UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Escuela Superior Ingeniería Informática

DSI
DEPARTAMENTO DE SISTEMAS INFORMÁTICOS

XUNTA DE GALICIA
CONSELLERÍA DE CULTURA, EDUCACIÓN E UNIVERSIDADE

CFR FERROL

Puesta en producción segura

- Tema 2. Determinación del nivel de seguridad requerido por aplicaciones

UNIÓN EUROPEA
Fondo Social Europeo
EL FSE invierte en tu futuro

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL

Índice

- Fuentes abiertas para el desarrollo seguro.
  - Common Vulnerabilities and Exposures (CVE).
  - Common Weakness Enumeration (CWE).
  - OWASP Top Ten (web y móvil).
- Requisitos de verificación necesarios asociados a los niveles de seguridad (ENS y CCN-STIC 803).
  - Procedimiento de valoración.
  - Tipos de información y servicios.
  - Criterios de valoración.
- Comprobaciones de seguridad a nivel de aplicación.
  - Application Security Verification Standard (ASVS).

Introducción

- La seguridad es un proceso continuo y heterogéneo.
  - Actualizaciones, pentesting, sistemas operativos.
- Es necesaria una metodología o estándar para establecer los requisitos en cuanto a seguridad de los sistemas.
- Los requisitos de seguridad dependen de los activos a proteger y de la infraestructura desplegada.
  - Tipos de datos de carácter personal.
  - Infraestructuras críticas.
- Debemos ser capaces de evaluar los riesgos de una determinada aplicación.

UCLM UNIVERSIDAD DE CASTILLA-LA MANCHA

Escuela Superior Ingeniería Informática

DSI DEPARTAMENTO DE SISTEMAS INFORMÁTICOS

XUNTA DE GALICIA | CONSELLERÍA DE CULTURA, EDUCACIÓN E UNIVERSIDADE

CFR FERROL

Tema 2. Determinación del nivel de seguridad requerido por aplicaciones

- Fuentes abiertas para el desarrollo seguro

UNIÓN EUROPEA
Fondo Social Europeo
EL FSE invierte en tu futuro

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL

Fuentes abiertas para el desarrollo seguro

- El uso de fuentes de conocimiento abiertas en el desarrollo seguro es muy recomendable para no repetir errores.
- Podemos distinguir dos vertientes de fuentes abiertas en el contexto del desarrollo seguro.
  - Fuentes abiertas con amenazas conocidas:
    - CVE y OWASP Top Ten.
  - Aplicaciones completas de código libre o fragmentos funcionales de código:
    - **Cuidado con lo que ejecutamos!**

Antes de continuar…

- **Vulnerabilidad**: fallo/debilidad/punto débil que presenta un sistema (agujero).
  - Fallos de programación.
  - Errores de configuración (p.e. contraseñas por defecto).
  - Malas prácticas (p.e. ejecución de servicios que no se utilizan).
- **Amenaza**: cualquier acción que aproveche una vulnerabilidad para atacar un sistema.
  - Hackers, robo físico, terremotos…
  - Pueden ser internas o externas.
- **Riesgo**: probabilidad de que una amenaza se materialice.
  - Aprovechando una vulnerabilidad y produciendo daños.

Antes de continuar…

- **Exploit**: programa/script elaborado específicamente para aprovecharse de una vulnerabilidad.
  - Framework Metasploit.

- **Payload**: carga útil (código, metadatos) gestionada y enviada por el exploit.
  - Objetivo: ejecutar comandos en la máquina atacada.

- **Shellcode**: instrucciones bien definidas que se ejecutarán en la máquina objetivo (normalmente escritas en lenguaje ensamblador).

Antes de continuar…

- **Zero Day (0-day)**: vulnerabilidad, exploit y/o ataque desconocido a nivel global.
  - Quien lo descubre no lo ha hecho público todavía.
  - El fabricante no conoce de su existencia, por lo que no existen actualizaciones de seguridad que parcheen el error.
  - Mercado negro: https://0day.today
  - Mercado blanco.

Common Vulnerabilities and Exposures (CVE)

- Gran base de datos de vulnerabilidades de seguridad conocidas.
  - https://cve.mitre.org
- Gestionado por The MITRE Corporation (EEUU).
- Cada vulnerabilidad se etiqueta con un CVE-ID.
  - Formato → CVE-yyyy-nnnn
- A cada CVE se le asigna información:
  - Descripción de la vulnerabilidad.
  - Versiones software afectadas.
  - Soluciones o configuraciones correctas.
  - Referencias (foros, blogs, exploits).

