Unidad 8

Evaluación y gestión de seguridad

Sistemas de Evaluación - Objetivos

- **Mostrar que un sistema cumple requerimientos de seguridad específicos bajo ciertas condiciones**
  - El sistema se denomina “confiable”.
  - Basado en evidencia específica que respalda su confiabilidad.
- **Metodología formal de evaluación**
  - Técnica utilizada para proporcionar medidas de confianza basadas en requerimientos de seguridad específicos y en evidencia sobre su confiabilidad.

Metodología de evaluación

- **Proporciona:**
  - Un conjunto de requisitos:
    - que definen la funcionalidad de seguridad del sistema.
    - que delinean los pasos para establecer que el sistema cumple sus requisitos funcionales.
  - La metodología para determinar que el sistema cumple los requisitos funcionales basados en el análisis de evidencia específica que respalda su confiabilidad.
  - Una medida de resultado que indica cuan confiable es el sistema con respecto a requisitos funcionales de seguridad.
    - Llamado “nivel de confianza”

¿ Por qué evaluar ?

- **Proporciona un análisis independiente y una medida**
  - Análisis de los requerimientos para ver si son consistentes, completos, técnicamente adecuados, suficientes para contrarrestar amenazas
  - Análisis de la documentación (administración, usuario, instalación) que proporcione información sobre como configurar, administrar y usar el sistema.

TCSEC

- **Trusted Computer System Evaluation Criteria**
  - 1983-1999
  - También conocido como “Orange Book”
  - Desarrollado por el NCSC (National Computer Security Center - DoD)
- **Influenciado por el modelo Bell-LaPadula y el concepto de monitor de referencia.**
- **Pone énfasis en la confidencialidad**
- **Define 4 divisiones (D, C, B, A) en orden jerárquico ascendente, cada división representa el grado de confianza que se asigna al sistema evaluado.**

D - Minimal Protection

- **Reservado para los sistemas evaluados que no cumplen los requisitos de una clase de evaluación mas alta.**

C - Discretionary Protection

- **C1 - Discretionary Security Protection**
  - Tiene mínimos requerimientos funcionales para identificación y autenticación
  - Control de acceso discrecional
- **C2 - Controlled Access Protection**
  - Control de acceso discrecional más detallado
  - Utilización de procedimientos de login
  - Auditar la utilización de recursos

B - Mandatory Protection

- **B1 - Labeled Security Protection**
  - Requiere control de acceso mandatorio, pero este control puede ser restringido a un conjunto especifico de objetos.
  - Uso de etiquetas de clasificación de seguridad.
  - Modelo informal de política de seguridad.

- **B2 - Structured Protection**
  - Los controles de acceso mandatorios se aplican a todos los sujetos y objetos.
  - Separación de los roles de administración y operación.
  - Determinación de elementos críticos y no críticos con respecto a su protección.
  - Principio del menor privilegio.
  - Controles de configuración estrictos.
  - Modelo formal de política de seguridad.

- **B3 - Security Domains**
  - Utilización de monitor de referencia para acceder a los recursos.
  - Técnicas de desarrollo tendientes a simplificar la complejidad del sistema.
  - Procedimientos para recuperación segura del sistema.

A - Verified Protection

- **A1 — Verified Design**
  - Idéntica funcionalidad que B3
  - Técnicas de diseño y verificación formales incluyendo especificación formal de alto nivel.

Evaluación

- **Hecho por el gobierno, no por empresas.**
- **3 Etapas**
  - Solicitud de evaluación
    - Si el gobierno no necesita el producto puede ser denegada.
  - Revisión técnica preliminar
    - Discusión del proceso de evaluación, fechas, proceso de desarrollo, contenidos técnicos, etc.
    - Determinación del plan de evaluación
  - Fase de evaluación
- **Contempla un programa de actualización**
  - RAMP (Ratings Maintenance Program)

Impacto

- **Introdujo una nueva forma de evaluar seguridad**
  - Basada en el análisis del diseño, implementación, documentación y procedimientos.
  - Introdujo el concepto de clases de evaluación, requerimientos de seguridad y evaluaciones basadas en información confiable.
  - Evaluación técnica en profundidad.
- **Problemas**
  - El proceso de evaluación es difícil (falta de recursos)
  - Las evaluaciones solo son reconocidas en EEUU.

