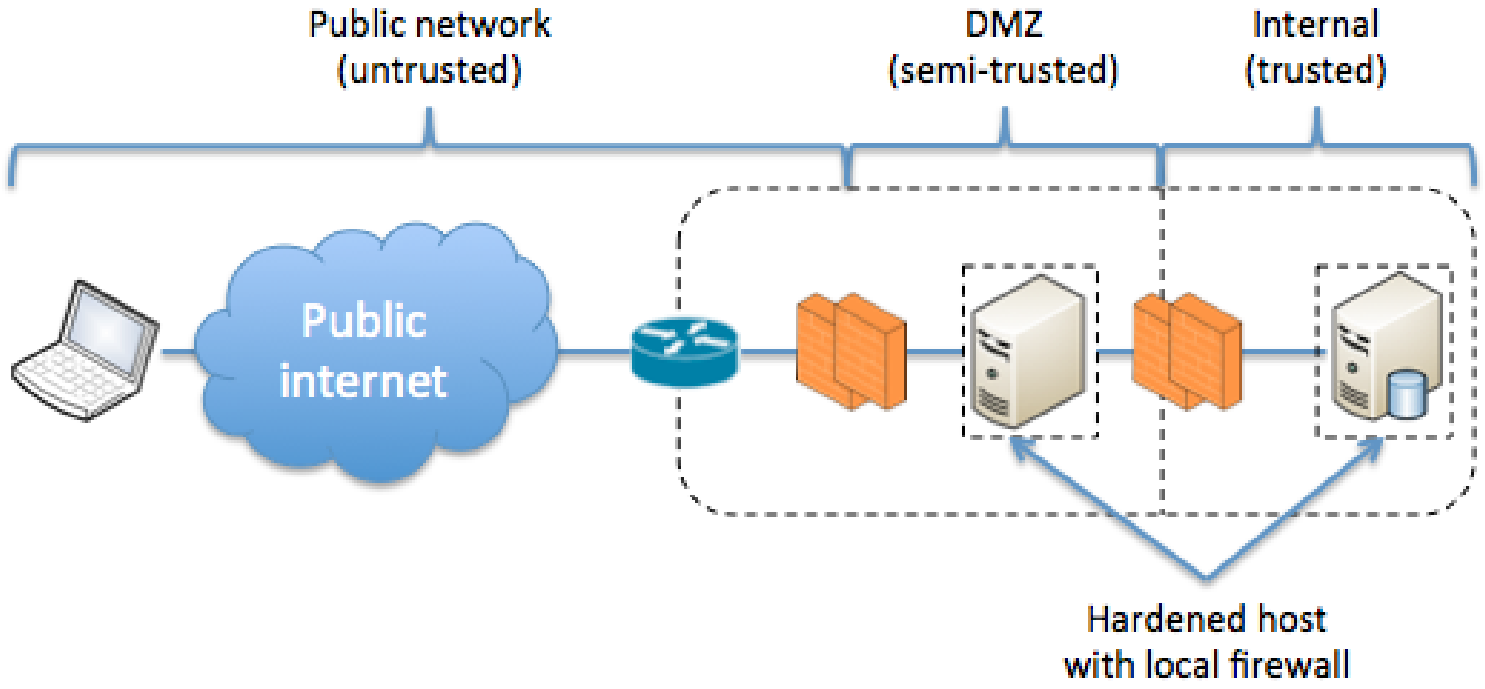
Data Hiding

- Es justamente lo que dice Intencionalmente posicionar datos donde no sean visibles o accesibles para un sujeto no autorizado.
- Sujetos no pueden ver o acceder los datos.
  - Mantener bases de datos fuera de acceso para usuarios sin nivel apropiado de acceso.
- Distinto a seguridad por medio de oscuridad (donde no se esconden, pero no se informa a los usuarios) **ej: Honeypot.**

Encryption

- Ocultar contenido o comunicaciones de sujetos no autorizados
- Posee muchos usos y es uno de los pilares de la ciberseguridad.

