

# Controles CIS



# Cual es su origen?

CIS son publicaciones de mejores practicas desarrolladas por el instituto SANS (en conjunto con NSA, DoD, entre otros) desde el 2008, en respuesta a los ciberataques sufridos por organizaciones de la base industrial de defensa de EEUU. En aquella época se les conocía como SANS Top 20.

- **No fueron creados sobre una base teórica, sino a partir de practicas defensivas reales que habrían prevenido o mitigado ataques.**
- A partir del 2011, el “Center for internet Security” asume el liderazgo del proyecto.



# Que son los Controles CIS?

- Los **Controles de Seguridad Critica** de CIS son un conjunto prescriptivo y prioritario de mejores practicas en seguridad cibernética
- Son formuladas por u grupo de expertos en tecnologías de la información, utilizando la información obtenida de **Ataques Reales y sus Defensas Efectivas**
- Los Controles CIS proporcionan una orientación especifica y una vía clara para que las organizaciones alcancen las metas y los objetivos descritos por múltiples **marcos jurídicos, reglamentarios y normativos.**

# Importancia de CIS para una organizacion

- Desarrollo de una estructura fundamental para su programa de seguridad de la información y un marco para toda su estrategia de seguridad.
  - Básicamente es un escudo que se le aplica a la organización.
- Medidas técnicas mas eficaces y especificas disponibles para mejorar su postura y defensa de la organización.
- Enfoque de gestión de riesgos para la ciberseguridad basado en la eficiencia del mundo real.
- Cumplimiento con marcos y regulaciones: **NIST, NIST 800-53, NIST 800-171, Normas ISO 27000, PCI DSS, HIPAA, NERC CIP y FISMA**



# Estructura de los Controles CIS

## 20 Recomendaciones de Defensa Informática

### Divididas en 3 Categorías:

1. Básicas.
2. Fundamentales.
3. Organizacionales.



Los Controles CIS no son una solución única para todos, ya que estos dependen de la **madurez** de la ciberseguridad de la organización.



**PEQUEÑA  
EMPRESA**

### **Grupo 1 (IG1) (56)**

Experiencia limitada en ciberseguridad y datos de baja sensibilidad deberán implementar medidas de ciberseguridad de la categoría IG1 (generalmente)



**MEDIANA  
EMPRESA**

### **Grupo 2 (IG2) (130)**

Organizaciones con recursos moderados y con mayor exposición al riesgo por manejo de activos mas confidenciales deberán implementar los controles IG2 junto con IG1.  
**Foco en ayudar a administrar información confidencial de clientes o empresas**



**GRAN  
EMPRESA**

### **Grupo 3 (IG3) (153)**

Recursos Significativos y exposicion de alto riesgo, necesitan implementar controles IG3 con IG2 e IG1. Esto busca reducir los ataques de adversarios sofisticados

CONTROL **01** Inventory and Control of Enterprise Assets

5 Safeguards **IG1** 2/5 **IG2** 4/5 **IG3** 5/5

CONTROL **02** Inventory and Control of Software Assets

7 Safeguards **IG1** 3/7 **IG2** 6/7 **IG3** 7/7

CONTROL **03** Data Protection

14 Safeguards **IG1** 6/14 **IG2** 12/14 **IG3** 14/14

CONTROL **04** Secure Configuration of Enterprise Assets and Software

12 Safeguards **IG1** 7/12 **IG2** 11/12 **IG3** 12/12

CONTROL **05** Account Management

6 Safeguards **IG1** 4/6 **IG2** 6/6 **IG3** 6/6

CONTROL **06** Access Control Management

8 Safeguards **IG1** 5/8 **IG2** 7/8 **IG3** 8/8

CONTROL **07** Continuous Vulnerability Management

7 Safeguards **IG1** 4/7 **IG2** 7/7 **IG3** 7/7

CONTROL **08** Audit Log Management

12 Safeguards **IG1** 3/12 **IG2** 11/12 **IG3** 12/12

CONTROL **09** Email and Web Browser Protections

7 Safeguards **IG1** 2/7 **IG2** 6/7 **IG3** 7/7

CONTROL **10** Malware Defenses

7 Safeguards **IG1** 3/7 **IG2** 7/7 **IG3** 7/7

CONTROL **11** Data Recovery

5 Safeguards **IG1** 4/5 **IG2** 5/5 **IG3** 5/5

CONTROL **12** Network Infrastructure Management

8 Safeguards **IG1** 1/8 **IG2** 7/8 **IG3** 8/8

CONTROL **13** Network Monitoring and Defense

11 Safeguards **IG1** 0/11 **IG2** 6/11 **IG3** 11/11

CONTROL **14** Security Awareness and Skills Training

9 Safeguards **IG1** 8/9 **IG2** 9/9 **IG3** 9/9

CONTROL **15** Service Provider Management

7 Safeguards **IG1** 1/7 **IG2** 4/7 **IG3** 7/7

CONTROL **16** Applications Software Security

14 Safeguards **IG1** 0/14 **IG2** 11/14 **IG3** 14/14

CONTROL **17** Incident Response Management

9 Safeguards **IG1** 3/9 **IG2** 8/9 **IG3** 9/9

CONTROL **18** Penetration Testing

5 Safeguards **IG1** 0/5 **IG2** 3/5 **IG3** 5/5



# Porque usar los controles CIS?

- Están priorizados por efectividad, permitiendo maximizar el resultado (el famoso 80/20).
- Están anidados con el MITRE ATT&CK
  - Contiene todas las técnicas utilizadas en los últimos tiempos respecto a incidentes de ciberseguridad
- Son Escalables.