Common Vulnerabilities and Exposures (CVE)

CVE-ID

CVE-2020-8143 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

An Open Redirect vulnerability was discovered in Revive Adserver version < 5.0.5 and reported by HackerOne user hoangn144. A remote attacker could trick logged-in users to open a specifically cra destination.The CSRF protection of the “/www/admin/*-modify.php” could be skipped if no meaningful parameter was sent. No action was performed, but the user was still redirected “returnurl” GET parameter.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://hackerone.com/reports/794144
- MISC:https://www.revive-adserver.com/security/revive-sa-2020-002/

Assigning CNA

HackerOne

Date Entry Created

20200128 Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shar updated in CVE.

Phase (Legacy)

Assigned (20200128)

Common Vulnerabilities and Exposures (CVE)

- Ejemplos:
  - **CVE-2011-5165** (Free MP3 CD Ripper).
  - **CVE-2020-0601** (Windows CryptoAPI).
  - **CVE-2019-0708** (BlueKeep, RDP).
    - https://www.exploit-db.com
    - https://0day.today
    - https://github.com/zerosum0x0/CVE-2019-0708/tree/master/scanner

Common Weakness Enumeration (CWE)

- Sistema centrado en la categorización de tipos de debilidades/vulnerabilidades (también gestionado por The MITRE Corporation).
  - https://cwe.mitre.org

- Además de una descripción de la debilidad, ofrece información adicional:
  - Tipo de lenguaje de programación, plataforma o tecnología a la que afecta.
  - Posibles consecuencias.
  - Ejemplos demostrativos.
  - Mitigaciones potenciales.

Common Weakness Enumeration (CWE)

- Ejemplos:
  - **CWE-321** (Use of Hard-coded Cryptographic Key).
  - **CWE-473** (PHP External Variable Modification).
  - **CWE-927** (Use of Implicit Intent for Sensitive Communication).

Common Weakness Enumeration (CWE)

1337 - Weaknesses in the 2021 CWE Top 25 Most Dangerous Software Weaknesses

- Out-of-bounds Write - *(787)*
- Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - *(79)*
- Out-of-bounds Read - *(125)*
- Improper Input Validation - *(20)*
- Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') - *(78)*
- Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') - *(89)*
- Use After Free - *(416)*
- Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') - *(22)*
- Cross-Site Request Forgery (CSRF) - *(352)*
- Unrestricted Upload of File with Dangerous Type - *(434)*
- Missing Authentication for Critical Function - *(306)*
- Integer Overflow or Wraparound - *(190)*
- Deserialization of Untrusted Data - *(502)*
- Improper Authentication - *(287)*
- NULL Pointer Dereference - *(476)*
- Use of Hard-coded Credentials - *(798)*
- Improper Restriction of Operations within the Bounds of a Memory Buffer - *(119)*
- Missing Authorization - *(862)*
- Incorrect Default Permissions - *(276)*
- Exposure of Sensitive Information to an Unauthorized Actor - *(200)*
- Insufficiently Protected Credentials - *(522)*
- Incorrect Permission Assignment for Critical Resource - *(732)*
- Improper Restriction of XML External Entity Reference - *(611)*
- Server-Side Request Forgery (SSRF) - *(918)*
- Improper Neutralization of Special Elements used in a Command ('Command Injection') - *(77)*

https://cwe.mitre.org/data/definitions/1337.html

OWASP Top Ten

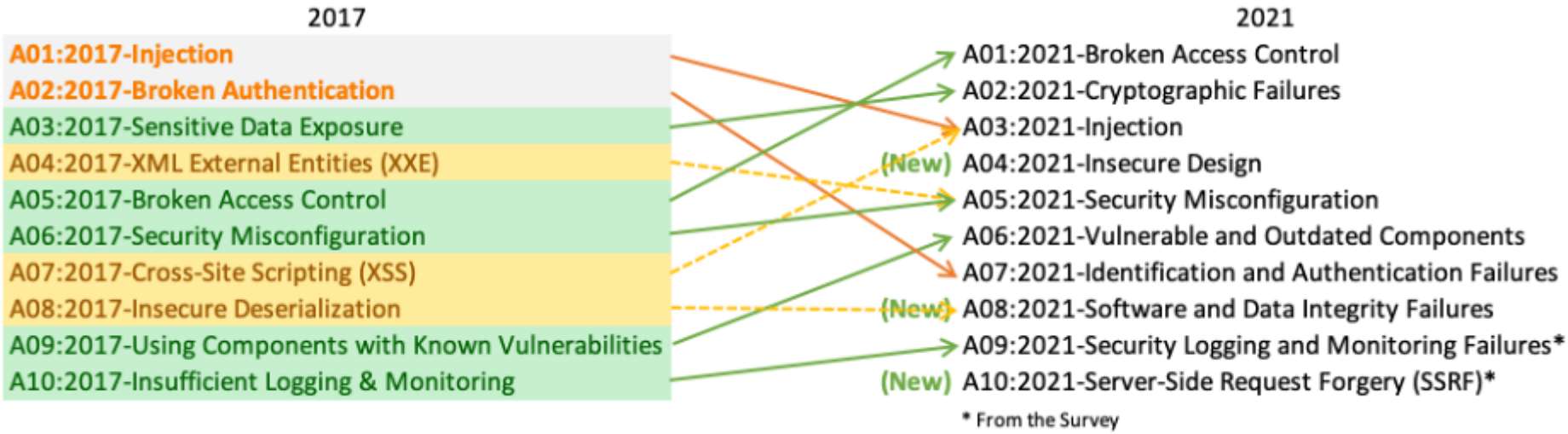
- Open Web Application Security Project (OWASP) es una fundación sin ánimo de lucro para la mejora de la seguridad web.
- El proyecto es open source y está formado por multitud de entidades y organizaciones.
- El **OWASP Top Ten**, es un documento que se actualiza cada cierto tiempo (2, 3, 4 años) en el que se recogen las vulnerabilidades más recurrentes y críticas que afectan a la seguridad web.
- También existe la versión móvil de OWASP Top Ten.