Security Boundaries



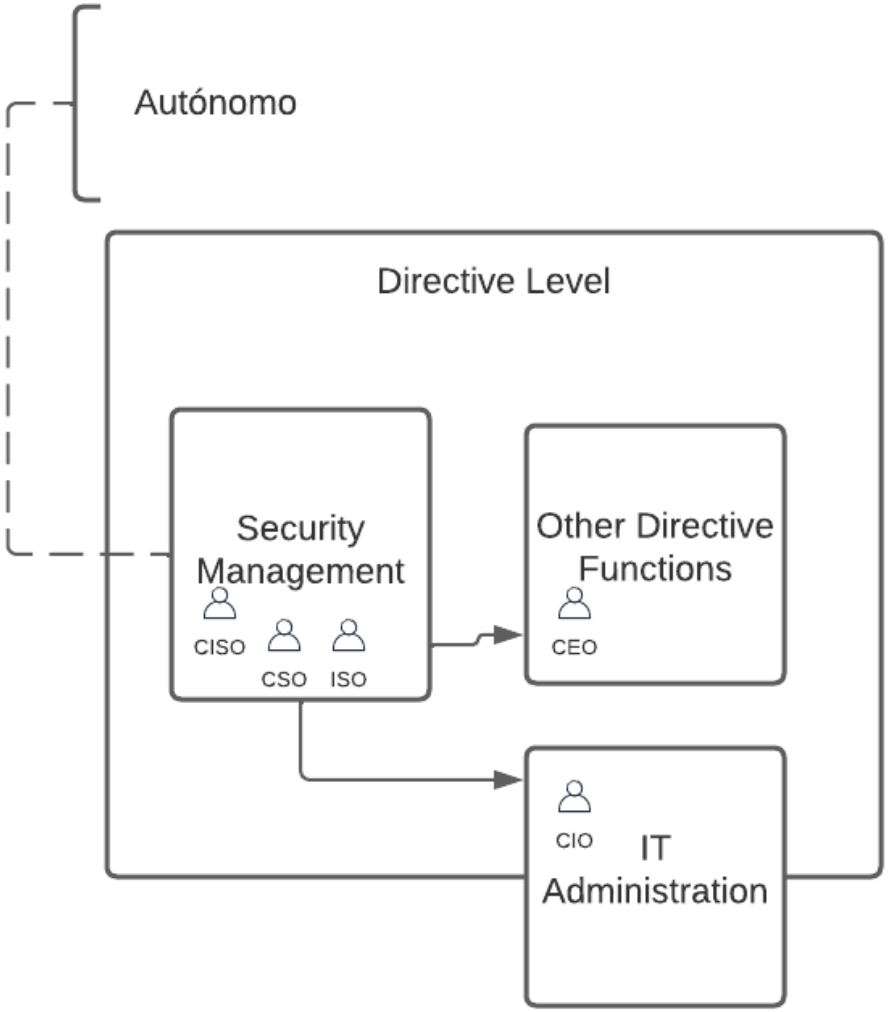
Security Governance

- Colección de prácticas relacionadas con **soportar, evaluar, definir y dirigir el esfuerzo de seguridad** de una organización
- Dirigido por una junta directiva, organizaciones pequeñas pueden estar a cargo de un:
  - Chief executive officer **(CEO)**
  - O Chief information security officer **(CISO)**
- Dirección estrechamente relacionado con Gobierno TI.
- **Security es actualmente considerado un proceso de la organización.**
- Existen múltiples frameworks y guías de gobierno de la ciberseguridad NIST SP 800-53, NIST SP 800-100, enfocados en gobierno y defensa per adoptado y adaptado a otros tipos de organizaciones.

Administrando la Función de Seguridad

- La **seguridad debe ser medible**.
  - Esto permite evaluar la postura
  - Evaluar el efecto de los controles adoptados
  - Se debe desarrollar e implementar una estrategia
  - Debe asegurar la apropiada creación, implementación y aplicación de una **política de seguridad**.
  - Debe alinearse a objetivos, misión y metas de la organización.
  - **Seguridad basada en casos de negocio**
  - **Lo mejor es asumir un enfoque Top-Down**