Common Criteria

- **Aparece en 1998 con la firma del "Common Criteria Recognition Agreement"**
  - EEUU, Reino Unido, Canadá, Francia, Alemania
- **Es el estándar ISO 15408**
- **Estándar de evaluación de facto en EEUU**

Metodología de evaluación

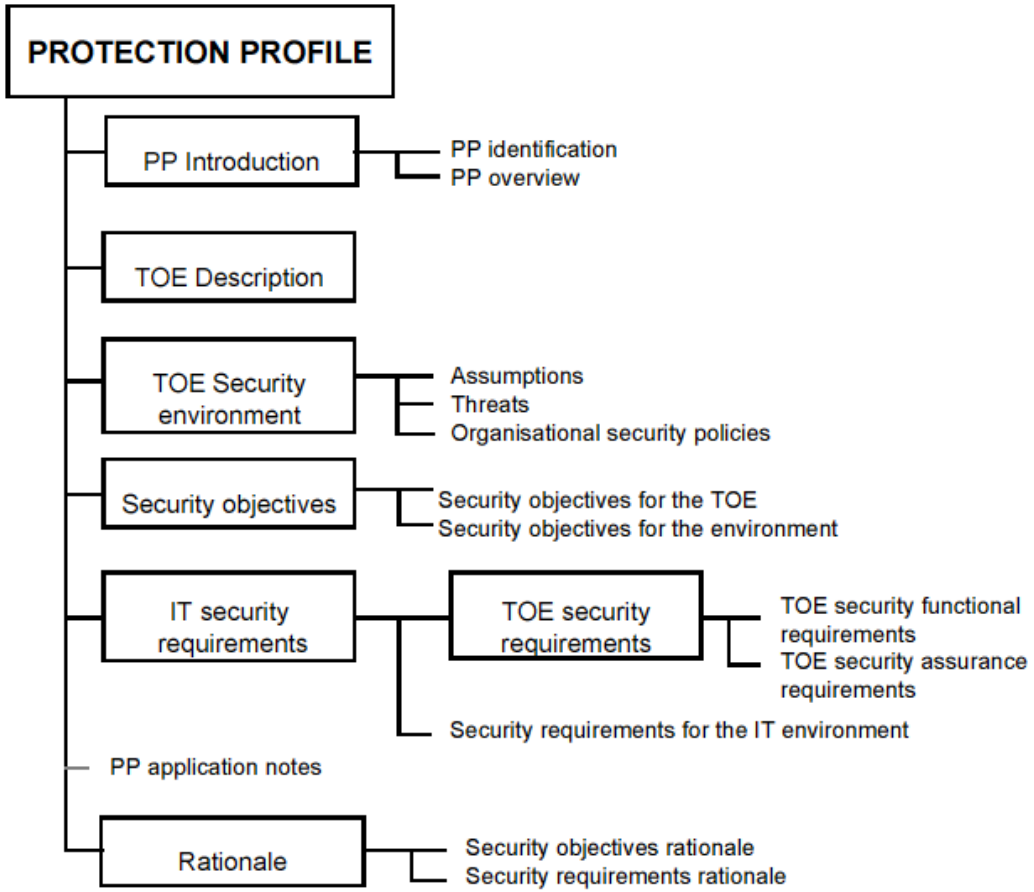
- **Se compone de tres partes**
  - Documentos CC
    - Introducción de la metodología, requerimientos funcionales y requerimientos de seguridad.
  - Metodología de evaluación CC (CEM)
    - Guías detalladas de evaluación para cada EAL (Evaluation Assurance Levels).
  - Esquema de evaluación nacional
    - Infraestructuras nacionales especificas que implementan CEM
    - En EEUU el NIST acredita a laboratorios comerciales para realizar las evaluaciones (CC Evaluation and Validation Scheme)

Terminología

- ***Target of Evaluation*** **(TOE)**
  - es el sistema o producto que se esta evaluando.
- ***TOE Security Policy*** **(TSP)**
  - es el conjunto de reglas que regulan como se manejan, protegen y distribuyen los activos en el TOE.
- ***TOE Security Functions*** **(TSF)**
  - consiste en todo el hardware, software y firmare en el que el TOE se apoya para aplicar correctamente el TSP.