OWASP Top Ten 2013-2017

OWASP Top 10 2013	±	OWASP Top 10 2017
A1 – Inyección	→	A1:2017 – Inyección
A2 – Pérdida de Autenticación y Gestión de Sesiones	→	A2:2017 – Pérdida de Autenticación y Gestión de Sesiones
A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	↘	A3:2017 – Exposición de Datos Sensibles
A4 – Referencia Directa Insegura a Objetos [Unido+A7]	∪	A4:2017 – Entidad Externa de XML (XXE) [NUEVO]
A5 – Configuración de Seguridad Incorrecta	↘	A5:2017 – Pérdida de Control de Acceso [Unido]
A6 – Exposición de Datos Sensibles	↗	A6:2017 – Configuración de Seguridad Incorrecta
A7 – Ausencia de Control de Acceso a las Funciones [Unido+A4]	∪	A7:2017 – Secuencia de Comandos en Sitios Cruzados (XSS)
A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	☒	A8:2017 – Deserialización Insegura [NUEVO, Comunidad]
A9 – Uso de Componentes con Vulnerabilidades Conocidas	→	A9:2017 – Uso de Componentes con Vulnerabilidades Conocidas
A10 – Redirecciones y reenvíos no validados	☒	A10:2017 – Registro y Monitoreo Insuficientes [NUEVO, Comunidad]

https://wiki.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

OWASP Top Ten 2021



https://owasp.org/Top10

OWASP Top Ten 2021

- **A01:2021 → Broken Access Control**: mal funcionamiento del control de acceso de los usuarios a los recursos de una aplicación (IDs como parámetros, en URLs, etc).

- **A02:2021 → Cryptographic Failures**: fallos relacionados con el cifrado de datos de protección especial (contraseñas, tarjetas de crédito, datos médicos, etc).
  - Ejemplo: algoritmos criptográficos débiles vs. ataques de fuerza bruta.

- **A03:2021 → Injection:** envío de código malicioso al no validarse o parsearse los parámetros de entrada de una aplicación (SQLi, NoSQL Injection, etc).

- **A04:2021 → Insecure Design:** una aplicación puede implementarse adecuadamente sin fallos de seguridad y aun así ser insegura si el diseño no es el correcto.
  - Ejemplo: compra masiva de hardware mediante bots para la reventa.

OWASP Top Ten 2021

- **A05:2021 → Security Misconfiguration:** configuración incorrecta de servidores y servicios (puertos innecesarios, contraseñas por defecto, descubrimiento de mensajes de error, etc).

- **A06:2021 → Vulnerable and Outdated Components:** software y servicios sin actualizar, incompatibles o de los cuales no se conoce qué versión se está utilizando (y que podrían ser vulnerables).

- **A07:2021 → Identification and Authentication Failures**: gestión incorrecta de los ID de sesión, permitir contraseñas por defecto o débiles (usuarios) y aplicaciones vulnerables a ataques automatizados/fuerza bruta.

OWASP Top Ten 2021

- **A08:2021 → Software and Data Integrity Failures:** terceras partes capaces de atentar contra la integridad de los datos de una aplicación (bibliotecas, plugins o repositorios inseguros). También se refiere a software y actualizaciones alteradas por terceros.

- **A09:2021 → Security Logging and Monitoring Failures:** falta de registro y monitorización de eventos que ocurren en una aplicación (monitorización escasa o nula de actividades sospechosas, logs almacenados localmente, etc).

