Webinar Gratuito

Grupo de Implementación 1 de CIS

Alonso Eduardo Caballero Quezada

:|: Hacking :|: Forense :|: Linux :|: OSINT :|: Ciberseguridad :|:

Sitio Web: www.ReYDeS.com -:- Correo: ReYDeS@gmail.com

Miércoles 22 Junio 2026

Alonso Eduardo Caballero Quezada

Cuento con más de diecinueve años de experiencia en el área y desde hace quince años me especializo en la áreas de Hacking, Forense, OSINT, Ciberseguridad y temas relacionados.

https://www.linkedin.com/in/alonsocaballeroquezada/

https://x.com/Alonso_ReYDeS

https://www.youtube.com/c/AlonsoCaballero

https://www.facebook.com/alonsoreydes/

https://www.instagram.com/alonso_reydes/

reydes@gmail.com

www.reydes.com

https://wa.me/51949304030

https://t.me/ReYDeS

La Realidad de las Amenazas

El panorama de la seguridad actual exige un enfoque pragmático y estructurado:

- **Aumento del cibercrimen:** Los ciberataques son cada vez más frecuentes, automatizados, y sofisticados.
- **Tiempos de contención:** Las organizaciones tardan un promedio de más de 200 días en detectar brechas de ciberseguridad.
- **Recursos limitados:** Gran parte de las PYMES asignan roles de TI sin entrenamiento formal en ciberseguridad avanzada.
- **Higiene como escudo:** Más del 85% de los ataques exitosos se previenen con controles básicos bien implementados.

¿Qué es el Framework CIS?

18 Controles de Seguridad

El Center for Internet Security (CIS) define directrices de mejores prácticas compuestas por 18 controles de seguridad críticos.

Están diseñados de manera priorizada para detener amenazas y vectores de ataque más comunes y peligrosos del mundo real.

Grupos de Implementación

Para facilitar la adopción, los controles de la v8 se dividen en tres Grupos de Implementación (IG) según los recursos y perfiles de riesgo.

Esto permite a cualquier equipo de TI ejecutar la ciberseguridad por etapas lógicas, sin abrumar la operación diaria.

Higiene Esencial: Grupo 1 (IG1)

153 Salvaguardas Totales en CIS v8

El Punto de Partida Obligatorio

El Grupo de Implementación 1 (IG1) define el estándar mínimo de ciberseguridad esencial para cualquier organización.

Consiste en las salvaguardas prioritarias las cuales son realistas de implementar, incluso para empresas pequeñas o con presupuesto limitado, utilizando soluciones, y hardware comercial estándar (COTS).

Conocer y Mapear tu Entorno

Inventarios de Activos

La base de toda estrategia defensiva es saber cuales elementos componen tu red:

- **Control 1: Inventario de Hardware:** No puedes proteger aquello no sabes existe. Identifica, registra, y autoriza cada dispositivo físico conectado a tu infraestructura.

- **Control 2: Inventario de Software:** Mantén visibilidad de todas las aplicaciones utilizándose. Evita el uso de software sin licencia o no autorizado.

Proteger la Información Sensible

Inventario de Datos

Localiza donde reside la información sensible, bases de datos de clientes, y propiedad intelectual dentro de la organización.

Clasificación

Categoriza los archivos según su nivel de confidencialidad para priorizar el esfuerzo de encriptación y control de acceso.

Retención Segura

Establece políticas claras para eliminar datos innecesarios de manera segura, reduciendo la exposición ante robos de información.

Robustecer Accesos y Sistemas

- **Configuración Segura (Control 4):** Modifica las credenciales y configuraciones por defecto de encaminadores, servidores y terminales para mitigar ciberataques oportunistas automatizados.

- **Gestión de Cuentas (Control 5):** Limita estrictamente los privilegios administrativos. Los usuarios únicamente deben acceder a las herramientas necesarias para su rol laboral diario.

- **Autenticación Segura (Control 6):** Implementa políticas de contraseñas robustas y despliega autenticación multifactor (MFA) obligatoria para el correo electrónico y accesos VPN.

Resiliencia y Defensas Activas

Control 10: Anti-Malware

Despliega y actualiza de manera centralizada software de protección en endpoints para neutralizar malware (virus, ransomware, etc.)

Control 11: Respaldos

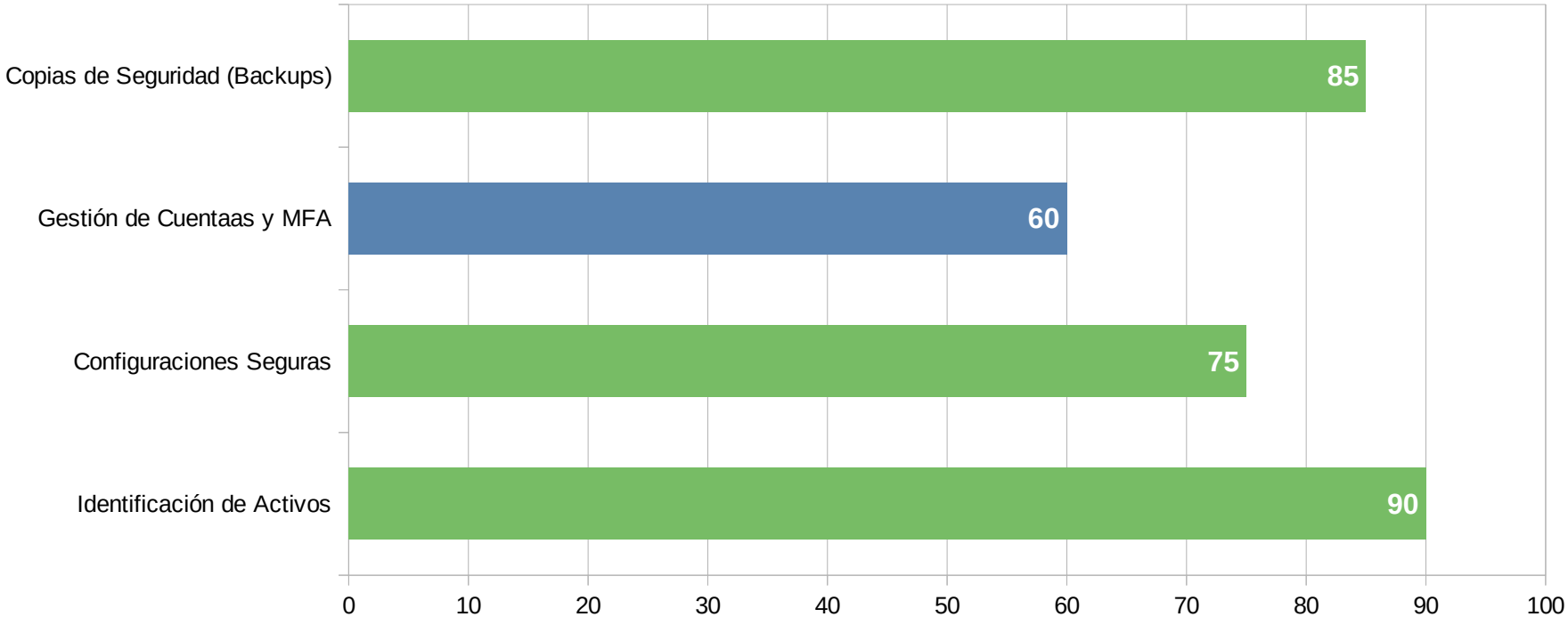
Realiza copias de seguridad automáticas y aisladas de la red para garantizar la recuperación ante secuestros de datos.

Control 14: Capacitación

Educa a tus empleados para reconocer intentos de ingeniería social (Phishing) y configurar redes domésticas seguras.

Métricas de Implementación

La implementación del IG1 dota a la empresa de una cobertura medible en sus áreas más críticas de TI, facilitando el reporte a la alta dirección.

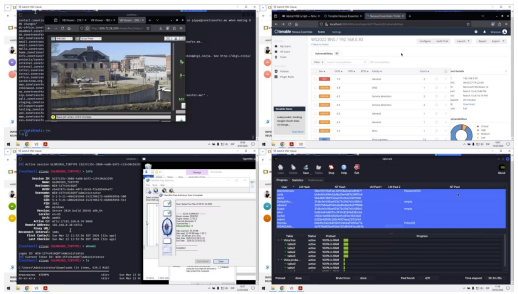


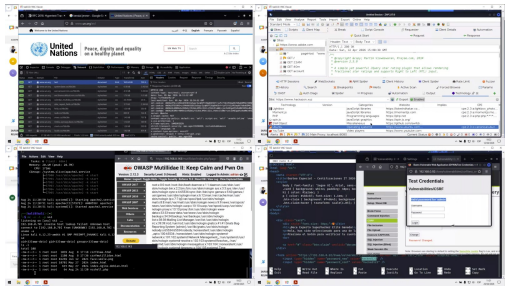
Impacto Comercial de CIS IG1

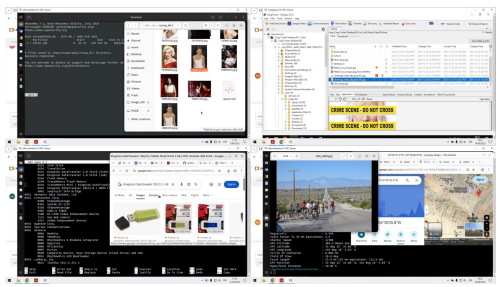
Beneficio del Negocio	Enfoque Técnico en IG1	Impacto Operativo
Reducción de Riesgos Directos	Detiene vectores automatizados de malware y ransomware comunes.	Muy Alto
Cumplimiento Normativo	Sienta bases operativas compatibles con ISO 27001 o NIST CSF.	Alto
Retorno de Inversión (ROI)	Aplica herramientas accesibles, de bajo costo operativo y uso de COTS.	Alto
Conciencia Organizacional	Reduce drásticamente errores humanos mediante entrenamiento simple.	

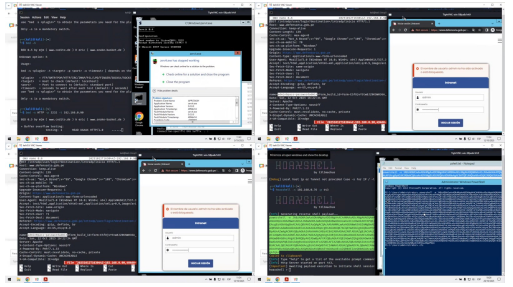
Cursos (Aula Virtual)

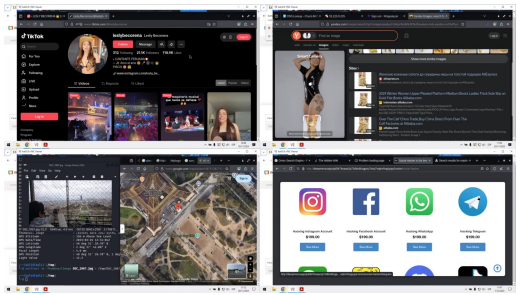
- Curso Hacking Ético
- Curso Hacking Aplicaciones Web
- Curso Informática Forense
- Curso Hacking con Kali Linux
- Curso OSINT - Open Source Intelligence
- Curso Forense de Redes
- Curso CiberSeguridad
- Curso Ciberseguridad Windows y Linux
- Curso OWASP Top 10
- Curso Análisis de Malware
- Curso Hacking OT
- Curso Maltego Graph CE
- Y más...

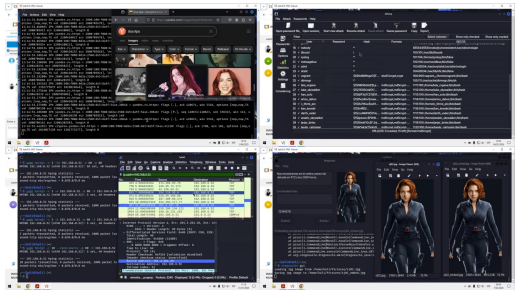












Alonso Eduardo Caballero Quezada :|: Sitio web: www.reydes.com :|: Correo: reydes@gmail.com

Webinar Gratuito

Grupo de Implementación 1 de CIS

Alonso Eduardo Caballero Quezada

:|: Hacking :|: Forense :|: Linux :|: OSINT :|: Ciberseguridad :|:

Sitio Web: www.ReYDeS.com -:- Correo: ReYDeS@gmail.com

Miércoles 22 Junio 2026