**NIST**  
**CSF**



**NIST**  
**SP**  
**800-53**

**COBIT**



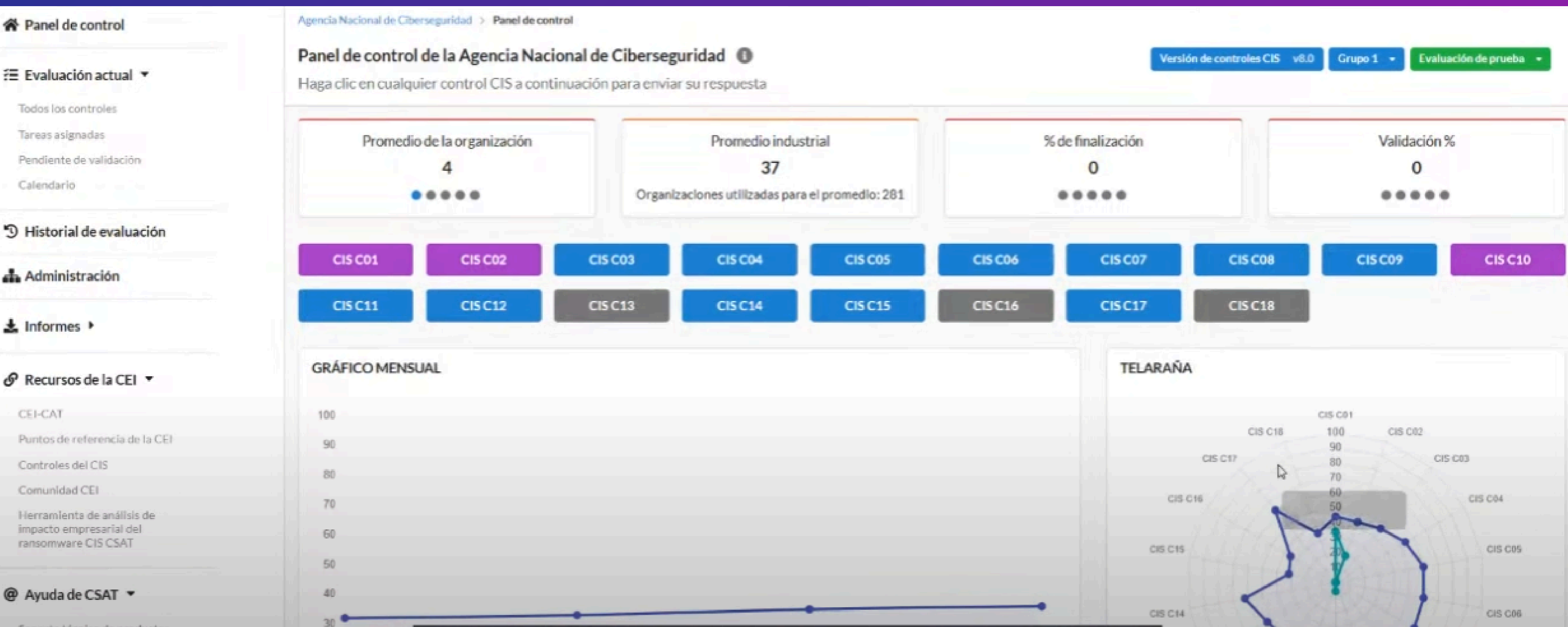
# Por que son una buena estrategia?

- Estan enfocados en lo practico y accionable.
- Mejora continua que cuenta con el respaldo de diversas organizaciones.
- Los nuevos controles integran regularmente nuevas técnicas para protegerse de nuevas amenazas.
  - Ej. Servicios Cloud o Zero trust.
- Optimización de costos, ya que se enfoca en los errores mas críticos primero



# Mirada General de los Controles

<https://csat.cisecurity.org>

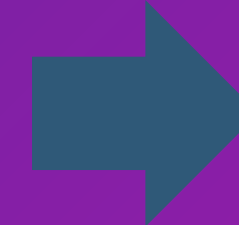




# Actividad RansomWare VanHelsing

## Chile, abril 2025

Actividad del ransomware VanHelsing en Chile - Alerta - CSIRT Nacional



# Charla: "Controles CIS: Mejorando la seguridad en las instituciones"

CIS-Controls-v8-Espanol-2.pdf