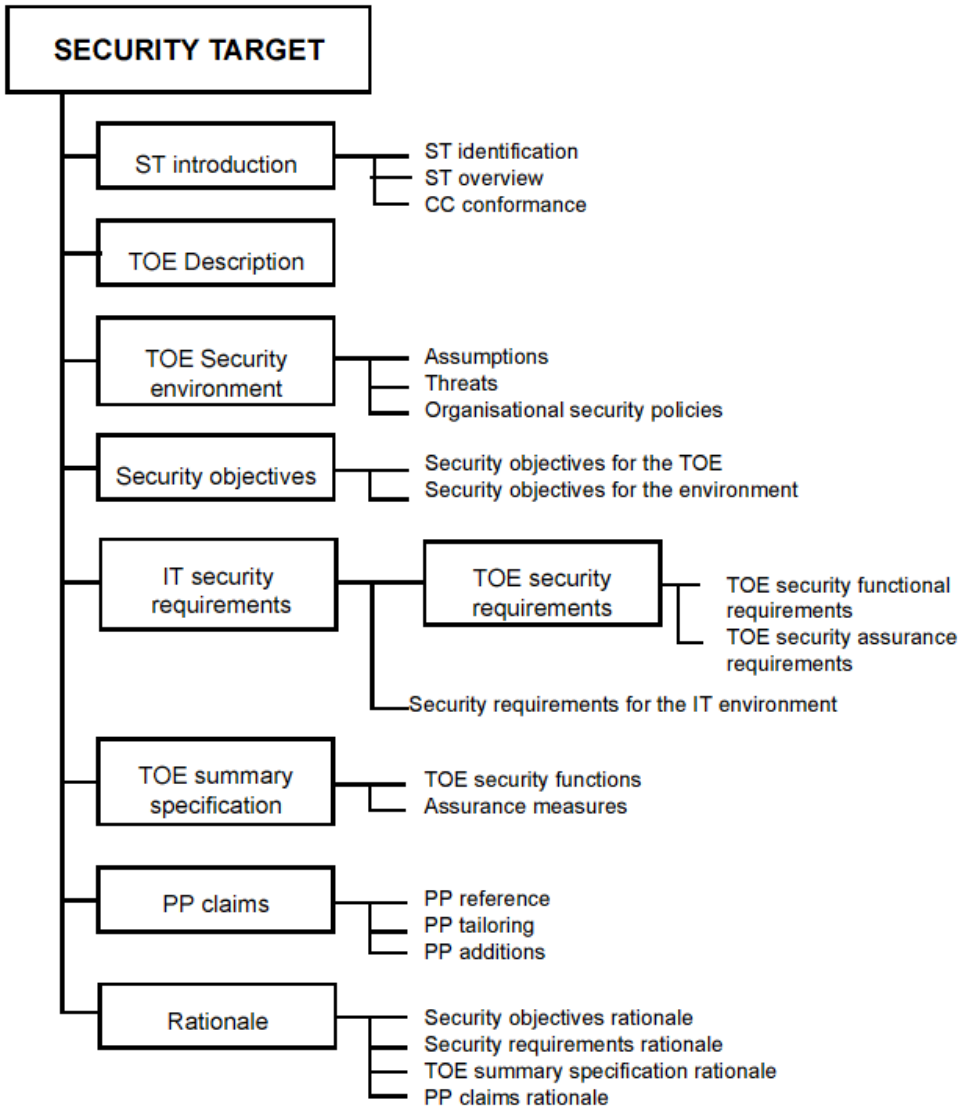
Terminología

- ***CC Protection Profile* (PP)**
  - Conjunto de requerimientos de seguridad independientes de la implementación de una categoría de productos o sistemas.
  - Incluye requerimientos funcionales
  - Incluye requerimientos de seguridad
  - Esta orientado a familias de productos o sistemas:
    - Hay PPs para firewalls, sistemas de escritorio, etc.



Terminología

- **CC Security Target (ST)**
  - Conjunto de requerimientos de seguridad y especificaciones que van a ser utilizadas como base para la evaluación de un producto o sistema.
  - Por lo general se deriva del un PP.
  - Esta orientado a un producto o sistema especifico



Terminología

- **CC Evaluation Assurance Levels (EAL)**
  - Conjunto de requerimientos de seguridad que cubren el desarrollo completo de un producto o sistema.
  - CC define siete niveles desde el más básico EAL1 (más barato y fácil de implementar y evaluar) al más estricto EAL7 (más costoso de implementar y evaluar)
  - Los niveles EAL no necesariamente implican “mejor seguridad” solo nos aseguran que el nivel de seguridad declarado por el TOE ha sido validado.

Niveles de seguridad

- **EAL1: Functionally Tested**
  - Análisis de las funciones de seguridad usando las especificaciones y la documentación.
- **EAL2: Structurally Tested**
  - Análisis de las funciones de seguridad incluyendo la información de diseño y análisis.
- **EAL3: Methodically Tested and Checked**
  - Análisis de las funciones de seguridad incluyendo la información de diseño y análisis. Utilización controles en el entorno de desarrollo.
- **EAL4: Methodically Designed, Tested and Reviewed**
  - Agrega diseño de bajo nivel, descripción completa de las interfaces, etc. Requiere un modelo informal del producto o una política de seguridad del sistema.
- **EAL5: Semiformally Designed and Tested**
- **EAL6: Semiformally Verified Design and Tested**
- **EAL7: Formally Verified Design and Tested**

Clasificación de vulnerabilidades

- **Las vulnerabilidades se pueden describir desde diferentes perspectivas**
  - Técnicas usadas para explotarlas.
  - Componente de hardware o software e interfaces que las componen.

