



CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

Séptimo Ciclo

FUNDAMENTOS DE CONTROLES CIS

Sesión 1: Introducción practica

Índice de contenidos

- HORARIOS
- PROGRAMA
- CONOCIENDO AL PROFESOR
- OBJETIVO GENERAL
- GLOSARIO DE TERMINOS
- SIGLAS Y ABREVIATURAS
- PORQUE IMPLEMENTAR CONTROLES

Cuerpo Académico



Eder Patricio Morán Heredia

Bachiller en Ingeniería de Sistemas e Informática en la Universidad Privada Telesup, cursando el Magister de Educación Superior en la Universidad Gabriela Mistral y una segunda carrera de Ingeniería en Tecnologías de la Información y Comunicaciones en la Universidad San Sebastián.

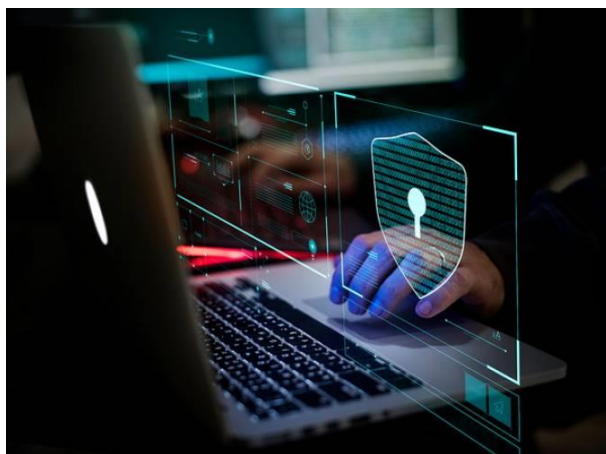
Profesional con 17 años de experiencia en Tecnología de la información y 8 años de experiencia en la docencia superior. Con una especialización en Gobernanza, Gestión y Auditoría a la Ciberseguridad. Posee certificaciones internacionales de CCNA Instructor Cyber Ops (Cisco), Cyber Security Foundation (CSFPC) – Certiprof, Lead Cybersecurity Professional Certificate LCSPC^o (Certiprof). AZ-900 Microsoft Azure Fundamentals.

.

Inicio de CIS Control

CIS Controls® comenzó como una simple actividad básica para identificar los ciberataques más comunes e importantes del mundo real que afectan a las empresas todos los días.

Inicialmente se debía traducir ese conocimiento y experiencia en acciones positivas y constructivas para los defensores y luego compartir esa información con un público más amplio . Los objetivos originales eran modestos:



Ayudar las personas y las empresas a dar los pasos más importantes para defenderse de los ataques importantes.

Evolución de los controles CIS

Liderados por el Center for Internet Security® (CIS®), los controles CIS han madurado hasta convertirse en una comunidad internacional de personas e instituciones voluntarias que:

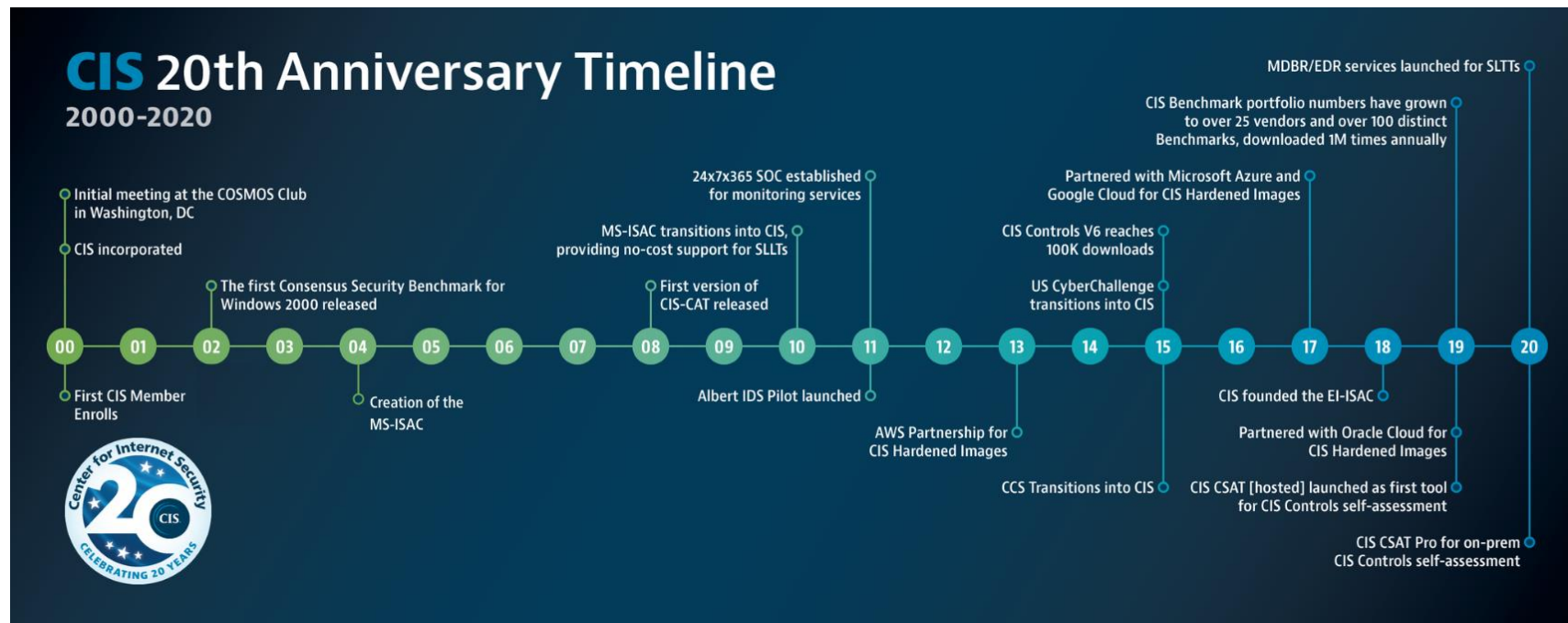
Comparte información sobre ataques y atacantes, identifique las causas fundamentales y traduzca eso en clases de acción defensiva.