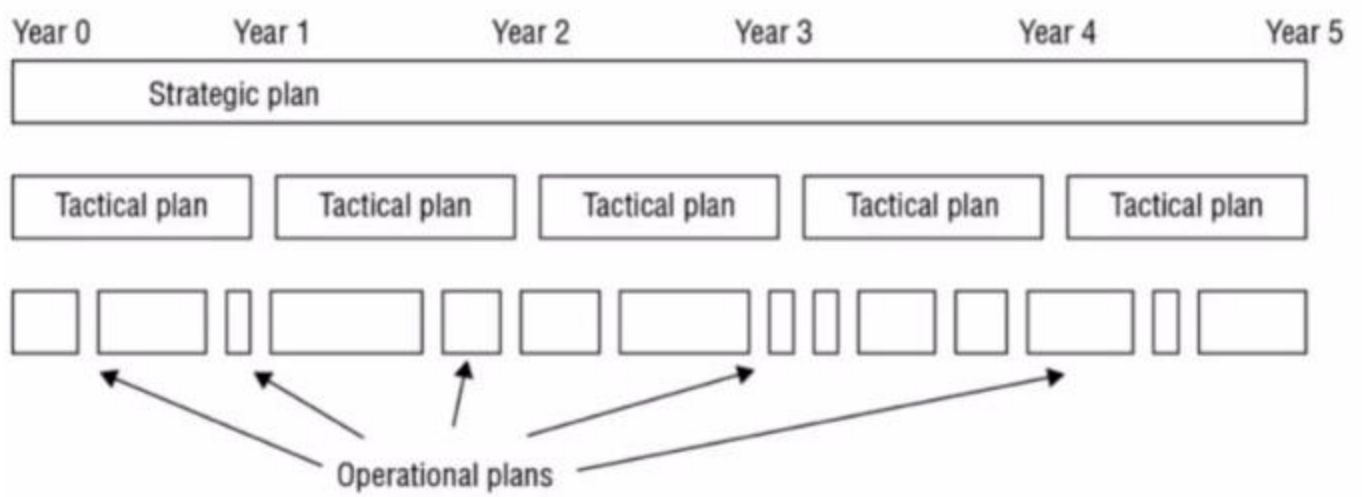
Organización



Funciones de Dirección de Seguridad

- Definir roles de seguridad
- Establecer como se administrará la seguridad
- Cómo se verificará la efectividad de los controles
- Desarrollar políticas de seguridad
- Realizar análisis de riesgos
- Educar a los trabajadores

Strategic, tactical and operational plan timeline comparison



Roles y Responsabilidades

- Los roles más comunes en seguridad de la información son los siguientes:
  - **Senior Manager**: organizational owner, último responsable, firma todas las políticas, en la mayoría de los casos es un ente de gestión y no profesional en ciberseguridad.
  - **Security professional:** incluye a infoSec officer, Computer Incident Reponse Team (CIRT), entre otros y está asignado a personal entrenado y con experiencia en redes, sistemas y seguridad. Deben seguir las directivas del Senior Manager.
  - **Asset Owner:** Encargado de clasificar la información para su protección y acceso. Típicamente gestores de alto rango
  - **Custodian:** Encargado de implementar la protección definida por políticas de seguridad y Senior Management. Encargado de preservar la Triada CIA, y cumplir con responsabilidades delegadas de Asset Owner. Cumplen tareas como: testing backups, validar integridad de datos, implementar soluciones de seguridad, administrar data storage basados en clasificación de datos.
  - **User:** personas que operan sistemas asegurados, están limitados por el principio de mejor privilegio posible, y son responsables de conocer y observar las políticas de seguridad.
  - **Auditor:** encargados de verificar que la política de seguridad esté implementada y que las soluciones de seguridad son adecuadas, aporta al cumplimiento y reportes de efectividad revisados por Senior Management, entregan información importante para la toma de decisiones.