- **A10:2021 → Server-Side Request Forgery (SSRF):** falsificación de peticiones para que un servidor o servicio obtenga información de otros servidores, servicios o redes que confían en este. El objetivo es superar firewalls e IDSs.

OWASP Mobile Top Ten 2016

https://owasp.org/www-project-mobile-top-10

OWASP Mobile Top Ten 2016

- **M1 → Improper Platform Usage:** se refiere al mal uso de la plataforma móvil y sus características.
  - Android: mala gestión de permisos o mal uso de intents.
  - iOS: mal uso del Touch ID o de los servicios de Keychain.

- **M2 → Insecure Data Storage:** el almacenamiento de datos no es lo suficientemente seguro en caso de robo del dispositivo móvil o ejecución de aplicaciones que contienen malware.
  - Ejemplo: un hacker podría obtener acceso al sistema de archivos mediante software de desarrollo si el dispositivo está rooteado y/o los datos no se han almacenado cifrados.

- **M3 → Insecure Communication:** comunicación insegura con la parte del servidor o backend.
  - Conexiones HTTP no seguras, ataques de MITM, monitorización de paquetes Wi-Fi, etc.

- **M4 → Insecure Authentication:** gestión incorrecta de tokens de acceso al backend de una aplicación, permitir a los usuarios utilizar contraseñas débiles…

OWASP Mobile Top Ten 2016

- **M5 → Insufficient Cryptography:** las aplicaciones utilizan algoritmos de cifrado débiles (MD5) o los procesos de cifrado son deficientes (implementación).
  - Un atacante puede aprovechar esto para descifrar información confidencial.

- **M6 → Insecure Authorization:** mala gestión/implementación de los mecanismos de control de acceso a los recursos de una aplicación.
  - Un usuario que una vez iniciada su sesión es capaz de acceder a la zona de administrador.

- **M7 → Client Code Quality:** prácticas de implementación deficientes en el lado del cliente que permiten a terceros ejecutar código maliocioso.
  - Aprovechando buffer overflows, memory leaks…

OWASP Mobile Top Ten 2016

- **M8 → Code Tampering:** se refiere a la manipulación de aplicaciones ya existentes en las cuales se inyecta código malicioso, se reempaqueta la aplicación (.ipa o .apk) y se redistribuye con el malware.

- **M9 → Reverse Engineering:** utilización de herramientas específicas que descifran el binario de una aplicación para recrear el código fuente.
  - **Exploits!**

- **M10 → Extraneous Functionality:** bloques de código o características en proceso de desarrollo/testing que los desarrolladores dejan expuestas y pueden servir como entradas a los atacantes.

UCLM UNIVERSIDAD DE CASTILLA-LA MANCHA

Escuela Superior Ingeniería Informática

DSI DEPARTAMENTO DE SISTEMAS INFORMÁTICOS

XUNTA DE GALICIA | CONSELLERÍA DE CULTURA, EDUCACIÓN E UNIVERSIDADE

CFR FERROL

Tema 2. Determinación del nivel de seguridad requerido por aplicaciones

- Requisitos de verificación necesarios asociados a los niveles de seguridad. Esquema Nacional de Seguridad (ENS).

UNIÓN EUROPEA
Fondo Social Europeo
EL FSE invierte en tu futuro

GOBIERNO DE ESPAÑA | MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL

Esquema Nacional de Seguridad (ENS)

- Es necesario evaluar correctamente un sistema/aplicación para saber qué medidas de seguridad debemos implementar.
  - Lo que conlleva la valoración de la información y los servicios prestados.

- El **Esquema Nacional de Seguridad (ENS)** está regulado por el Real Decreto 3/2010, de 8 de enero.
  - https://www.boe.es/buscar/doc.php?id=BOE-A-2010-1330

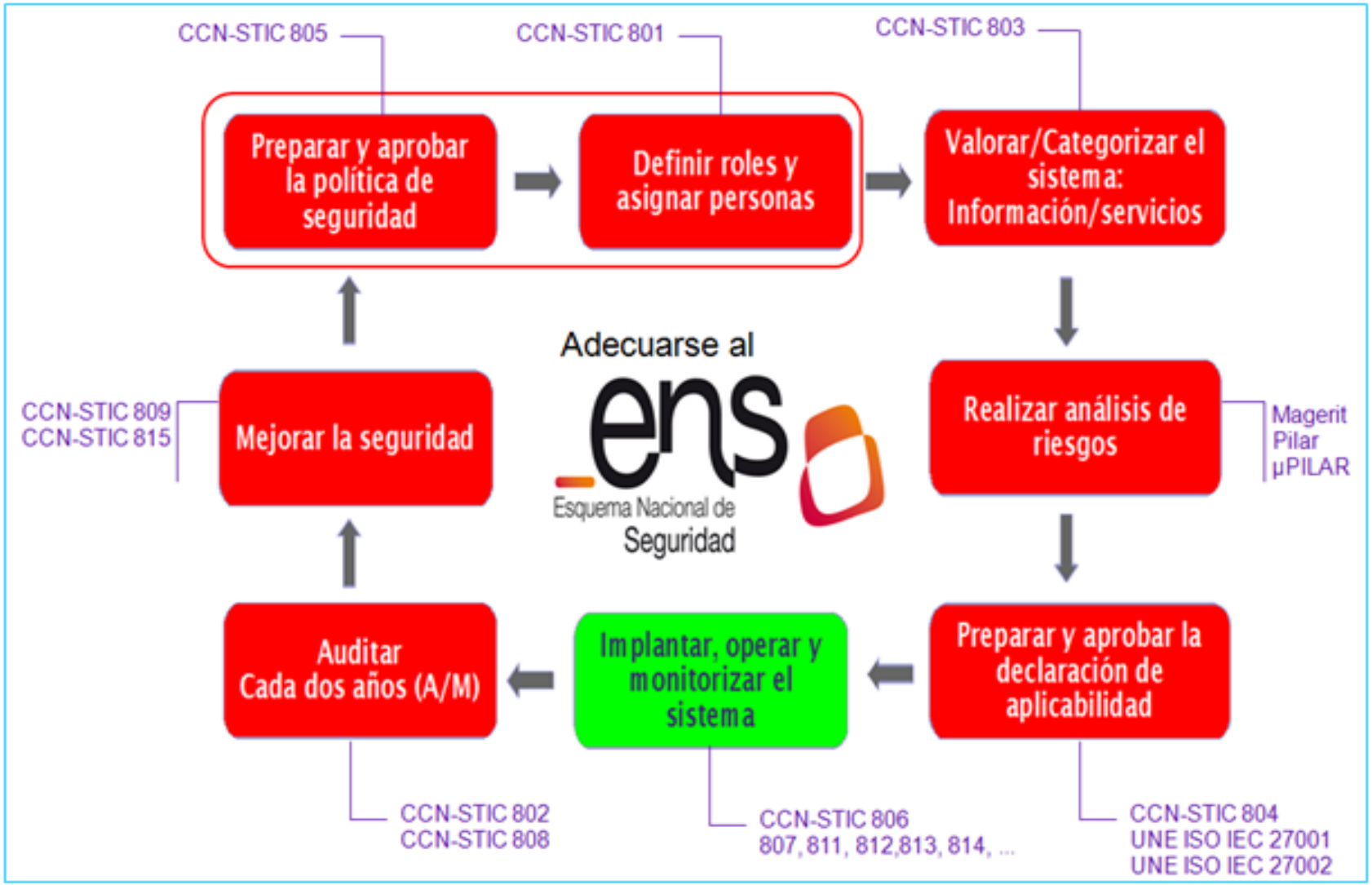
- El objetivo del ENS es el establecimiento de mecanismos de control y políticas para la utilización segura de los sistemas informáticos (tanto de la Administración Pública como en empresas).

Esquema Nacional de Seguridad (ENS)

- Dentro de la adecuación al ENS existen diferentes cuestiones o ámbitos de la seguridad.

- Para cada una de estas se desarrollan y publican documentos con normas, instrucciones, guías y recomendaciones para mejorar la seguridad.

Esquema Nacional de Seguridad (ENS)



Valoración de los sistemas (CCN-STIC 803)

- El Centro Criptológico Nacional (CCN) publica en enero de 2011 (versión actual mayo 2020) una guía de seguridad para la valoración de sistemas:
  - CCN-STIC 803

- Esta guía no es un dogma, cada empresa/institución puede adaptarla a sus condiciones e infraestructura.

Valoración de los sistemas (CCN-STIC 803)

- El valor de un sistema se concentra en los **activos esenciales,** los cuales deben cumplir unas **dimensiones de seguridad** específicas.

- Es conveniente centrarse en las tuplas activo-dimensión que tengan un impacto importante.

- Establece tres categorías de seguridad para los sistemas de información:
  - **BÁSICA**, **MEDIA**, **ALTA**.

- Establece tres niveles de seguridad para cada dimensión (de acuerdo al ENS):
  - **BAJO**, **MEDIO**, **ALTO.**

Valoración de los sistemas (CCN-STIC 803)

- La categoría de seguridad de un sistema se determina a partir de las dimensiones:
  - Máximo nivel de seguridad requerido por dimensión en todos los activos.

- La guía distingue dos tipos de activo esencial:
  - Información.
  - Servicios.

Valoración de los sistemas (CCN-STIC 803)

- Dimensiones de seguridad (CITAD):
  - **Confidencialidad**: revelación de información a entidades no autorizadas.
  - **Integridad**: modificación de información por terceras partes.
  - **Trazabilidad**: posibilidad de comprobar a posteriori qué entidad ha accedido o modificado ciertos datos.
  - **Autenticidad**: cómo de auténticos son los datos que gestiona el sistema/aplicación.
  - **Disponibilidad**: tiempo que el servicio permanece activo y puede ser accedido con normalidad por los usuarios.

- Los cuatro primeros normalmente relacionados con activos de información y el último con activos de servicios.

Valoración de los sistemas (CCN-STIC 803)

- Aclaremos las ideas…

Denominación del activo esencial	tipo[10]	C[11]	I	T	A	D
Valor máximo del nivel registrado en las dimensiones de seguridad						

Fuente: CCN-STIC 803

Criterios de valoración

- Aunque es posible valorar cada activo por separado, en ocasiones no es lo más recomendable → puede crear escenarios demasiado heterogéneos.

- Los activos esenciales sí deben ser evaluados por separado de forma restrictiva.

- Existen distintos criterios para valorar los activos:
  - Criterios comunes a todas las dimensiones.
  - Criterios para información de carácter personal.
  - Criterios para disponibilidad de servicios.

Criterios comunes a todas las dimensiones

CRITERIOS COMUNES APLICABLES A TODAS LAS DIMENSIONES DE TIPOS DE INFORMACIÓN Y SERVICIOS					
		No Aplicable (N/A)	BAJO	MEDIO	ALTO
Disposición legal o administrativa		COM.DIS.N No existe ninguna disposición legal o administrativa que condicione su nivel.	COM.DIS.B Por disposición legal o administrativa: ley, decreto, orden, resolución...	COM.DIS.M Por disposición legal o administrativa: ley, decreto, orden, resolución...	COM.DIS.A Por disposición legal o administrativa: ley, decreto, orden, resolución...
Perjuicio Directo al ciudadano (de cualquier índole)		COM.PER.N No supone ningún perjuicio directo al ciudadano.	COM.PER.B Algún perjuicio.	COM.PER.M Daño importante, aunque subsanable.	COM.PER.A Grave daño, de difícil o imposible reparación.
Incumplimiento de una Norma	Legal o administrativa	COM.LEG.N No implica incumplimiento de una norma jurídica.	COM.LEG.B Incumplimiento formal leve de una norma jurídica, de carácter subsanable.	COM.LEG.M Incumplimiento material de una norma jurídica, o incumplimiento formal no subsanable.	COM.LEG.A Incumplimiento formal y material grave de una norma jurídica.
	Regulatoria	COM.REG.N No implica incumplimiento de normativa de un regulador.	COM.REG.B Implica incumplimiento de normativa de un regulador.	COM.REG.M Implica sanción significativa de un regulador.	COM.REG.A Implica sanción grave de un regulador y/o pérdida de licencia de operar.
	Contractual	COM.CON.N No implica incumplimiento de una obligación contractual.	COM.CON.B Incumplimiento formal leve de una obligación contractual.	COM.CON.M Incumplimiento material o formal de una obligación contractual.	COM.CON.A Incumplimiento formal o material grave de una obligación contractual.
	Interna	COM.INT.N No implica incumplimiento de normativa interna.	COM.INT.B Incumplimiento formal leve de una norma interna.	COM.INT.M Incumplimiento material o formal de una norma interna.	COM.INT.A Incumplimiento formal o material grave de una norma interna.

Fuente: CCN-STIC 803

Criterios comunes a todas las dimensiones

CRITERIOS COMUNES APLICABLES A TODAS LAS DIMENSIONES DE TIPOS DE INFORMACIÓN Y SERVICIOS				
	No Adscrito (N/A)	BAJO	MEDIO	ALTO
Pérdidas económicas	COM.ECO.N No implica pérdidas económicas.	COM.ECO.B Pérdidas económicas apreciables (no superiores al 4% del presupuesto anual de la organización).	COM.ECO.M Pérdidas económicas importantes (superiores al 4% e inferiores al 10% del presupuesto anual de la organización).	COM.ECO.A Pérdidas económicas o alteraciones financieras significativas (superiores al 10% del presupuesto anual de la organización).
Reputación	COM.REP.N No implica daño reputacional.	COM.REP.B Daño reputacional moderado con los ciudadanos o con otras organizaciones.	COM.REP.M Daño reputacional significativo con los ciudadanos o con otras organizaciones.	COM.REP.A Daño reputacional grave con los ciudadanos o con otras organizaciones.
Protestas	COM.PRO.N No se prevé que pueda desembocar en protestas.	COM.PRO.B Múltiples protestas individuales.	COM.PRO.M Protestas públicas (alteración del orden público).	COM.PRO.A Protestas masivas (alteración seria del orden público).
Delitos	COM.DEL.N No facilitaría la comisión de delitos ni dificultaría su investigación.	COM.DEL.B Favorecería la comisión de delitos.	COM.DEL.M Favorecería significativamente la comisión de delitos o dificultaría su investigación.	COM.DEL.A Podría incitar a la comisión de delitos, constituiría en sí un delito, o dificultaría enormemente su investigación.

Fuente: CCN-STIC 803

Criterios para información de carácter personal

- Estos activos seguirán las directrices marcadas por el reglamento UE 2016/67 (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre.

- A modo de referencia, los derechos sobre nuestros datos personales son ARCO y POL:
  - **Acceso**.
  - **Rectificación**.
  - **Cancelación**.
  - **Oposición**.
  - **Portabilidad**.
  - **Olvido o supresión**.
  - **Limitación del tratamiento**.

Criterios para disponibilidad de servicios

- Hay dos conceptos clave a tratar cuando hablamos de disponibilidad de servicios:
  - **Periodos críticos**:
    - Los servicios no siempre son homogéneos. Es muy común que necesitemos de un servicio en unos periodos concretos.
    - El responsable del servicio debe definir los periodos donde aplicamos cada nivel de seguridad.
    - El responsable de seguridad velará para mantener los mínimos requisitos en cada periodo.

Criterios para disponibilidad de servicios

- **Resiliencia**:
  - Capacidad de un sistema para volver a funcionar tras un incidente → se establece un tiempo de recuperación objetivo (RTO).
  - Es importante encontrar un balance en el RTO. Un RTO muy alto puede mermar seriamente la disponibilidad, uno muy bajo genera mucha presión sobre la organización.

CRITERIOS PARA LA DISPONIBILIDAD DE SERVICIOS				
	No Aplicable (N/A)	BAJO	MEDIO	ALTO
RTO – Tiempo Objetivo de Recuperación	DIS.RTO.N La restauración de los niveles mínimos de servicio puede realizarse en un plazo superior a 5 días (RTO)	DIS.RTO.B La restauración de los niveles mínimos de servicio debe realizarse en un plazo máximo de 5 días (RTO)	DIS.RTO.M La restauración de los niveles mínimos de servicio debe realizarse en un plazo máximo de 1 día (RTO)	DIS.RTO.A La restauración de los niveles mínimos de servicio debe realizarse en un plazo máximo de 4 horas (RTO)

Fuente: CCN-STIC 803

Determinación de los activos

- Debemos centrarnos en determinar los activos de información y servicios de mayor relevancia.
  - Si hablamos de una entidad pública, estos están bien recogidos en la Ley 39/2015 y la Ley 40/2015.

- Para cada activo de información/servicio relevante se determina:
  - Un nombre que lo identifica.
  - Un responsable de seguridad.
  - Características relevantes (estimación de riesgos, posibles vulnerabilidades, etc).

Valoración de los activos

- La valoración de cada activo de información o servicio debe identificarla su **responsable**:
  - Es necesario que tenga conocimiento de la importancia, naturaleza y características del activo y de la normativa y consecuencias legales que pueda acarrear.
  - Con lo anterior, el responsable puede imponer requisitos para cada dimensión de seguridad de los activos.

Determinación de los niveles y categoría del sistema

- **En resumen**: por cada activo esencial relevante, ya sea de tipo información o de tipo servicio, el responsable de seguridad realiza una valoración de su nivel en cada dimensión de seguridad.

Denominación del activo esencial	tipo[10]	C[11]	I	T	A	D
Valor máximo del nivel registrado en las dimensiones de seguridad						

Fuente: CCN-STIC 803

Determinación de los niveles y categoría del sistema

- Los niveles de seguridad determinados para la información deben imputarse a todos los activos que manejen esa información.

- Los niveles de seguridad que se determinan para los servicios también se imputan a los activos que trabajen en la prestación de dicho servicio.

- Si un activo está sometido a requisitos diferentes pueden generarse **subsistemas** con valoraciones independientes.

Formulación de la categoría de un sistema

- Para cada sistema/subsistema se indica de forma explícita el nivel de cada dimensión, así como su categoría.

Categoría que se ha asignado al/los sistema(s) de << Nombre de la entidad>> es:
(Categoría): [C(Nivel), I(Nivel), T(Nivel), A(Nivel), D(Nivel)]

- Ejemplos de categorización:

CATEGORÍA BÁSICA: [C(N/A), I(B), T(B), A(B), D(B)]

CATEGORÍA MEDIA: [C(N/A), I(B), T(B), A(M), D(B)]

CATEGORÍA ALTA: [C(M), I(B), T(B), A(M), D(A)]

Ejemplo de valoración

SUBSISTEMA "APOYO A LA DOCENCIA"						
Denominación del Activo	**Tipo[8]**	**C[9]**	**I**	**D**	**A**	**T**
Cursos del sistema de docencia virtual	Información	B	B		B	B
Guías Docentes	Información	N/A	B		B	B
Repositorio	Información	N/A	B		B	B
CRUE_01_01 Docencia Virtual	Servicio			M		
CRUE_01_05 Soporte a la elaboración de contenidos docentes	Servicio			B		
CRUE_03_11 Gestión Académica. Guías Docentes	Servicio			B		
CRUE_03_54 Biblioteca Universitaria. Repositorio institucional	Servicio			B		
CRUE_04_12 Videoconferencia. Sala	Servicio			B		
CRUE_05_09 Contenidos Digitales.	Servicio			B		

SUBSISTEMA "INVESTIGACIÓN E.T..S"						
Denominación del Activo	**Tipo[8]**	**C[9]**	**I**	**D**	**A**	**T**
Categoría especial de datos: datos de salud (cáncer)	Información	M	M		M	M
Servidor del Grupo de Investigación	Servicio			B		
Valor máximo del nivel registrado en las dimensiones de seguridad		M	M	B	M	M
CATEGORÍA MEDIA [C=M, I = M, D=B, A= M, T= M]						

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Escuela Superior Ingeniería Informática

DSI
DEPARTAMENTO DE SISTEMAS INFORMÁTICOS

XUNTA DE GALICIA
CONSELLERÍA DE CULTURA, EDUCACIÓN E UNIVERSIDADE

CFR FERROL

Tema 2. Determinación del nivel de seguridad requerido por aplicaciones

- Comprobaciones de seguridad a nivel de aplicación: ASVS

UNIÓN EUROPEA
Fondo Social Europeo
EL FSE invierte en tu futuro

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL

Objetivos y motivación de ASVS

- El **Application Security Verification Standard (ASVS)** es un estándar que tiene como objetivo ayudar en el diseño, desarrollo y testeo de las aplicaciones web desde el punto de vista de la seguridad.
  - Estándar internacional que depende del proyecto OWASP.
  - ASVS 4.0.2

- Tiene dos objetivos principales:
  - Ayudar a las organizaciones a desarrollar y mantener aplicaciones seguras.
  - Permitir a los proveedores de herramientas de seguridad alinear sus productos con las necesidades de los usuarios.

Niveles de verificación de seguridad de ASVS

- ASVS define tres niveles de seguridad diferentes en base a las características de la aplicación:
  - **ASVS nivel 1**: dirigido a todo tipo de software (que requieren bajos niveles de seguridad).
  - **ASVS nivel 2**: para aplicaciones que manejan datos sensibles.
  - **ASVS nivel 3**: aplicaciones críticas o con datos muy sensibles (p.e. datos médicos, transacciones de alto valor).

- Estos niveles no son excluyentes. Es decir, una aplicación de nivel 3 pasa también por los niveles 1 y 2.

- Cada nivel ASVS cuenta con su lista de requisitos de seguridad.

Cómo aplicar ASVS

- La mejor forma de aplicar el estándar es emplear un checklist personalizado para nuestro sistema/aplicación. Como ocurría con el ENS, no es un dogma y debe ser adaptado a nuestras necesidades.

- Algunas organizaciones tienen activos de información únicos y valiosos y deben cumplir regulaciones específicas de dichas industrias.

- Independientemente de la naturaleza de nuestra aplicación, el estándar recomienda validar siempre los requisitos del nivel 1.

Cómo aplicar ASVS

V5.4 Memory, String, and Unmanaged Code Requirements

The following requirements will only apply when the application uses a systems language or unmanaged code.

#	Description	L1	L2	L3	CWE
5.4.1	Verify that the application uses memory-safe string, safer memory copy and pointer arithmetic to detect or prevent stack, buffer, or heap overflows.		✓	✓	120
5.4.2	Verify that format strings do not take potentially hostile input, and are constant.		✓	✓	134
5.4.3	Verify that sign, range, and input validation techniques are used to prevent integer overflows.		✓	✓	190

Fuente: ASVS 4.0.2

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Escuela Superior Ingeniería Informática

DSI
DEPARTAMENTO DE SISTEMAS INFORMÁTICOS

XUNTA DE GALICIA
CONSELLERÍA DE CULTURA, EDUCACIÓN E UNIVERSIDADE

CFR FERROL

Puesta en producción segura

- Tema 2. Determinación del nivel de seguridad requerido por aplicaciones

UNIÓN EUROPEA
Fondo Social Europeo
EL FSE invierte en tu futuro

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL