TEMA 4
POLÍTICAS DE SEGURIDAD Y HARDENING AUTOMATIZADO

Defensa contra las artes oscuras

José Manuel Redondo López Proyecto *"S-81 Isaac Peral"* v4.0

Fuente: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

Logo: @creative_vanesa (*Instagram*)

ÍNDICE

¿QUÉ ES ESTE TEMA?

- **Al final del tema anterior esbozamos dos elementos clave para lograr una seguridad adecuada con menos esfuerzo**
  - **Listas de controles de seguridad** validados, debidamente documentados y mantenidos
    - Para cualquier producto de software / SO del que necesitemos mejorar la seguridad
  - Una forma de **automatizar su verificación** y/o implementar la solución a las vulnerabilidades que resuelven
- **En este tema se describirán algunas fuentes de estas listas y las tecnologías de automatización de seguridad**
  - Relacionándolos con elementos de un nivel de abstracción mucho más alto
    - Como políticas de seguridad, frameworks y Sistemas de Gestión de Seguridad de la Información (SGSI)
  - Empezaremos con la parte técnica de bajo nivel
    - Y mostraremos el camino hacia técnicas de gestión de seguridad mucho más abstractas

< Ir al índice

ENS >

SCAP >

AUTOMATIZACIÓN DEL HARDENING DE SEGURIDAD

El hardening no tiene por qué ser “hard”

Fuente: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

*Iconos por Bing Chat AI

¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

- **En este bloque aprenderás**
  - Qué es el concepto de **Compliance as Code**
  - Lo que es y lo que incluye el **Esquema Nacional de Seguridad**
  - Qué es y para qué sirve el **protocolo SCAP**, y su importancia a la hora de automatizarla

Compliance as code (Cumplimiento como Código)

- **Herramientas y prácticas que permiten integrar las tres actividades centrales de cumplimiento: Prevenir (Prevent), Detectar (Detect), Corregir (Remediate)**
  - **Prevenir** el incumplimiento asegurando automáticamente que los cambios planeados son conformes
  - **Detectar** el incumplimiento con escaneos automatizados, notificándolo si se identifican problemas
  - **Corregir** el incumplimiento realizando cambios inmediatos en las infraestructuras y garantizar el máximo nivel de cumplimiento en toda ella
- **Por lo tanto, es la codificación de nuestros controles de seguridad**
  - Por lo tanto, su cumplimiento, aplicación y remediación **pueden automatizarse**
  - Esto se aplica a ciberseguridad (**los controles de cumplimiento son los controles de seguridad**)
  - En este tema vamos a revisar distintas formas de lograr esto
  - Y cómo se puede utilizar esto para facilitar la implementación de frameworks de seguridad
- **Esta codificación se hace en lenguajes de programación especiales (Domain-Specific Languages, DSL (TPP, DLP))**
  - ¡Somos ingenieros de software! ¡Los lenguajes de programación son el pan nuestro de cada día!

De controles de seguridad a metodologías

Seguridad de Sistemas Informáticos

5 — Usar una **Metodología de Auditoría de Seguridad** (como **OSSTMM**) para revisar la seguridad de los sistemas y el cumplimiento de **frameworks** de seguridad implementados

Gestionado por

4 — Asignar los controles y **Safeguards** implementados a un **Framework de Seguridad** internacional reconocido (**ISO 27001**, **PCI-DSS**…) para facilitar la implementación de un **SGSI**

Mapea a

3 — Usar **Implementation Groups** (solo 3) para implementar solo los **Safeguards** más adecuados a un escenario particular según los recursos disponibles

Se pueden distribuir en

2 — Agrupar los controles de seguridad implementados en CIS **Critical Security Controls** (CSC) y **Safeguards**

Se pueden agrupar en

1 — Verificar e implementar **Controles técnicos de seguridad** adecuados y validados en un producto de software / SO de forma altamente **automatizada** (varios cientos de controles)

Nivel de Abstracción

+

-

Fuente: Bing Chat AI

Esquema Nacional de Seguridad (ENS) Español

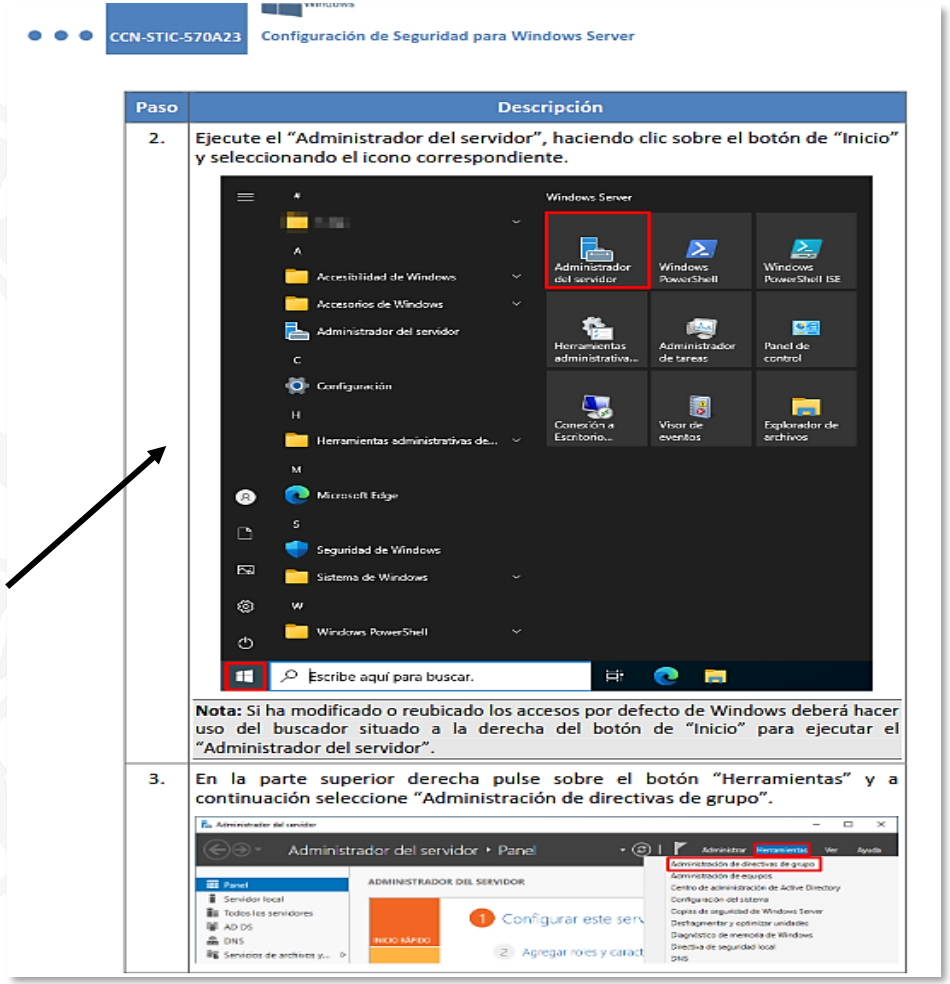
Ley 11/2007 (22 Junio): Acceso electrónico de los ciudadanos a los servicios públicos. Controles de seguridad de nuestro país

*Iconos por Bing Chat AI

Esquema Nacional de Seguridad Español

- **Establece principios y requisitos de una política de seguridad para usar medios electrónicos**
  - **Contenidos**: https://www.ccn-cert.cni.es/publico/ens/ens/index.html
  - **Marco normativo**: https://ens.ccn.cni.es/es/ens-marco-normativo/ens-marco-normativo-es
- **Para configurar correctamente el SO/software**
  - El CCN-STIC publica **guías de seguridad gratuitas** de muchos productos con listas de controles de seguridad
    - Y explicaciones detalladas paso a paso de cada uno
    - Si quieres un **manual minucioso con capturas**, pocos mejores podrás encontrar por ahí...
  - Están organizadas en series en: https://www.ccn-cert.cni.es/es/guias.html
    - Windows (serie **500**), Otros sistemas operativos (serie **600**), Software (serie **800**)...
  - **Actualizado recientemente**: https://www.linkedin.com/pulse/esquema-nacional-de-seguridad-ens-un-a%C3%B1o-despu%C3%A9s-su-actualizaci%C3%B3n/?originalSubdomain=es

Estas guías se crean para la administración pública, pero las empresas privadas las pueden usar también



Fuente: https://www.ccn-cert.cni.es/es/guias-de-acceso-publico-ccn-stic/7104-ccn-stic-570a23-perfilado-de-seguridad-para-windows-server-controlador-de-dominio-o-servidor-miembro/file.html

Esquema Nacional de Seguridad Español

- **El ENS define perfiles de aplicación para los controles de seguridad**
  - Pero son distintos para cada tipo de SO/software
  - No hay por tanto la homogeneidad* que se puede encontrar en otras soluciones (Ej.: Controles CSC)
- **Para Windows se definen tres perfiles**
  - Basándose en la calificación de la información manejada por los sistemas de información
  - **ESTÁNDAR**, **USO OFICIAL** y **MATERIAS CLASIFICADAS**
- **Estos tres perfiles englobarán configuraciones en función de la categoría de los sistemas de información**
  - Que se definen bajo el Real Decreto del ENS
  - **BÁSICA**, **MEDIA**, **ALTA** y **SISTEMAS CLASIFICADOS**

***Los sistemas Red Hat por ejemplo usan una clasificación muy diferente a esta...**

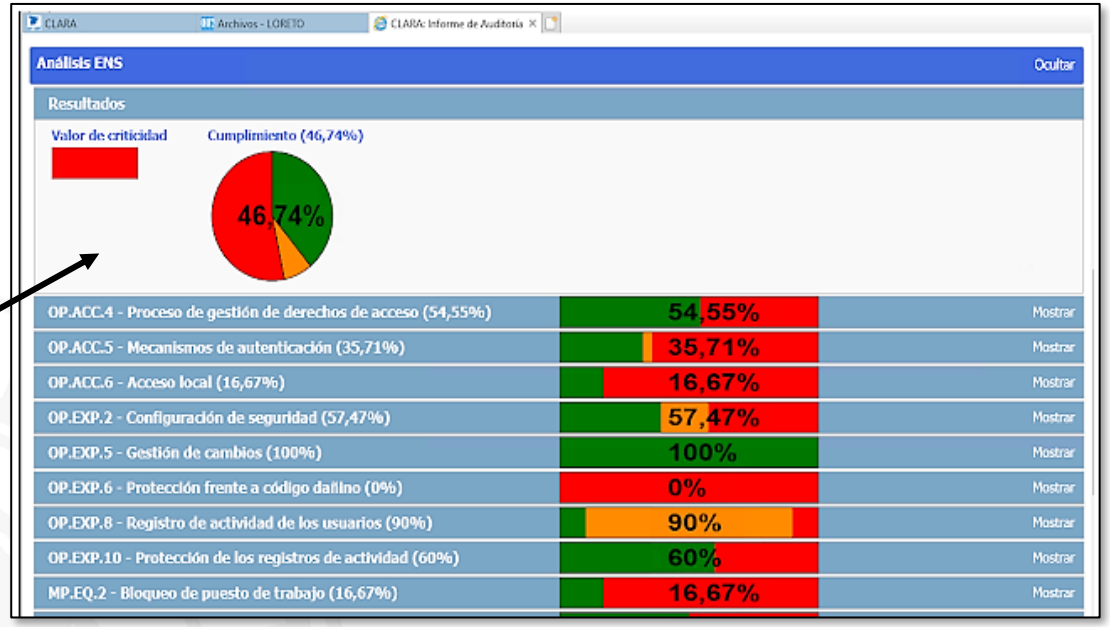
		CALIFICACIÓN DE LA INFORMACIÓN/PERFIL		
		ESTÁNDAR	USO OFICIAL	MATERIAS CLASIFICADAS
CATEGORÍA DEL SISTEMA DE INFORMACIÓN	BÁSICA	✓	✗	✗
	MEDIA	✓	✓	✗
	ALTA DIFUSIÓN LIMITADA	✗	✓	✗
	CONFIDENCIAL RESERVADO	✗	✗	✓

Perfiles aplicables según la categoría del sistema de información a los que se van a aplicar. Date cuenta por ejemplo que un perfil USO OFICIAL se puede aplicar a sistemas clasificados como MEDIA o ALTA

Esquema Nacional de Seguridad Español

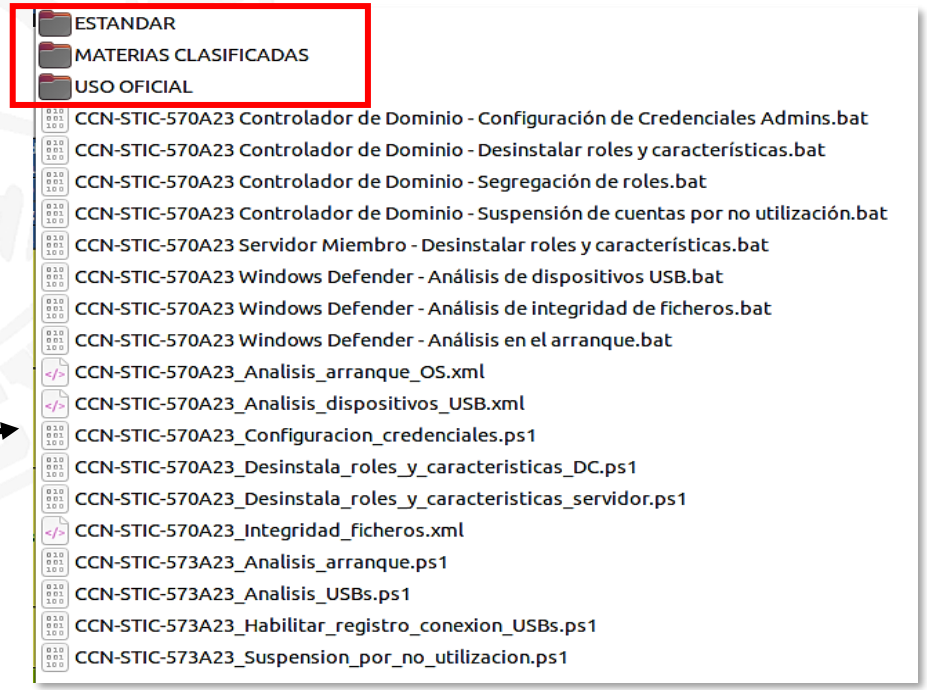
Seguridad de Sistemas Informáticos

- **CCN-CERT ofrece software de seguridad para sus socios o gratis**
  - https://www.ccn-cert.cni.es/soluciones-seguridad.html
  - Una es CLARA, herramienta gratuita y automatizada de verificación de cumplimiento ENS (Windows/CentOS)
  - **Tutorial**: http://kinomakino.blogspot.com/2020/08/si-quieres-auditar-tu-windows-y-no-lo.html



- **Pero el ENS no facilita compliance as code**
  - No están estructurados como otras soluciones
    - Problema - descripción - comprobación – remediación
    - Están pensados para **requerir una intervención manual**
  - Las medidas de corrección automatizadas son scripts
    - Ficheros `.sh`, `.bat`, `.ps1`...
    - **No siguen estándares internacionales de automatización** de seguridad (SCAP)
    - Se ejecutan durante algunos de los pasos de los diferentes controles de la guía paso a paso relacionada

Scripts adecuados para los perfiles de la transparencia anterior



Security Content Automation Protocol (SCAP)

Protocolo estándar de automatización para operaciones de hardening que facilita el Compliance as Code

*Iconos por Bing Chat AI

Fuente: Bing Chat AI

SECURITY CONTENT AUTOMATION PROTOCOL (SCAP)

- **Estándar del NIST para el hardening automatizado en sistemas de software**
  - Las herramientas compatibles con SCAP cargan archivos creados en dos formatos de lenguaje de marcas basados en XML (**OVAL** y **XCCDF**)
  - Estos archivos se usan para automatizar
    - La **evaluación** de controles de seguridad (ver si cada control ya está aplicado)
    - Y también, su **remediación** (aplicar el control de seguridad para resolver las vulnerabilidades asociadas)
  - A diferencia del ENS, **todas las operaciones están especificadas en archivos XML procesables**
    - A diferencia de en una guía PDF y scripts sueltos vinculados a la misma
- **El proyecto OpenSCAP es su implementación más popular**
  - Conjunto de herramientas open source que cumplen con SCAP 1.2: https://www.open-scap.org/
    - https://static.open-scap.org/openscap-1.3/oscap_user_manual.html
  - Estas herramientas permiten
    - Configuración, comprobación de vulnerabilidades y parches automatizada
    - Actividades de cumplimiento de controles técnicos de seguridad
    - Medición del nivel de seguridad actual
  - A diferencia del ENS, es posible crear herramientas que lean y usen esos XML (**estándar abierto**)

LENGUAJES DE HARDENING AUTOMATIZADO

Seguridad de Sistemas Informáticos

Fuente:
https://www.ipa.go.jp/security/english/vuln/OVAL_en.html

Open Vulnerability Assessment Language (OVAL)

- https://oval.mitre.org/language/
- Vocabulario XML creado por MITRE (https://www.mitre.org/)
- Permite **representar la información** de los diferentes elementos que forman la configuración de un sistema
  - También permite analizar y evaluar estos elementos
  - Para detectar si una máquina está en un estado determinado (vulnerabilidad, configuración, nivel de parches...)
- Permite crear un **informe** con los resultados de la evaluación

```
<?xml version="1.0" encoding="UTF-8" ?>
 <oval_definitions>
  <definitions>
   <definition id="oval:jp.jvn.jvndb.oval:def:20091130"
   class="vulnerability" version="1">
    <metadata>
     <title>MyJVN バージョンチェッカの セキュリティチェック</title>
    </metadata>
    <criteria operator="AND">
     <criterion comment="MyJVN バージョンチェッカが最新かどうかのテスト項目"
     test_ref="oval:jp.jvn.jvndb.oval:tst:20091130" />
    </criteria>
   </definition>
  </definitions>
```

Tests element

```
  <tests>
   <registry_test id="oval:jp.jvn.jvndb.oval:tst:20091130"
   version="1" comment="レジストリCurrentVersion値が1.0であれば最新である"
   check_existence="at_least_one_exists" check="at least one"
   xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
    <object object_ref="oval:jp.jvn.jvndb.oval:obj:1111" />
    <state state_ref="oval:jp.jvn.jvndb.oval:ste:2222" />
   </registry_test>
  </tests>
```

Objects element

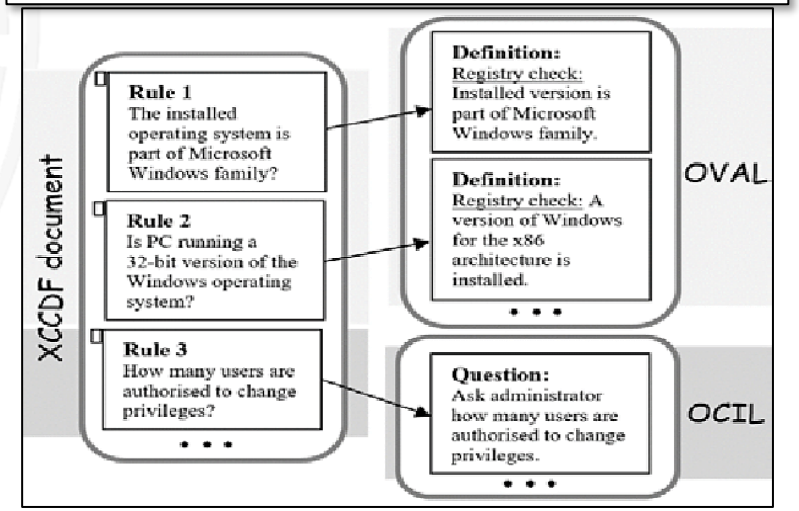
```
  <objects>
   <registry_object id="oval:jp.jvn.jvndb.oval:obj:1111"
   version="1" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
    <hive>HKEY_LOCAL_MACHINE</hive>
    <key>SOFTWARE¥IPA¥MyJVN</key>
    <name>CurrentVersion<name />
   </registry_object>
  </objects>
```

States element

```
  <states>
   <registry_state id="oval:jp.jvn.jvndb.oval:ste:2222"
   version="1" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
    <value>1.0</value>
   </registry_state>
  </states>
 </oval_definitions>
```

Extensible Configuration Checklist Description Format (XCCDF)

- https://csrc.nist.gov/projects/security-content-automation-protocolo/specifications/xccdf
- Otra especificación de lenguaje basada en XML del NIST
- Permite escribir **listas de controles de seguridad**, benchmarks de seguridad y otros documentos relacionados



Fuente:
https://www.researchgate.net/figure/XCCDF-sample-use-case-scenario_fig3_311447068

Lenguajes de hardening automatizado

Seguridad de Sistemas Informáticos

Source Data Stream

- https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/sect-scap_format-data_stream
- Formato de archivo compatible con SCAP 1.2+
- **Incluye** archivos XCCDF, OVAL y otros componentes
  - Para definir una directiva de cumplimiento con listas de comprobación hechas en XCCDF
- También está basado en XML, y contiene un **índice**, **un catálogo** y una **tabla de contenido**
  - Permiten dividirlo en archivos, según el tipo de componente SCAP (puede haber varios del mismo tipo)
  - Pueden cubrir así todas las políticas de seguridad de una organización
- Es el formato recomendado, si está disponible, ya que debe ser más completo que los otros dos
- Tiene su herramienta de edición, SCAP Composer
  - https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8290.pdf

```
<ds:data-stream-collection xmlns:ds="http://scap.nist.gov/schema/scap/source/1.2"
    xmlns:xlink="http://www.w3.org/1999/xlink"
    xmlns:cat="urn:oasis:names:tc:entity:xmlns:xml:catalog"
    id="scap_org.open-scap_collection_from_xccdf_ssg-rhel6-xccdf-1.2.xml"
    schematron-version="1.0">
  <ds:data-stream id="scap_org.open-scap_datastream_from_xccdf_ssg-rhel6-xccdf-1.2.xml"
      scap-version="1.2" use-case="OTHER">
  <ds:dictionaries>
    <ds:component-ref id="scap_org.open-scap_cref_output--ssg-rhel6-cpe-dictionary.xml"
        xlink:href="#scap_org.open-scap_comp_output--ssg-rhel6-cpe-dictionary.xml">
      <cat:catalog>
        <cat:uri name="ssg-rhel6-cpe-oval.xml"
            uri="#scap_org.open-scap_cref_output--ssg-rhel6-cpe-oval.xml"/>
      </cat:catalog>
    </ds:component-ref>
  </ds:dictionaries>
  <ds:checklists>
    <ds:component-ref id="scap_org.open-scap_cref_ssg-rhel6-xccdf-1.2.xml"
        xlink:href="#scap_org.open-scap_comp_ssg-rhel6-xccdf-1.2.xml">
      <cat:catalog>
        <cat:uri name="ssg-rhel6-oval.xml"
            uri="#scap_org.open-scap_cref_ssg-rhel6-oval.xml"/>
      </cat:catalog>
    </ds:component-ref>
  </ds:checklists>
  <ds:checks>
    <ds:component-ref id="scap_org.open-scap_cref_ssg-rhel6-oval.xml"
        xlink:href="#scap_org.open-scap_comp_ssg-rhel6-oval.xml"/>
    <ds:component-ref id="scap_org.open-scap_cref_output--ssg-rhel6-cpe-oval.xml"
        xlink:href="#scap_org.open-scap_comp_output--ssg-rhel6-cpe-oval.xml"/>
    <ds:component-ref id="scap_org.open-scap_cref_output--ssg-rhel6-oval.xml"
        xlink:href="#scap_org.open-scap_comp_output--ssg-rhel6-oval.xml"/>
  </ds:checks>
</ds:data-stream>
<ds:component id="scap_org.open-scap_comp_ssg-rhel6-oval.xml"
    timestamp="2014-03-14T16:21:59">
  <oval_definitions xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5"
      xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5"
      xmlns:ind="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent"
      xmlns:unix="http://oval.mitre.org/XMLSchema/oval-definitions-5#unix"
      xmlns:linux="http://oval.mitre.org/XMLSchema/oval-definitions-5#linux"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="http://oval.mitre.org/XMLSchema/oval-common-5
      oval-common-schema.xsd
          http://oval.mitre.org/XMLSchema/oval-definitions-5
      oval-definitions-schema.xsd
          http://oval.mitre.org/XMLSchema/oval-definitions-5#independent
      independent-definitions-schema.xsd
          http://oval.mitre.org/XMLSchema/oval-definitions-5#unix
      unix-definitions-schema.xsd
          http://oval.mitre.org/XMLSchema/oval-definitions-5#linux
      linux-definitions-schema.xsd">
```

Security Content Automation Protocol (SCAP)

- Por tanto, este protocolo y sus lenguajes XML son un estándar mundial para
  - **Comprobar las configuraciones** de software, **administrar vulnerabilidades** y **evaluar** si un sistema cumple con una política de seguridad particular, todo con un **alto grado de automatización**
- Usando procedimientos documentados y validados para minimizar los errores
  - **Evaluación automática de la aplicación de controles de seguridad** (*¿esto ya está hecho?*)
  - **Remediación automática de los controles de seguridad** (si la respuesta es no, arréglalo)
  - **Generar un informe con los resultados de la evaluación/corrección** (normalmente, HTML)
- **OpenSCAP** es una herramienta que lo hace, ¡pero puede haber muchas más!
- Más información
  - **Políticas de seguridad SCAP**: https://www.open-scap.org/security-policies/
  - **Manual de usuario de OpenSCAP**: https://static.open-scap.org/openscap-1.2/oscap_user_manual.html
  - **Documentación, manuales y guías de seguridad para varios SO:** https://static.open-scap.org/
- *¿Entiendes ahora la diferencia con la propuesta del ENS?*

Estado actual de la automatización de seguridad

- **Por lo tanto, SCAP, OVAL y XCCDF son un esfuerzo muy importante y en desarrollo para tratar de estandarizar y automatizar procesos de seguridad**
- **Existen archivos escritos en estos lenguajes que nos permiten comprobar o remediar los controles de seguridad sobre una gran cantidad de software/SO**
  - La siguiente sección revisará algunos lugares de los que obtener estos archivos
- **Estos archivos suelen incluir diferentes perfiles de uso o políticas de seguridad**
  - Un fichero puede contener distintas listas de controles de seguridad para comprobar o remediar
  - Dependiendo de cómo vayamos a utilizar el software (Ej.: servidor, estación de trabajo...)
  - La definición de lo que es un perfil de uso / política de seguridad depende de la fuente de los archivos
- **El problema es encontrar listas gratuitas de controles de seguridad completas, validadas y compatibles con SCAP para todo nuestro software y SO**
  - **Este problema no lo tiene el ENS**: Todo lo que ofrece está centralizado en su web

¿CREES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

?

- **Eres capaz de hacer lo siguiente**
  - *Entender que la seguridad de un software puede gestionarse con código*
  - *Comprender que dicho código puede detectar y corregir problemas de configuración que puedan causar vulnerabilidades en dicho software*
    - *Y que gracias a él se pueden automatizar esas tareas para que un sistema cumpla con un estándar de seguridad*
  - ***Respecto al ENS***
    - *Entender que son una serie de principios y requisitos de seguridad de nuestro país*
    - *Tienes claro lo que incluyen sus guías de seguridad y para qué puedes usarlas*
    - *Comprendes que no todas las máquinas de una infraestructura son tratadas con la misma importancia y hay tres perfiles de uso y cuatro categorías de configuración*
    - *Tienes claro para que puedes usar la herramienta del ENS CLARA*
  - ***Respecto a SCAP***
    - *Entiendes que está basado en tres vocabularios de XML: OVAL, XCCDF y Source Data Stream*
    - *Comprendes que, gracias al protocolo SCAP, puedes evaluar sistemas, detectar que controles de seguridad faltan por implementar y remediarlos*
      - *Así como generar un informe de cómo está el sistema en cuanto a implementación de controles*
    - *Tienes claro que, sin una lista de controles de seguridad adecuada, el protocolo SCAP por sí solo no sirve para mejorar la seguridad*

< Ir al índice

Fuentes de controles de seguridad validados

Algunos sitios de dónde obtener guías técnicas adecuadas (listas de controles de seguridad) para nuestros productos

*Iconos por Bing Chat AI

Fuente: Bing Chat AI

SCAP Sec. Guide >

STIGs >

CIS Benchmarks >

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

En la primera sección de este bloque aprenderás

- Lo que incluye el paquete **scap-security-guide** y sus perfiles de seguridad
- Las distintas formas de **usar los ficheros** que incluye
- Cómo son los **informes de seguridad** que se obtienen al usar el protocolo SCAP

En el siguiente, aprenderás

- De donde salen los estándares **STIG** y su carácter militar
- Los **criterios** que se usan para subdividir los controles de seguridad STIG
- De donde puedes **descargar STIG gratis** y cómo navegar por ellos
- Las distintas partes de la definición de un **control de seguridad** de un STIG y su significado

Y finalmente, en la última sección del bloque aprenderás

- Que son los **controles de seguridad del CIS** y quién los avala
- Que todas las instrucciones de implementación y su justificación están disponibles **gratuitamente en PDF**
- La **estructura general** de todo control CIS
- Como conseguir **compliance CIS gratuito** y automático con herramientas oficiales y de 3ºs

Fuente: Bing Chat AI

El paquete SCAP Security Guide (scap-security-guide)

Una forma sencilla de encontrar controles de seguridad gratuitos y fiables

*Iconos por Bing Chat AI

El paquete scap-security-guide

https://www.open-scap.org/security-policies/scap-security-guide/

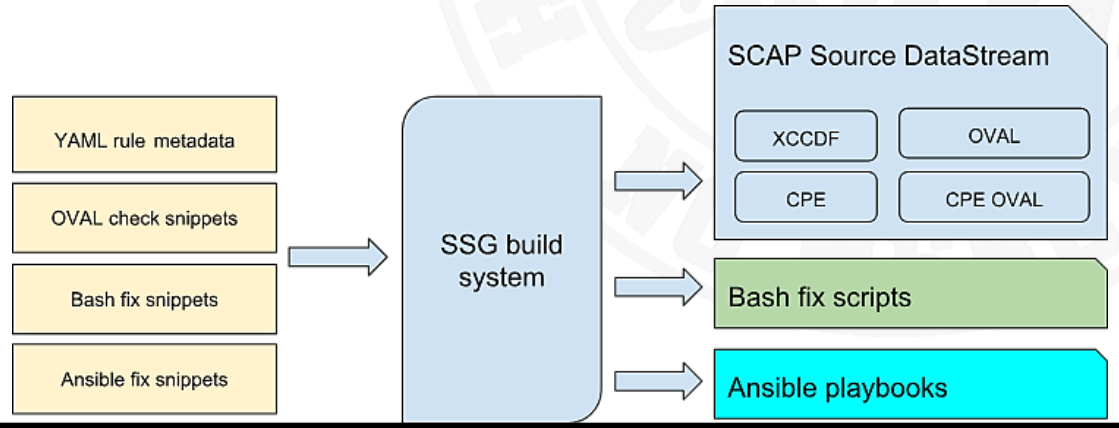
- **OpenSCAP debe usar archivos SCAP también libres y abiertos necesarios para proteger sistemas software**
- **Este paquete cubre este requisito y contiene**
  - La herramienta `oscap` (la implementación de OpenSCAP)
  - **Un conjunto de políticas de seguridad SCAP prediseñadas**
    - Con controles de seguridad aplicables sobre productos software o SO (Red Hat, Fedora, Ubuntu,...)
    - Con ellos podemos alcanzar con poco esfuerzo niveles de seguridad más altos que instalaciones predeterminadas
    - No todos los controles de seguridad que contienen se pueden corregir con OpenSCAP (todavía)
    - La capacidad de corrección automática mejora a medida que continúa su desarrollo (¡actualiza el paquete frecuentemente!)
    - Sus archivos SCAP se crean utilizando partes de otras recomendaciones de seguridad que revisaremos (CIS, STIG...)

SCAP Workbench es un GUI para `openscap`, por si no quieres usar línea de comandos:
https://static.open-scap.org/scap-workbench-1.1/

➢ Ejercicio **L6B1_OSCAPUPD**

El paquete scap-security-guide: Remediación

- **Mantener actualizado este paquete mejora y amplia sus controles de seguridad**
  - https://github.com/ComplianceAsCode/content
- **Hay tres formas de remediación (corrección) automática**
  - **Usar los ficheros SCAP** con la herramienta OpenSCAP
  - Playbooks de Ansible (https://www.ansible.com/, conjuntos de directorios y archivos `.yml`)
    - Ansible es una herramienta de configuración automática de infraestructuras Windows y/o Linux
    - Si tenemos acceso vía SSH a máquinas, se puede usar para **hacer hardening a todas al mismo tiempo**
  - Scripts bash destinados a ejecutarse en máquinas para ponerlas en conformidad con la política
    - No necesitan instalar nada (ni OpenSCAP, ni Ansible...) son scripts Linux a ejecutar
  - Así tienes opciones para cualquier máquina a la que quieras mejorar la seguridad



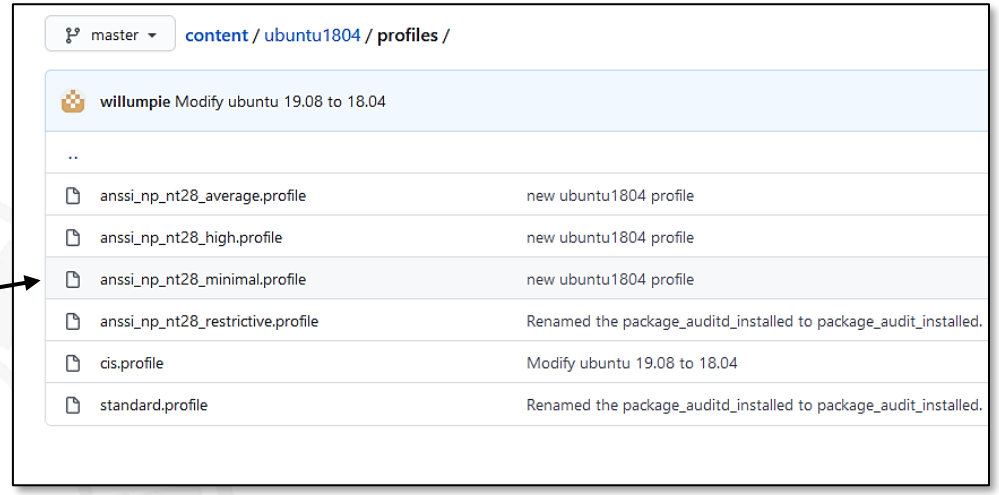
Hay tres formas de hacer la remediación, y tú eliges cual te conviene más. Algunas remedian más controles que otras, aunque parten de una misma base. Los scripts de bash se pueden copiar a cualquier máquina para ejecutarlos. Mucho cuidado con la remediación automática: Podría romper algún servicio legítimo

➢ Ejercicios **L6B2_OSCAPREMWB, L6B2_OSCAPREMBASH, L6B2_OSCAPREMANS**

El paquete scap-security-guide: Perfiles de seguridad

Seguridad de Sistemas Informáticos

- **La imagen muestra los perfiles de seguridad SCAP del paquete para el SO Ubuntu 18.04**
  - Un perfil de seguridad standard, que representa una seguridad mínima base que cada Ubuntu debe cumplir
  - Cuatro perfiles de la normativa de seguridad francesa ANSSI DAT-NT28
  - Un perfil basado en las listas de controles de seguridad de los CIS Benchmarks (vistas luego)
- **La 2ª imagen muestra la ejecución del contenido bash asociado al perfil** `standard`
  - Cada perfil tiene su script de Ansible y de bash asociado
  - **Recuerda**: Los perfiles se usan con `openscap`, pero si no lo tienes o puedes instalar, ¡hay otras opciones!



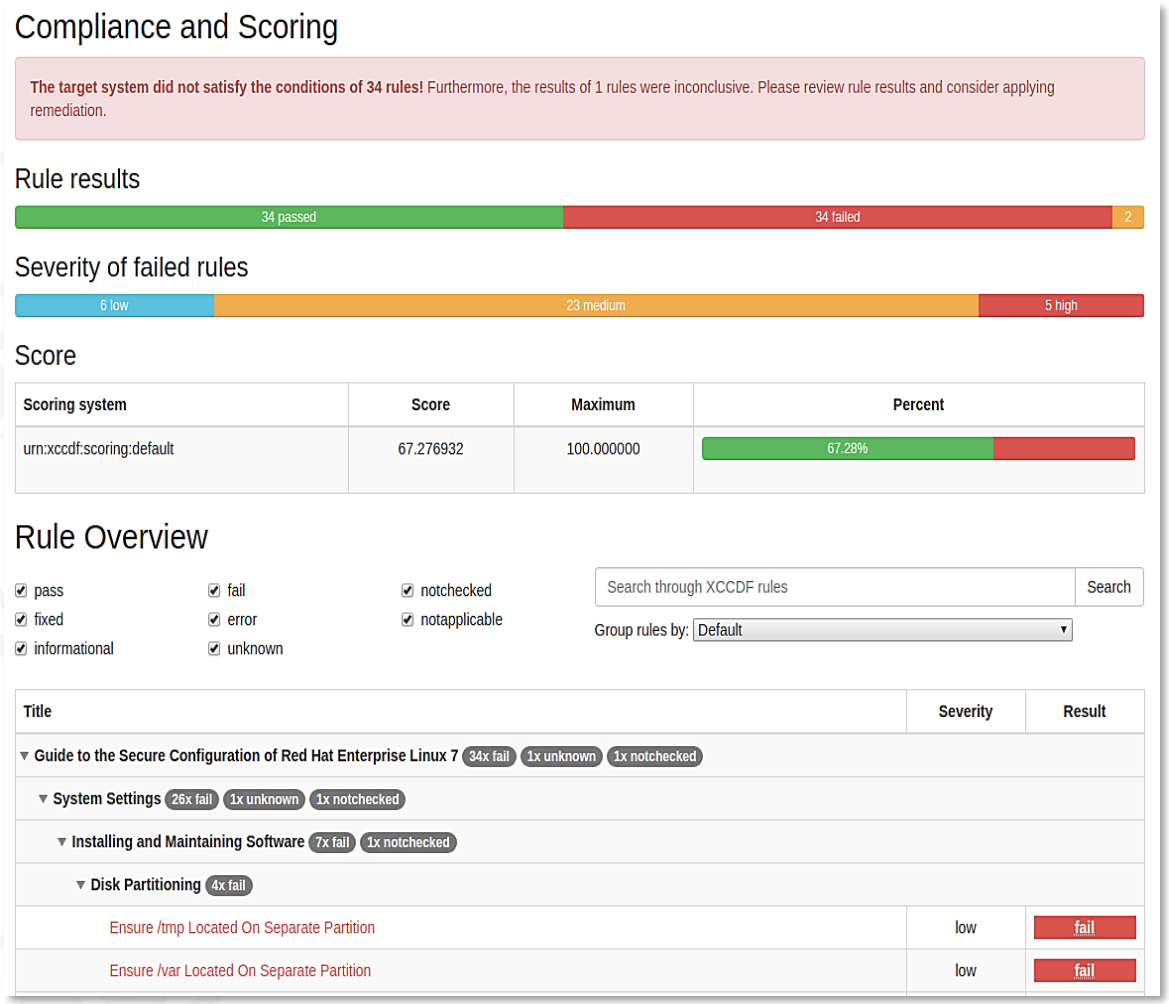
Ficheros compatibles con SCAP (perfiles)

```
operario@server1804:/etc/oscap/content/bash$ sudo bash ubuntu1804-script-standard.sh
Remediating rule 22/45: 'package_rsyslog_installed'
FIX FOR THIS RULE 'package_rsyslog_installed' IS MISSING!
Remediating rule 23/45: 'service_rsyslog_enabled'
FIX FOR THIS RULE 'service_rsyslog_enabled' IS MISSING!
Remediating rule 24/45: 'file_groupowner_etc_group'
Remediating rule 25/45: 'file_groupowner_etc_gshadow'
Remediating rule 26/45: 'file_groupowner_etc_passwd'
Remediating rule 27/45: 'file_groupowner_etc_shadow'
Remediating rule 28/45: 'file_owner_etc_group'
Remediating rule 29/45: 'file_owner_etc_gshadow'
Remediating rule 30/45: 'file_owner_etc_passwd'
Remediating rule 31/45: 'file_owner_etc_shadow'
Remediating rule 32/45: 'file_permissions_etc_group'
Remediating rule 33/45: 'file_permissions_etc_gshadow'
Remediating rule 34/45: 'file_permissions_etc_passwd'
Remediating rule 35/45: 'file_permissions_etc_shadow'
Remediating rule 36/45: 'file_permissions_systemmap'
FIX FOR THIS RULE 'file_permissions_systemmap' IS MISSING!
```

➢ Ejercicios **L6B1_OSCAPAUDITSW, L6B1_OSCAPAUDITSO, L6B1_OSCAPCMD**

El paquete scap-security-guide: Informes de seguridad

- `oscap` **se puede ejecutar con el parámetro** `eval` **para crear un informe HTML**
  - Este es el modo de **solo evaluación**
  - Se puede ejecutar con `--remediate` para intentar **corregir** los controles aún no implementados
- **El informe HTML de un sistema analizado contiene**
  - **El nº de controles de seguridad** que el sistema ya implementa, las que no y las que no es posible saberlo
    - Unos pocos requieren comprobación manual
  - De los que no, detalla su **criticidad**
    - Muestra la importancia de sus carencias de seguridad
  - Da un % de compliance (**puntuación de seguridad**)
  - Y finalmente un **listado detallado** de cada control
    - Cuyas entradas podemos abrir para conocer los detalles



Compliance and Scoring

The target system did not satisfy the conditions of 34 rules! Furthermore, the results of 1 rules were inconclusive. Please review rule results and consider applying remediation.

Rule results

34 passed | 34 failed | 2

Severity of failed rules

6 low | 23 medium | 5 high

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	67.276932	100.000000	67.28%

Rule Overview

pass, fail, notchecked, fixed, error, notapplicable, informational, unknown

Search through XCCDF rules — Search

Group rules by: Default

Title	Severity	Result
Guide to the Secure Configuration of Red Hat Enterprise Linux 7 (34x fail, 1x unknown, 1x notchecked)		
System Settings (26x fail, 1x unknown, 1x notchecked)		
Installing and Maintaining Software (7x fail, 1x notchecked)		
Disk Partitioning (4x fail)		
Ensure /tmp Located On Separate Partition	low	fail
Ensure /var Located On Separate Partition	low	fail

Es muy interesante crear un informe antes de la remediación y otro después de hacerla, para comparar puntuaciones y lo que se ha podido automatizar con estas herramientas

➢ Ejercicio **L6B1_OSCAPREPORT**

Ventajas / desventajas

Ventajas

- Disponible de forma **gratuita**
- **Aumenta sustancialmente el nivel de seguridad** base de un software compatible recién instalado con poco esfuerzo, facilitando Compliance as Code
- **Mantenimiento y mejoras** frecuentes, siendo fácilmente **actualizable**
- *¿Tienes ficheros compatible con SCAP 1.2 de otros sitios?* Puedes validarlos / hacer la remediación que contienen con OpenSCAP
  - Algunos solo tienen validación y otros están pensados para que se procese todo manualmente
  - Son listas de tareas a realizar para cumplir con el perfil dado
  - ¡A lo mejor puedes **usar las guías paso a paso del ENS** para hacer esas tareas manuales!

Desventajas

- **Incompleto** para algunos productos, o la remediación no está disponible para algunos controles
- **Admite muchos menos productos software** que otras opciones (básicamente, solo SO tipo Linux)
- **No están tan validados** como las otras fuentes de controles de seguridad, ya que no están respaldados por gobiernos / empresas privadas

¿CREES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

?