Security Control Frameworks

- Existen varios marcos de referencia, uno de los más conocido es *Control Objetives for Información and Related Technology* (**COBIT**), desarrollado *por Information System Audit and Control Association* (ISACA)
- Principios de COBIT:
  - Provide Stakeholder value
  - Holistic Approach
  - Dynamic Gobernance System
  - Governance distinct from Management
  - Tailored to Enterprise Needs
  - End-to-End Governance System

Otras guías disponibles

- NIST 800-53 Rev. 5 https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final Recomendaciones del Gobierno US.
- Center of Internet Security (CIS), provee información sobre configuración segura de OS, aplicaciones, y hardware en https://learn.cisecurity.org/benchmarks
- NIST Risk Management Framework (RMF) https://csrc.nist.gov/projects/risk-management/about-rmf
- NIST Cybersecurity Framwork (CSF) https://www.nist.gov/cyberframework
- Internationa Organization form Standarization (ISO) Familia 27000 https://www.itgovernanceusa.com/iso27000-family
- Information Technology Infraestructure Library (ITIL) https://www.itlibrary.org/

Políticas de Seguridad

- La **capa más alta de formalización** es la política de seguridad
  - Define **ámbito de seguridad y recursos a ser protegidos**
  - Determina que **tipos de soluciones de seguridad se consideran**
  - Es una **vista general de la seguridad** necesaria para la organización
  - La política define: **objetivos de seguridad estratégicos, visión, metas y alcances, define roles y responsabilidades, especifica requerimientos de auditoría, requerimientos de cumplimento y establece los niveles de riesgo aceptables**.
  - De la política **se derivan otros documentos**: estándares, baselines, guías, procedimientos.

Una Política de Seguridad no se vende ni se compra

- No existen productos que hagan todo.
- Establece lo que se puede hacer y lo que no, de forma escrita y formal.
- Demuestra que la empresa se lo quiere tomar en serio. **Implica un compromiso con los directivos.**
- Útil frente a una auditoria, sobre todo si se siguen las normalizaciones.
- Útil para demostrar casos de intrusiones o delitos contra los sistemas informáticos.

Security Standards, Baselines, and Guidelines

Standards definen requerimientos a ser cumplidos, ej: homogeidad de hardware y software, tecnología y controles de seguridad.

Baselines define los nivenes mínimos de seguridad que cada sistema de la organización debe poseer. Es una versión más operacional del standard., muchas veces hace referencia a estándares gubernamentales o de la industria.

Guidelines, ofrecen guías para la implementación de estándares y baselines, son guías operacionales para profesionales y usuario, pueden ser sugerencias y no necesariamente obligatorias.

Security Procedures

- Elemento final de la formalización de la seguridad también llamados *standard operating procedure* (SOP)
- Son documentos detallados paso paso que describen acciones exactas para implementar mecanismos de seguridad, controles o soluciones.
- Se actualizan regularmente con nuevo software y hardware

Nombre	Código	Descripción	Estado	Vigencia
Documentos Componentes	PSI_DC01	Declaración Oficial de Documentación las Políticas de Seguridad	Esperando Aprobación	Indefinida
Guía Elemental de Elaboración	PSI_GE01	Definición de Metodología, roles y responsabilidades como fases de generación de políticas de seguridad	Revisión	Indefinida
Política de la Seguridad de La Información (Política de Primer Nivel)	PSI_SI01	Definiciones básicas, clasificaciones de información y declaración de riesgo	Declarada	No especificado
Políticas de Seguridad del Personal	PSI_SP01	Normas de actuación como usuarios respecto a buenas prácticas, uso adecuado de recursos y seguridad de información	Declarada	No especificado
Política de Administración de Sistemas	PSI_SE_AS01	Normas y procedimientos de buenas prácticas en administración de sistemas.	Declarada	No especificado
Política de Redes	PSI_SE_PR01	Procedimientos de gestión, uso y coordinación con empresas externas	Declarada	No especificado
Estándares de Desarrollo de Software Departamental	PSI_PD01	Declaración de plataforma departamental, arquitectura de servicios y restricciones de desarrollo	Revisión	Indefinida
Plan General de Continuidad Operativa	PSI_CN01	Procedimientos para garantizar operatividad administrativa en caso de incidentes mayores	Declarada	No especificado
Declaración de faltas a las políticas de seguridad y sanciones asociadas	PSI_SA01	Definiciones basadas en estatuto administrativo y potestades departamentales	Declarada	No especificado
Control de Acceso Físico a Laboratorios y NOC Departamental	PSI_SE_AS01_01	Procedimientos de Implantación Rápida, de uso temporal	Aplicada	Temporal