ANCI

AGENCIA NACIONAL
DE CIBERSEGURIDAD

ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

Controles CIS

Benjamín Iturra

Profesional ANCI

Julio 2025

ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

Objetivo:

Brindar a los participantes un barniz de los conceptos y temas tratados en los controles CIS con el propósito de orientarlos con los primeros pasos en la definición de su plan o estrategia de ciberseguridad institucional.

Temario:

1. ¿Qué son los Controles CIS?
2. ¿Por qué los controles CIS pueden ser una buena estrategia?
3. Mirada general de los controles DEMO evaluación.
4. Ejemplos de incidentes que hemos gestionado que se habrían simplificado con una implementación mínima de controles CIS.
5. Comentarios finales y consultas.

ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

¿Qué son los Controles CIS?

Controles CIS

Historia:

Por su sigla en inglés "*Center for Internet Security, Critical Security Controls for Effective Cyber Defense*", son una publicación de mejores prácticas desarrollada por el instituto SANS (en conjunto con la NSA, DoD, entre otros) desde el año 2008 en respuesta a importantes **ciberataques sufridos por organizaciones de la base industrial de defensa de Estados Unidos**. En esa época los controles recibieron el nombre de "*SANS Top 20*".

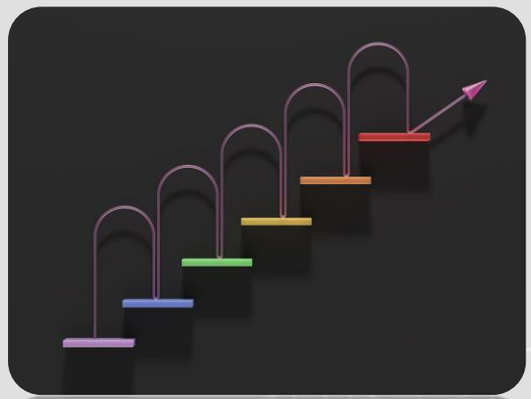
- Estos controles **no fueron creados en base a teoría académica**, sino a partir de **prácticas defensivas reales que habrían prevenido o mitigado los ataques**.
- A contar del año 2011 el "Center for Internet Security (CIS)" asume el liderazgo del proyecto y por eso su nombre pasa a ser "CIS Critical Security Controls"

Controles CIS

Características que ha incluido en el tiempo:

- ✓ Impulso de la colaboración publico y privada.
- ✓ Alineación con normas y estándares como ISO 27001, COBIT y NIST.
- ✓ Incorpora prácticas para diferentes tamaños de organizaciones.
- ✓ Enfoque en amenazas reales.

- ✓ En medida que han salido nuevas versiones, ha dado prioridad a la facilidad de entendimiento e implementación.
- ✓ Enfoque en lo operativo y no en lo administrativo.
- ✓ A contar del año 2021 se han incorporado lineamientos con MITRE ATT&CK, lo que le da un enfoque práctico y concreto.



Controles CIS

Hoy:

Se encuentran en su versión 8.1 publicada en junio de 2024.

Considera 18 controles principales y 153 subcontroles

IG1 Grupo básico pymes 56

IG2 Intermedio 130

IG3 Avanzado 153

Controles CIS

Hoy:

ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

¿Por qué podrían ser una buena estrategia?

¿Por qué son una buena estrategia?

ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD

Priorizados por efectividad, lo que permite maximizar los resultados.

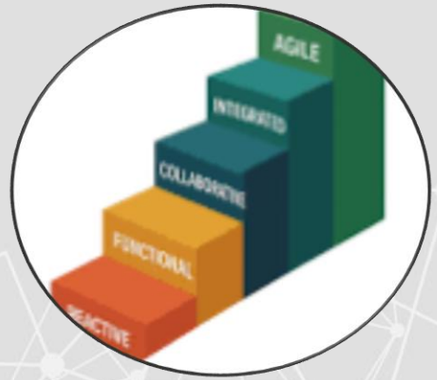
Han sido desarrollados basados en amenazas reales como las del marco MITRE ATT&CK y no de la teoría.

MITRE ATT&CK™

NIST CSF
ISO 27001
NIST SP 800-53
COBIT

Se encuentran alineados con marcos internacionales, lo que le entrega una consistencia mayor a la decisión de su utilización.

Son escalables, o más específicos, para los distintos tipos y tamaños de las organizaciones, lo que por una parte acorta la meta y por otra parte permite una evolución con la madurez.



¿Por qué son una buena estrategia?

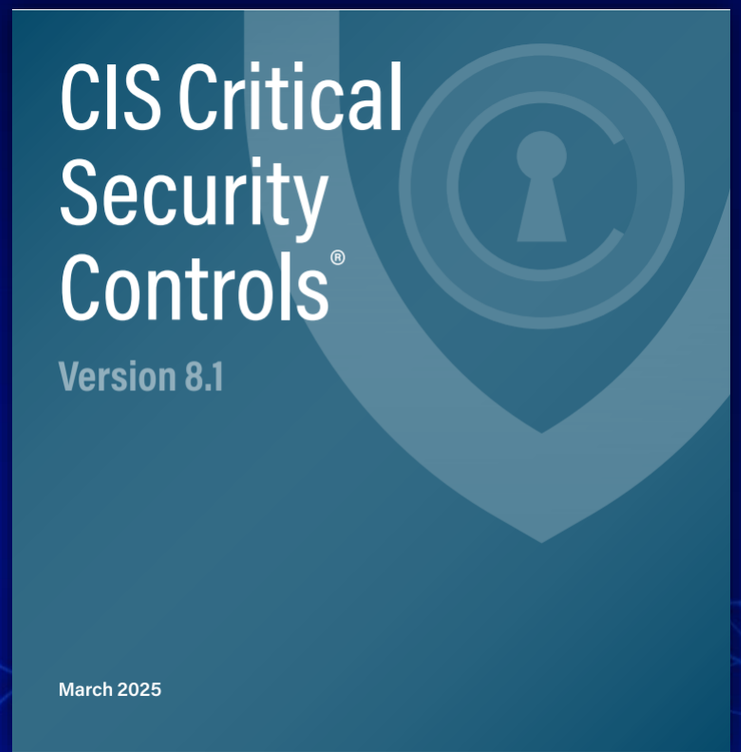
Enfocados en lo práctico y accionable, existen guías concretas de qué hacer a diferencia de otros marcos que se enfocan en aspectos más estratégicos.

Mejora continua, como cuentan con el respaldo de diversas organizaciones, los controles integran regularmente nuevas técnicas para protegerse de nuevas amenazas, como por ejemplo servicios cloud, movilidad o zero trust.

Optimización de costos, al concentrarse en los controles más críticos primero, evitan inversiones mal dirigidas en soluciones poco efectivas. Adicionalmente, toda la documentación oficial está disponible sin costo, lo que facilita el acceso, entrenamiento y difusión dentro de la organización.

ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

Mirada general de los controles y Medidas Esenciales de ciberseguridad ANCI 2025



Controles CIS v8.1

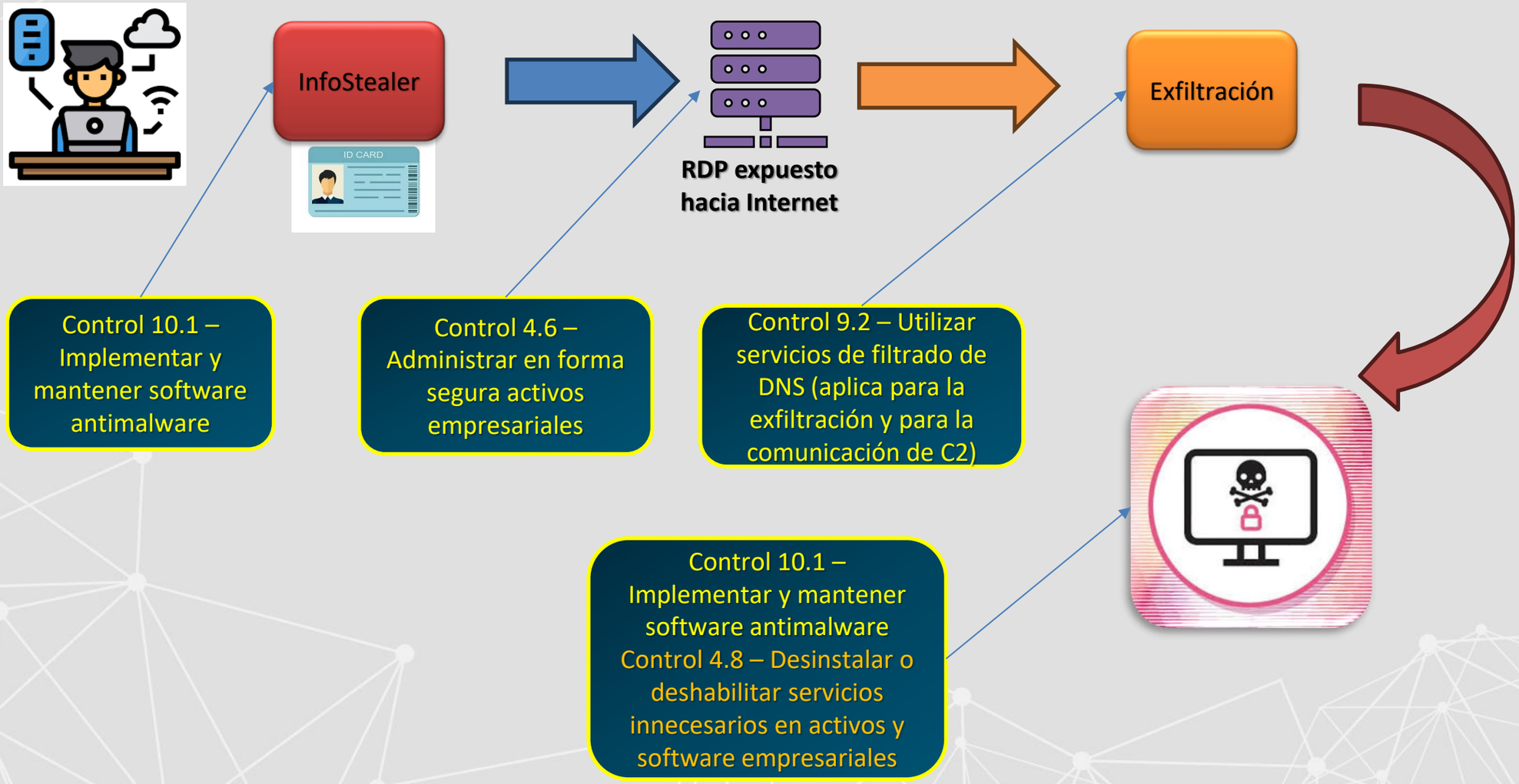
Plataforma de auto evaluación

DEMO: https://csat.cisecurity.org/

Ejemplos de incidentes gestionados durante el 2025 por el CSIRT Nacional.

Actividad del ransomware VanHelsing en Chile, abril 2025

https://csirt.gob.cl/alertas/cnd25-00134/



Actividad del ransomware Safepay en Chile, junio 2025

https://csirt.gob.cl/alertas/aia25-00006/

InfoStealer

2FA

Exfiltración

Control 10.1 – Implementar y mantener software antimalware

Controles 6.3 y 6.4 – Requerir MFA para aplicaciones expuestas externamente y para acceso remoto a la red

Control 9.2 – Utilice servicios de filtrado de DNS (aplica para la exfiltración y para la comunicación de C2)

Control 10.1 – Implementar y mantener software antimalware
Control 4.8 – Desinstalar o deshabilitar servicios innecesarios en activos y software empresariales

Consultas y comentarios finales

anci.gob.cl

Muchas gracias!!!