- **Eres capaz de hacer lo siguiente**
  - *Entender que el paquete **scap-security-guide** es básicamente una fuente de listas de controles de seguridad abierta y gratuita para determinados SO*
  - *Saber que, como parte de ese paquete, se incluye un GUI sencillo para aplicarlos, **oscap**, que es una alternativa a usarlos en línea de comando*
  - *Entender que no todos los controles de seguridad incluidos tienen implementada la remediación con OSCAP*
    - *Pero que dicha remediación puede estar implementada igualmente en los ficheros **Ansible** y/o **bash** que también se incluyen dentro del paquete*
  - *Entender que cada fichero SCAP distribuido puede tener distintos perfiles de seguridad aplicables al producto sobre el que trabaja*
    - *Y que estos perfiles cambian según el producto*
  - *Tener clara la estructura de un informe SCAP generado sobre un software evaluado, donde está su índice global de seguridad y los controles que pasa y no pasa*

Security Technical Implementation Guides (STIGs)

Listas de controles de seguridad para “mazar” a tu software ☺

*Iconos por Bing Chat AI

Fuente: Bing Chat AI

National Institute of Standards and Technology (NIST)

https://www.nist.gov/

- **Agencia del Departamento de Comercio de los Estados Unidos**
  - Archivo de STIGs gratuitos y públicos: 560+ benchmarks de seguridad de muchos productos
    - Los **benchmarks** son básicamente **listas de controles de seguridad**
    - Muchos de ellos también son compatibles con **SCAP**: https://public.cyber.mil/stigs/scap/
    - Cada **benchmark** es una guía detallada sobre cómo configurar correctamente un SO, aplicación, **software**...
  - Son gratuitos porque las empresas civiles que obtienen contratos públicos con el gobierno de los EEUU pueden estar obligadas a proporcionar sistemas **software** que cumplan con ciertas STIG
- **STIG es uno de los estándares de configuración utilizados por el Departamento de Defensa de EEUU (DoD) y DISA (Defense Information Systems Agency)**
  - Por lo tanto, podrían considerarse guías de seguridad de grado militar
- **También publica la SP 800-115**
  - Technical Guide to Information Security Testing and Assessment
  - Ayudar a las organizaciones a planificar y realizar pruebas y exámenes de seguridad técnicos
  - Analizando lo que se encuentre y desarrollando estrategias de mitigación
    - https://csrc.nist.gov/publications/detail/sp/800-115/final
  - **Descripción**: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-70r4.pdf

CATEGORÍAS STIG

- Las categorías se aplican a los **controles de seguridad**
- Para cada tipo de dispositivo o aplicación, un STIG contiene **cientos de controles** para determinar si cumplen con el estándar de seguridad que especifica
  - Por ejemplo, un STIG de Windows Server especifica cómo configurar la contraseña, asignar permisos a los usuarios, configurar la auditoría...
- **A cada uno de los controles** en un STIG se le asigna un nivel de gravedad
  - **CAT I**: Si no se remedia, puede desencadenar una vulnerabilidad cuya explotación cause directamente una pérdida de confidencialidad, disponibilidad o integridad (**muy grave**)
  - **CAT II**: Si no se remedia, puede desencadenar una vulnerabilidad cuya explotación pueda causar una pérdida de confidencialidad, disponibilidad o integridad (**intermedio**)
  - **CAT III**: Si no se remedia, puede desencadenar una vulnerabilidad cuya explotación cause una degradación de las medidas que impidan la pérdida de confidencialidad, disponibilidad o integridad (**menos grave**)

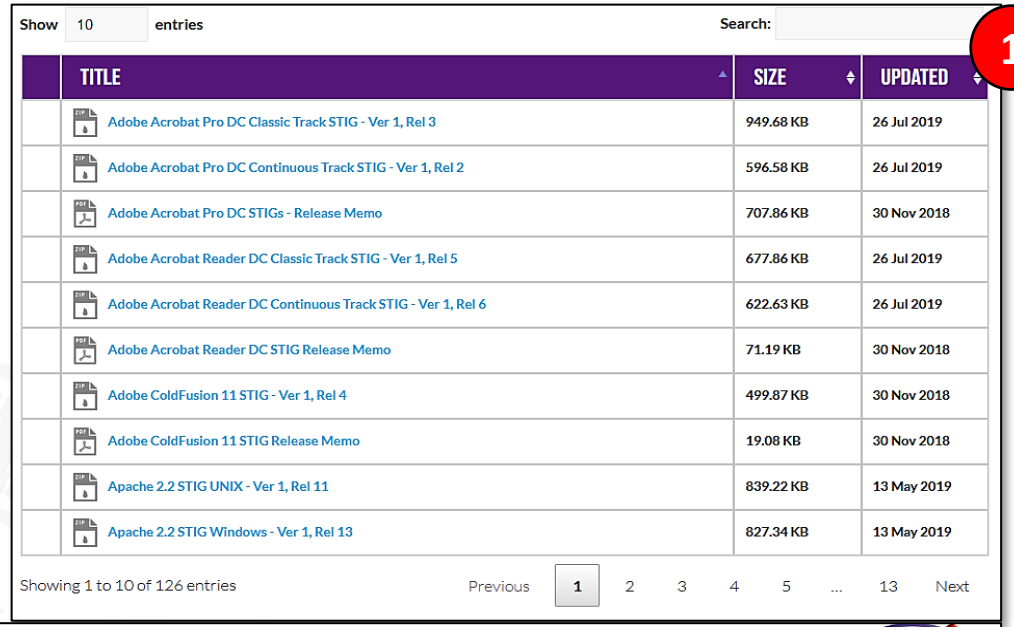
Niveles Mission Assurance Category (MACs)

- Los MACs se aplican a máquinas / sistemas (como ALTA, BAJA... en el ENS)
- **Todos los sistemas** cubiertos por una STIG también se clasifican en **función de la importancia de la información** que administran y **cuán crítica es**
  - **MAC I**: Sistemas que gestionan información vital para garantizar la eficacia de su funcionalidad
    - Perder uno es inaceptable; implementan las **medidas de seguridad más fuertes**
  - **MAC II**: Sistemas que gestionan información importante para la funcionalidad realizada
    - Perder uno es un problema importante, **implementan medidas de seguridad medias**
  - **MAC III**: Sistemas que gestionan información necesaria para la actividad diaria del sistema
    - Pero perderlos no afecta a cumplir con la funcionalidad del sistema a corto plazo
    - Perder uno es aceptable, implementan seguridad basada en las **mejores prácticas de gestión**
- También hay tres niveles para clasificar la confidencialidad de la información
  - Definidos por el DoDI 8500.2: https://fas.org/irp/doddir/dod/d8500_2.pdf: **Classified**, **Sensitive**, **Public**
- MAC y los niveles de confidencialidad son independientes
  - Los sistemas MAC I pueden manejar información pública, los MAC III información clasificada...

DESCARGA DE STIGs

Seguridad de Sistemas Informáticos

- **Podemos descargar STIGs de varios sitios**
  - **STIGs document library** (1)
    - https://public.cyber.mil/stigs/downloads
  - **National Checklist Program Repository** (2)
    - https://nvd.nist.gov/ncp/repository
    - También contiene enlaces a muchos otros archivos compatibles con SCAP de otras autoridades externas, no solo STIGs
    - Incluso benchmarks CIS (ver sección siguiente)
  - **Motores de búsqueda de terceros**
    - https://cyber.trackr.live/stig
  - Varios se pueden encontrar también en el paquete SCAP Security Guide package que vimos antes

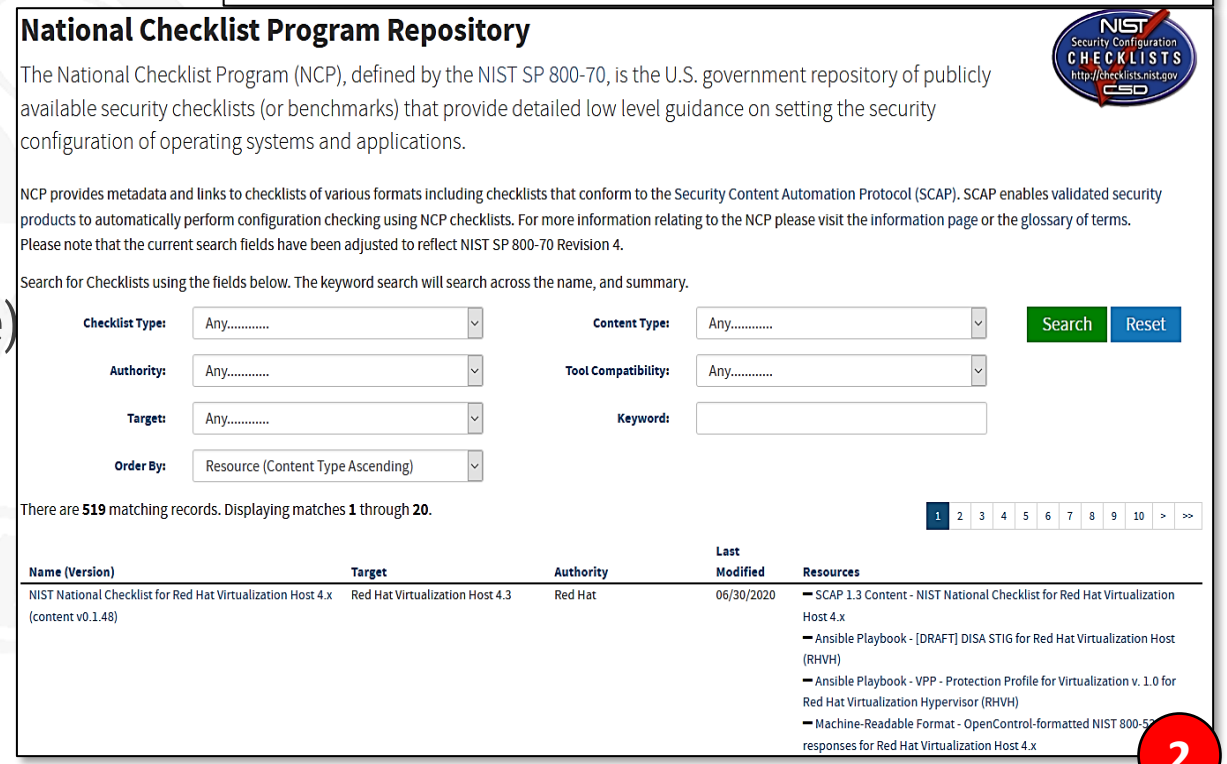


Show 10 entries Search:

	TITLE	SIZE	UPDATED
	Adobe Acrobat Pro DC Classic Track STIG - Ver 1, Rel 3	949.68 KB	26 Jul 2019
	Adobe Acrobat Pro DC Continuous Track STIG - Ver 1, Rel 2	596.58 KB	26 Jul 2019
	Adobe Acrobat Pro DC STIGs - Release Memo	707.86 KB	30 Nov 2018
	Adobe Acrobat Reader DC Classic Track STIG - Ver 1, Rel 5	677.86 KB	26 Jul 2019
	Adobe Acrobat Reader DC Continuous Track STIG - Ver 1, Rel 6	622.63 KB	26 Jul 2019
	Adobe Acrobat Reader DC STIG Release Memo	71.19 KB	30 Nov 2018
	Adobe ColdFusion 11 STIG - Ver 1, Rel 4	499.87 KB	30 Nov 2018
	Adobe ColdFusion 11 STIG Release Memo	19.08 KB	30 Nov 2018
	Apache 2.2 STIG UNIX - Ver 1, Rel 11	839.22 KB	13 May 2019
	Apache 2.2 STIG Windows - Ver 1, Rel 13	827.34 KB	13 May 2019

Showing 1 to 10 of 126 entries Previous 1 2 3 4 5 ... 13 Next

1



National Checklist Program Repository

The National Checklist Program (NCP), defined by the NIST SP 800-70, is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications.

NCP provides metadata and links to checklists of various formats including checklists that conform to the Security Content Automation Protocol (SCAP). SCAP enables validated security products to automatically perform configuration checking using NCP checklists. For more information relating to the NCP please visit the information page or the glossary of terms. Please note that the current search fields have been adjusted to reflect NIST SP 800-70 Revision 4.

Search for Checklists using the fields below. The keyword search will search across the name, and summary.

Checklist Type: Any..... Content Type: Any..... Search Reset

Authority: Any..... Tool Compatibility: Any.....

Target: Any..... Keyword:

Order By: Resource (Content Type Ascending)

There are **519** matching records. Displaying matches **1** through **20**.

1 2 3 4 5 6 7 8 9 10 > >>

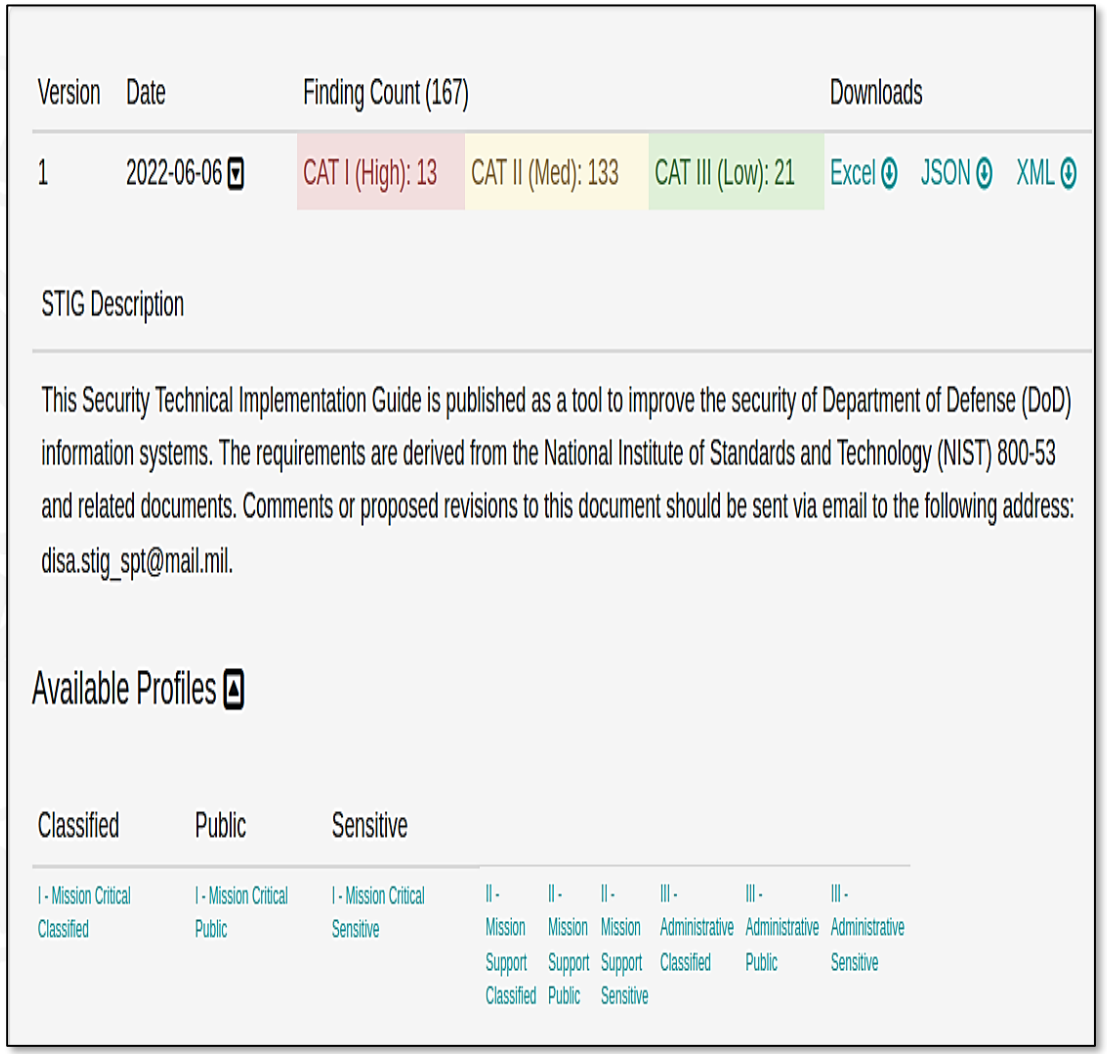
Name (Version)	Target	Authority	Last Modified	Resources
NIST National Checklist for Red Hat Virtualization Host 4.x (content v0.1.48)	Red Hat Virtualization Host 4.3	Red Hat	06/30/2020	– SCAP 1.3 Content - NIST National Checklist for Red Hat Virtualization Host 4.x – Ansible Playbook - [DRAFT] DISA STIG for Red Hat Virtualization Host (RHVH) – Ansible Playbook - VPP - Protection Profile for Virtualization v. 1.0 for Red Hat Virtualization Hypervisor (RHVH) – Machine-Readable Format - OpenControl-formatted NIST 800-5 responses for Red Hat Virtualization Host 4.x

2

Ejemplo. STIG "Canonical Ubuntu 20.04 LTS": Perfiles

- **Todos los controles contenidos en un STIG se agrupan por su clasificación CAT**
  - Aquí tenemos 13 CAT I, 133 CAT II y 21 CAT III
- **Cada STIG tiene 9 perfiles de aplicación (3 niveles de confidencialidad por cada MAC)**
  - Seleccionar una varía el número de controles que se deben realizar en cada CAT
  - Y, por tanto, la longitud de la lista de controles de seguridad que se van a validar
- **También tenemos descargas**
  - Archivos XML/JSON para comprobar, **con las herramientas adecuadas**, automáticamente si se cumple este nivel
  - Un Excel (`.csv`) para facilitar **comprobaciones manuales**

Fuente: https://www.stigviewer.com/stig/canonical_ubuntu_20.04_lts/



Version	Date	Finding Count (167)			Downloads
1	2022-06-06	CAT I (High): 13	CAT II (Med): 133	CAT III (Low): 21	Excel JSON XML

STIG Description

This Security Technical Implementation Guide is published as a tool to improve the security of Department of Defense (DoD) information systems. The requirements are derived from the National Institute of Standards and Technology (NIST) 800-53 and related documents. Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil.

Available Profiles

Classified	Public	Sensitive						
I - Mission Critical Classified	I - Mission Critical Public	I - Mission Critical Sensitive	II - Mission Support Classified	II - Mission Support Public	II - Mission Support Sensitive	III - Administrative Classified	III - Administrative Public	III - Administrative Sensitive

Ejemplo. STIG "Canonical Ubuntu 20.04 LTS": Lista de controles de seguridad de un perfil

- **Una vez elegido un perfil de MAC-confidencialidad, el STIG presenta la lista aplicable de controles de seguridad con**
  - **ID para búsquedas (Finding ID)**: Clave de única de cada control de seguridad
  - **Severidad**: Gravedad asociada a la vulnerabilidad si se descubre en el sistema auditado
  - **Título**: Resumen de los objetivos del control
  - **Descripción**: Descripción detallada de efectos o particularidades del control
- **Haciendo clic en cada control de seguridad se ven sus detalles**

Findings (MAC III - Administrative Sensitive)

Finding ID	Severity	Title	Description
V-238204	High	Ubuntu operating systems when booted must require authentication upon booting into single-user and maintenance modes.	To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must...
V-238206	High	The Ubuntu operating system must ensure only users who need access to security functions are part of sudo group.	An isolation boundary provides access control and protects the integrity of the hardware, software, and firmware that perform security functions. Security functions are the hardware, software,...
V-238201	High	The Ubuntu operating system must map the authenticated identity to the user or group account for PKI-based authentication.	Without mapping the certificate used to authenticate to the user account, the ability to determine the identity of the individual user or group will not be available for forensic analysis.
V-238363	High	The Ubuntu operating system must implement NIST FIPS-validated cryptography to protect classified information and for the following: to provision digital signatures, to generate cryptographic hashes, and to protect unclassified information requiring confidentiality and cryptographic protection in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. The operating system must implement cryptographic modules adhering to the higher...
V-238219	High	The Ubuntu operating system must be configured so that remote X connections are disabled, unless to fulfill documented and validated mission requirements.	The security risk of using X11 forwarding is that the client's X11 display server may be exposed to attack when the SSH client requests forwarding. A System Administrator may have a stance in...
V-238218	High	The Ubuntu operating system must not allow unattended or automatic login via SSH.	Failure to restrict system access to authenticated users negatively impacts Ubuntu operating system security.

Fuente: https://www.stigviewer.com/stig/canonical_ubuntu_20.04_lts/2022-06-06/MAC-3_Sensitive/

STIG "Canonical Ubuntu 20.04 LTS": Información detallada de un control

Seguridad de Sistemas Informáticos

- La descripción de cada control nos dice **cómo verificar y cómo arreglar los problemas detectados**
- Por tanto, son formas validadas y fiables de comprobar vulnerabilidades potenciales
  - Y cómo remediarlas
- Pero **clasificadas según un punto de vista militar**
  - La confidencialidad y lo crítica que sea la misión de los sistemas

The Ubuntu operating system must use SSH to protect the confidentiality and integrity of transmitted information.

Overview

Finding ID	Version	Rule ID	IA Controls	Severity
V-238215	UBTU-20-010042	SV-238215r653820_rule		High

Description

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered. This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa. Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

STIG	Date
Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide	2022-06-06

Details

Check Text (C-41425r653818_chk)

Verify the SSH package is installed with the following command:

$ sudo dpkg -l | grep openssh
ii openssh-client 1:7.6p1-4ubuntu0.1 amd64 secure shell (SSH) client, for secure access to remote machines
ii openssh-server 1:7.6p1-4ubuntu0.1 amd64 secure shell (SSH) server, for secure access from remote machines
ii openssh-sftp-server 1:7.6p1-4ubuntu0.1 amd64 secure shell (SSH) sftp server module, for SFTP access from remote machines

If the "openssh" server package is not installed, this is a finding.

Verify the "sshd.service" is loaded and active with the following command:

Fuente: https://www.stigviewer.com/stig/canonical_ubuntu_20.04_lts/2022-06-06/finding/V-238215

Ventajas / Desventajas

Ventajas

- Guías de seguridad validadas que están disponibles para una **amplia gama de productos**
- Permiten alcanzar **un nivel de seguridad alto** (grado militar) y son gratis
- Facilitan el Compliance as Code

Desventajas

- Están muy enfocadas en las necesidades militares / de ciertos departamentos de EE.UU
  - Por lo tanto, algunas de ellas pueden requerir modificaciones para adaptarlas a requisitos civiles
- Requieren monitorizar constantemente las nuevas versiones por si sus especificaciones cambian
- Su **herramienta oficial de automatización SCAP** (SCC, SCAP Compliance Checker) **está restringida**
  - Solo para empleados del gobierno de EEUU y contratistas con direcciones `.gov` O `.mil`,
  - **Solo es pública para determinados productos concretos**
- Por tanto, necesitamos confiar en implementaciones de automatización de terceros de las guías STIG
  - ¡Como la que se incluye en Ubuntu Pro! (visto luego)
  - O quizá desarrollar nuestros propios scripts de automatización, o usar la guía **para comprobación manual**
  - **¡Sin embargo, algunos de ellos sí que tienen procedimientos gratuitos de remediación con Ansible!**

¿CREES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

?