Crear y compartir herramientas, ayudas de trabajo e historias de adopción y resolución de problemas.

Asignar los controles CIS a los marcos regulatorios y de cumplimiento para garantizar la alineación y darles prioridad y enfoque colectivos.

Identificar problemas y barreras comunes (como la evaluación inicial y las hojas de ruta de implementación) y resolverlos como comunidad.

Evolución de los controles CIS



Historial de versiones

Versión 1.0: Borrador original de los controles

Versión 2.0: Revisión principal de los subcontroles basada en los comentarios de la comunidad y la agencia.

Versión 2.1: Revisión menor de los subcontroles basada en los comentarios de la comunidad y la agencia.

Versión 2.3: Adición de medidas y metodologías de evaluación básicas

Versión 3.0: Revisión importante de subcontroles y adición de mapas y sensores estándar

Versión 3.1. Reordenamiento de controles en base a prioridad de controles

Versión 4.0. Revisión de subcontroles, eliminación de sensores, adición de ERDS.

Versión 4.1 Ediciones menores y mayor alineación con Aus DSD Top 4

Versión 5.0: Actualizaciones de subcontroles y controles de limpieza

Versión 5.1: Corrección de errores menores y ediciones (sin cambios de control)

Versión 6.0: Evaluación de control majar, nuevas medidas y puntos de referencia

Versión 6.1: Definición de estándar de debido cuidado (subcapas fundamentales vs avanzadas)

Versión 7.0: Mayor simplificación del control, se centra en las medidas y métricas

Versión 7.1: Aclaraciones de redacción y adición de clases de control

Versión 8: Reinterpretación de los controles CIS y consolidación de subcontrole

Alineación de los controles CIS

El objetivo es crear y demostrar una "coexistencia pacífica" con otros esquemas, marcos y estructuras de gobernanza, regulación y gestión de procesos.

Cooperar y señalar los estándares independientes y las recomendaciones de seguridad existentes cuando existan.



Modelo MITRE ATT&CK

MITRE Corporation (organización sin fines de lucro para el funcionamiento de institutos de investigación en nombre de los Estados Unidos) publicó por primera vez en 2013 el precursor del marco MITRE ATT&CK actual. "ATT&CK" significa "Tácticas adversarias, técnicas y conocimiento común" y es una lista categorizada sistemáticamente de patrones de comportamiento de atacantes.

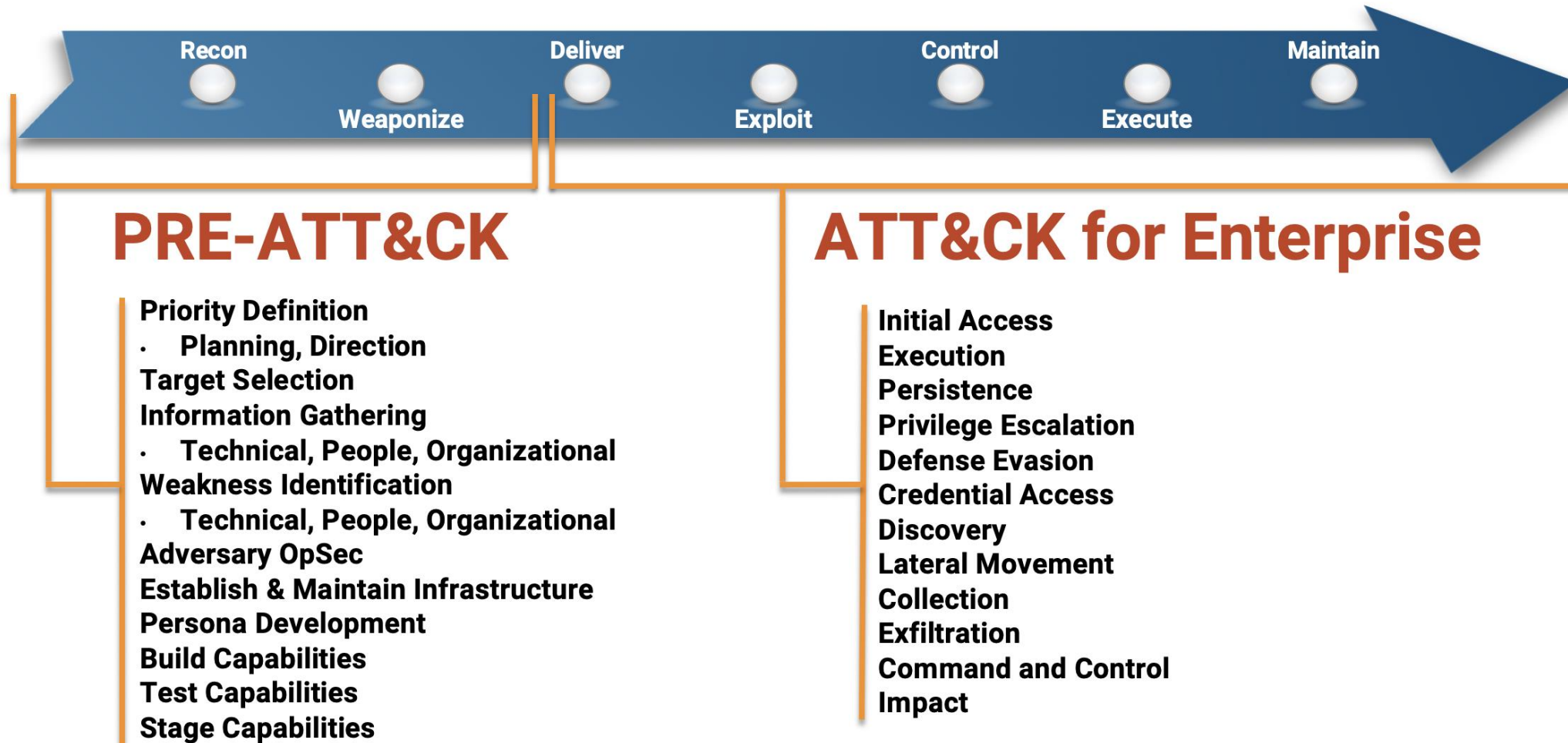
En esta lista se presentan detalladamente las formas en que los ciberdelincuentes operan en las redes. Por lo tanto, es muy útil para muchos análisis, evaluaciones y otros mecanismos ofensivos y defensivos diferentes y ha sido ampliamente reconocido durante años.