- **Es necesario definir un esquema que permita realizar la clasificación.**

Vulnerabilidades

Esquemas de clasificación

- **El esquema de clasificación se define en base a un objetivo:**
  - Servir de guía para desarrollo de herramientas de detección de ataques

    → foco en los pasos necesarios para explotar una vulnerabilidad.
  - Servir de ayuda para el proceso de desarrollo de software

    → foco el los errores de diseño y programación que causan la vulnerabilidad.
- **El objetivo del esquema define su estructura.**

CWE (Common Weakness Enumeration)

- **Lista de tipos de debilidades de software dirigida a desarrolladores y profesionales de la seguridad.**
- **Fue creada al igual que CVE para unificar la descripción de las debilidades de seguridad de software en cuanto a arquitectura, diseño y código se refiere.**
- **http://cwe.mitre.org/**
- **http://cwe.mitre.org/top25/index.html**

3 CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Summary

Weakness Prevalence	High	Consequences	Code execution, Denial of service, Data loss
Remediation Cost	Low	Ease of Detection	Easy
Attack Frequency	Often	Attacker Awareness	High

Discussion

Buffer overflows are Mother Nature's little reminder of that law of physics that says: if you try to put more stuff into a container than it can hold, you're going to make a mess. The scourge of C applications for decades, buffer overflows have been remarkably resistant to elimination. However, copying an untrusted input without checking the size of that input is the simplest error to make in a time when there are much more interesting mistakes to avoid. That's why this type of buffer overflow is often referred to as "classic." It's decades old, and it's typically one of the first things you learn about in Secure Programming 101.

Technical Details | *Code Examples* | *Detection Methods* | *References*

Prevention and Mitigations

Requirements

Use a language that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.
For example, many languages that perform their own memory management, such as Java and Perl, are not subject to buffer overflows. Other languages, such as Ada and C#, typically provide overflow protection, but the protection can be disabled by the programmer.

Be wary that a language's interface to native code may still be subject to overflows, even if the language itself is theoretically safe.

Architecture and Design

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

Scoring

- **Dada una vulnerabilidad, se necesita tener un valor indicativo de su severidad que ayude a determinar la urgencia y prioridad con que se debe responder a la misma (Ej: aplicar un parche).**

- **Problemas**
  - Diferentes organizaciones involucradas (Vendors, CSIRTs, Investigadores, Usuarios)
  - Diferencias entre las organizaciones de un mismo tipo
  - Diferentes sistemas de scoring
  - Diferentes métricas

Sistemas de scoring (ejemplos)

- **Microsoft**
  - Critical, Important, Moderate, Low
- **CERT/CC, US-CERT**
  - Usan un numero entre 0 y 180 para establecer la severidad de la vulnerabilidad.
    - ¿La información sobre la vulnerabilidad es ampliamente conocida o disponible?
    - ¿La vulnerabilidad se está explotando en los incidentes reportados?
    - ¿La infraestructura de Internet está en riesgo debido a esta vulnerabilidad?
    - ¿Cuántos sistemas en Internet están en riesgo con esta vulnerabilidad?
    - ¿Cuál es el impacto de explotar la vulnerabilidad?
    - ¿Cuán fácil es explotar la vulnerabilidad?
    - ¿Cuáles son las precondiciones para explotar la vulnerabilidad?
- **Secunia**
  - Extremely Critical, Highly Critical, Moderately Critical, Less Critical, Not Critical

Sistemas de scoring

- **Dada una vulnerabilidad …**
  - Microsoft → “Important”
  - CERT/CC → “47.31”
  - Secunia → “Less Critical”
- **Según CERT/CC en 2007 se reportaron 7.236 vulnerabilidades.**
  - ¿ Qué implica esto ?
    - Leer las descripciones
      - 7.236 vulnerabilidades * 15 minutos = 227 días (8 hs por día)
    - Supongamos que nos afecta sólo el 10% de las vulnerabilidades
    - Instalar los parches en un equipo
      - 724 vulnerabilidades * 1 hora = 90 días
    - Leer los reportes y aplicar los parches cuesta 227 + 90 = 317 días
- **Durante los primeros 9 meses de 2008 se reportaron 6058 vulnerabilidades.**