- **Eres capaz de hacer lo siguiente**
  - *Entender que los STIG son controles de seguridad del departamento de defensa de los EEUU y que muchos de ellos se distribuyen en formato SCAP*
  - *Comprender que cada control de seguridad tiene asignado un nivel de seguridad en función de la criticidad de la vulnerabilidad que podría causar no tenerlos implementados (clasificación CAT)*
  - *Tener claro que los sistemas a los que se les aplican los controles están clasificados en función de la importancia de la información que administran (clasificación MAC)*
  - *Tener claro además que la información administrada además está clasificada en función de su confidencialidad*
  - *Entender que MAC y niveles de confidencialidad son independientes*
  - *Saber que muchos STIG se pueden obtener gratuitamente, e incluso la herramienta oficial para auditar sistemas (SCC) está disponible para algunos SO también gratis*
  - *Entender la estructura general de un control de seguridad de un STIG*

Fuente: Bing Chat AI

Benchmarks del Center for Internet Security (CIS)

Controles de seguridad para ser un “Top Gun” ☺

***Icono del Center for Internet Security:**
https://www.cisecurity.org/

CIS BENCHMARKS

https://www.cisecurity.org/

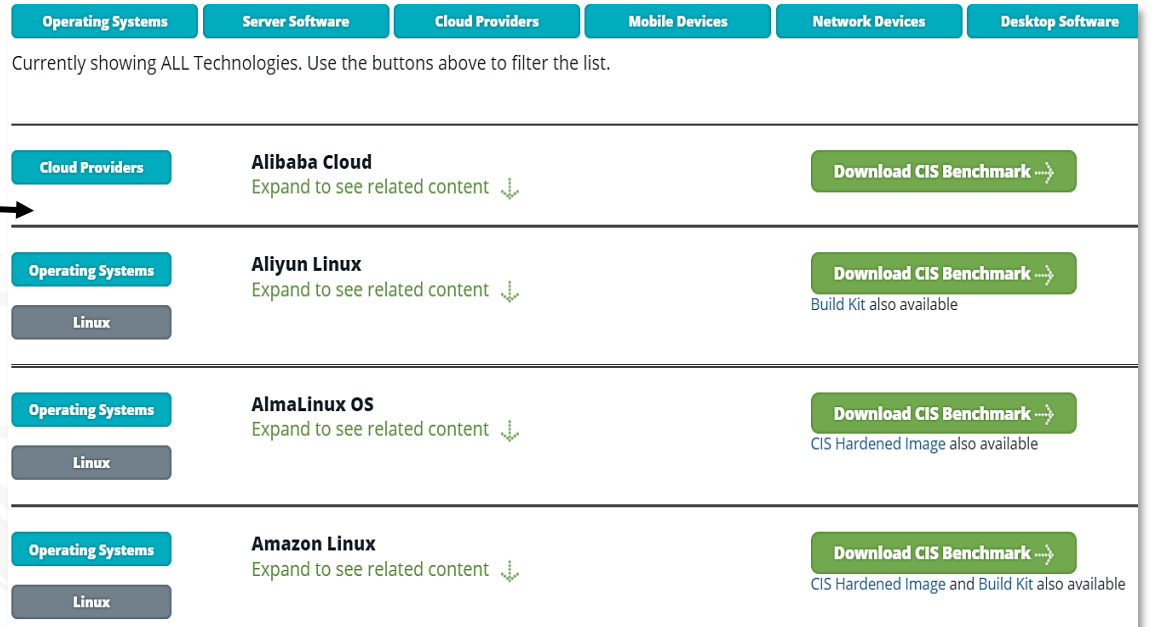
- **Fuente bien establecida de guías de hardening**
  - Recomiendan valores y **controles técnicos de seguridad** para dispositivos de red, SO, software...
  - Una guía por producto y versión
  - Actualmente hay más de 100 disponibles: https://www.cisecurity.org/cis-benchmarks/
- **Son creados y utilizados por consenso del gobierno de los Estados Unidos**
  - Junto con 1800 empresas conocidas de diferentes industrias (Adobe, HP,...)
  - Lo que **garantiza la calidad y fiabilidad de sus contenidos...**
  - Contienen el conocimiento más actualizado y las mejores prácticas de seguridad
    - Y la experiencia de grandes **empresas civiles** privadas e **instituciones públicas** de todo el mundo
- **Además de guías, incluyen (aunque no gratis)**
  - **Máquinas virtuales prediseñadas con hardening** en Azure, AWS y Google Cloud
    - https://www.cisecurity.org/cis-hardened-image-list
  - **Kits de construcción** para automatizar la configuración de software existente siguiendo las especificaciones del benchmark
    - https://www.cisecurity.org/cis-securesuite/cis-securesuite-build-kit-content

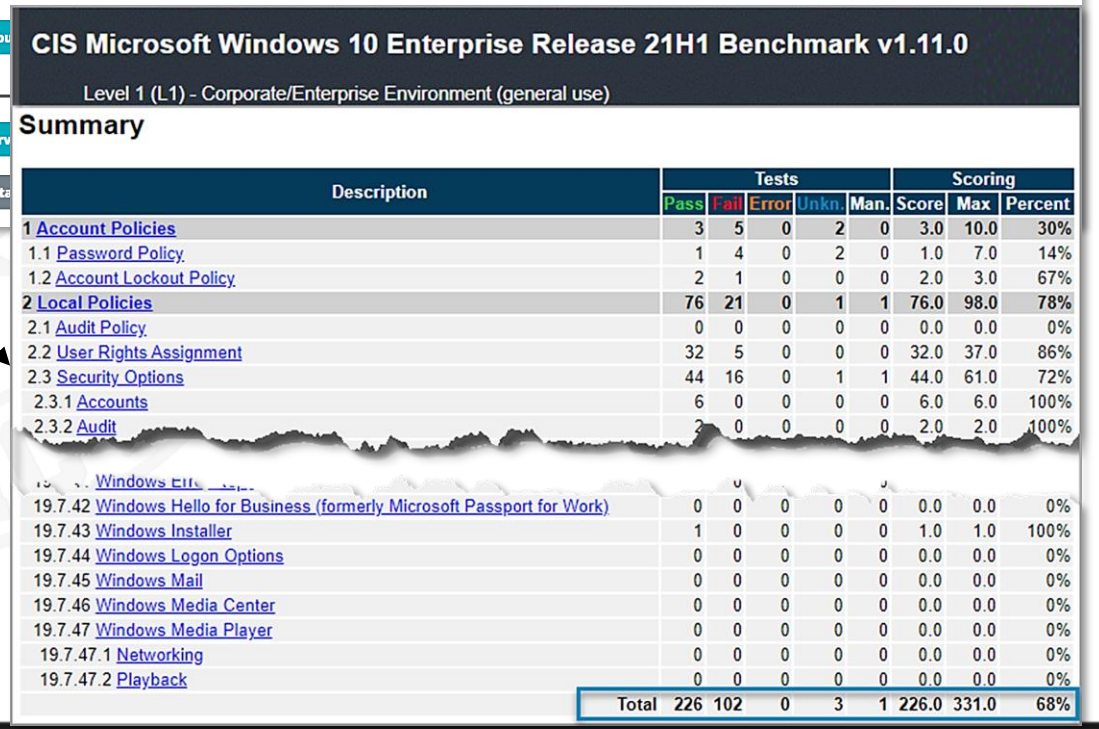
CIS BENCHMARKS

Seguridad de Sistemas Informáticos

Fuente: https://www.cisecurity.org/cis-benchmarks/

- **Disponibles en formato PDF**
  - ¡Gratis, y ya no es necesario registrarse!
  - https://downloads.cisecurity.org/#/
- **También disponibles en formatos SCAP**
  - Con su propia herramienta SCAP (CIS CAT Pro)
  - Gratis para instituciones educativas / autorizadas de EE. UU., de pago para el resto ☹
  - También existe una versión **gratuita** limitada (3 benchmarks solamente) de la herramienta
    - **CIS-CAT Lite**: https://learn.cisecurity.org/cis-cat-lite
- **Los archivos del paquete SCAP security guide también incluyen perfiles de seguridad basados en CIS**
  - **Validan y corrigen controles de seguridad de CIS Benchmarks para algunos SO**
  - Están incompletos (faltan controles por incluir)





CIS Microsoft Windows 10 Enterprise Release 21H1 Benchmark v1.11.0

Level 1 (L1) - Corporate/Enterprise Environment (general use)

Summary

Description	Tests					Scoring		
	Pass	Fail	Error	Unkn.	Man.	Score	Max	Percent
1 Account Policies	3	5	0	2	0	3.0	10.0	30%
1.1 Password Policy	1	4	0	2	0	1.0	7.0	14%
1.2 Account Lockout Policy	2	1	0	0	0	2.0	3.0	67%
2 Local Policies	76	21	0	1	1	76.0	98.0	78%
2.1 Audit Policy	0	0	0	0	0	0.0	0.0	0%
2.2 User Rights Assignment	32	5	0	0	0	32.0	37.0	86%
2.3 Security Options	44	16	0	1	1	44.0	61.0	72%
2.3.1 Accounts	6	0	0	0	0	6.0	6.0	100%
2.3.2 Audit	2	0	0	0	0	2.0	2.0	100%
19.7.42 Windows Hello for Business (formerly Microsoft Passport for Work)	0	0	0	0	0	0.0	0.0	0%
19.7.43 Windows Installer	1	0	0	0	0	1.0	1.0	100%
19.7.44 Windows Logon Options	0	0	0	0	0	0.0	0.0	0%
19.7.45 Windows Mail	0	0	0	0	0	0.0	0.0	0%
19.7.46 Windows Media Center	0	0	0	0	0	0.0	0.0	0%
19.7.47 Windows Media Player	0	0	0	0	0	0.0	0.0	0%
19.7.47.1 Networking	0	0	0	0	0	0.0	0.0	0%
19.7.47.2 Playback	0	0	0	0	0	0.0	0.0	0%
Total	226	102	0	3	1	226.0	331.0	68%

¿Por qué usar los CIS Benchmarks?

- **Validado por expertos**
  - No es un blog, un artículo de Internet, un tutorial... u otras fuentes cuya fiabilidad no es comprobable
- **Completo**
  - No falta ningún elemento para obtener un cierto nivel de seguridad
- **Totalmente explicado**
  - Te dice **qué está mal**, **cómo arreglarlo**, y **por qué necesita arreglarse**
- **Actualizado**
  - Las erratas se corrigen y se adaptan a las nuevas versiones de los productos (son **mantenidos**)
- **Internacional**
  - Un sistema que cumpla con estos benchmarks podrá ser introducido en ciertos entornos que requieren certificaciones o garantías de seguridad oficiales
- **Adaptado a cada producto software**
  - Cada benchmark tiene un **nº distinto de controles** de seguridad y se adapta al software con **perfiles**

Estructura de sus controles de seguridad: Automated o manual

- **Los sistemas se evalúan en función de los controles de seguridad de sus CIS benchmarks**
- **Algunos controles de seguridad pueden automatizarse por completo, otros no**
  - Esto se indica en cada uno
- **Automatizado**
  - Recomendaciones para las cuales la evaluación de un control técnico puede ser totalmente automatizada y validada a un pass/fail
  - Incluye la información para **implementar la automatización**
- **Manual**
  - Representa recomendaciones para las que la evaluación de un control técnico no puede automatizarse por completo
  - Requiere todos o algunos pasos manuales para validar que el estado configurado se establece según lo esperado
    - El estado esperado puede variar en función del entorno

Fuente: PDF del Ubuntu 22.04 Benchmark

5.3.3 Ensure sudo log file exists (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

sudo can use a custom log file

Rationale:

A sudo log file simplifies auditing of sudo commands

Impact:

WARNING: Editing the `sudo` configuration incorrectly can cause `sudo` to stop functioning. Always use `visudo` to modify `sudo` configuration files.

Audit:

Run the following command to verify that sudo has a custom log file configured:

```
# grep -rPsi
"^\h*Defaults\h+([^#]+,\h*)?logfile\h*=\h*(\"|\')?\H+(\"|\')?(,\h*\H+\h*)*\h*
(#.*)?$" /etc/sudoers*
```

Verify the output matches:

```
Defaults logfile="/var/log/sudo.log"
```

Remediation:

Edit the file `/etc/sudoers` or a file in `/etc/sudoers.d/` with `visudo` or `visudo -f <PATH TO FILE>` and add the following line:
Example:

```
Defaults logfile="/var/log/sudo.log"
```

References:

1. SUDO(8)
2. VISUDO(8)

Additional Information:

visudo edits the sudoers file in a safe fashion, analogous to vipw(8). visudo locks the sudoers file against multiple simultaneous edits, provides basic sanity checks, and checks for parse errors. If the sudoers file is currently being edited you will receive a message to try again later.

Estructura de sus controles de seguridad: Perfiles y niveles

- Los controles de seguridad se dividen en **perfiles de uso** y **niveles**
- Los **perfiles** dependen de la funcionalidad que el software / SO cumpla
  - El Ubuntu 18.04 CIS Benchmark define 2 perfiles
    - Servidor (Server) y Estación de trabajo (Workstation)
  - El Windows Server 2019 CIS Benchmark define otros dos diferentes
    - **Servidor miembro** (Member Server) y Controlador de dominio (Domain controller)
- Los niveles son normalmente dos en todos los **benchmarks** CIS
  - **Nivel 1**: los controles de este nivel tienen la intención de
    - Ser prácticos y no causar "daños" innecesarios (mantener la funcionalidad del **software** aceptablemente)
    - Proporcionar una ventaja de seguridad sustancial
  - **Nivel 2**: amplía el nivel 1 con controles que tienen las siguientes características
    - Diseñados para entornos o casos de uso donde la seguridad es clave (**por encima de otras cosas**)
    - Implementar una defensa en profundidad
    - **Podría afectar a la funcionalidad** de la máquina o sus servicios de alguna manera, o a su rendimiento
  - **Niveles especiales**: algunos productos tienen niveles especiales creados sólo para ellos
    - Ej.. Windows Server 2019 tiene un tercer nivel llamado "Seguridad de Windows de próxima generación"

Estructura de sus controles de seguridad: Perfiles y niveles

- **Cada control de seguridad se etiqueta con los perfiles de uso en los que es aplicable**
  - Uno, varios o todos los perfiles definidos
- **Ejemplos de controles de seguridad etiquetados**
  - El Ubuntu 18.04 CIS Benchmark tiene
    - 204 controles de seguridad Nivel 1 - Servidor
    - 37 controles de seguridad Nivel 2 - Servidor
    - 200 controles de seguridad Nivel 1 - Estación de trabajo
    - 40 controles de seguridad Nivel 2 - Estación de trabajo
  - El Windows Server 2019 CIS Benchmark tiene
    - 289 controles de seguridad Nivel 1 - Controlador de dominio
    - 60 controles de seguridad Nivel 2 - Controlador de dominio
    - 6 controles de seguridad Seguridad de Windows de próxima generación - Controlador de dominio
    - 293 controles de seguridad Nivel 1 - Servidor miembro
    - 61 controles de seguridad Nivel 2 - Servidor miembro
    - 6 controles de seguridad Seguridad de Windows de próxima generación - Servidor miembro

5.3.3 Ensure sudo log file exists (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Fuente: PDF del Ubuntu 22.04 Benchmark

Description:

sudo can use a custom log file

Rationale:

A sudo log file simplifies auditing of sudo commands

Impact:

WARNING: Editing the `sudo` configuration incorrectly can cause `sudo` to stop functioning. Always use `visudo` to modify `sudo` configuration files.

Audit:

Run the following command to verify that sudo has a custom log file configured:

```
# grep -rPsi
"^\h*Defaults\h+([^#]+,\h*)?logfile\h*=\h*(\"|\')?\H+(\"|\')?(,\h*\H+\h*)*\h*
(#.*)?$" /etc/sudoers*
```

Verify the output matches:

```
Defaults logfile="/var/log/sudo.log"
```

Remediation:

Edit the file `/etc/sudoers` or a file in `/etc/sudoers.d/` with `visudo` or `visudo -f <PATH TO FILE>` and add the following line:
Example:

```
Defaults logfile="/var/log/sudo.log"
```

References:

1. SUDO(8)
2. VISUDO(8)

Additional Information:

visudo edits the sudoers file in a safe fashion, analogous to vipw(8). visudo locks the sudoers file against multiple simultaneous edits, provides basic sanity checks, and checks for parse errors. If the sudoers file is currently being edited you will receive a message to try again later.

Estructura de sus controles de seguridad: Datos técnicos

- **Descripción**
  - Detalles de la acción
- **Fundamento (Rationale)**
  - Describe por qué es necesario implementar este control
  - Y su impacto en la seguridad del sistema
- **Auditoría**
  - Procedimiento técnico para comprobar si el control de seguridad está implementado actualmente o no
  - Implementado por procedimientos de **verificación automática**
- **Implementación (Remediation)**
  - Cómo implementar el control de seguridad
  - Si los procedimientos de la sección de auditoría determinan que no está implementado
  - Implementado por procedimientos de **corrección automática**

Fuente: PDF del Ubuntu 22.04 Benchmark

5.3.3 Ensure sudo log file exists (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

sudo can use a custom log file

Rationale:

A sudo log file simplifies auditing of sudo commands

Impact:

WARNING: Editing the `sudo` configuration incorrectly can cause `sudo` to stop functioning. Always use `visudo` to modify `sudo` configuration files.

Audit:

Run the following command to verify that sudo has a custom log file configured:

```
# grep -rPsi
"^\h*Defaults\h+([^#]+,\h*)?logfile\h*=\h*(\"|\')?\H+(\"|\')?(,\h*\H+\h*)*\h*
(#.*)?$" /etc/sudoers*
```

Verify the output matches:

```
Defaults logfile="/var/log/sudo.log"
```

Remediation:

Edit the file `/etc/sudoers` or a file in `/etc/sudoers.d/` with `visudo` or `visudo -f <PATH TO FILE>` and add the following line:
Example:

```
Defaults logfile="/var/log/sudo.log"
```

References:

1. SUDO(8)
2. VISUDO(8)

Additional Information:

visudo edits the sudoers file in a safe fashion, analogous to vipw(8). visudo locks the sudoers file against multiple simultaneous edits, provides basic sanity checks, and checks for parse errors. If the sudoers file is currently being edited you will receive a message to try again later.

Ventajas / Desventajas

Ventajas

- Guías completas y detalladas de los controles técnicos de seguridad que vuelven un software más seguro y facilitan Compliance as Code
- Te dicen exactamente qué hacer, por qué hacerlo y cómo hacerlo
- Validado en términos de eficacia e y completitud por miles de expertos de todo el mundo
- Sus perfiles permiten adaptar las operaciones de seguridad al propósito del software desplegado

Desventajas

- Sólo cubre una parte de los productos más usados
- La herramienta SCAP completa es propietaria y de pago
  - Podríamos que usar la versión Lite , que solo soporta Windows 10, Ubuntu, y Chrome
  - https://learn.cisecurity.org/cis-cat-lite
  - https://www.youtube.com/watch?v=76XpFVwdRYg
- De manera gratuita, tendríamos que confiar en **herramientas/scripts no oficiales para automatizar su verificación / aplicación**
  - O confiar en que el soporte de `scap-security-guide` para los benchmarks de CIS mejorará
- Al ser tan extensos, adaptarlos a una funcionalidad específica puede ser tedioso

COMPLIANCE AUTOMATIZADO GRATUITO OFICIAL

- **La licencia Ubuntu Pro convierte a Ubuntu en un Linux de categoría empresarial**
  - https://ubuntu.com/pro
  - Amplía a 10 años el soporte de los paquetes incluidos
  - Y permite usar la Ubuntu Security Guide (paquete `usg`)
    - Incluye el **cumplimiento automatizado de Ubuntu con los benchmarks CIS y los STIG de la DISA**
      - Defense Information System Agency del Departamento de Defensa (DoD) de EEUU
    - **CIS**: https://ubuntu.com/security/certifications/docs/usg/cis
    - **DISA STIG**: https://ubuntu.com/security/certifications/docs/disa-stig
  - Requiere registro y es gratis para hasta 5 máquinas Ubuntu 18.04LTS+
    - ¡Sí, ahora puedes crear oficialmente máquinas Ubuntu a prueba de balas automáticamente! ☺
    - Usando cualquiera de las dos fuentes de ficheros SCAP vistas hasta ahora

- **Microsoft también publica sus propias "líneas base" de seguridad (controles de seguridad a implementar) y software de automatización**
  - Por tanto, Microsoft sigue su propio estándar para hacer esto (no es CIS ni STIG)
  - https://learn.microsoft.com/es-es/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines

Compliance automatizado con herramientas o scripts de 3os

- **Hay herramientas que tienen integradas auditorías con controles CIS**
  - Por ejemplo, el XDR Wazuh integra una **auditoría automatizada** de los SO que supervisa
- **Estos son ejemplos que usan Ansible para aplicar una política CIS para Ubuntu**
  - **Pero cuidado**: Debes fiarte mucho de que su contenido es correcto y sin "sorpresas" ☹
  - https://medium.com/@cosmin.ciobanu/the-quest-for-os-hardening-8affa979f36a
  - https://github.com/florianutz/Ubuntu1804-CIS
  - https://github.com/florianutz/ubuntu2004_cis
- **También hay STIGs y CIS Benchmarks disponibles para sistemas Windows**
  - Versiones de cliente (Windows 10, 11) y servidor
  - La corrección usando Bash se reemplaza por la corrección usando PowerShell
  - Ansible no se puede instalar directamente en Windows, pero se puede configurar una máquina Windows desde una Linux remota si tenemos los permisos adecuados
    - Nuestra alumna María Flórez implementó esto como su trabajo fin de grado
    - https://github.com/Yori1999/vagrant-ansible-hardening
  - También tenemos los scripts de Hardening Kitty: https://github.com/scipag/HardeningKitty

¿Crees que lo has entendido todo? ¡Autoevalúate!

?

- **Eres capaz de hacer lo siguiente**
  - *Entender qué son los CIS Benchmarks, quien los mantiene y de dónde se pueden descargar*
  - *Comprender el significado de un control de seguridad clasificado como automatizado respecto a uno clasificado como manual*
  - *Entender qué son los perfiles de uso y que dependen de cada sistema*
  - *Comprender la diferencia entre un control CIS Nivel 1 y Nivel 2*
  - *Entender qué información puedes encontrar en las secciones descripción, fundamento, auditoría e implementación de cada control*
  - *Tener claro lo que ofrece la licencia Ubuntu Pro relativo al CIS (y a STIGs)*
  - *Y también que existen formas de conseguir compliance CIS con herramientas de terceros, pero entendiendo los riesgos que supone*

< Ir al índice

FRAMEWORKS DE SEGURIDAD

Usando controles técnicos de seguridad para crear políticas de seguridad y un nivel de abstracción mayor

*Iconos por Bing Chat AI

Fuente: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

En este bloque aprenderás

- Entender qué son los **controles de seguridad CSC** y cómo se relacionan con los CIS Benchmarks
- Cómo puedes **implementar controles CSC** a base de implementar los controles técnicos de seguridad de los CIS Benchmarks
- Qué es y lo que significan los **Implementation Groups**
- Como usar la implementación de controles CSC para facilitar posteriormente el **cumplimiento** con diferentes estándares de seguridad

De controles de seguridad a metodologías

Seguridad de Sistemas Informáticos

Usar una **Metodología de Auditoría de Seguridad** (como **OSSTMM**) para revisar la seguridad de los sistemas y el cumplimiento de **frameworks** de seguridad implementados

5

Gestionado por

Asignar los controles y **Safeguards** implementados a un **Framework de Seguridad** internacional reconocido (**ISO 27001**, **PCI-DSS**…) para facilitar la implementación de un **SGSI**

4

Mapea a

Usar **Implementation Groups** (solo 3) para implementar solo los **Safeguards** más adecuados a un escenario particular según los recursos disponibles

3

Se pueden distribuir en

Agrupar los controles de seguridad implementados en CIS Critical Security Controls (CSC) y Safeguards

2

Se pueden agrupar en

Verificar e implementar **Controles técnicos de seguridad** adecuados y validados en un producto de software / SO de forma altamente **automatizada** (varios cientos de controles)

1

Nivel de Abstracción

+

-

Más allá de las guías técnicas de controles de seguridad

- **Aplicar cientos de controles validados nos da un nivel de seguridad adecuado**
  - Pero son difíciles de manejar si la seguridad es a nivel de infraestructura (¡demasiados!)
- **Necesitamos abstracciones de más nivel que los agrupen en menos entidades**
  - Necesitamos identificar **qué tipo de hardening** se ha hecho en cada sistema más fácilmente
    - Esto es clave para implementar frameworks y facilitar las auditorías de seguridad
  - En un **nivel de abstracción alto**, necesitamos cosas como *"las password deben ser fuertes"*
    - No acciones técnicas de bajo nivel como las de los controles de seguridad. Ej.:
      - Instalar y configurar el paquete `libpam` de Linux
      - Asignar los valores X, Y, Z a entradas de una directiva de seguridad de controlador de dominio de Windows
  - Por tanto, necesitamos algo que nos **aísle de los detalles técnicos** de cada sistema.
    - Centrarse en "**qué**" en lugar de "cómo" (**¡la información técnica detallada no pertenece a este nivel**!)
    - Estas abstracciones "qué" agrupan 100s de controles de seguridad "cómo" **en menos entidades**
- **Los benchmarks CIS permiten alcanzar un nivel de abstracción más alto**
  - A partir de los controles técnicos de seguridad implementados descritos anteriormente

CIS Critical Security Controls (CSC controls) v8

- **Son un conjunto organizado de Safeguards**
  - Llamados CSC Controls o sólo CIS Controls
- **Se diseñaron para mitigar los ciberataques a sistemas y redes más importantes**
- **Se mapean y referencian desde muchos frameworks de seguridad, gestión y legales**
- **La versión v8 se ha diseñado para lidiar con las amenazas modernas**
  - Cloud, virtualización, ataques en el teletrabajo, nuevas tácticas de ataque…

Organización general de los CSC Controls v8 y sus Safeguards:
https://www.linkedin.com/pulse/cis-critical-security-controls-v8-steps-template-download-dan-duran/

CIS Critical Security Controls (CSC controls) v8

- **Al final de cada control técnico de seguridad de cualquier benchmark CIS podemos encontrar qué CSC Controls y Safeguards están asociados con él**
  - Los CSC Controls son **18** (**v8**) o **20** (**v7.1**) mejores prácticas de ciberseguridad defensiva reconocidas
  - Se subdividen en **153 Safeguards** (**v8**) (o **170 CSC Subcontrols** (**v7.1**))
  - https://www.cisecurity.org/controls/cis-controls-navigator
- ***¿Qué significa esta tabla?***
  - Que este control técnico de seguridad pertenece al **CSC Control v8 nº 3** "*Data Protection*"
    - Ver la tabla de la transparencia anterior
  - Dentro de él, pertenece a la **Safeguard 3.3** "*Configure Data Access Control Lists*"

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

- Si usásemos la v7.1 Esta imagen significa que este control técnico de seguridad pertenece al CSC Control v7 nº 14 "*Controlled Access Based on Net to Know*"
- Dentro de él, también es aplicable al CSC Subcontrol 14.6 de ese control CSC 14
- **La versión 7.1 será reemplazada por la v8**

CIS Critical Security Controls (CSC controls) v8

- **Los CSC Controls...**
  - Se desarrollan por **consenso**, y contienen **información experta** sobre amenazas y tecnologías
  - Modelan desde operaciones básicas hasta muy avanzadas de ciberseguridad
  - Se usan para crear rápidamente protecciones que podrían beneficiar a cualquier empresa
- **Los 18 CSC Controls v8 y sus 153 Safeguards asociados son siempre los mismos**
  - No importa el producto de software / SO
  - Se diseñaron para cubrir las s consideraciones de seguridad de **TODO** software
- **Pero cada CIS Benchmark solo contiene Safeguards razonables para su software**
  - Ej.: El CIS Benchmark de Google Chrome explica cómo hacer hardening a este navegador
    - No tiene ningún control técnico de seguridad asignado a ningún Safeguard del CSC Control 1 "*Inventory and Control of Hardware Assets*"
    - ¡**Es un navegador, no una infraestructura**!
  - Por tanto, el software **no tiene que implementar las 153 Safeguards**, ¡sino muchas menos!
  - Entonces los 100s de controles técnicos de seguridad se agrupan en pocas 10s de entidades

De los controles técnicos de seguridad a los CSC Controls

Seguridad de Sistemas Informáticos

CIS Benchmark (PDF) de Ubuntu 22.04 → **CSC Controls v8 (y sus Safeguards)**

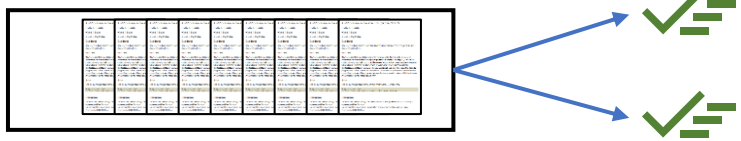
https://www.cisecurity.org/controls/cis-controls-navigator

Todos los controles de seguridad técnicos del Safeguard 3.3

CSC Control 3 – *Data Protection*

- ***Safeguard 3.3***: *Configure Data Access Control Lists*

Todos los controles de seguridad técnicos de los Safeguards 4.3 y 4.8



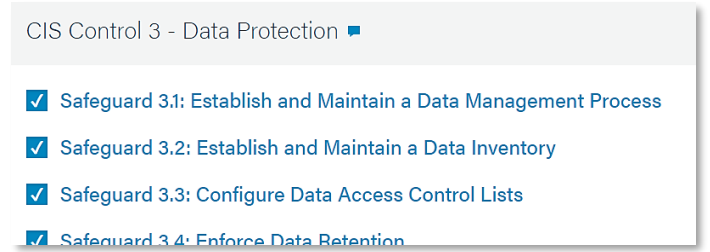
CSC Control 4 – *Secure Configuration of Enterprise Assets and Software*

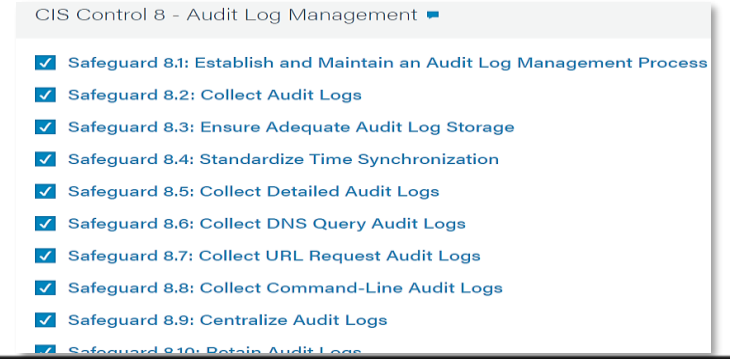
- ***Safeguard 4.3***: *Configure Automatic Session Locking on Enterprise Assets*
- ***Safeguard 4.8***: *Uninstall or Disable Unnecessary Services on Enterprise Assets and Software*

Todos los controles de seguridad técnicos los Safeguards 8.2 y 8.9

CSC Control 8 – *Audit Log Management*

- ***Safeguard 8.2***: *Collect Audit Logs*
- ***Safeguard 8.9***: *Centralize Audit Logs*





De controles de seguridad a metodologías

Seguridad de Sistemas Informáticos

Usar una **Metodología de Auditoría de Seguridad** (como **OSSTMM**) para revisar la seguridad de los sistemas y el cumplimiento de **frameworks** de seguridad implementados

5

Gestionado por

Asignar los controles y **Safeguards** implementados a un **Framework de Seguridad** internacional reconocido (**ISO 27001**, **PCI-DSS**…) para facilitar la implementación de un **SGSI**

4

Mapea a

Usar **Implementation Groups** (solo 3) para implementar solo los **Safeguards** más adecuados a un escenario particular según los recursos disponibles

3

Se pueden distribuir en

Agrupar los controles de seguridad implementados en **CIS Critical Security Controls (CSC)** y **Safeguards**

2

Se pueden agrupar en

Verificar e implementar **Controles técnicos de seguridad** adecuados y validados en un producto de software / SO de forma altamente **automatizada** (varios cientos de controles)

1

Nivel de Abstracción

+

-

Implementation groups (IGs)

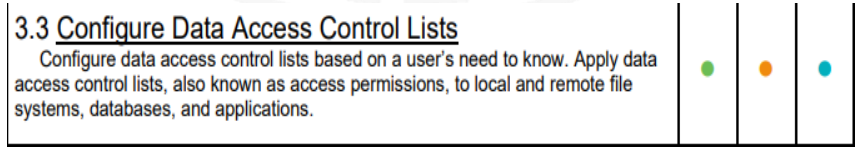
- En una diapositiva anterior sobre los **CSC Controls**, vimos esto... *¿Qué es un IG?*
- Los **CSC Controls** los usan empresas que se preocupan y quieren invertir en ciberseguridad
  - Con exposiciones de riesgo muy diferentes
  - Y para crear una política de ciberseguridad eficiente
- Pero en algunos escenarios la aplicación de **CSC Controls** podría ser difícil
  - Sobe todo si el presupuesto de seguridad es limitado
- Esta es la razón por la que se crearon **IGs** (**Implementation Groups**)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

Implementation Groups (IGs)

- Los IG proporcionan
  - Una nueva **clasificación / priorización** de los Safeguards de cada control CSC
  - Una **metodología** para mejorar la evaluación del nivel de seguridad de los recursos de la empresa
- Las empresas se **evalúan a sí mismas** y eligen un IG
  - Ahora solo tienen que centrarse en cumplir con todos los Safeguards pertenecientes a ese IG
- En otras palabras: **reduce la cantidad de Safeguards que debe implementar**
  - Teniendo en cuenta los **riesgos de seguridad percibidos** por la empresa y sus **recursos económicos**
  - Como ves, los Safeguards de los controles técnicos de seguridad se asignan a uno o más IG
  - Por lo tanto, los **IG filtran qué controles técnicos debe implementar en sus sistemas**
  - **¡Solo aquellos que están incluidos en los Safeguards del IG que elijan!**
    - En la tabla anterior, el control técnico de seguridad debe implementarse, sin importar el IG elegido
    - ¡Está asignado a los tres!



Implementation groups (IGs)

- **Por tanto, los IG son categorías que las propias empresas pueden utilizar para auto-evaluarse su seguridad**
  - En función de los aspectos de seguridad que ellas consideren relevantes para su caso particular
  - Cada IG identifica qué Safeguards (y Controles CSC) son razonables para las empresas con un cierto perfil de riesgo y cantidad de recursos económicos para implementar operaciones de seguridad
    - Cualquier empresa puede clasificarse a sí misma en un IG y enfocar sus recursos económicos disponibles a mejorar su seguridad usando **sólo** los Safeguards de ese IG
- **Cada IG incluye al anterior, y hay tres**
  - **IG1**: un conjunto básico de Safeguards a implementar por empresas con una limitada exposición al riesgo, experiencia y recursos para invertir en ciberseguridad
    - Nivel de "**ciber higiene**": protecciones esenciales que deben crearse para defenderse de ataques comunes
    - **Todas las empresas deberían implementar al menos un nivel IG1**
  - **IG2**: Safeguards adicionales que deben implementar las empresas con más recursos y experiencia
    - Pero también con una exposición al riesgo más alta que las empresas IG1
  - **IG3**: el resto de Subcontroles CSC no incluidos en el nivel anterior se agrupan para formar el IG3
    - **Exposición al riesgo máximo** y por tanto coste económico mayor, pero también máximo nivel de seguridad

IMPLEMENTATION GROUPS (IGS)

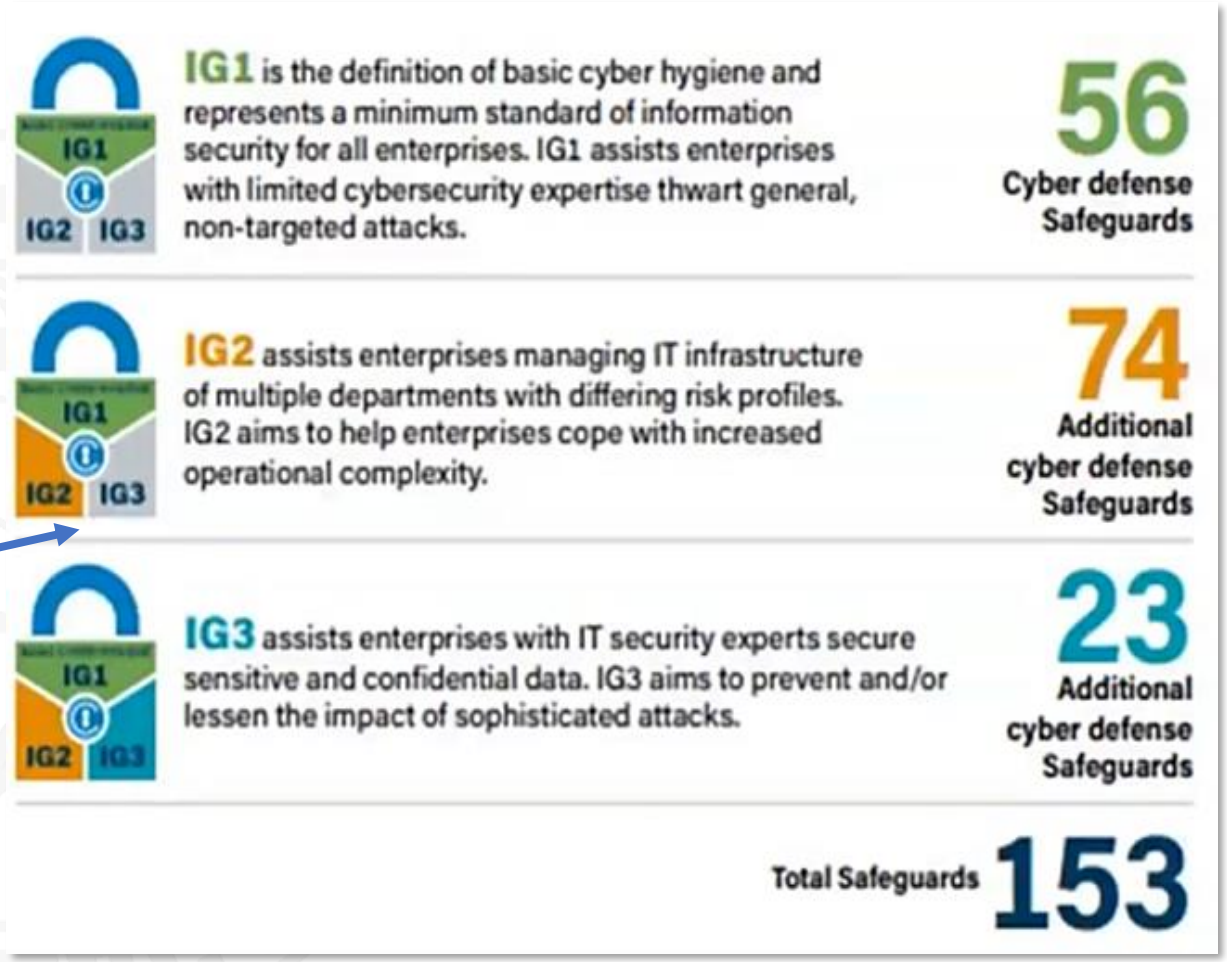
Fuente: https://www.itpromentor.com/cisv8-assessment-tool/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●

A que IGs pertenece este control de seguridad

De los 14 Safeguards del CSC Control 3 "*Data Protection*", 6 pertenecen al IG1, 6 más (12 en total) al IG2 y los 14 al IG3



Ej..: Soy una pequeña tienda que vende un catálogo limitado de ropa en Internet. Todos mis pagos son gestionados por **PayPal**, y la autenticación de usuarios se basa en **Google**, por lo que realmente no almaceno datos muy críticos.
Me clasificaré como **IG1**, así que ahora seguiré sólo los **Safeguards** de este **Implementation Group**, e implementaré todos los **controles técnicos de seguridad** del **Benchmark CIS** de mi **Ubuntu 22.04 + Apache 2 web server** que estén incluidos en ellos

CIS, MARCOS Y POLÍTICAS DE SEGURIDAD

- **Los IG centran los esfuerzos de ciberseguridad en las áreas más importantes**
  - Maximizando el uso de recursos teniendo en cuenta el riesgo
- **Sin embargo, es una metodología CIS**
  - Podemos necesitar algo que siga estándares y marcos internacionales de seguridad
  - Necesitamos **procedimientos de gestión aceptados a nivel mundial**
- **Cuando las empresas invierten en su ciberseguridad de forma seria, deben cumplir con un marco de seguridad (security framework)**
  - **¡Pero no significa que se pierda el tiempo usando los benchmarks CIS como controles técnicos!**
  - Al contrario, muchos de los frameworks de seguridad populares los mencionan o utilizan
  - https://www.cisecurity.org/cybersecurity-tools/mapping-compliance/
- **Hay muchos frameworks de seguridad utilizados en todo el mundo, algunos aplicados solo a ciertos sectores**
  - Los CIS Benchmarks **pueden ayudar a cumplir con muchos de ellos**
  - En las siguientes transparencias se ven algunos

CIS, MARCOS Y POLÍTICAS DE SEGURIDAD

- **Payment Card Industry Data Security Standard** (PCI DSS)
  - Usado por algunos de los **principales minoristas** del mundo
  - Menciona los benchmarks CIS como estándar recomendado para facilitar su cumplimiento
- **National Institute of Standards and Technology** (NIST) y **Federal Information Security Modernization Act** (FISMA)
  - NIST es una **agencia líder en cumplimiento técnico**; FISMA es parte del NIST
  - Los controles CIS facilitan en gran medida el cumplimiento de las normas de seguridad del NIST
  - El National Checklist Program Repository recomienda los benchmarks CIS a las agencias federales y empresas que tratan de lograr el cumplimiento de las normas FISMA
- **Health Insurance Portability and Accountability Act** (HIPAA)
  - Líneas básicas de seguridad para proteger los **datos de los pacientes en empresas/organizaciones relacionadas con la salud**
  - Los controles CIS tienen muchas características comunes con HIPAA; pueden complementarlos
  - También son una manera de permitir que las empresas/organizaciones relacionadas con la salud respondan mejor a las últimas técnicas de ataque

CIS, MARCOS Y POLÍTICAS DE SEGURIDAD

- **Reglamento General de Protección de Datos** 2016/679 de la UE, RGPD/GDPR (**ASLEPI**)
  - https://www.cisecurity.org/gdpr/
- **International Organization for Standardization** (ISO) ISO/IEC 27001 (SGSI, siguiente sección)
  - Proporciona **estándares mundiales independientes y validados para garantizar la ciberseguridad**
  - Ayuda a las empresas a defenderse de las amenazas cibernéticas y los riesgos de seguridad
- **Hay mapeos entre STIGs y CIS Benchmarks**
  - https://www.cisecurity.org/blog/new-options-from-cis-for-stig-compliance/
- **No hay entre el ENS y los CIS Benchmarks**
  - Pero como ambos pueden mapearse a controles ISO 27001, se puede usar como “puente” entre ellos

CIS Controls v8 Mappings

Download individual mappings below or visit our CIS Controls Navigator for all mappings to CIS Controls v8.

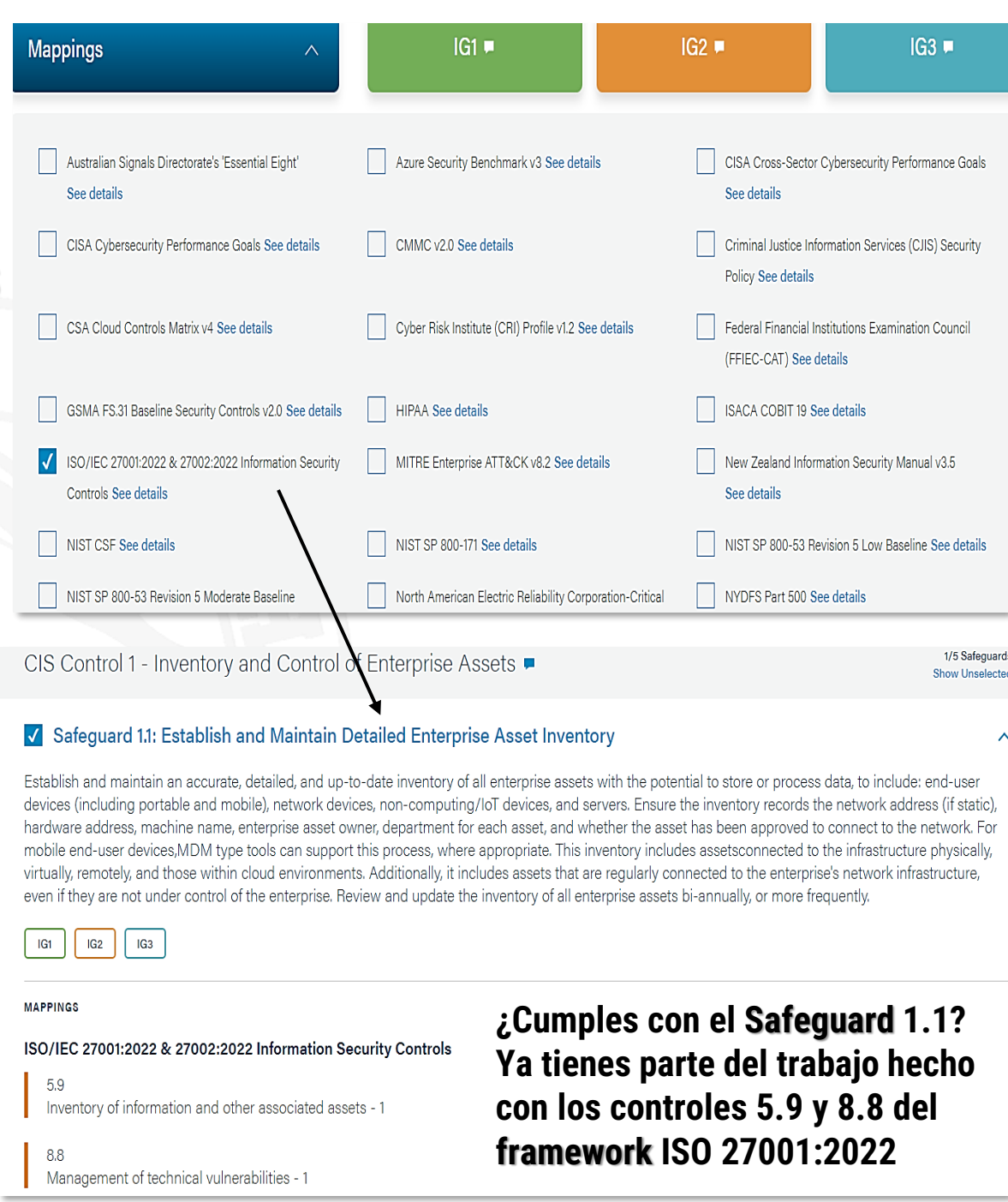
- AICPA Trust Services Criteria (SOC2)
- ASD's Essential Eight
- Azure Security Benchmark
- CISA's Cross-Sector CPGs
- CMMC Cybersecurity Maturity Model Certification v2.0
- CRI Profile v1.2
- Criminal Justice Information Services
- CSA CCM Cloud Security Alliance Cloud Control Matrix
- Cyber Essentials v2.2
- FFEIC-CAT
- GSMA FS.31 Baseline Security Controls
- HIPAA Health Insurance Portability and Accountability Act of 1996
- ISACA COBIT 19
- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- MITRE Enterprise ATT&CK v8.2
- NCSC Cyber Assessment Framework v3.1
- NERC-CIP
- New Zealand Information Security Manual (NZISM) v3.5
- NIST CSF
- NIST Special Publication 800-53 Rev.5 (Moderate and Low Baselines)
- NIST Special Publication 800-171 Rev.2
- NYDFS Part 500
- PCI Payment Card Industry v4.0
- TSA Security Directive Pipeline 2021-02

Mapeos de los CSC Controls v8 a otros frameworks:
https://www.cisecurity.org/controls/v8

De los CIS CSC Controls a los Security Frameworks

Seguridad de Sistemas Informáticos

- **Como CIS ayuda a cumplir con frameworks de seguridad está documentado**
  - Existe un mapeo entre CSC Controls y Safeguards a los elementos usados por otros frameworks
    - https://www.cisecurity.org/controls/cis-controls-navigator
- **De esta forma**
  - Los controles técnicos de los Benchmarks CIS mejoran la seguridad del software
  - Una vez implementados, se calcula cuántos CSC Controls y Safeguards están cubriendo
  - Luego se pueden **mapear** al marco de ciberseguridad que desea implementarse
    - De esta manera, el trabajo se puede traducir a cualquiera de esos frameworks
  - Así se implementa un SGSI más fácilmente
    - Veremos qué son en la sección siguiente



¿Crees que lo has entendido todo? ¡Autoevalúate!

?

- **Eres capaz de hacer lo siguiente**
  - *Entender que los controles CSC son siempre los mismos para cualquier **software**, y que son un nivel de abstracción más que los controles técnicos como los **CIS Benchmarks***
  - *Tener claro dónde puedes encontrar la relación de un control técnico con su control CSC asociado*
  - *Entender la relación que hay entre los controles técnicos CIS y los **Safeguards***
  - *Comprender el concepto de **Safeguard** y su relación con los **CSC Controls***
  - *Tienes claro qué es cada **Implementation Group**, qué significan, como se usan y quien elige en cuál esta cada organización que los aplica*
    - *Incluida su relación con los **Safeguards** de los controles CSC*
  - *Entiendes cómo se puede pasar de los controles técnicos de seguridad CIS a los **Safeguards**, de ahí a los **CSC Controls** y, gracias a estos últimos, poder implementar parcialmente los controles de muchos **frameworks** de seguridad usados actualmente*
    - *Entendiendo así por tanto que todo el trabajo hecho en consola (manual o automatizado) puede ser usado en niveles de abstracción superiores*

< Ir al índice

Fuente: Bing Chat AI

Cómo implementarlo >

IMPLEMENTACIÓN DE UN SGSI

¿Qué es un Sistema de Gestión de la Seguridad de la Información?

*Iconos por Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

- **En este bloque aprenderás**
  - Qué es exactamente un **SGSI** y las ventajas que tiene implementar uno
  - Qué significa **implementar un SGSI** y sus controles de seguridad
  - Que hay varios **estándares de seguridad** y que el ISO 27000 es uno reconocido internacionalmente
  - Y sobre el **estándar ISO 27000:2022** específicamente...
    - Qué son los estándares 27001 y 27002 y cómo se relacionan entre ellos
    - Cómo es la estructura de un control de seguridad de la ISO 27002:2022

De controles de seguridad a metodologías

Seguridad de Sistemas Informáticos

Usar una **Metodología de Auditoría de Seguridad** (como **OSSTMM**) para revisar la seguridad de los sistemas y el cumplimiento de **frameworks** de seguridad implementados

5

Gestionado por

Asignar los controles y **Safeguards** implementados a un **Framework de Seguridad** internacional reconocido (**ISO 27001**, **PCI-DSS**…) para facilitar la implementación de un **SGSI**

4

Mapea a

Usar **Implementation Groups** (solo 3) para implementar solo los **Safeguards** más adecuados a un escenario particular según los recursos disponibles

3

Se pueden distribuir en

Agrupar los controles de seguridad implementados en **CIS Critical Security Controls** (**CSC**) y **Safeguards**

2

Se pueden agrupar en

Verificar e implementar **Controles técnicos de seguridad** adecuados y validados en un producto de software / SO de forma altamente **automatizada** (varios cientos de controles)

1

Nivel de Abstracción

+

-

Sistema de Gestión de la Seguridad de la Información (SGSI)

- **La gestión de la seguridad debe hacerse**
  - Con un proceso **sistemático**, **documentado** y **conocido**
  - **Aceptado** en toda la empresa (sin exclusiones, sin importar la experiencia, la posición...)
- **El proceso de gestión se llama Sistema de Gestión de la Seguridad de la Información** (SGSI)
  - Information Security Management System, ISMS
- **Su objetivo es**

  *"Garantizar que los **riesgos** para la seguridad de la información son **conocidos**, **asumidos**, **administrados** y **minimizados** por la empresa, que utiliza un procedimiento documentado, sistemático, estructurado, repetible y eficiente, que también debe adaptarse para responder **a los cambios de los riesgos, entorno y tecnología**"*
- **La garantía total NUNCA es posible**
  - Pero asegura que la empresa está preparada para asumir la **pérdida de CIA** de la información

Competencias que debe cumplir cualquier estándar para implementar un SGSI

Elementos de un SGSI

- Son necesarios para su implementación: una **política de seguridad**, **estructura organizativa**, **procedimientos**, **procesos** y **recursos**
- Implementar un SGSI significa que una empresa ha
  - **Estudiado** los riesgos a los que está sometida toda su información
  - **Evaluado** qué nivel de riesgo asume
  - **Implementado controles** (no sólo tecnológicos, sino también organizativos)
    - Para aquellos riesgos que superan dicho nivel
  - **Documentado** las políticas y procedimientos relacionados
  - Entrado en un proceso continuo de **revisión y mejora** de todo el sistema
- Los SGSI se implementan por medio de estándares que garanticen las propiedades de la imagen anterior como, por ejemplo
  - **El framework ITIL** (Information Technology Infrastructure Library, mencionado en DPPI)
  - **El framework COBIT** (Control Objectives for Information and Related Technologies):
    - https://www.isaca.org/resources/cobit
  - La **familia de estándares ISO 27000** (vistas en la sección siguiente)

Estándares para implementar un SGSI

Seguridad de Sistemas Informáticos

- **Estándares hay muchos, e implementar uno u otro depende del contexto**
  - Objetivos a lograr
  - País en el que esté la empresa
    - Ej.: En EEUU es muy probable que se pida usar los estándares del NIST
  - Las certificaciones que nos pidan nuestros potenciales clientes
- **La ventaja del ISO 27000 es que es de adopción internacional**

COBIT	ISO 27001	NIST
Control Objectives for Information and Related Technologies	**International Organization for Standardization**	**National Institute of Standards and Technology**
It's a framework developed by ISACA that focuses on governance and management of information & technology. It provides a set of control objectives to help organizations achieve their business objectives through effective management and governance of their IT assets.	It's a global standard for Information Security Management Systems (ISMS). It outlines the criteria for establishing, implementing, maintaining, and continually improving an information security management system. The standard includes a set of controls that organizations can implement to manage information security risks.	The NIST Cybersecurity Framework provides a set of guidelines and best practices for organizations to manage and improve their ability to prevent, detect, respond to, and recover from cybersecurity events. It is widely used in the United States and has been adopted globally.
FOCUS : Business and IT Governance. Emphasizes information governance and process improvement	**FOCUS :** Information security systems. Systematic approach to managing sensitive company information	**FOCUS :** Cybersecurity and Risk Management. Emphasizes continuous monitoring and risk assessment
PURPOSE : Aligning business goals with IT functions and ensuring effective risk management	**PURPOSE :** Establishing, implementing, maintaining, and improving an information security management system	**PURPOSE :** Providing a flexible and comprehensive approach to managing and mitigating cybersecurity risk
APPLICABILITY : Broad spectrum, suitable for all organization sizes	**APPLICABILITY :** Globally recognized, suitable for any organization	**APPLICABILITY :** Widely used in the United States, adopted globally
KEY FUNCTIONS : Control objectives, Risk management, Information governance, Process improvement, IT alignment	**KEY FUNCTIONS :** Risk assessment, Security policy, Access control, Cryptography, Incident response, Continual improvement	**KEY FUNCTIONS :** Identify, Protect, Detect, Respond, Recover, Continuous monitoring

VENTAJAS DE LA IMPLEMENTACIÓN DE UN SGSI

- **Reducción de riesgos** al seguir sus controles de supervisión
  - Las amenazas se reducen; los daños, si los hay, se minimizan
- **Ahorro de costes** debido a la optimización del uso de recursos
  - La estimación de los riesgos reduce el riesgo de inversiones innecesarias e ineficientes
- La seguridad de la empresa tiene **un ciclo de vida metódico y controlado** en el que participa toda la organización
- **Cumplimiento del marco legal** que protege a la organización (**ASLEPI**)
  - https://www.agpd.es/portalwebAGPD/canalresponsable/obligaciones/medidas_seguridad/index-ides-idphp.php
  - http://administracionelectronica.gob.es/ctt/ens
- **Mejora la competitividad en el mercado**: las administraciones públicas suelen exigir certificaciones de seguridad a empresas
  - Cuando compiten en concursos públicos de servicios relacionados con sistemas de información
  - El CCN CERT exige el cumplimiento del ENS que vimos al software de las AAPP Españolas

La norma internacional ISO 27001:2022/27002:2022

Un marco internacional para implementar un SGSI

Fuente: Bing Chat AI

*Icono oficial de la organización ISO

ISO (International Organization for Standardization) / IEC (International Electrotechnical Commission) 27000

- **Marco de gestión de la seguridad de la información** para cualquier organización compuesto por varias normas, como la **ISO/IEC 27001** y la **27002**
  - Contiene los requisitos para establecer, implementar, operar, monitorizar, mantener y mejorar un SGSI
  - La única norma de la familia 27000 que es **certificable** una vez implementada **es la 27001**
  - La 27001 es un **estándar de gestión** que recopila
    - Los **componentes** del sistema
    - Los **documentos mínimos** que forman parte de él
    - Los **registros** (logs) de información,
    - Los **controles de seguridad** a implementar (**93 en total,** listados **en el Anexo A de la norma**)
      - Contiene la visión general básica de los controles de seguridad necesarios para implementar un SGSI
    - Las **medidas de seguridad adaptadas** a las necesidades de cada organización
- En España, **AENOR** es la principal agencia de certificación
  - Asociación Española de NORmalización y certificación http://www.aenor.es/aenor/inicio/home/home.asp

El Anexo A de la norma 27001:2022

Seguridad de Sistemas Informáticos

- **Divide en 4 capítulos sus 93 controles de seguridad**
  - Controles **organizacionales** (37)
  - Controles de **personas** (8)
  - Controles **físicos** (14)
  - Controles **tecnológicos** (34)
- **Evolución de la 27001:2013**
  - **Descripción detallada** (gratuita):
    - https://normaiso27001.es/
  - **Más información**
    - https://www.escuelaeuropeaexcelencia.com/2022/11/publicada-la-nueva-iso-270012022-novedades-del-estandar-de-seguridad-de-la-informacion/
    - https://blog.innevo.com/iso27001-2022

ISO 27001 and ISO 27002. Information security controls, 2022

5. Organizational controls	6. People controls	8. Technological controls
5.1. Policies for information security	6.1. Screening	8.1. User endpoint devices
5.2. Information security roles and responsibilities	6.2. Terms and conditions of employment	8.2. Privileged access rights
5.3. Segregation of duties	6.3. Information security awareness, education and training	8.3. Information access restriction
5.4. Management responsibilities	6.4. Disciplinary process	8.4. Access to source code
5.5. Contact with authorities	6.5. Responsibilities after termination or change of employment	8.5. Secure authentication
5.6. Contact with special interest groups	6.6. Confidentiality or non-disclosure agreements	8.6. Capacity management
5.7. Threat intelligence	6.7. Remote working	8.7. Protection against malware
5.8. Information security in project management	6.8. Information security event reporting	8.8. Management of technical vulnerabilities
5.9. Inventory of information and other associated assets	**7. Physical controls**	8.9. Configuration management
5.10. Acceptable use of information and other associated assets	7.1. Physical security perimeter	8.10. Information deletion
5.11. Return of assets	7.2. Physical entry	8.11. Data masking
5.12. Classification of information	7.3. Securing offices, rooms and facilities	8.12. Data leakage prevention
5.13. Labelling of information	7.4. Physical security monitoring	8.13. Information backup
5.14. Information transfer	7.5. Protecting against physical and environmental threats	8.14. Redundancy of information processing facilities
5.15. Access control	7.6. Working in secure areas	8.15. Logging
5.16. Identity management	7.7. Clear desk and clear screen	8.16. Monitoring activities
5.17. Authentication information	7.8. Equipment siting and protection	8.17. Clock synchronization
5.18. Access rights	7.9. Security of assets off-premises	8.18. Use of privileged utility programs
5.19. Information security in supplier relationships	7.10. Storage media	8.19. Installation of software on operational systems
5.20. Addressing information security within supplier agreements	7.11. Supporting utilities	8.20. Network security
5.21. Managing information security in the ICT supply chain	7.12. Cabling security	8.21. Security of network services
5.22. Monitoring, review and change management of supplier services	7.13. Equipment maintenance	8.22. Segregation of networks
5.23. Information security for use of cloud services	7.14. Secure disposal or re-use of equipment	8.23. Web filtering
5.24. Information security incident management planning and preparation		8.24. Use of cryptography
5.25. Assessment and decision on information security events		8.25. Secure development life cycle
5.26. Response to information security incidents		8.26. Application security requirements
5.27. Learning from information security incidents		8.27. Secure system architecture and engineering principles
5.28. Collection of evidence		8.28. Secure coding
5.29. Information security during disruption		8.29. Security testing in development and acceptance
5.30. ICT readiness for business continuity		8.30. Outsourced development
5.31. Legal, statutory, regulatory and contractual requirements		8.31. Separation of development, test and production environments
5.32. Intellectual property rights		8.32. Change management
5.33. Protection of records		8.33. Test information
5.34. Privacy and protection of PII		8.34. Protection of information systems during audit testing
5.35. Independent review of information security		
5.36. Compliance with policies, rules and standards for information security		
5.37. Documented operating procedures		

*New control, 2022

by Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001 - www.patreon.com/AndreyProzorov

Control: measure that maintains and/or modifies risk

Aquí vemos los 93 controles de seguridad de la ISO 27001 divididos en sus 4 capítulos. Fuente: https://twitter.com/hackinarticles/status/1714682070960615761

¿Qué es la norma ISO 27002:2022?

- **Es un complemento a la ISO 27001**
  - No es una norma de gestión, sino un **conjunto de directrices y buenas prácticas**
  - Explican **cómo implementar** los controles de seguridad contenidos en el Anexo A de la ISO 27001
- **No ser una norma de gestión implica qué**
  - Explica todos los controles del Anexo A **sin importar si una organización los necesita o no**
  - Es **mucho más detallada y precisa**
    - Y por eso ayuda a comprender si una organización debe aplicar o no ciertos controles de seguridad
  - Las organizaciones **NO** pueden certificarse contra la ISO 27002, sólo la ISO 27001
  - O más bien con la aplicación de la ISO 27001 que haya hecho
    - Una vez examinados todos los controles y **decidido cuáles tiene sentido pueden aplicar**

Obviamente, la ISO 27002:2022 usa la misma división en 4 capítulos que la ISO 27001:2022 a la que complementa. Fuente: https://twitter.com/Marce_I_P/status/1681992650751111169

¿Cómo es un control de seguridad de la ISO 27002:2022?

Seguridad de Sistemas Informáticos

- **NO SON** controles de carácter técnico
  - No proporcionan ese tipo de detalles, a diferencia de los controles de los Benchmarks CIS o STIGs
- Cada control hace una descripción general
  - Son **flexibles** en cuanto a su implementación
  - **Dependiendo de las necesidades** de la organización (tamaño, información manejada, requisitos legales...)
  - Cada control está justificado con una **tabla de 5 atributos asociados**
    - Los veremos en la siguiente transparencia
- La versión 2022 es de pago y no se puede consultar libremente
  - Podemos hacernos una idea de cómo son los controles por los de su versión anterior
  - Aquí: https://normaiso27001.es/a9-control-de-acceso/#

Objetivo 1:
Requisitos de negocio para el control de acceso

Limitar el acceso a la información y a las instalaciones de procesamiento de información.

Controles:

- 9.1.1 Política de control de acceso
- 9.1.2 Acceso a las redes y a los servicios de red

Objetivo 2:
Gestión del acceso de usuarios

Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios de información.

Controles:

- 9.2.1 Registro de usuarios y cancelación del registro
- 9.2.2 Gestión de acceso a los usuarios
- 9.2.3 Gestión de derechos de acceso privilegiados
- 9.2.4 Gestión de la información de autenticación secreta de los usuarios
- 9.2.5 Revisión de derechos de acceso de usuario
- 9.2.6 Remoción o ajuste de los derechos de acceso

Objetivo 3:
Responsabilidades del usuario

Hacer a los usuarios responsables de salvaguardar su información de autenticación.

- 9.3.1 Uso de la información de autenticación secreta

Objetivo 4:
Responsabilidades del usuario

Impedir el acceso no autorizado a los sistemas y las aplicaciones.

- 9.4.1 Restricción de acceso a la información
- 9.4.2 Procedimientos de conexión (log-on) seguros
- 9.4.3 Sistema de gestión de contraseñas
- 9.4.4 Uso de programas de utilidad privilegiados
- 9.4.5 Control de acceso al código de programas fuente

Un control de la ISO27002:2013 da una idea de cómo son los controles de la 2022: Objetivos generales y explicación abierta, adaptable a las necesidades de las empresas

ATRIBUTOS DE UN CONTROL DE LA ISO 27002:2022

Seguridad de Sistemas Informáticos

- **Cada control tiene 5 atributos**
  - **Control type** (Preventive, Detective, Corrective)
  - **Information security Properties** (CIA, **Tema 2**)
  - **Cybersecurity concepts** (siguiente página)
  - **Operational Capabilities** (15 distintas, ver imagen)
  - **Security domains** (4 distintos)

Operational capabilities de un control ISO 27002:2022.
Fuente: https://twitter.com/Marce_I_P/status/1663694032164225027

5.1 Policies for information security

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Resilience

Control

Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

Purpose

To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business, legal, statutory, regulatory and contractual requirements.

- **Security Domains**
  - Governance and Ecosystem
  - Protection
  - Defense
  - Resilience

Cabecera del control 5.1 de la ISO 27002:2002. Fuente: https://es.slideshare.net/AndreyProzorov/iso-270012022-what-has-changedpdf

Atributos de un control de la ISO 27002:2022

- No todos los controles sirven para lo mismo
- Unos son más “pasivos” (identificar, detectar, proteger)
  - Impiden que los incidentes de seguridad ocurran
- Y otros más “reactivos” (responder y recuperar)
  - Actúan cuando los incidentes de seguridad ya han ocurrido

¿CREES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

?

- **Eres capaz de hacer lo siguiente**
  - *Entender los objetivos para una organización de implementar correctamente un SGSI*
    - *Y sus ventajas, tanto a nivel interno como a nivel de reputación*
  - *Comprender que implementar un SGSI implica que la organización ha estudiado y evaluado sus riesgos, implementado controles (tecnológicos u organizativos) para los que considera más críticos y documentado sus procedimientos*
    - *Y también se ha comprometido a hacer un proceso de revisión y mejora continua*
  - *Tener claro que existen varios estándares para implementar un SGSI y que el ISO 27000 es uno de ellos*
  - ***Sobre el estándar ISO 27000...***
    - *Entender que el ISO 27001 es un estándar de gestión y que como tal te puedes certificar contra él*
      - *Pero no contiene información detallada de los controles de seguridad*
      - *Y que es el estándar ISO 27002, complementario al primero, el que tiene esa información*
    - *Tener claro que los controles se organizan en cuatro grupos y que, a diferencia de los vistos en el CIS, son de un carácter más abstracto (afectan a la organización, las personas...) y no de tipo técnico*
      - *Y que por ese motivo es posible mapearlos a los CSC vistos*
    - *Comprender que cada control tiene atributos que los clasifican y organizan para así poder implementarlos de acuerdo a prácticamente cualquier criterio que la organización necesite*
    - *Entender que, a nivel más abstracto, además de controles generales, puedes encontrar controles centrados en diferentes acciones que deben tener lugar en el transcurso de un ataque*
      - *Identificar objetivos, protegerse, detectar actividades, responder a los problemas y recuperarse de los daños*

Cómo se implementa un SGSI

Ejemplo con las normas internacionales ISO 2700X:2022

*Iconos por Bing Chat AI

Fuente: Bing Chat AI

¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

En este bloque aprenderás

- Qué es el **ciclo de Deming** a la hora de implementar un SGSI y sus 4 distintas fases
- Qué se hace en cada **fase** de ese ciclo exactamente
- La enorme importancia de tener un buen **inventario de activos** de una organización
- Como **gestionar los riesgos** de una empresa a nivel general
- Que la implementación de un SGSI es un ciclo de **mejora continua**

Fases de implementación de un SGSI (ciclo de Deming)

Seguridad de Sistemas Informáticos

- La norma ISO 27001 proporciona un marco para implementar un SGSI en cuatro fases
  - **PLAN** (**Planificar**): Establecer el SGSI
  - **DO** (**Hacer**): Implementarlo y usarlo
  - **CHECK** (**Verificar**): Supervisarlo, revisarlo y verificarlo
  - **ACT** (**Actuar**): Mantenimiento y mejora del SGSI

Fuente: http://www.iso27000.es/sgsi_implantar.html

Basado en la filosofía "Kaizen" de mejora continua: https://es.wikipedia.org/wiki/Kaizen

PLAN: DEFINIR LOS LÍMITES DEL SGSI

- El diseño del SGSI depende de los **objetivos**, **requisitos** y **estructura** de la organización
- Esto define las áreas involucradas en el despliegue del SGSI
  - Un solo departamento, ciertos edificios, algunas áreas de negocio...
- El tiempo de implementación no es fácil de predecir (normalmente 6 meses - 1 año) debido a
  - Tamaño de la organización
  - Estado de seguridad inicial
  - Inversión de recursos en la implementación del SGSI

PLAN: DEFINIR LOS LÍMITES DEL SGSI. EJEMPLO

- Una empresa de impresión 3D de piezas industriales
- 800 empleados (operadores, administrativos...)
- Varios departamentos
  - **Gestión de nóminas**: 4 empleados
  - **Recursos Humanos** (RRHH): 3 empleados
  - **Sistemas**: 5 empleados
  - **Diseño**: 8 empleados
  - **Producción**: resto de empleados
- El SGSI sólo es realmente necesario en departamentos que manejan información sensible
  - Gestión de nóminas, recursos humanos, sistemas y diseño
  - ¡20 empleados + CEO solamente!

Fuente: https://www.pexels.com/es-es/foto/edificio-blanco-15120-269077/

PLAN: DEFINIR LA POLÍTICA DE SEGURIDAD

- **Directrices y objetivos generales de la empresa** relacionados con la seguridad
  - Escritos formalmente y aprobados por la dirección de la misma
- **Las políticas deben expresar claramente sus objetivos**
  - Frecuentemente involucran a muchas personas durante su creación y mantenimiento
- **Incluye**
  - **Objetivos y alcance** general de seguridad
  - **Apoyo expreso de la dirección** (CEO / gestión)
  - Explicación de los **valores de seguridad** de la organización
  - **Definición de las responsabilidades** generales y específicas en materia de gestión de la seguridad de la información
  - **Referencias a documentos** que puedan respaldar la política

PLAN: DEFINIR LA POLÍTICA DE SEGURIDAD. EJEMPLO

Objetivo:
Definir las pautas de propósito general para asegurar una adecuada protección de la información del DAPRE.
Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.

Aplicabilidad:
Estas son políticas que aplican a la Alta Dirección, Ministros Consejeros, Consejeros Presidenciales, Directores, Secretarios, Jefes de Oficina, Jefes de Área, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales del DAPRE.

Directrices:

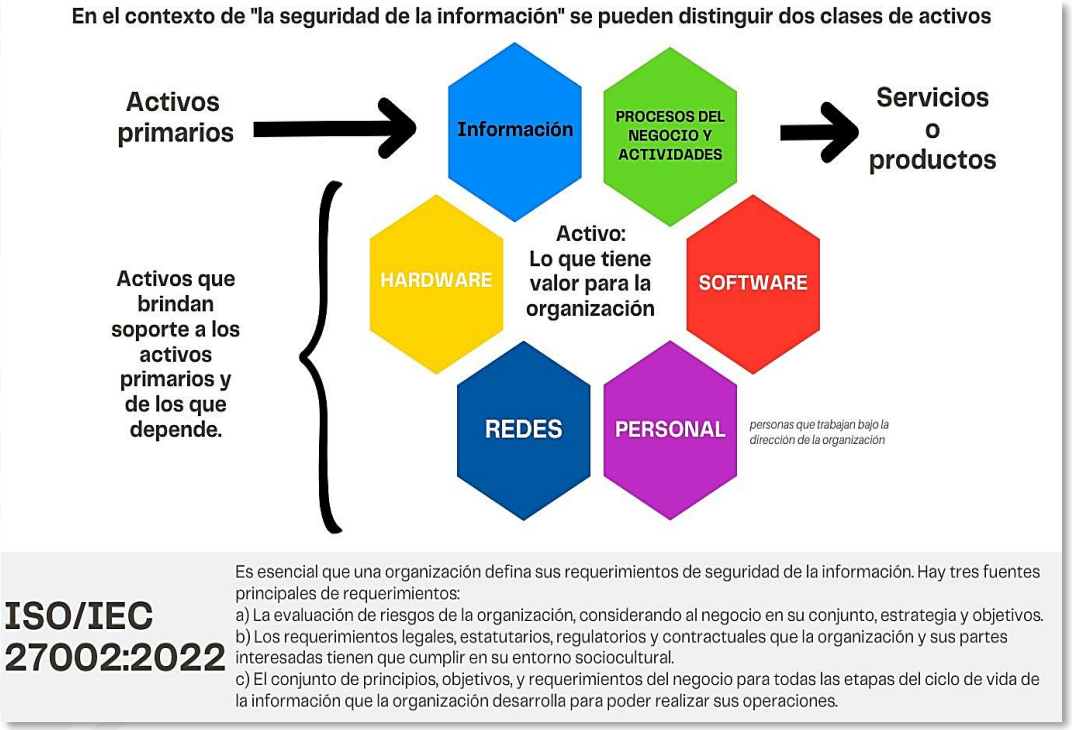
- Se debe verificar que se definan, implementen, revisen y actualicen las políticas de seguridad de la información.
- Diseñar, programar y realizar los programas de auditoría del sistema de gestión de seguridad de la Información, los cuales estarán a cargo de control interno.
- Todo aplicativo informático o software debe ser comprado o aprobado por el Área de Información y Sistemas en concordancia con la política de adquisición de bienes de la entidad de acuerdo con lo definido en el proceso **C-BS-07 Adquisición de Bienes y Servicios.**
- El DAPRE debe contar con un firewall o dispositivo de seguridad perimetral para la conexión a Internet o cuando sea inevitable para la conexión a otras redes en outsourcing o de terceros.
- La conexión remota a la red de área local del DAPRE debe realizarse a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada, a excepción de los casos que autorice el Área de Información y Sistemas.
- Los jefes de área o dependencia deben asegurarse de que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad se realizan correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información del DAPRE

Fuente: http://wp.presidencia.gov.co/sitios/dapre/sigepre/manuales/M-TI-01%20Manual%20general%20Sistema%20de%20Seguridad%20de%20la%20Informacion.pdf

PLAN: DEFINIR ACTIVOS

- **Recursos clave** para garantizar el correcto funcionamiento de la organización
- Son cualquier cosa lo suficientemente valiosa como para ser protegida
  - Información
  - Edificios
  - Sistemas informáticos y redes
  - Aplicaciones
  - Bases de datos
  - Medios de almacenamiento
  - ... (ver imagen)

Activos de la ISO 27002:2022. Fuente: https://twitter.com/Marce_I_P/



- La definición de activos debe incluir
  - Un **inventario**: Descripción, localización, propietario...
  - Análisis de **dependencias** entre activos
  - Una **clasificación / valoración** del activo, dependiendo de lo relevante que sea y del impacto potencial que pueda tener si se produce algún incidente sobre él

PLAN: DEFINIR ACTIVOS. EJEMPLO

- **Típico inventario de activos**

Fuente: https://www.metrici.com/metrici/forum/threads/Thread4

ISMS.online Search Home You Work David

Tracks ▸ Information Asset Inventory (ISO 27001)

Information Asset Inventory (ISO 27001)

Linked work Team Settings Tour

Showing: 16 of 16 Summary value £0.00 (from total £0.00)

View Archive View Updates feed View Stats New Item

Assigned to: All Team Members Category: Status All Statuses View: Columns List

Name	Status	Primary Location	Legal Owner	Classification	Owner/Lead	Type	Assigned To	Due
2 - Laptops: company provided	Live	Company Office On Person Teleworker (Home)	Company	Commercial in Confidence	CTO	Processing Devices	David Kelly	07/01/19 11:00
7 - Brand	Live	Everywhere	Company	Commercial in Confidence	CMO (marketing)	Sales & Marketing IPR	David Kelly	07/01/19 12:00
8 - Company financial data	Live	Company Office	Company	Commercial in Confidence	FD	Financial information	Karen Arnold	07/01/19 14:00
13 - Product X code base	Live	Third Party Datacentre	Company	Infrastructure Critical	CEO	Products & Services Infrastructure IPR	Gill Smith	07/01/19 14:00
9 - Product marketing materials (published)	Live	Everywhere	Company	Public	CMO (marketing)	Products & Services Sales & Marketing IPR		07/01/19 18:00
1 - Staff personal data	Resolved	Company Office	Company	Commercial in Confidence	HR	Personal Data		
3 - Laptops: Infrastructure Critical focused	To-do							
4 - Laptops: BYOD (employee)	To-do							
5 - Mobile Phones: company provided	To-do							
6 - Mobile Phones: BYOD (employee)	To-do							

Other Location

Legal Owner
- Company
- Employee (inc.BYOD)
- Supplier
- Customer
- Other

Classification
- Infrastructure Critical
- Commercial in Confidence
- Public
- Unknown

Owner/Lead
- CEO
- DPO

Uncategorised

Clear all options Apply filter

PLAN: ANÁLISIS DE RIESGOS

- **Probabilidad de que una amenaza pueda explotar una vulnerabilidad** y causar daños o pérdida total de un activo
- Por lo general se expresan combinando la probabilidad de un evento y sus consecuencias
- Hay varias metodologías de evaluación y análisis de riesgos hoy en día
  - El estándar ISO 27001 no obliga a utilizar uno concreto
  - MAGERIT se utiliza comúnmente en la administración española
- Este es sólo un breve resumen de algo que se analizará con más detalle en otra asignatura (DPPI)

PLAN: ANÁLISIS DE RIESGOS

- Para calcular **niveles de riesgo de activos identificados** tenemos que
  - Identificar **amenazas** a los activos cubiertos por el SGSI
  - Identificar **vulnerabilidades** que podrían ser explotadas por las amenazas
  - Identificar y evaluar el **impacto** (coste) que puede tener un fallo de seguridad en un activo
  - Evaluar la **probabilidad de fallo**
    - Teniendo en cuenta los 3 elementos anteriores
  - Calcular **niveles de riesgo** utilizando u método objetivo
  - Determinar si el riesgo calculado es **aceptable** o se requiere alguna acción

AMENAZA	VULNERABILIDAD
Ataque por una organización o individuo cibercriminal	Un problema de configuración permite la conexión a servicios privados evadiendo reglas del firewall
	XSS por falta de validación adecuada que lleva a ejecución de scripts
	XST causado por un error de filtrado y usar el verbo HTTP TRACE
Sobrecalentamiento de equipo	No hay monitorización de temperatura
Datos filtrados en un servidor	Instalación Tomcat por defecto
Incendio	No hay extintores en el edificio

Activo	Amenaza	Vulnerabilidad	Impacto			Probabilidad	Riesgo	Clasificación del riesgo
			Confidencialidad	Integridad	Disponibilidad			
Portátil	Robo	Portabilidad	2	3	1	1	3	
Servidor ficheros	Malware	Falta de actualizaciones	3	3	3	1	4	
Contrato cliente	Robo	No hay caja fuerte	4	4	1	2	5	
Datos cliente	Filtrado	No se autentica el acceso	5	4	3	2	6	

PLAN: GESTIÓN DE RIESGOS

- **Identificar y evaluar alternativas para tratar los riesgos** con cualquiera de los siguientes objetivos
  - **Eliminar** el riesgo
    - Ej.: eliminar un servidor obsoleto
  - **Mitigar** el riesgo
    - Ej.: aplicar controles técnicos de seguridad para eliminarlo
  - **Transferir la gestión de riesgos** a un agente externo
    - Ej.: subcontratar el servicio de mantenimiento de los servidores
  - **Asumir** el riesgo (no puedes tratarlo en estos momentos)

- El **riesgo residual** (el existente tras implementar las medidas) debe analizarse
- La implementación de los controles de la ISO 27001 depende del resultado de la evaluación de riesgos de la organización
  - La norma solo requiere que la organización implemente **los que sean realmente necesarios**
  - De acuerdo con los riesgos identificados, su **impacto** y su **probabilidad** de fallo

PLAN: DEFINIR CONTROLES Y PROCEDIMIENTOS

Seguridad de Sistemas Informáticos

- **Control**
  - Medidas, acciones y documentos que permitan auditar y cubrir un riesgo
- **Procedimiento**
  - Instrucciones de implementación de tareas / procesos de un control
  - Establece los pasos a seguir para implementar las tareas de forma concisa
- **Declaración de aplicabilidad / Statement Of Applicability (SOA)** con
  - Los **objetivos** de control
  - Los que **se han elegido** del estándar
  - **Por qué** se han elegido esos controles
  - **Las medidas de seguridad** adoptadas

Antes de la auditoría de certificación, una organización debe haber producido una Declaración de Aplicabilidad (SOA).

El requisito se describe en la ISO 27001. La SOA debe contener al menos 93 entradas con cada una de las categorías y controles enumerados. Una vez hecho esto, cada control debe ser seleccionado y justificado o excluido con una justificación similar. Todos los documentos SoA deben poder demostrar que se ha tenido en cuenta cada control. Esto significa que un SoA debe contener todas las entradas descritas, enumerando simplemente los controles seleccionados que no cumplan con el requisito.

Este ejemplo muestra cómo se podría presentar una diferencia entre un control seleccionado y excluido dentro de un SoA:

Declaración de aplicabilidad

Leyenda (para los controles seleccionados y razones por las que se han elegido)

Actual a fecha de

Versión Fecha-del-documennto

Controles ISO 27001				Controles actuales	Observacionnes (incluyendo justificación de la exclusión)	Observaciones (Resumen de la implemenntación)
Claúsula	**Sec**	**Control**	**Objetivo/Control**			
	9.4.2	Procedimientos de logon seguros	Cuando lo exija la política de control de acceso, el acceso a los sistemas y aplicaciones se controlará mediante un procedimiento de inicio de sesión seguro.	**Política**	Se requiere un inicio de sesión seguro para todos los sistemas y el acceso a las aplicaciones.	Documento Organizaciones ISMS Manual e Índice versión 1, de fecha 2 de agosto 2020, da orientaciones
	9.4.3	Sistema de gestión de passwords	Los sistemas de gestión de contraseñas deben ser interactivos y garantizar contraseñas de calidad.	**Política**	Todos los sistemas, plataformas y aplicaciones requieren contraseñas	La versión 1 de la política de contraseñas de las organizaciones para documentos, de fecha 2 de agosto del 2020, da orientaciones
	9.4.4	Uso de programas de utilidad privilegiados	El uso de programas de utilidad que puedan ser capaces de anular los controles del sistema y de la aplicación debe restringirse y controlarse estrictamente	**Exento**	No se usan programas de utilidad	
	9.4.5	Control de acceso al código fuente de programas	El acceso al código fuente de programas estará restringido	**Exento**	No se usa ningún código fuente del programa.	
	A.10	**Criptografía**				
	10.1	Controles de criptografía	**OBJETIVO**: Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad			

Un SOA para para la ISO 27001:2013, pero sirve perfectamente de ejemplo para la norma 2022. Fuente: https://www.nqa.com/es-es/certification/standards/iso-27001/implementation

PLAN: ¿QUÉ ES EXACTAMENTE EL SOA?

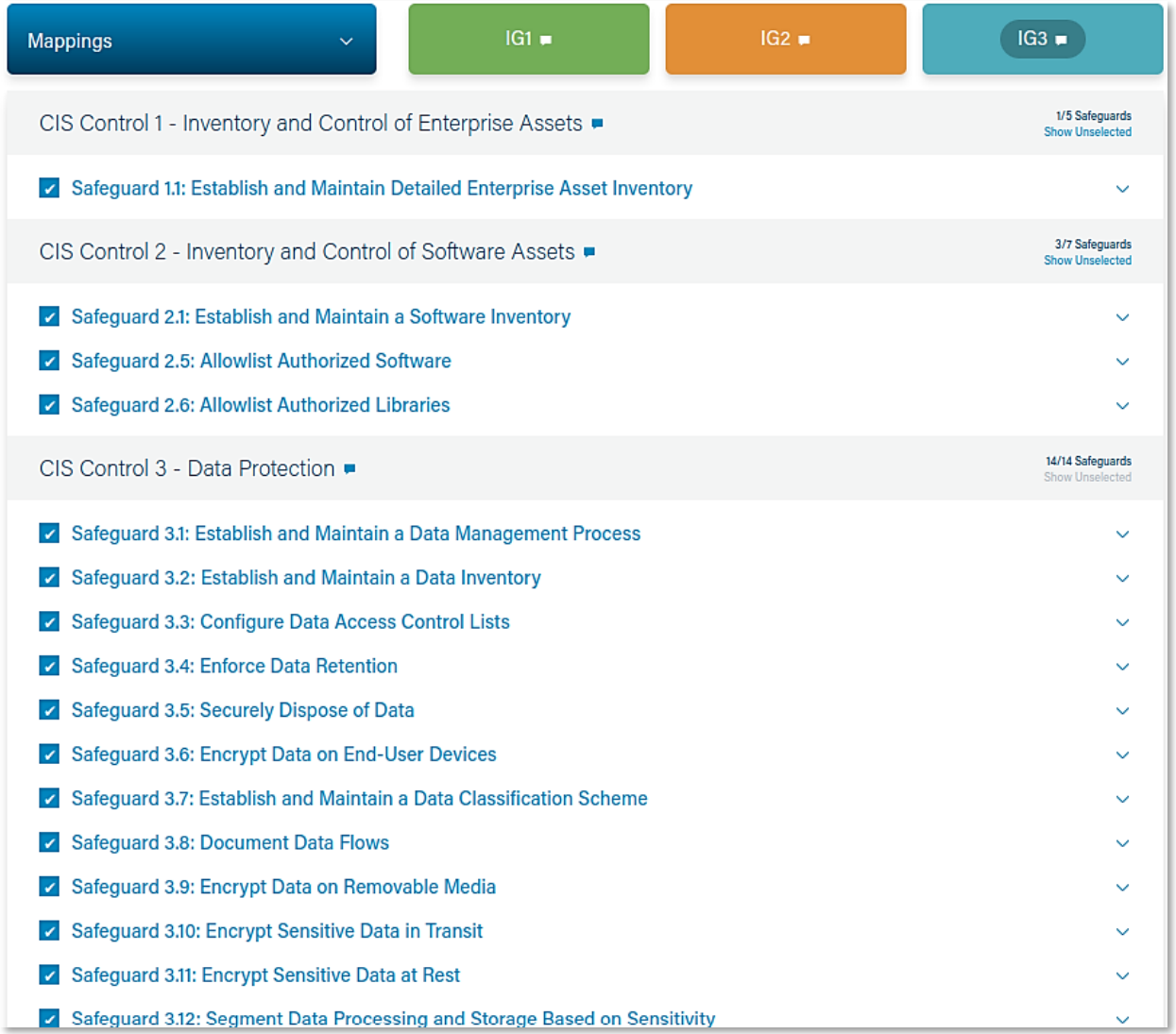
- **Tras el análisis y evaluación de riesgos, se debe definir las opciones para tratarlos**
  - Y aplicar las medidas de seguridad para mitigarlos
- **Es ahora cuando se define el SoA, que es un documento clave en la ISO 27001**
  - Contiene una **lista completa de los controles de seguridad del Anexo A** vistos
  - Para cada uno, **se indica si es aplicable** o no
    - Detallando los motivos y su estado de implementación
    - Puede **añadir otros controles** y objetivos de un control si se considera necesario
    - **Recuerda**: la norma es flexible y se adapta a las necesidades y particularidades de la organización
  - El SoA permite la **trazabilidad entre los controles**
    - Y una visión amplia de lo que está realizando la organización para proteger su información
    - Contribuyendo a la identificación, organización y registro de las medidas de seguridad implantadas

PLAN: DEFINIR CONTROLES Y PROCEDIMIENTOS DE IMPLEMENTACIÓN

- **Ahora que ya tenemos los controles ISO a aplicar elegidos gracias al SOA, hay que detallar como los vas a implementar (procedimientos técnicos)**
  - **Consultando con expertos en seguridad de la información**: Que te den orientación técnica detallada sobre cómo implementar los controles de seguridad específicos de la organización
  - **Capacitación y certificación**: Cursos que pueden proporcionar los conocimientos técnicos necesarios para implementarlos
  - **Recursos en línea y literatura**: Que puedan proporcionar orientación técnica detallada
    - STIG, ENS (recuerda que tienen procedimientos detallados) y, especialmente, **controles CSC**
    - Recuerda que los controles **CSC se pueden mapear a los ISO 27001**, entre otros frameworks
      - Permiten cumplir con múltiples frameworks implementando un único procedimiento técnico
    - Ten en cuenta que el mapeo no siempre es perfecto y **debe revisarse detalladamente** que se estén cumpliendo los requisitos del SGSI identificados anteriormente
    - Siempre de acuerdo a lo especificado en el documento de la ISO 27002:2022 para cada control
  - **Herramientas y software de seguridad**: Muchas herramientas y software de seguridad pueden ayudarte a implementar controles de seguridad específicos

PLAN: DEFINIR CONTROLES Y PROCEDIMIENTOS DE IMPLEMENTACIÓN

- **Como vimos, los controles CIS se pueden mapear a los de ISO 27001**
- **Así nuestro trabajo con los benchmarks CIS se puede usar para facilitar el cumplimiento de la norma ISO 27001**
  - Implementamos parte de los controles ISO a través de los Benchmarks CIS
- **No todos los controles de la ISO 27001 tienen un control CSC correspondiente**
  - Si la organización necesita finalmente implementar uno de ellos, hay que recurrir a alguna de las otras 3 fuentes vistas antes



Fuente: https://www.cisecurity.org/controls/cis-controls-navigator/

PLAN: DEFINIR CONTROLES Y PROCEDIMIENTOS DE IMPLEMENTACIÓN

CIS Benchmark (PDF) de Ubuntu 22.04 → **CSC Controls v8 (y sus Safeguards)** → Mapean a* → **Controles de seguridad de ISO 27001:2022**

Todos los controles técnicos de seguridad del Safeguard 3.3

CSC Control 3 – *Data Protection*

- ***Safeguard 3.3***: *Configure Data Access Control Lists*

→ **5.10 Acceptable use of information and other associated assets**
5.15 Access control
8.3 Information access restriction
8.4 Access to source code

Todos los controles técnicos de seguridad de los Safeguards 4.3 y 4.8

CSC Control 4 – *Secure Configuration of Enterprise Assets and Software*

- ***Safeguard 4.3***: *Configure Automatic Session Locking on Enterprise Assets*
- ***Safeguard 4.8***: *Uninstall or Disable Unnecessary Services on Enterprise Assets and Software*

→ **8.5 Secure authentication**
8.9 Configuration management

Todos los controles técnicos de seguridad los Safeguards 8.2 y 8.9

CSC Control 8 – *Audit Log Management*

- ***Safeguard 8.2***: *Collect Audit Logs*
- ***Safeguard 8.9***: *Centralize Audit Logs*

→ **8.15 Logging**
8.20 Networks security

→ **No tiene mapeo (pero se puede añadir al SoA si la organización lo estima oportuno)**

Fuente: https://www.cisecurity.org/controls/cis-controls-navigator, mapeo a ISO 27001 y 27002, IG3

PLAN: CREAR EL PLAN DE SEGURIDAD FINAL

- **Cada actividad creada genera un documento final**
  - Que refleja las acciones que se tomarán para implementar los controles de seguridad elegidos para crear el SGSI
- **Este plan abarca acciones a corto, medio y largo plazo**
  - **Objetivos** de seguridad
  - **Responsabilidades** (quién se encarga de qué)
  - **Presupuesto**
  - **Recursos estimados** (RRHH, materiales...) y **calendario** para implementar las acciones

DO: IMPLEMENTAR PROCEDIMIENTOS DE GESTIÓN DE RIESGOS

- **Ya hemos escogido qué controles ISO vamos a implementar (SoA)**
  - Y si usamos los CSC Controls, también hemos definido que múltiples controles ISO se pueden mapear a dichos CSC Controls
- **La siguiente fase es la implementación de controles y procedimientos**
  - Pero *¿recuerdas que dijimos que hay formas de automatizar la aplicación de controles técnicos?*
    - Es la finalidad del **protocolo SCAP** y sus implementaciones (STIGs, `scap-security-guide`, CIS Bencmarks)
  - *¿Recuerdas que incluso cada control técnico de los CIS Benchmark indicaba si podía automatizarse su auditoría (Audit) y su Remediación (Remediate)?* *5.3.3 Ensure sudo log file exists (Automated)*
  - Efectivamente, las **tecnologías de automatización de controles técnicos de seguridad** que explicamos pueden ser de gran ayuda para la implementación técnica del SGSI
    - **¡Transformamos acciones en la línea de comandos a cosas de mucho más alto nivel!** ☺
    - Tras hacer una fase **PLAN** en detalle, el tiempo en la fase **DO puede verse reducido** gracias a este tipo de **tecnologías de automatización**
- **Esta fase también incluye asignar recursos, responsabilidades y prioridades**

DO: FORMACIÓN DE USUARIOS

- **Los usuarios deben estar adecuadamente formados en el SGSI**
  - Se deben crear **cursos de capacitación y concienciación** en materia de seguridad de la información
    - Especialmente contra el ciber fraude, que es una amenaza enorme en la actualidad
  - Incluye **cómo realizar correctamente sus tareas asignadas** y los controles implementados
  - Debe impartirse a **todos** los empleados directamente involucrados en el SGSI
  - Pero todos los empleados de la empresa deben ser conscientes de las implicaciones de seguridad de sus acciones y las posibles amenazas
- **No hay un SGSI que tenga éxito sin una formación adecuada y concienciación de todos los empleados en la organización**
  - Dimos algunos elementos para formación en prevención en ciberfraudes en el tema de **Teoría 3**

CHECK: MEDIR LA EFICACIA DE LOS CONTROLES

- **La implementación de controles de seguridad de la información debe ser un esfuerzo continuo**
  - Que implica **monitorizar y revisar** regularmente su efectividad
  - Y hacer ajustes según sea necesario
- **Por tanto, se debe definir un sistema para medir los resultados obtenidos de la aplicación de controles**
  - Estos resultados deben ser **reproducibles y comparables** para medir si tienen éxito
  - Es como el testing, pero para nuestro SGSI en lugar de nuestros programas ☺
- **Ejemplos**
  - **Control ISO 8.20: Network security**: Estadísticas del cortafuegos -> intentos de acceder a páginas web prohibidas
  - **Control ISO 8.24: Use of cryptography**: Porcentaje de sistemas que manejan datos sensibles o valiosos y utilizan métodos de criptografía adecuados