Modelo MITRE ATT&CK

Beneficios del Marco MITRE ATT&CK:

- Estructuración/organización del análisis de las Tácticas, Técnicas y Procedimientos (TTPs) de los ciberdelincuentes.
- Descripción de las técnicas centrada en el actor
- Hoja de ruta/escenario para simular ciberataques 'reales'
- Enfoque estructurado para verificar cómo la tecnología de un proveedor se defiende de los ataques
- Ayudar en los esfuerzos de caza de amenazas (actividades del equipo rojo/azul/púrpura)

Modelo MITRE ATT&CK (Tácticas adversarias, técnicas y conocimiento común)



Que son los controles CIS

Son un conjunto de buenas practicas que fueron desarrollados por el center of internet security.

Nos indica que acciones defensivas podemos tomar para prevenir ataques menores y mayores.
Apoyando el cumplimiento de múltiples marcos.

Estos controles están diseñados para complementar los estándares, marcos y esquemas de cumplimiento existentes y proporcionan una línea base de protección contra los riesgos de toda organización.

Que son los controles CIS

Un conjunto de acciones priorizadas para proteger su organización y sus datos de los vectores de ciberataques conocidos.

Ayudan a supervisar, detectar, analizar, proteger, informar y responder contra vulnerabilidades, ataques y explotaciones conocidas. Asimismo, probar y evaluar continuamente los controles y técnicas de seguridad de la información, para garantizar que se implementen de manera efectiva.



Porque implementar los controles?

Los Controles son directrices específicas que los CISO, los CIO, y los profesionales de seguridad de la información pueden utilizar para administrar y medir la eficacia de sus defensas.

Las defensas deben enfocarse en abordar las actividades de ataque más comunes y dañinas que ocurren hoy y las que se anticipan en el futuro cercano.

Los entornos empresariales deben garantizar controles consistentes en toda la empresa para negar los ataques de manera efectiva.

Las defensas deben automatizarse cuando sea posible y de forma periódica o continua medido utilizando técnicas de medición automatizadas cuando sea factible.

Para hacer frente a los ataques actuales que ocurren con frecuencia contra numerosas organizaciones, se debe emprender una variedad de actividades técnicas específicas para producir una defensa más consistente.

Se deben establecer medidas que faciliten un terreno común para medir la eficacia de las medidas de seguridad, proporcionando un lenguaje común para comunicar sobre el riesgo

Estructura de los controles CIS

Un conjunto de acciones priorizadas para proteger su organización y sus datos de los vectores de ciberataques conocidos.

- **Descripción general.** Una breve descripción del objetivo del control y su utilidad como acción defensiva.
- **¿Por qué este control es crítico?.** Una descripción de la importancia de este control para bloquear, mitigar o identificar ataques, y una explicación de cómo los atacantes explotan activamente la ausencia de este control.
- **Procedimientos y herramientas.** Una descripción más técnica de los procesos y tecnologías que permiten la implementación y automatización de este Control.
- **Descripciones de salvaguardas.** Una tabla de las acciones específicas que las empresas deben tomar para implementar el Control.

Como ayuda la implementación en la organización

La implementación de los Controles de Seguridad Críticos de CIS en su organización puede ayudarle eficazmente a:

- Desarrollar una estructura fundamental para su programa de seguridad de la información y un marco para toda su estrategia de seguridad.
- Seguir un enfoque comprobado de gestión de riesgos para la seguridad informática basado en la eficacia del mundo real.
- Enfocarse en el conjunto más efectivo y específico de medidas técnicas disponibles para mejorar la postura de defensa de su organización.
- Ajustarse fácilmente a otros marcos y regulaciones, incluidos NIST Cybersecurity Framework, NIST 800-53, NIST 800-171, ISO 27000, PCI DSS, HIPAA, NERC CIP, y FISMA.

Evolución de los controles CIS

La versión 7.1 trajo la cyber hygiene.



Diferencia de las versiones 7.1 y 8

La versión 7.1 trae 20 controles, mientras que la versión 8, cuenta con 18 controles.

La versión 8 introduce un glosario de definiciones, acrónimos y abreviaturas que busca eliminar cualquier ambigüedad desde la perspectiva de la terminología; también brinda orientación sobre cómo las empresas pueden administrar sus servicios en la nube.

También prioriza lo siguiente:

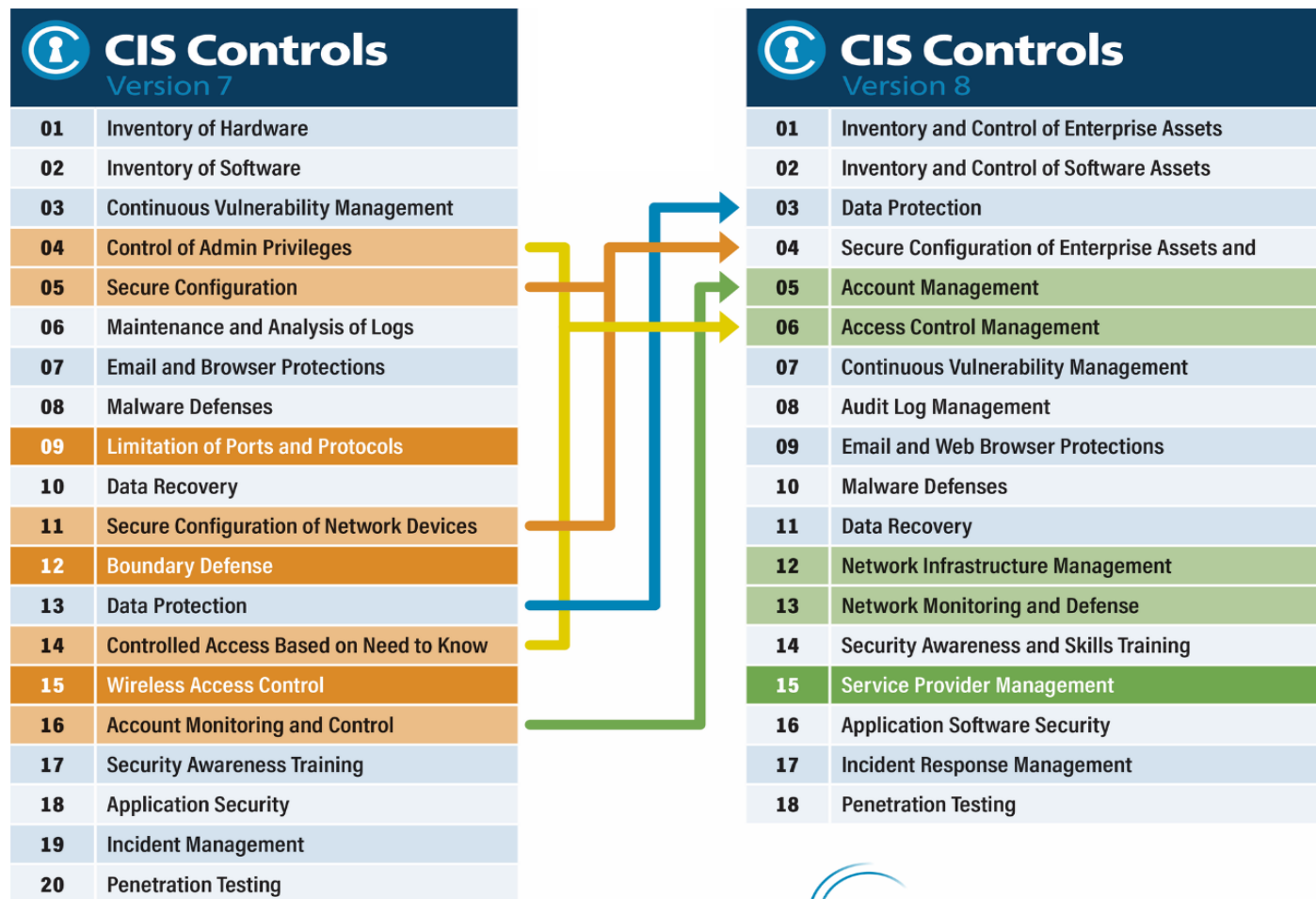
- El Ataque como referencia para la Defensa.
- Foco en la identificación y priorización de los aspectos más críticos para detener los ataques más relevantes.
- Salvaguardas viables y aplicables.
- Controles medibles.



CIS Control v8

CONTROL 01 Inventory and Control of Enterprise Assets	CONTROL 02 Inventory and Control of Software Assets	CONTROL 03 Data Protection
CONTROL 04 Secure Configuration of Enterprise Assets and Software	CONTROL 05 Account Management	CONTROL 06 Access Control Management
CONTROL 07 Continuous Vulnerability Management	CONTROL 08 Audit Log Management	CONTROL 09 Email and Web Browser Protection
CONTROL 10 Malware Defenses	CONTROL 11 Data Recovery	CONTROL 12 Network Infrastructure
CONTROL 13 Network Monitoring and Defense	CONTROL 14 Security Awareness and Skills Training	CONTROL 15 Service Provider Management
CONTROL 16 Applications Software Security	CONTROL 17 Incident Response Management	CONTROL 18 Penetration Testing

Diferencia de las versiones 7.1 y 8



Diferencia de las versiones 7.1 y 8

La versión v8 no es solo una actualización de los controles; todo el ecosistema que rodea a los controles también se ha actualizado , como:

Herramienta de autoevaluación de controles CIS CSAT : una forma para que las empresas realicen, rastreen y evalúen su implementación de los controles CIS a lo largo del tiempo y midan la implementación en comparación con sus pares de la industria; CIS CSAT alojado es gratuito para su uso en una capacidad no comercial

Modelo de defensa comunitaria (CDM): enfoque riguroso, transparente y basado en datos que ayuda a priorizar los controles en función de la amenaza en evolución; CDM v1.0 utilizó el Informe de Investigaciones de Violación de Datos (DBIR) de Verizon 2019 para determinar los principales ataques y el Marco MITRE ATT&CK (Tácticas Adversarias, Técnicas y Conocimiento Común) v6.3

Diferencia de las versiones 7.1 y 8

Método de evaluación de riesgos CIS CIS RAM: ayuda a una empresa a justificar las inversiones para la implementación razonable de los controles CIS, definir su nivel aceptable de riesgo, priorizar e implementar los controles CIS de manera razonable y ayudar a demostrar el "debido cuidado" CIS RAM 2.0: incluye una hoja de trabajo CIS RAM simplificada para IG1 y módulos adicionales diseñados para desarrollar indicadores clave de riesgo mediante análisis cuantitativo.

CIS Controls Mobile Companion Guide: ayuda a las empresas a implementar las mejores prácticas desarrolladas por consenso utilizando CIS Controls v8 para teléfonos, tabletas y aplicaciones móviles.

Guía complementaria de CIS Controls Cloud: orientación sobre cómo aplicar las mejores prácticas de seguridad que se encuentran en CIS Controls v8 a cualquier entorno de nube desde la perspectiva del consumidor / cliente
CIS Control Navigator

Herramienta de evaluación de controles (AuditScripts)

CIS tiene un enfoque centrado en el control de seguridad para la evaluación de riesgos.

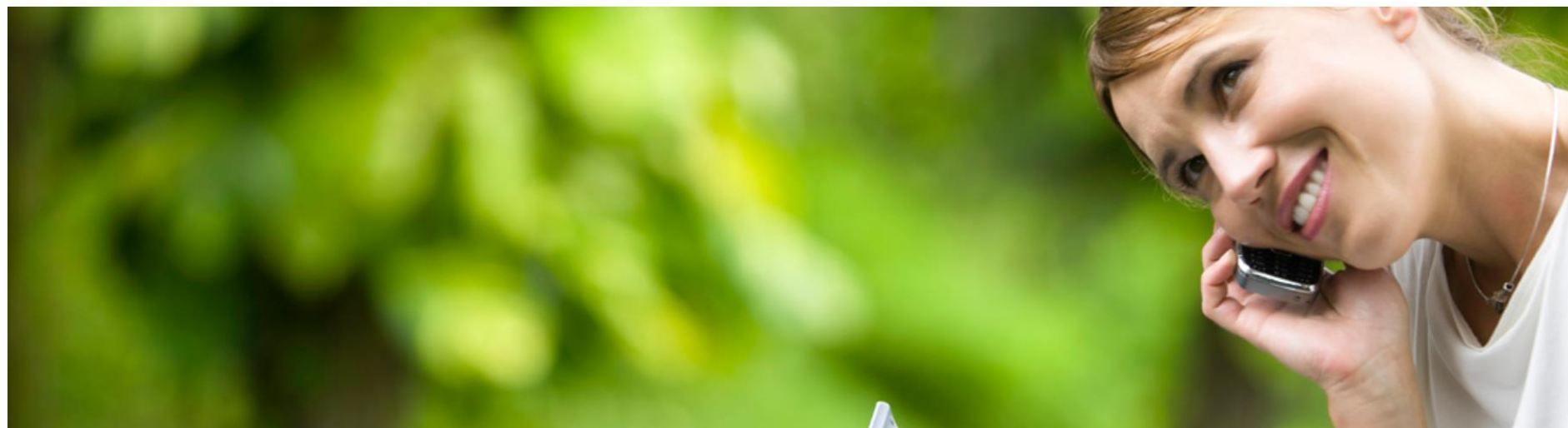
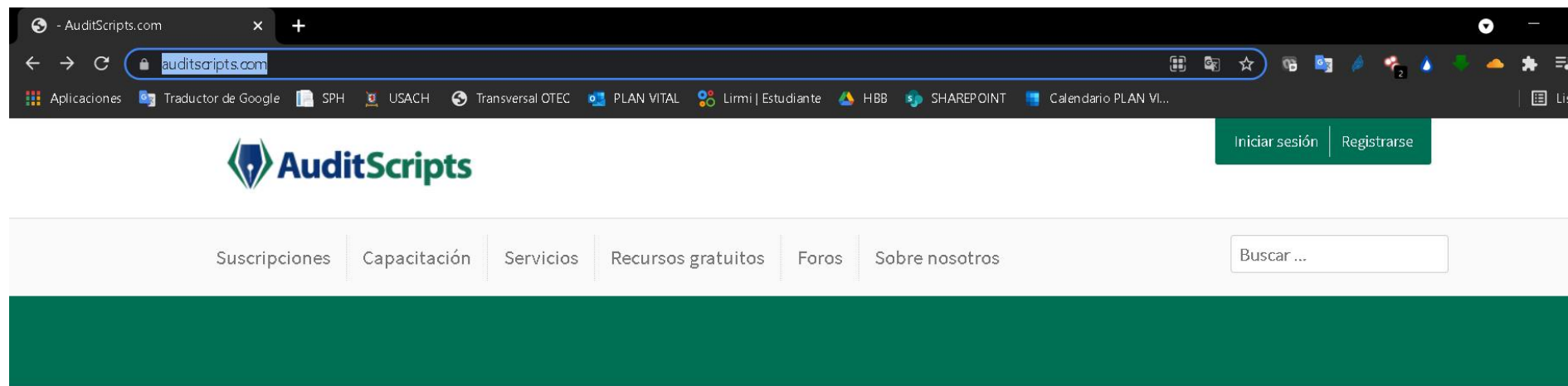
La herramienta es mantenida por Enclave Security y AuditScripts.com

La organización se evalúa en función de su implementación exitosa de controles de seguridad específicos.

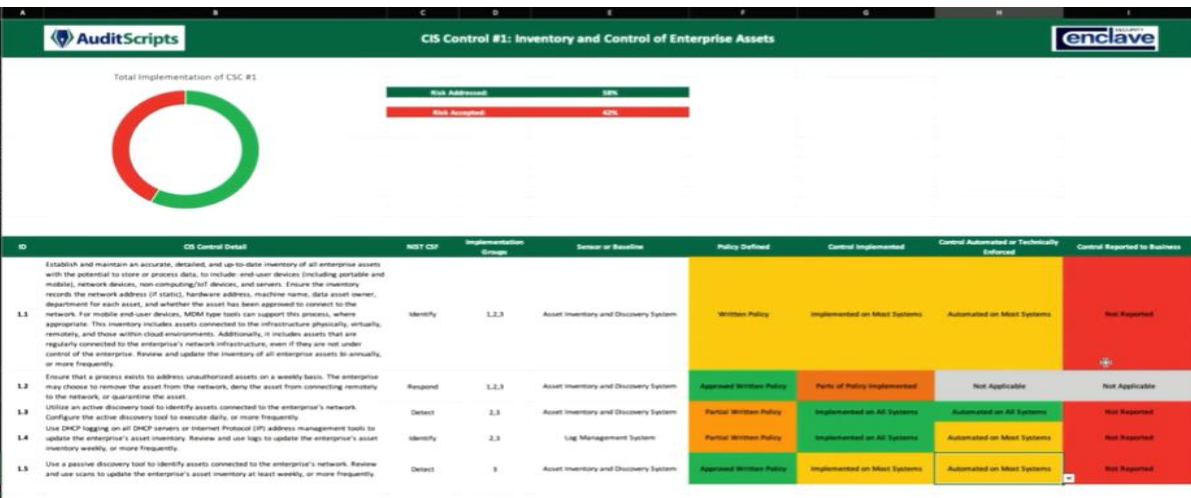
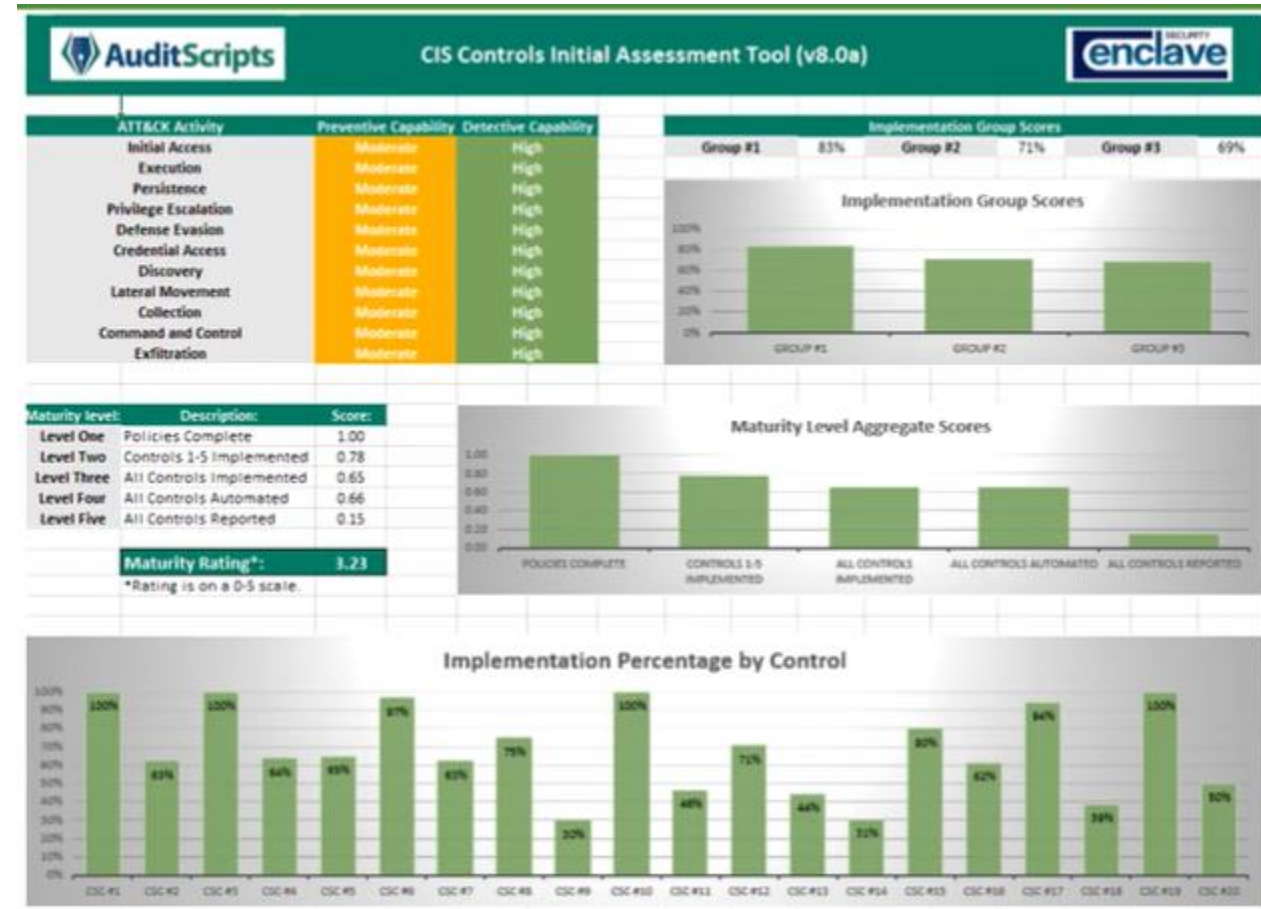
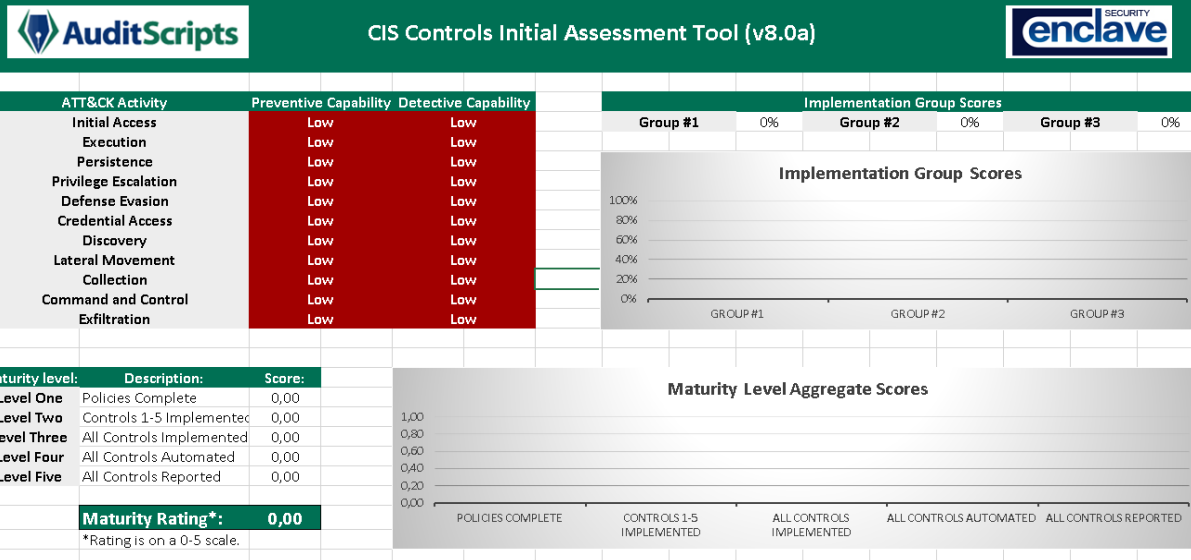
El resultado es un tablero/puntaje de madurez basado en la implementación exitosa del Control de seguridad, la lista se basa en el proyecto de controles de CIS.

Se podrían crear herramientas de riesgo similares utilizando también otras listas de controles (NIST 800-53, ISO 27002:2013)

Como realizo un seguimiento de los controles




Como realizo un seguimiento de los controles



Como realizo un seguimiento de los controles?

CIS CSAT (Control Selft Assesment Tool)


Eder Moran ▾

Dashboard

Current Assessment ▾

Assessment History

Organizations ▾

Administration

Reports ▾

CIS Resources ▾

@ CIS Product Technical Support

AIEP > Dashboard

AIEP Dashboard ⓘ

Group 1 ▾ Current assessment ▾

Click on any CIS Control below to submit your response

Organization Average

0

● ● ● ● ●

Industry Average

8

Organizations used for average: 654

Completion %

0

● ● ● ● ●

Validation %

0

● ● ● ● ●

CIS C01

CIS C02

CIS C03

CIS C04

CIS C05

CIS C06

CIS C07

CIS C08

CIS C09

CIS C10

CIS C11

CIS C12

CIS C13

CIS C14

CIS C15

CIS C16


CIS C17

CIS C18

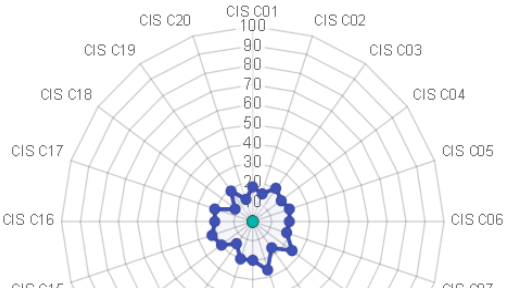
CIS C19


CIS C20


MONTHLY GRAPH



SPIDER WEB







DIPLOMADO
CIBERSEGURIDAD

Nivel de madurez de los controles

Puntaje del modelo de madurez

Estos pasos nos llevan hacia un modelo de madurez de implementación y evaluación general:

Nivel 1: Políticas de controles documentados

Nivel 2: Controles 1-5 completamente implementados

Nivel 3: Todos los controles completamente implementados

Nivel 4: Todos los controles completamente automatizados

Nivel 5: Todos los controles informados regularmente

Descripción general del modelo de riesgo colectivo

Un enfoque práctico y pragmático para la gestión de riesgos

Mantenido por un consorcio de profesionales de ciberseguridad del sector privado

El objetivo es ser un enfoque utilizable, no centrado en modelos de gestión de riesgos académicos o ambiguos

Reconoce la limitación de los modelos cuantitativos

Define un programa de diez pasos para la gestión de riesgos centrándose en cómo definir los controles apropiados y realizar evaluaciones

Navegando por la web

CIS control: <https://www.cisecurity.org/controls/>

➤ CIS RAM

<https://learn.cisecurity.org/cis-ram>

➤ CIS CSAT

<https://csat.cisecurity.org/accounts/login/?next=/>

➤ CIS Benchmarks

<https://www.cisecurity.org/cis-benchmarks/>

➤ Guía complementaria de CIS Controls Cloud:

<https://www.cisecurity.org/white-papers/cis-controls-mapping-to-cloud-security-alliance-cloud-control-matrix/>

➤ CIS Controls Mobile Companion Guide

<https://www.cisecurity.org/white-papers/cis-controls-v8-mobile-companion-guide/>

➤ Modelo de defensa comunitaria

<https://www.cisecurity.org/white-papers/cis-community-defense-model/>

Grupo de implementación

Desde la versión 7.1 se priorizan los controles en Grupos de Implementación (IG).

Cada IG identifica cuales sub-controles se deberían implementar en una organización, en función de su perfil de riesgo y de los recursos que disponga.

Se sugiere a las organizaciones a que se autoevalúen y se clasifiquen dentro de uno de los tres IG para priorizar los controles de CIS, con la finalidad de mejorar su postura de seguridad informática.

La implementación de IG1 se debe considerar como una de las primeras cosas que se deben hacer como parte de un programa de seguridad informática. CIS se refiere a IG1 como «higiene cibernética»; es decir, las protecciones esenciales que se deben poner en marcha para defenderse de los ataques comunes



Grupo de implementación



Grupo de implementación IG1

Una empresa IG1 es de tamaño pequeño a mediano con experiencia limitada en TI y ciberseguridad para dedicarla a proteger los activos y el personal de TI.

La principal preocupación de estas empresas es mantener el negocio operativo, ya que tienen una tolerancia limitada al tiempo de inactividad. La sensibilidad de los datos que están tratando de proteger es baja y principalmente rodea la información financiera y de los empleados.

Las salvaguardas seleccionadas para IG1 deben ser implementables con experiencia limitada en ciberseguridad y estar dirigidas a frustrar ataques generales no dirigidos.



56 salvaguardas



Grupo de implementación IG2 (incluido IG1)

Una empresa IG2 emplea a personas responsables de administrar y proteger la infraestructura de TI.

Estas empresas apoyan a varios departamentos con diferentes perfiles de riesgo según la función y la misión del trabajo.

Las empresas IG2 a menudo almacenan y procesan información confidencial de clientes o empresas y pueden soportar breves interrupciones del servicio.

Una de las principales preocupaciones es la pérdida de confianza del público si se produce una infracción.



76 salvaguardas
+ 56 salvaguardas (IG1)



Grupo de implementación IG3 (incluido IG1 y IG2)

Una empresa de IG3 emplea expertos en seguridad que se especializan en las diferentes facetas de la ciberseguridad (por ejemplo, gestión de riesgos, pruebas de penetración, seguridad de aplicaciones).

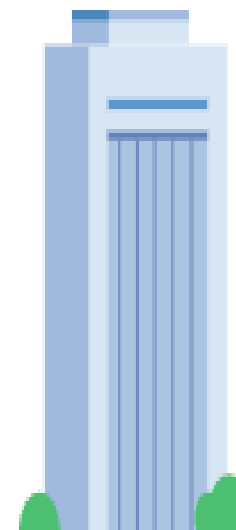
Los activos y datos de IG3 contienen información o funciones sensibles que están sujetas a supervisión regulatoria y de cumplimiento.

Una empresa IG3 debe abordar la disponibilidad de servicios y la confidencialidad e integridad de los datos sensibles.

Los ataques exitosos pueden causar daño significativo al bienestar público.



23 salvaguardas
+ 76 salvaguardas (IG2)
+ 56 salvaguardas (IG1)





CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

Séptimo Ciclo

GRACIAS

Fundamentos de Controles CIS