Fuente: http://www.cert.org/stats/vulnerability_remediation.html

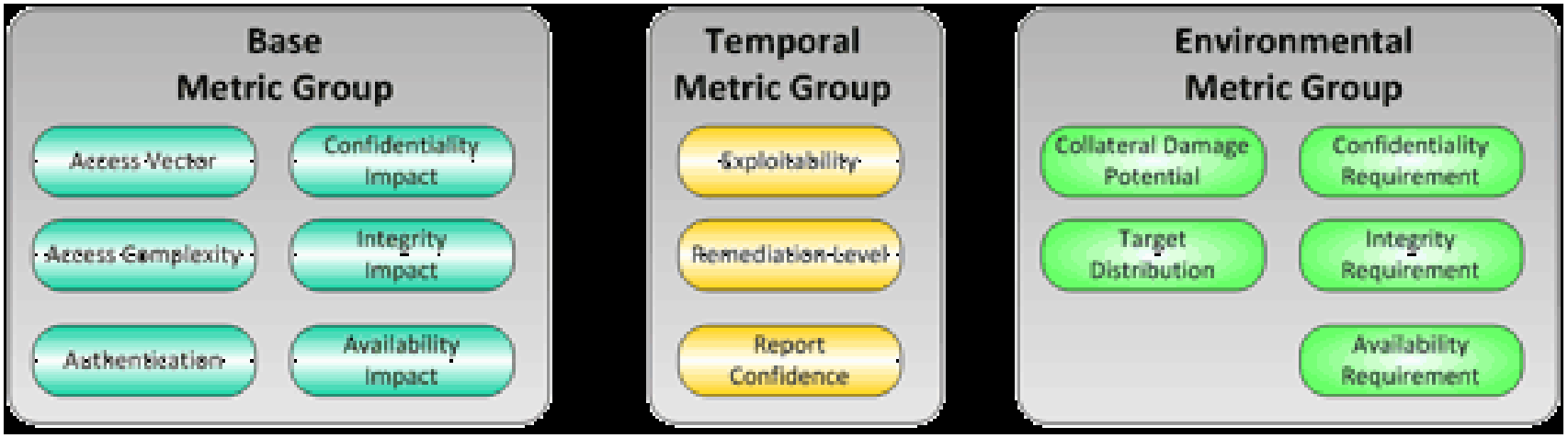
CVSS

- **Common Vulnerability Scoring System (CVSS)**
  - Estándar abierto diseñado para asignar un valor indicativo de la severidad de una vulnerabilidad y ayudar a determinar la urgencia y prioridad con que se debe responder a la misma.
  - Soluciona el problema que presenta la existencia de varios sistemas de scoring incompatibles entre sí.
  - Es usable y comprensible por cualquier persona.
  - En Junio de 2015 se publicó la versión 3
  - Es mantenido por FIRST (Forum of Incident Response and Security Teams)

¿ Como funciona ?

- **Métricas**
  - Mediciones sobre propiedades de la vulnerabilidad
- **Formulas**
  - Usan las métricas para calcular las valoraciones correspondientes
- **Score**
  - Resultado de usar las formulas con las métricas, valor entre 1 y 10.

Como funciona (V2)



Métricas Base

- **Características**
  - Atributos inherentes a a vulnerabilidad.
  - Se evalúan una sola vez.
  - Pueden ser evaluadas por un Vendor o un CSIRT
  - Condiciones de acceso que se requieren
    - Vector de Acceso
    - Complejidad de Acceso
    - Autenticación
  - Impacto
    - Confidencialidad
    - Integridad
    - Disponibilidad
- **Métricas**
  - Access Vector, Access Complexity, Authentication, Confidentiality Impact, Integrity Impact, Availability Impact
- **Score**
  - Representa la gravedad intrínseca de la vulnerabilidad

Métricas Temporales

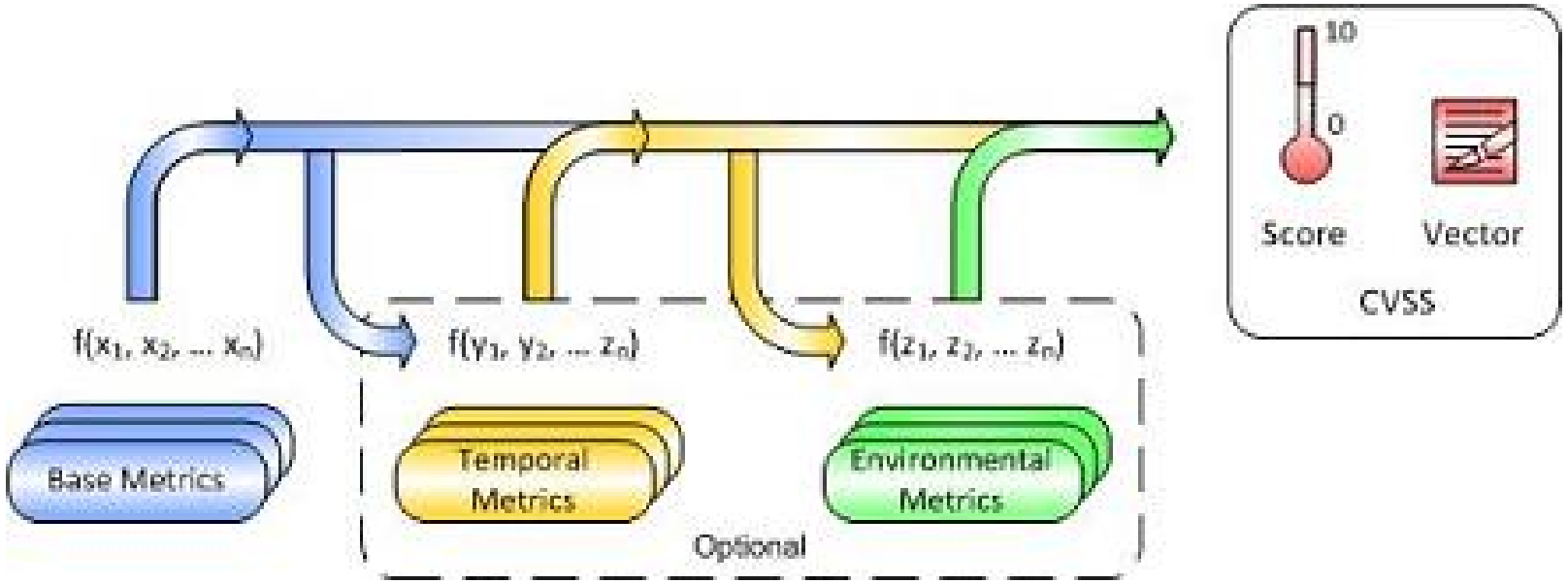
- **Características**
  - Varían en el tiempo.
  - Diseñadas para ser reevaluadas.
  - Pueden ser evaluadas por un Vendor o un CSIRT
- **Métricas**
  - Exploitability, Remediation Level, Report Confidence
- **Score**
  - Representa la severidad de la vulnerabilidad considerando factores dependientes del tiempo
  - Como máximo puede ser igual que el Base, como mínimo un 33% menos

Métricas de Ambiente

- **Características**
  - Son localizadas, dependen de factores específicos de un entorno/ambiente.
  - Evaluadas por un usuario de CVSS
- **Métricas CVSS**
  - Collateral Damage Potential, Target Distribution, Security Requirements
- **Score**
  - Representa la gravedad de la vulnerabilidad para un entorno/ambiente dado
  - No puede ser mayor al score temporal

Scoring

- **Más información:**



http://www.first.org/cvss/

http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2

https://www.first.org/cvss/calculator/3.0

Ejemplo: ms08-067

Boletín de seguridad de Microsoft MS08-067

Una vulnerabilidad en el servicio de servidor podría permitir la ejecución remota de código.

Afecta a Windows 2000, XP, 2003, Vista* y 2008*.

*** En Vista y 2008 es necesario autenticarse previamente.**

Ejemplo: ms08-067

- **Microsoft: Critical**
- **Cert/cc: 88.2**
- **Secunia: Highly Critical**

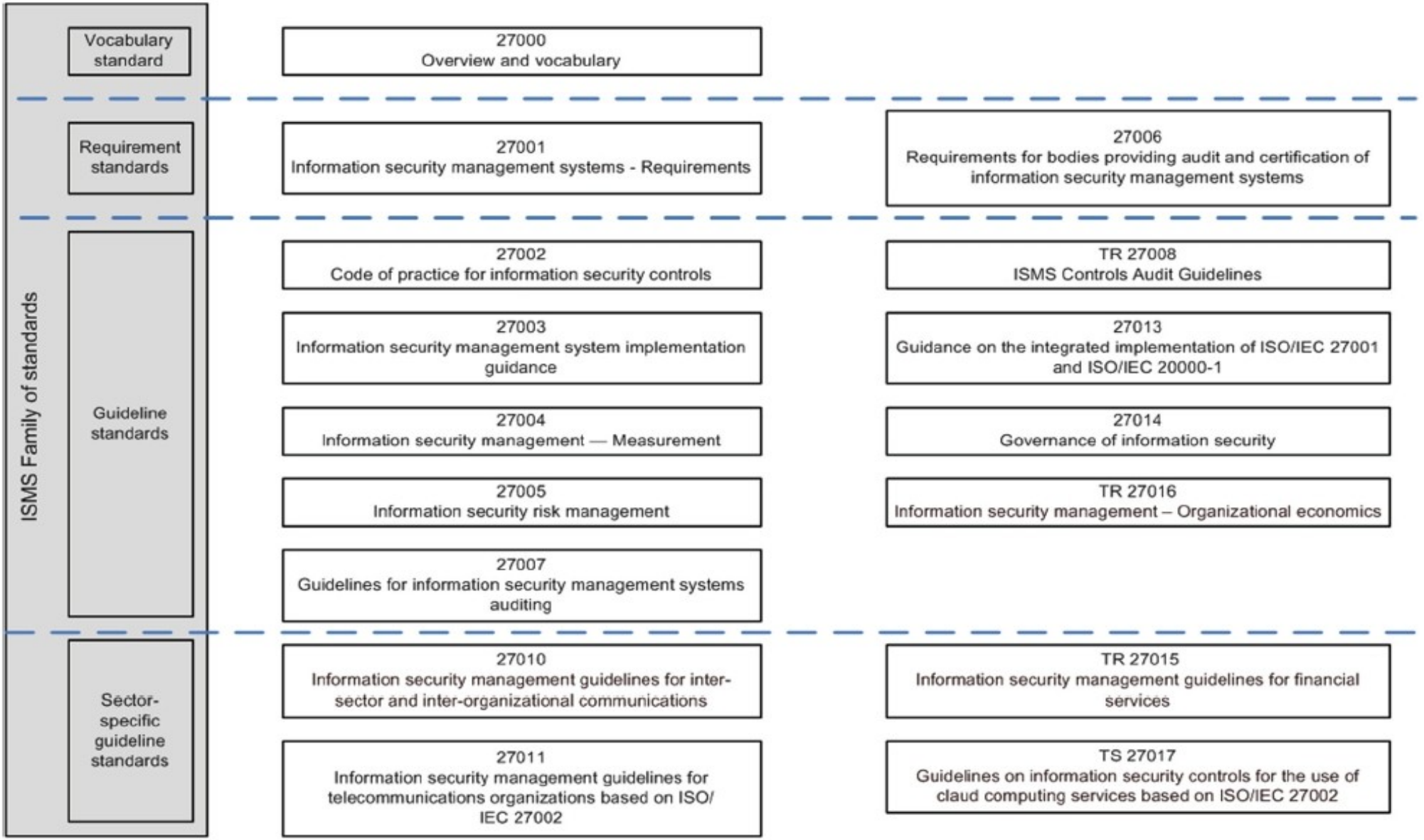
- **CVSS v2 Base Score:10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C)**

  Impact Subscore: 10.0

  Exploitability Subscore: 10.0

Normas ISO 27000

Normas ISO 27000



Normas ISO 27000

- **ISO/IEC 27002**
- **Recomendaciones de las mejores prácticas en la gestión de la seguridad de la información.**
- **Organizada en Dominios. Ultima versión 27002/2013**

Ver http://www.infoleg.gob.ar/infolegInternet/anexos/240000-244999/242859/norma.htm

ISO/IEC 27002/2013

- **Organización de la Seguridad de la Información.**
- **Seguridad de los Recursos Humanos.**
- **Gestión de los Activos.**
- **Control de Accesos.**
- **Criptografía.**
- **Seguridad Física y Ambiental.**
- **Seguridad de las Operaciones: procedimientos y responsabilidades; protección contra malware; resguardo; registro de actividad y monitorización; control del software operativo; gestión de las vulnerabilidades técnicas; coordinación de la auditoría de sistemas de información.**
- **Seguridad de las Comunicaciones: gestión de la seguridad de la red; gestión de las transferencias de información.**

ISO/IEC 27002/2013

- **Adquisición de sistemas, desarrollo y mantenimiento: requisitos de seguridad de los sistemas de información; seguridad en los procesos de desarrollo y soporte; datos para pruebas.**
- **Relaciones con los Proveedores: seguridad de la información en las relaciones con los proveedores; gestión de la entrega de servicios por proveedores.**
- **Gestión de Incidencias que afectan a la Seguridad de la Información: gestión de las incidencias que afectan a la seguridad de la información; mejoras.**
- **Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio: continuidad de la seguridad de la información; redundancias.**
- **Conformidad: conformidad con requisitos legales y contractuales; revisiones de la seguridad de la información.**

ISO/IEC 27001

- **Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el "Ciclo de Deming": Plan-Do-Check-Act**

ISO/IEC 27001

- **Es consistente con las mejores prácticas descritas en ISO/IEC 27002.**
- **Última versión 27001/2013.**
- **Incluye 114 controles en 14 grupos.**
- **Es la norma que se certifica.**

Ejemplo de controles 27001/2013

A.7 Seguridad ligada a los recursos humanos		
A.7.1 Previo al empleo		
Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades, y que sea aptos para los roles para los cuales están siendo considerados.		
A.7.1.1	Selección	*Control* Se debe realizar la verificación de antecedentes en todos los candidatos al empleo, de acuerdo con las leyes, regulaciones y normas éticas relevantes y en proporción a los requisitos del negocio, la clasificación de la información a ser accedida, y los riesgos percibidos.
A.7.1.2	Términos y condiciones de la relación laboral	*Control* Los acuerdos contractuales con los empleados y contratistas deben indicar sus responsabilidades y las de la organización en cuanto a seguridad de la información.
A.7.2 Durante el empleo		

Ejemplo de controles 27001/2013

A.9.4 Control de acceso al sistema y aplicaciones		
Objetivo: Evitar el acceso sin autorización a los sistemas y aplicaciones.		
A.9.4.1	Restricción de acceso a la información	*Control* Se debe restringir el acceso a la información y a las funciones del sistema de aplicaciones, de acuerdo con la política de control de acceso.
A.9.4.2	Procedimientos de inicio de sesión seguro	*Control* Cuando lo exija la política de control de acceso, el acceso a los sistemas y aplicaciones debe ser controlado por un procedimiento de inicio de sesión seguro.
A.9.4.3	Sistema de gestión de contraseñas	*Control* Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.
A.9.4.4	Uso de programas utilitarios privilegiados	*Control* Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden estar en capacidad de anular el sistema y los controles de aplicación.
A.9.4.5	Control de acceso al código fuente de los programas	*Control* Se debe restringir el acceso al código fuente de los programas.

Ejemplo de controles 27001/2013

A.12.2 Protección contra código malicioso		
Objetivo: Asegurar que la información y las instalaciones de procesamiento de información están protegidas contra el código malicioso.		
A.12.2.1	Controles contra código malicioso	*Control* Se deben implantar controles de detección, prevención y recuperación para protegerse contra códigos maliciosos, junto con los procedimientos adecuados para concientizar a los usuarios.
A.12.3 Respaldo		
Objetivo: Proteger en contra de la pérdida de datos.		
A.12.3.1	Respaldo de la información	*Control* Se deben hacer copias de respaldo y pruebas de la información, del software y de las imágenes del sistema con regularidad, de acuerdo con la política de respaldo acordada.
A.12.4 Registro y monitoreo		
Objetivo: Registrar eventos y generar evidencia.		
A.12.4.1	Registro de evento	*Control* Se deben generar, mantener y revisar con regularidad los registros de eventos de las actividades del usuario, excepciones, faltas y eventos de seguridad de la información.

Ejemplo de controles 27001/2013

A.13.2.4	Acuerdos de confidencialidad o no divulgación	*Control* Se deben identificar y revisar regularmente los requisitos de confidencialidad o acuerdos de no divulgación que reflejan las necesidades de protección de la información de la organización.
A.14 Adquisición, desarrollo y mantenimiento del sistema		
A.14.1 Requisitos de seguridad de los sistemas de información		
Objetivo: Asegurar que la seguridad de la información es parte integral de los sistemas de información en todo el ciclo. Esto también incluye los requisitos para los sistemas de información que proporcionan servicios en las redes públicas.		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	*Control* Los requisitos relacionados a la seguridad de la información deben ser incluidos en los requisitos para los sistemas de información nuevos o las mejoras para los sistemas de información existentes.
A.14.1.2	Aseguramiento de servicios de aplicación en redes públicas	*Control* La información relacionada a servicios de aplicación que pasan por redes públicas debe ser protegida de la actividad fraudulenta, disputas contractuales, y su divulgación y modificación no autorizada.

PCI

- **Payment Card Industry Data Security Standard**
- **Aplica a empresas que almacenan, procesan o transmiten datos de tarjetas de crédito.**
- **Dependiendo del volumen de transacciones, auditoría obligatoria o Declaración Jurada.**
- **Quick ref:** https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_2.pdf

PCI

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Otros estandares

SOAX: Aplica a empresas que cotizan en bolsa. Su finalidad es evitar fraudes y riesgo de bancarrota, protegiendo al inversor.

HIPAA (Health Insurance Portability and Accountability Act): Protección de información de pacientes, sector de salud.

Otros estandares - BCRA

Requisitos mínimos de gestión,implementación y control de los riesgos relacionados con tecnología informática...

Comunicación “A” 4609. ult mod: “A” 6290

http://www.bcra.gov.ar/Pdfs/Texord/t-rmsist.pdf

Medidas mínimas de seguridad en entidades financieras

Comunicación “A” 2985. ult mod: “A” 6272

http://www.bcra.gob.ar/Pdfs/Texord/t-seguef.pdf