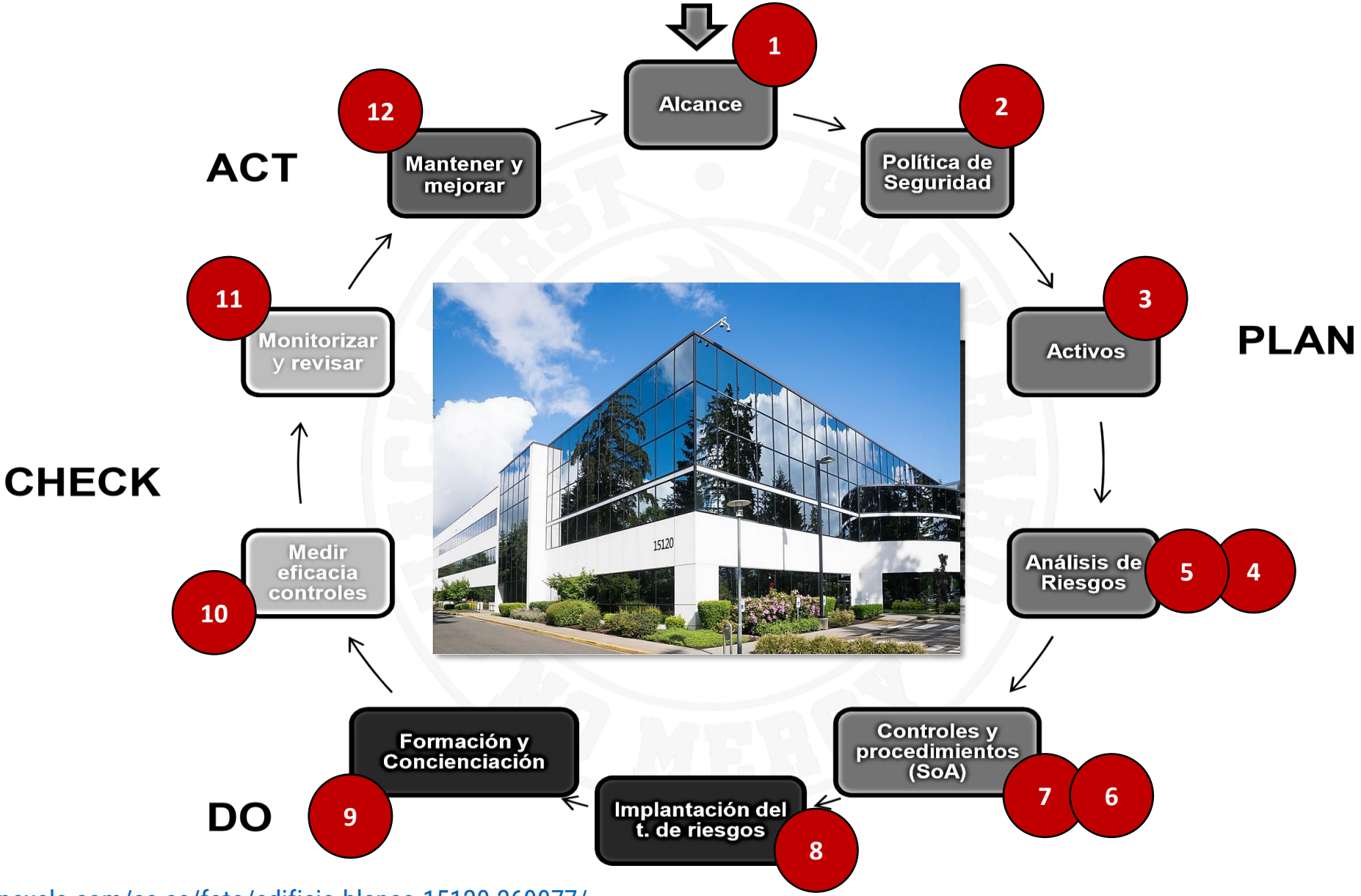
CHECK: MONITORIZACIÓN Y REVISIÓN

- **Ejecutar procedimientos de supervisión y revisión del SGSI**
- **Consiste en revisar regularmente la efectividad del SGSI, considerando**
  - El **cumplimiento** de la política y sus objetivos
  - Los **resultados de auditorías** de seguridad
  - **Incidentes**
  - Resultados de las **mediciones de eficacia** del paso anterior
  - **Sugerencias y observaciones** de todas las partes implicadas
- **Hay que revisar regularmente, en intervalos planificados, las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables**
  - Teniendo en cuenta los posibles cambios que hayan ocurrido en la empresa
  - Realizar periódicamente **auditorías internas** del SGSI en intervalos planificados
  - Revisar periódicamente el SGSI **por parte de la dirección**
    - Para garantizar que el **alcance definido** sigue siendo el adecuado
    - Y que las mejoras en los procesos del SGSI son evidentes

ACT: MANTENIMIENTO Y MEJORA DEL SGSI

- **La organización deberá (de forma regular)**
  - Implementar en el SGSI las **mejoras** identificadas
  - Realizar las acciones preventivas y correctivas apropiadas en relación con la **cláusula de mejora continua** de la ISO 27001
    - Teniendo en cuenta todo lo aprendido de la propia experiencia y de otras organizaciones
  - **Comunicar las acciones y mejoras** a todas las partes interesadas
    - Con el nivel de detalle adecuado
    - Y acordar, si es pertinente, la forma de proceder
  - Asegurarse que las mejoras realizadas **cumplan los objetivos previstos**

Resumen: Implementación de un SGSI



Fuente: https://www.pexels.com/es-es/foto/edificio-blanco-15120-269077/

ISO 27001 vs ENS

Seguridad de Sistemas Informáticos

ISO 27001

- **Norma Voluntaria Internacional y Certificable para cualquier sistema de gestión de la seguridad de la información**. Puede ser "obligatoria" por requisito de clientes y del mercado.
- Gestionada por **ISO – International Organization for Standardization.**
- Se recomienda siempre certificaciones con **certificadoras acreditadas.**
- El certificado se expide por **3 años.** A los 12 y 24 meses hay que hacer una auditoría externa de seguimiento. Es obligada una auditoría interna anual.
- **No existen** categorías o niveles dentro de la norma.
- La ISO 27001 responde al modelo **de Ciclo PDCA-Mejora continua**. Podemos estar en proceso de cumplir ciertos controles siempre que se justifiquen. La modulación de las medidas están bajo el criterio del auditor.
- **ISO no certifica productos.** El alcance es el "Sistema de Gestión de Seguridad de la Información que da soporte a..."

ENS

- **Disposición de carácter legal, de obligado cumplimiento para los sistemas de información** para el sector público y para la empresa privada que trabaja para el sector público.
- Gestionada por el **CCN-CERT - Centro Criptológico Nacional**, dependiente del Ministerio de Defensa.
- Las entidades de certificación tienen que estar **acreditadas por el CCN**.
- El certificado se expide por **2 años**. No hay auditorías intermedias. Son siempre "auditorías iniciales". Es obligada una auditoría interna anual.
- Hay tres **categorías: básico, medio y alto.**
- El ENS marca una serie de requisitos organizativos, documentales y técnicos a cumplir. **Es obligatorio cumplir con el 100% de los requisitos** en función de la categoría del sistema para superar la auditoría de certificación.
- Podemos enfocar el **alcance a productos concretos o a servicios generales** que presta la organización.

Fuente: https://www.linkedin.com/in/v%C3%ADctor-carmona-esteban-4112a717/?originalSubdomain=es

¿Crees que lo has entendido todo? ¡Autoevalúate!

Eres capaz de hacer lo siguiente

- *Comprender las cuatro fases del ciclo de **Deming** y qué hace a grandes rasgos cada una de ellas*
- *Entender que la implementación de un SGSI es un trabajo continuo, y su implementación inicial tarda varios meses normalmente*
- *Entender que un SGSI solo debe aplicarse a los empleados que manejan información sensible*
- *Comprender los contenidos generales de una política de seguridad*
- *Tener claro que el control de todos los activos es clave para poder implementar un SGSI*
  - *Y que por activo de una organización se entienden muchas cosas, no solo máquinas*
- *Comprender el concepto de riesgo, cómo se calculan y que cuatro cosas pueden hacerse a la hora de responder a los riesgos que se han identificado*
- *Entender qué te puedes encontrar dentro de un documento SOA*
- *Comprender que, una vez elegidos los controles de seguridad a implementar, debemos implementarlos*
  - *Y que es entonces donde se conectan los controles CSC vistos*
  - *U otros recursos que nos guíen en como implementarlos de forma fiable (STIG, ENS...)*
- *Comprender definitivamente cómo la automatización de la seguridad vista en este tema puede ser clave a la hora de aligerar la implementación de un SGSI*
  - *Junto con la importancia de la formación de los usuarios, que debe incluirse en el mismo*
- *Entender que, tras la implementación, es necesario un procedimiento de medida de la eficacia, monitorización y revisión de los controles de seguridad*
  - *Antes de empezar de nuevo el ciclo de **Deming** para seguir mejorando el SGSI implementado*
  - *Entendiendo que solo podemos mejorar cosas que hemos medido 1º y sabemos que no alcanzan un nivel*

< Ir al índice

Metodologías de auditoría y revisión de la seguridad

¿Cómo podemos usarlas?

*Iconos por Bing Chat AI

Fuente: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

De controles de seguridad a metodologías

Seguridad de Sistemas Informáticos

Usar una **Metodología de Auditoría de Seguridad** (como **OSSTMM**) para revisar la seguridad de los sistemas y el **cumplimiento** de **frameworks** de seguridad implementados

Gestionado por

Asignar los controles y **Safeguards** implementados a un **Framework de Seguridad** internacional reconocido (**ISO 27001**, **PCI-DSS**…) para facilitar la implementación de un **SGSI**

Mapea a

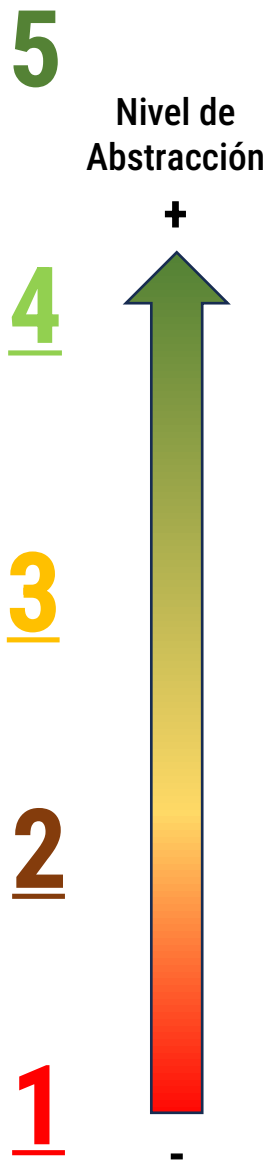
Usar **Implementation Groups** (solo 3) para implementar solo los **Safeguards** más adecuados a un escenario particular según los recursos disponibles

Se pueden distribuir en

Agrupar los controles de seguridad implementados en **CIS Critical Security Controls** (**CSC**) y **Safeguards**

Se pueden agrupar en

Verificar e implementar **Controles técnicos de seguridad** adecuados y validados en un producto de software / SO de forma altamente **automatizada** (varios cientos de controles)



DIAGNOSTICANDO LA SEGURIDAD

- **Hay que realizar pruebas de seguridad exhaustivas en cada sección que tenga aspectos relativos a la seguridad de una organización para iniciar cualquiera de las fases de la ISO 27001**
  - Esto determinará las **vulnerabilidades de los activos** de la organización
- **Para ello se puede usar la metodología de auditoría de seguridad OSSTMM**
  - Manual de Metodología Abierta de Testeo de Seguridad, Open Source Security Testing Methodology Manual
  - Es una de las normas profesionales más completas y de uso más común para revisar la seguridad de los sistemas
  - Proporciona un método estandarizado para realizar pruebas de seguridad exhaustivas en cada sección relacionada con la seguridad de una organización
  - También abarca el cumplimiento de las normas y las mejores prácticas, como las establecidas por ISO 27001 – 27002, NIST o ITIL

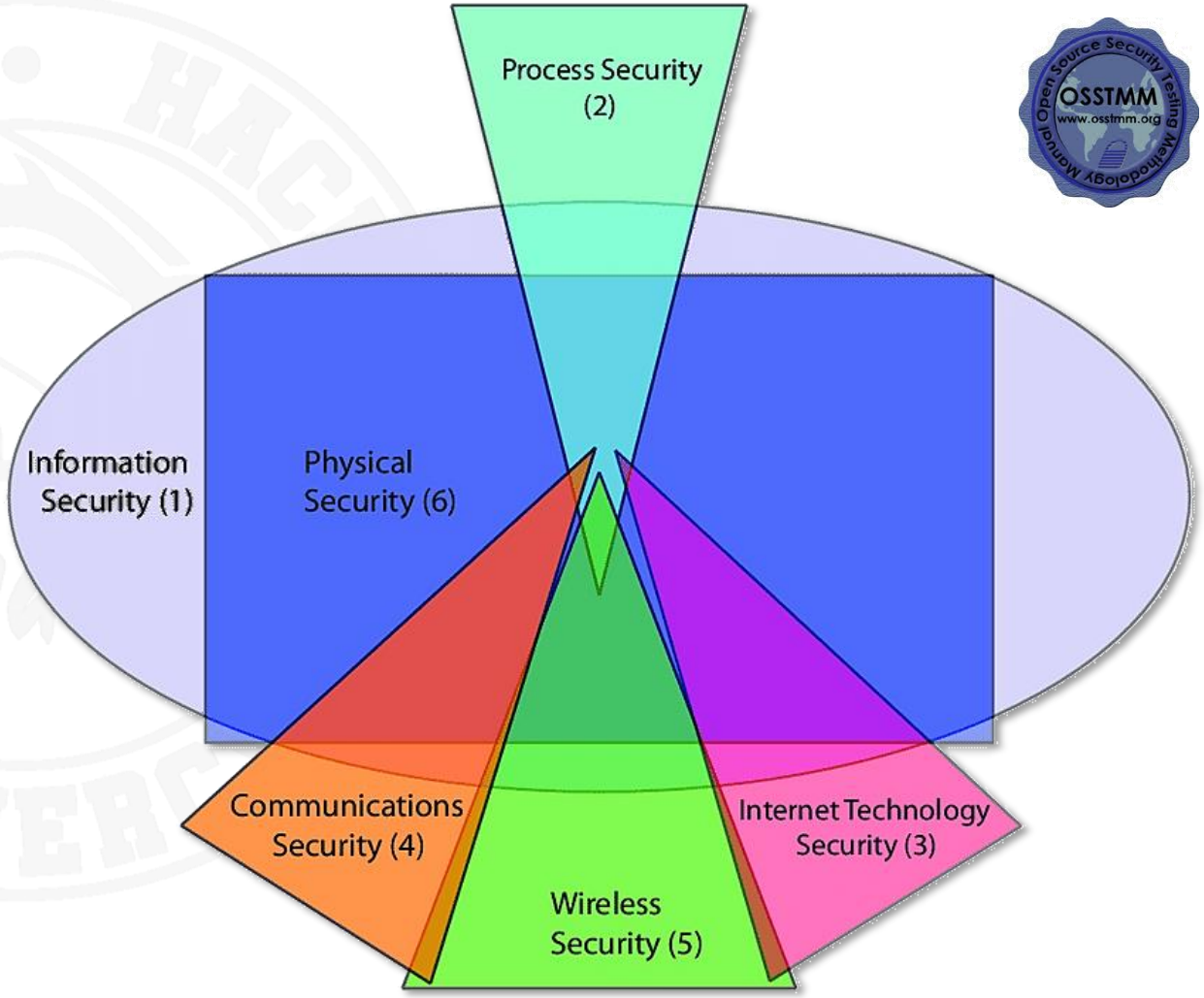
¿Qué es OSSTMM?

- **Es una metodología desarrollada por ISECOM para llevar a cabo pruebas, análisis y medición de la seguridad operativa real**
  - Es decir, es una **metodología para realizar auditorías técnicas de seguridad**
- **Está diseñada para ser consistente y repetible**
- **Permite que cualquier profesional en auditoría de seguridad contribuya con propuestas para realizar testeos de seguridad**
  - De forma que puedan ser más precisos, concretos y eficientes
- **Permite también la libre difusión de la documentación sin problemas de propiedad intelectual**

Secciones OSSTMM

Fuente: https://www.researchgate.net/figure/The-figure-illustrates-the-security-testing-sections-in-the-Open-Source-Security_fig6_268418932

- **Las secciones relacionadas con la seguridad son**
  1. Seguridad de la información
  2. Seguridad de procesos
  3. Seguridad de las tecnologías de Internet
  4. Seguridad de las comunicaciones
  5. Seguridad inalámbrica
  6. Seguridad física
- **La versión 3 (final) se puede descargar aquí**
  - https://www.isecom.org/OSSTMM.3.pdf



Módulos OSSTMM

- Cada sección está compuesta por módulos. Ejemplo

Seguridad en Tecnologías de Internet

- ...
- Revisión del sistema de detección de intrusiones (IDS)
- Sondas de red
- Reconocimiento de servicios y sistemas
- Prueba de aplicaciones de Internet
- Descifrado de contraseñas
- Prueba de denegación de servicio
- …

- Cada módulo tiene una descripción, propone una serie de acciones y enumera sus resultados esperados

OSSTMM: Ejemplo de descifrado de contraseñas

Descripción

- Descifrar contraseñas es el proceso de validar la robustez de contraseñas
  - Mediante herramientas automatizadas de recuperación de contraseñas
- Estas podrían descubrir
  - El uso de **algoritmos criptográficos débiles**
  - **Implementaciones incorrectas** de estos algoritmos
  - **Contraseñas débiles** debido a factores humanos

Resultados esperados

- **Archivos de contraseñas** descifradas y sin descifrar
- **Lista de cuentas** (de usuario o de sistema, **Tema 3**) con contraseñas
- **Lista de sistemas vulnerables** a ataques de descifrado de contraseñas
- **Lista de archivos o documentos vulnerables** a ataques de descifrado de contraseñas
- Lista de sistemas con cuentas de usuario o sistema **que usan las mismas contraseñas**

OSSTMM: Ejemplo de descifrado de contraseñas

- **Acciones de verificación**
  - Obtener el fichero de contraseñas del sistema
  - Iniciar un **ataque automatizado de diccionario** al fichero de contraseñas
  - Iniciar un **ataque de fuerza bruta** al fichero de contraseñas
  - Usar las contraseñas obtenidas o variaciones de ellas para **acceder a sistemas** o aplicaciones adicionales
  - Usar **programas automatizados de descifrado** contra ficheros cifrados que se hayan localizado (como documentos PDF u Office) para intentar recopilar más datos
  - **Verificar la fecha** en la que se establecieron las contraseñas
- **Estas acciones se realizan con herramientas como las que describiremos en el bloque de pentesting de esta asignatura** (Tema 7)

Respuesta a incidentes (IR)

Seguridad de Sistemas Informáticos

- **Consiste en tener un plan organizado para saber qué hacer ante determinados incidentes de seguridad**
  - Preparación, detección y análisis, contención, eliminación, recuperación, aprendizaje y pruebas
- **Proceso de aprendizaje y madurez de una organización**
  - A medida que **adquiere experiencia en gestión** de la ciberseguridad
  - "Manual de operaciones para ciber desastres en nuestra organización" ☺
- **Hay metodologías para evaluar la IR de una empresa, como la CREST**
  - https://www.crest-approved.org/cyber-security-incident-response-maturity-assessment/index.html

INCIDENT RESPONSE FOR COMMON ATTACK TYPES

Attack Name	What It Is?	Threat Indicators	Where to Investigate	Possible Actions
Brute Forcing	Attacker trying to guess a password by attempting several different password	Multiple login failures in a short period of time	Active Directory Logs Application Logs Operational System logs Contact User	**If not legit action**, disable the account and investigate/block attacker
Botnets	Attackers are using the victim server to perform DDOS attacks or other malicious activities	Connection to suspicious IPs. Abnormal high volume of network traffic	Network Traffic OS Logs (New processes) Contact Server Owner Contact Support Team	**If confirmed:** Isolate the server Remove malicious processes Patch the vulnerability utilized for infection
Ransomware	A type of malware that encrypts files and reuests a ransom(money payment) from the user to decrypt the files	User contacting; Burst of "file update"logs Anti Virus alerts Connection to suspicious IPs.	AV Logs OS Logs Account Logs Network Traffic	Request AV Checks Isolate the machine
Data Exfiltration	Attacker (or rogue employee) exfiltrate data to external sources	Abnormal high network traffic Connection to cloud-storage solutions(Dropbox, Google Cloud) Unusual USB Sticks	Network Traffic Proxy Logs OS Logs	**If rougue employee:** Contact manager, perform full forensics **If external Threat:** Isolate the machine, disconnect from network
Compromised Account	Attackers get access to one account (via social engineering or any other method)	Off-hours account logins, Account group changes, Abnormal high network rtaffic	Active Directory Logs, OS Logs, Network Traffic, Contact User for Clarifications	**If confirmed:** Disable Account, Password Changes, Forensic investigations
Denial Of Service (DoS/DDos)	When attacker is able to cause interference in a system by exploiting DoS Vulnerabilities or by generating a high volume of traffic	Abnormal high network traffic in public facing servers	Network traffic, Firewall Logs, OS Logs	**If DoS due to vulnerabilities:** Contact patching team for remediation. **If DDoS due to network traffic:** Contact network Support or ISP.
Advanced Persistent Threats (APTs)	Attackers get access to the system and create backdoors for further exploitation. Usually hard to detect.	Connection to suspicious IPs, Abnormal high volume of network tarffic, Off-hours access logs, New Admin account creations.	Netwotk traffic, Access Logs, OS Logs (new processes, new connections, abnormal users), Contact server owner/support teams.	**If confirmed;** Isolate the machine, start formal forensics process, Start escalation/commuication plan.

¿Y AHORA?

- **La implementación de un SGSI completo está más allá del alcance de la asignatura**
  - La gestión de riesgos forma parte de una asignatura de 4º (DPPI)
  - Los temas relacionados con leyes también forman parte de otra asignatura de 4º (ASLEPI)
- **Pero hemos visto formas de automatizar su objetivo práctico final: el hardening de sistemas informáticos**
  - Automatizar la evaluación y corrección de las posibles vulnerabilidades de seguridad que detectamos
  - Tener **fuentes de información confiables para proteger el SO y productos software comunes** (Firefox, Chrome..) siguiendo una serie de directrices
  - Saber cómo utilizar este trabajo para hacer las cosas de manera documentada y profesional e implementar frameworks de seguridad
  - Así, tenemos una manera de lograr rápidamente el hardening de un sistema de una manera eficiente
  - Y, con el tiempo, escalarlo para implementar algo más complejo y de un nivel de abstracción más alto
  - ¡Lo mejor de ambos mundos! ☺

TEMA 4
POLÍTICAS DE SEGURIDAD Y HARDENING AUTOMATIZADO

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo