



OWASP

Open Web Application
Security Project

¿ Cómo lo Lograron ?



Jonathan Maderos

 **@JTMaderos**

Acerca de Mí



OWASP

Open Web Application
Security Project

Investigador





OWASP

Open Web Application
Security Project

**Los hechos narrados en esta
presentación son reales y pueden
estar ocurriendo en cualquier
empresa, incluyendo donde laboras
actualmente.**



OWASP

Open Web Application
Security Project

Seguridad Perimetral

Corresponde a la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuación de intrusos en instalaciones especialmente sensibles.



OWASP

Open Web Application
Security Project

Defensa en Profundidad

“En el área militar se utiliza el término defensa en profundidad para denotar el uso de varias líneas de defensa consecutivas, cada una de ellas con un nivel de protección creciente , en vez de una única barrera muy fuerte .”

Defensa en Profundidad



OWASP

Open Web Application
Security Project

Controles Físicos: Control de acceso físico, Cámaras de vigilancia, Controles ambientales, Sistemas de detección y supresión de incendios, etc.

Controles lógicos o Técnicos: Control de acceso lógico, Cifrado de datos y enlaces, Autenticación, Sistemas Automalware, Sistemas de monitoreo, etc

Controles administrativos: Políticas, Normas, Procesos, Procedimientos, Estándares, Guías, Programas de entrenamiento y concientización, etc.

Datos y Activos de la Organización

Investigación



OWASP

Open Web Application
Security Project

007





OWASP

Open Web Application
Security Project

Control de Chequeo Manual el cual incluía un personal Militar (2) ó más, armados con fusiles y/o armas cortas ,un personal Civil (2) ó más, distribuidos uno en Recepción y el resto para Revisiones y registro de Equipos.

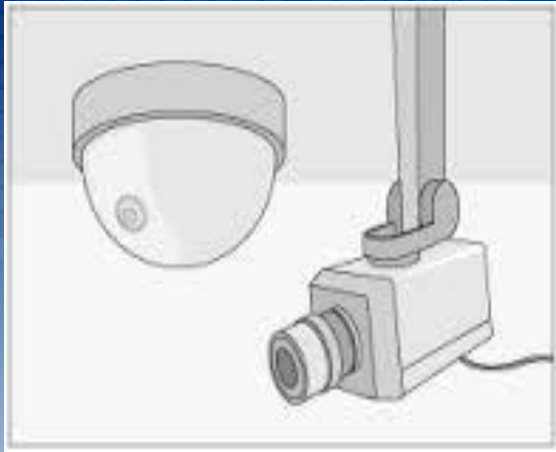


OWASP

Open Web Application
Security Project

Todas las áreas estaban cerradas con torniquetes y cercas de seguridad. El paso a través de ellas era sólo con un carnet electrónico.



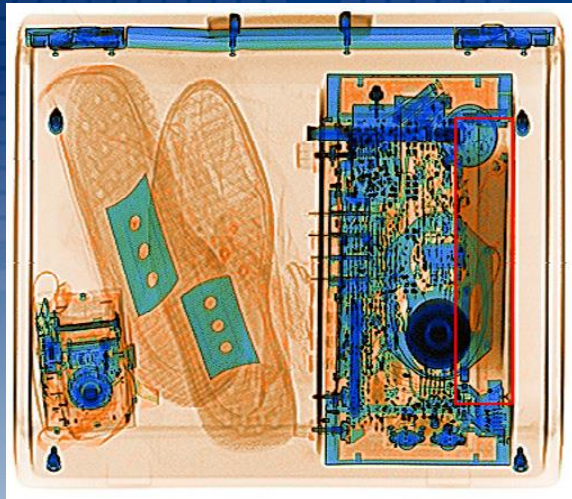


OWASP

Open Web Application
Security Project

Por cada nivel habían no menos de 3 cámaras de video. El acceso a las puertas era a través de carnets electrónicos

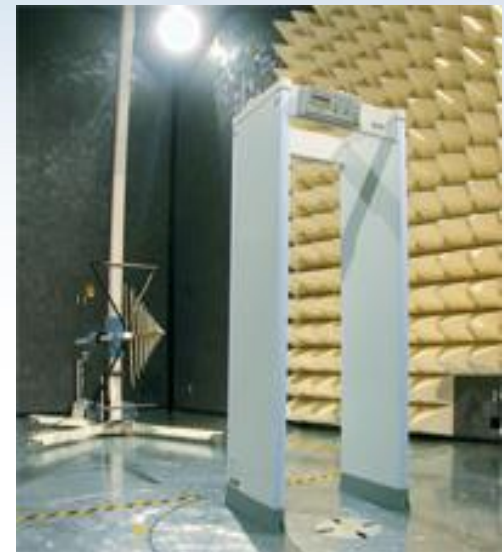




OWASP

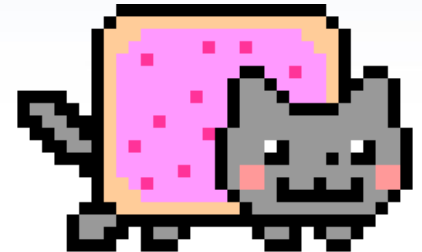
Open Web Application
Security Project

Scanner de RX y un Arco detector de Metales





Cada equipo que entraba a la institución se les tomaban los seriales del equipo y la descripción externa del mismo (Marcas, stickers, etc.).





OWASP

Open Web Application
Security Project

¿ Cómo lo Lograron ?

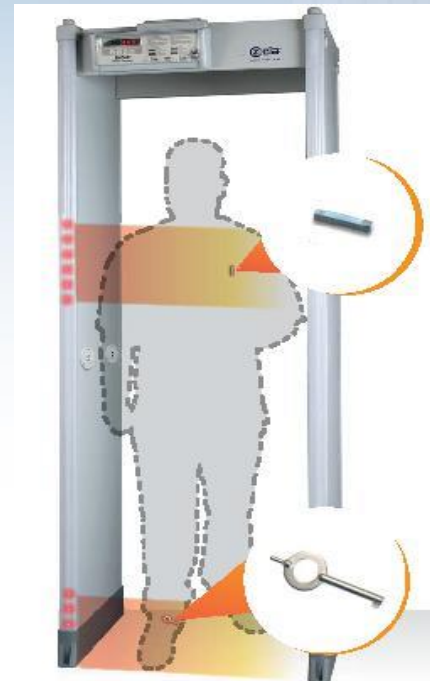




OWASP

Open Web Application
Security Project

Arco Detector de Metales SMD-600 Multi Zone de la empresa CEIA





OWASP

Open Web Application
Security Project

***HI-SCAN 6046SI (SMITH DETECTION)
HEIMANN X-RAY INSPECTION SYSTEM
de la empresa Heimann & Smith***



Consideraciones



OWASP

Open Web Application
Security Project

- ✓ **El personal de seguridad era externo.**
- ✓ **Toda actividad en los pasillos, ascensores y áreas comunes era filmada.**
- ✓ **Todo equipo que entraba o salía quedaba registrado en un chequeo manual.**

Plantear Hipótesis



OWASP

Open Web Application
Security Project



Ataque a las Cámaras



OWASP

Open Web Application
Security Project

Fallo en Siemens SIPASS

<http://www.zonavirus.com/noticias/2012/vulnerabilidad-en-sistema-de-seguridad-fisica-siemens-sipass-integrated.asp>

Dirección de Memoria Afectada SIPASS

<http://security.biz.tr/tag/siemens-sipass-integrated-2-6-dospoc/>

The screenshot displays the SIPASS integrated security system interface. The top menu bar includes options like 'Aplicación', 'Zobrazit', 'Archív', 'Snímáče', 'Uživatelé', 'Systém', 'Okno', and 'Pomocník'. The main window is divided into several sections. On the left, there's a tree view showing the system hierarchy: 'Snímáče' (Cameras) with sub-items 'HK II', 'S680', 'SCR100', and 'Stance'; 'Server (100) (*** APIS ***)' and 'Patrol (1) (*** APIS ***)'.

The central part of the interface shows a table of transactions. The table has columns for 'Typ transakce', 'Zdroj', 'Datum', 'Čas', 'Uživatel ID', 'Uživatel', 'Transakce', 'Činnost', 'Přerušeno / Identif.', 'Přístroj', and 'Stav'. The table contains multiple rows of data, including transactions for 'B Recepce', 'E Administrativa', 'Patrol', 'BI Urgent', and 'B Recepce'.

On the right side, there's a status panel with icons for 'HK II', 'S680', and 'SCR100', each with a status indicator (S, T, or a combination). Below this, there's a section for 'Snímáče' and 'Uživatelé'.

At the bottom, there's a legend for transaction types: 'Všechny aktuální transakce' (All current transactions), 'Docházkové listy' (Attendance lists), 'Technické listy' (Technical lists), 'Stavové listy' (Status lists), and 'Oběžné listy' (Circulating lists). The bottom status bar shows 'NUM' and the date '24.8.2011 8:35:56'.

Eslabón más Débil: El Humano



OWASP

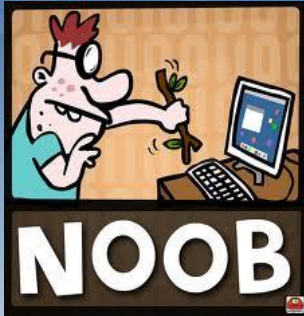
Open Web Application
Security Project

El personal encargado de verificar los seriales de los equipos no tenía preparación para la tarea.

Los equipos no eran revisados de forma correcta

El acceso de las personas a la institución no era controlado de forma correcta (carnet visible, motivo de la visita, etc..)

Los equipos de seguridad podían tener fallos.



Verificación de los seriales



Verificación de los Equipos



Verificación de las Personas

Acceso a Equipo No Autorizado



OWASP

Open Web Application
Security Project

El atacante entraba un equipo dañado identificado con un sticker y lo registraba.

En el proceso de Registro , dictaba o falseaba los seriales electrónicos del equipo.

Con un carnet auténtico, se validaba en el torniquete y entraba.

Acceso a Equipo No Autorizado



OWASP

Open Web Application
Security Project

Dentro de la institución, tomaba el equipo falso, y le quitaba el(los) sticker(s).

Sustituía el equipo falso por uno de la empresa y le colocaba un sticker igual al del equipo falso.

Se retiraba de la institución y permitía que revisaran el equipo al salir.

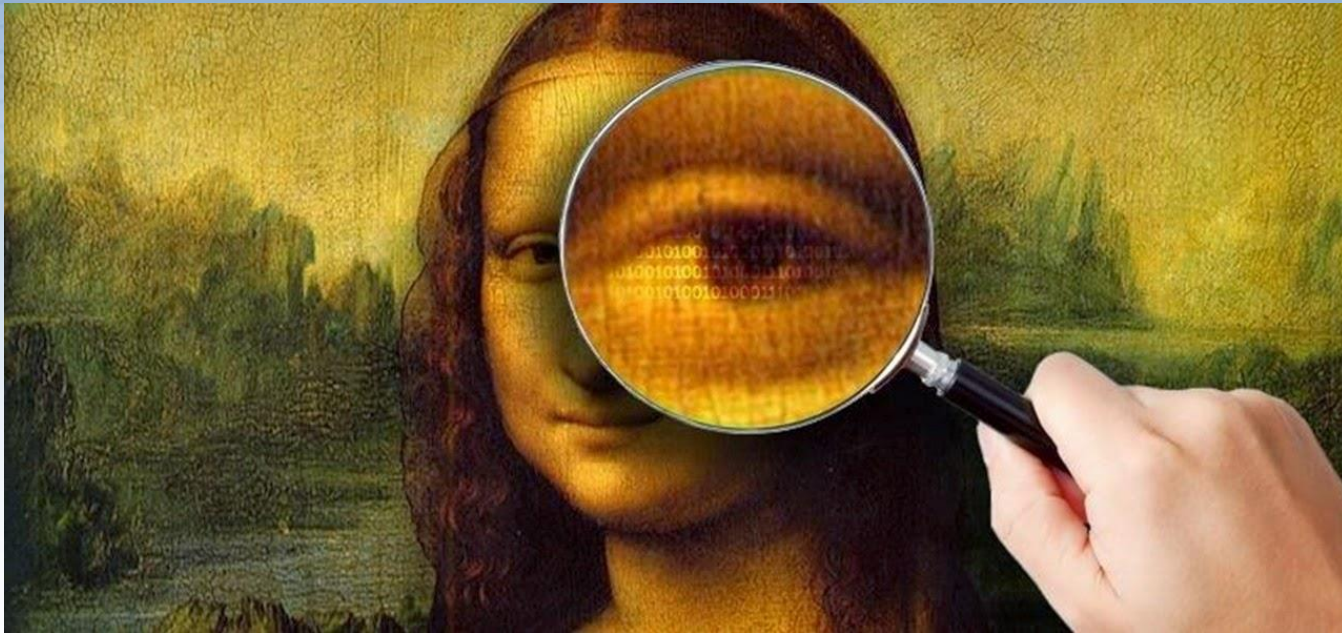


Acceso No Autorizado Sin Uso de Carnets



OWASP

Open Web Application
Security Project





OWASP

Open Web Application
Security Project

Análisis del Hardware

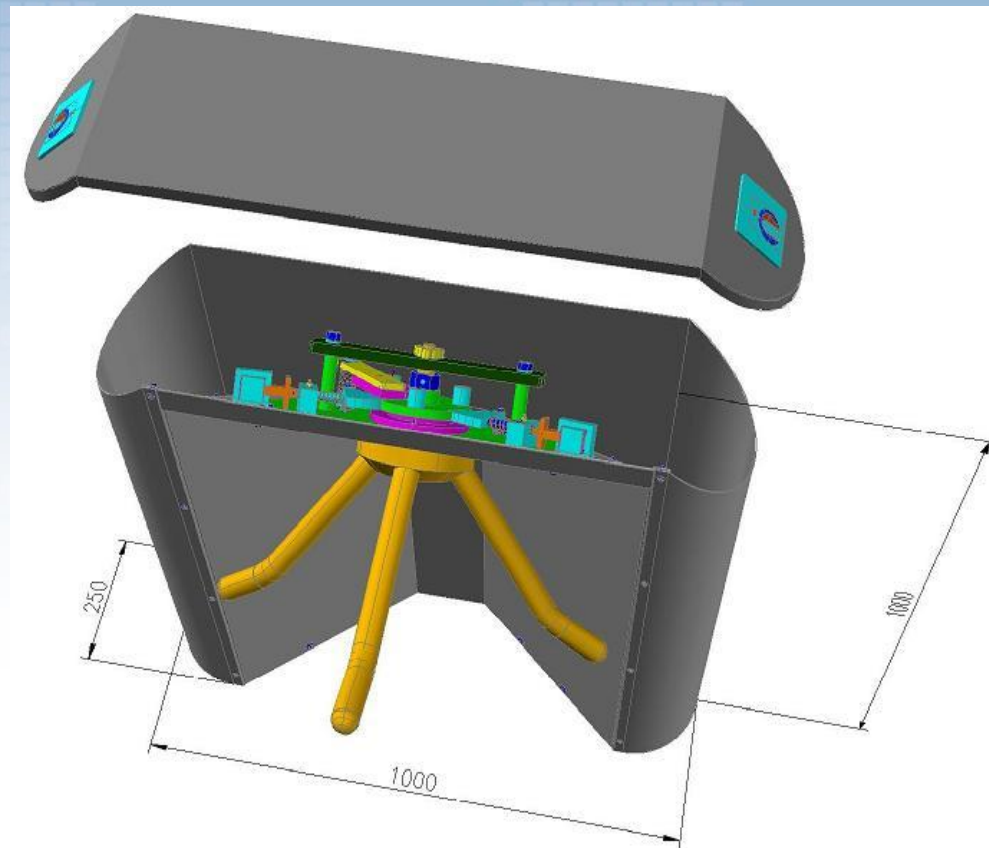




OWASP

Open Web Application
Security Project

Torniquete de Seguridad



Vista Interna de los Mecanismos



Verificando . . .



OWASP

Open Web Application
Security Project

Revisión de los Equipos y verificación de Seriales y Marcas Externas.

Revisión de las Cámaras para comparar el conteo de personas que accesaron contra las personas que el sistema Siemens SIPass registró y la hora y fecha de acceso.

Revisión de la Cámaras para observar coincidencias en el acceso y la salida de personas en pares.

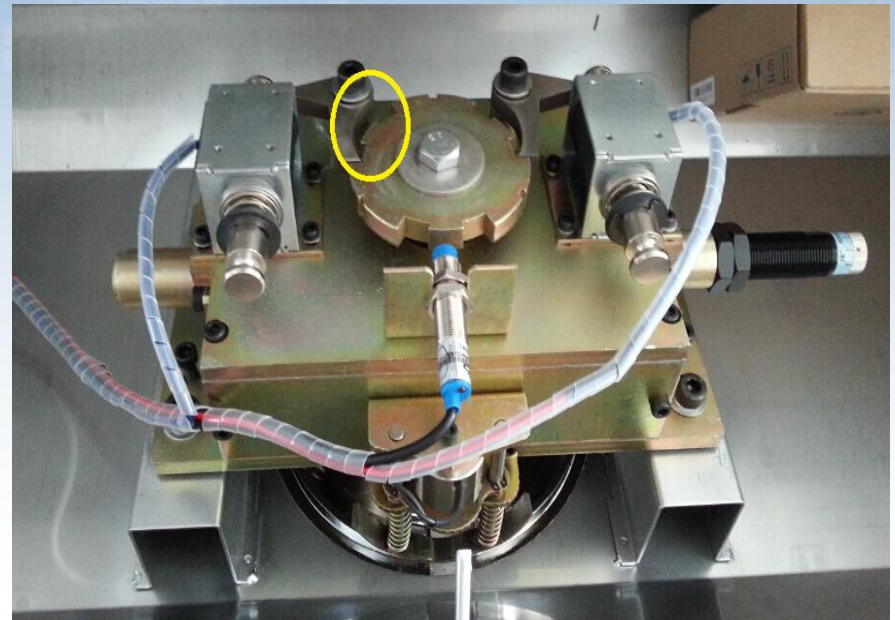
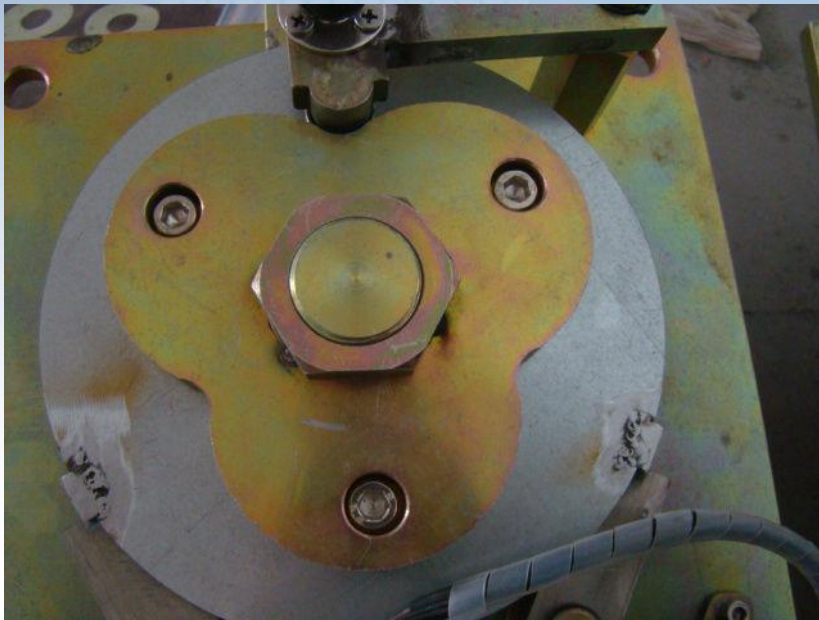


0 Day de Hardware ?



OWASP

Open Web Application
Security Project



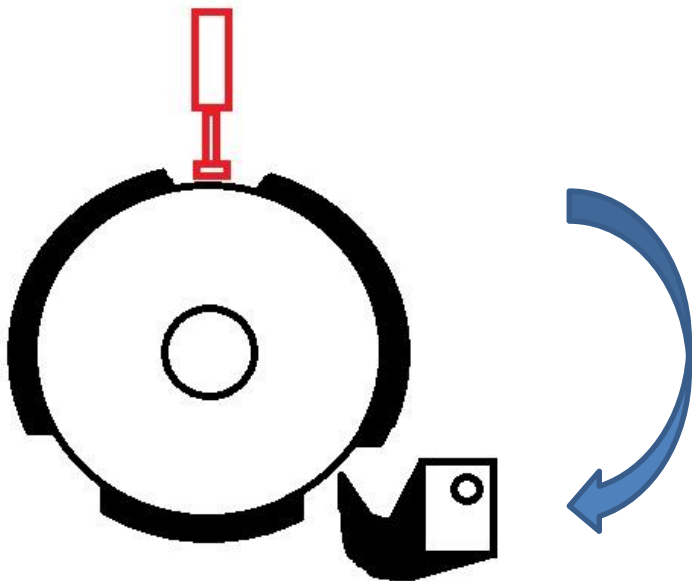
Torniquete en Modo Bloqueado



OWASP

Open Web Application
Security Project

Podemos ver el pistilo extendido y la cuña o pasador en modo de bloqueo. Acá la luz del Torniquete se encuentra en Rojo



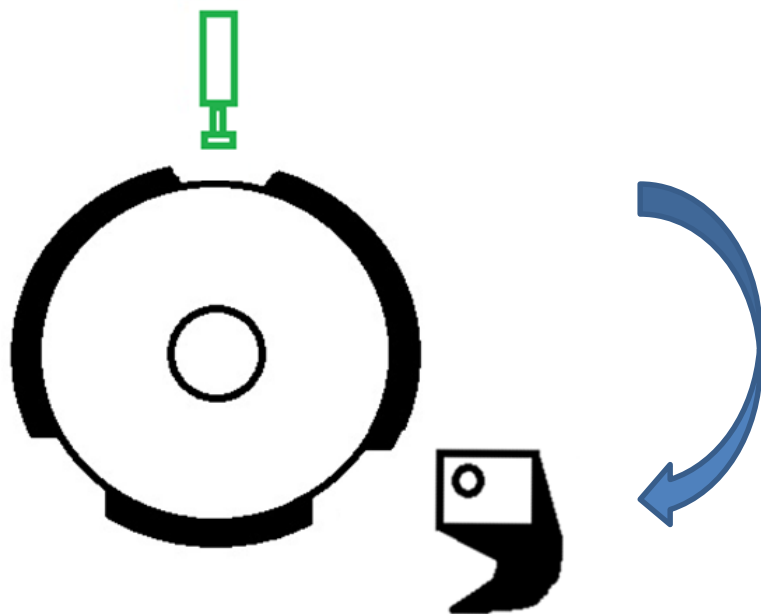
Torniquete en Modo Desbloqueado



OWASP

Open Web Application
Security Project

Podemos ver el pistilo retraído y la cuña o pasador en modo de desbloqueo. Acá la luz del Torniquete se encuentra en verde. Acá ya las aspas del torniquete pueden girar.



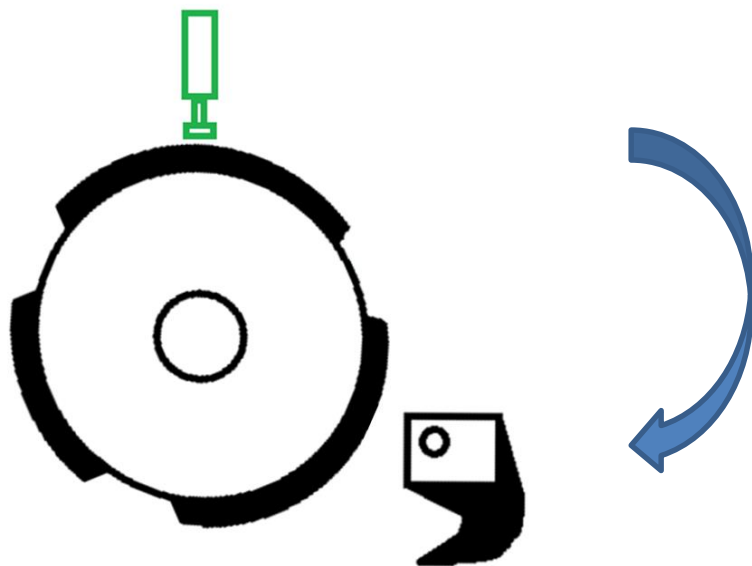
Torniquete en Modo Desbloqueado



OWASP

Open Web Application
Security Project

Podemos ver el pistilo retraído y la cuña o pasador en modo de desbloqueo. Acá la luz del Torniquete continúa en verde. Acá ya las aspas del torniquete han girado un poco más de su posición inicial.



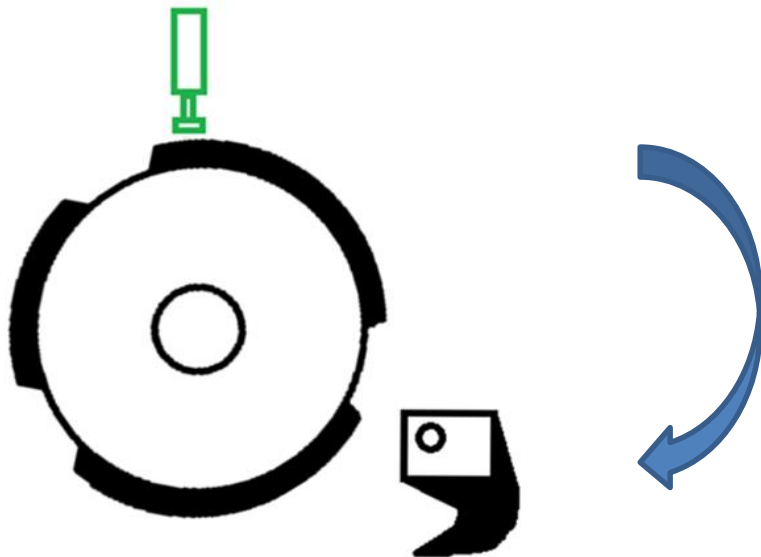
Torniquete en Modo Desbloqueado



OWASP

Open Web Application
Security Project

Podemos ver el pistilo retraído a punto de activar la posición de bloqueo y la cuña o pasador en modo de desbloqueo. La luz del Torniquete en este punto aún se mantiene en verde.



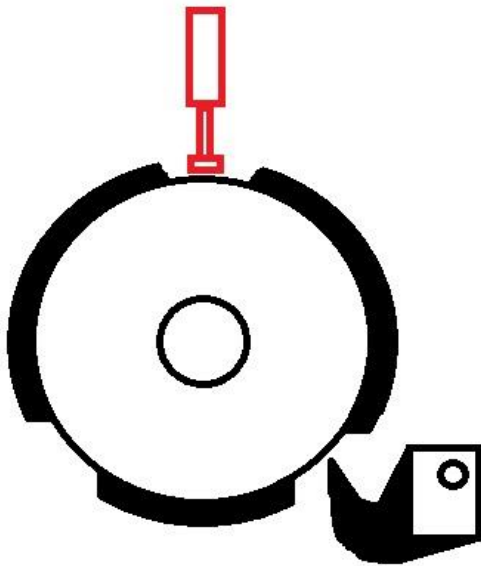
Torniquete en Modo Bloqueado



OWASP

Open Web Application
Security Project

Si la persona continúa el recorrido por el torniquete de forma frontal las aspas llegan a su tope activando el pistilo, el cual a su vez activa el pasador y bloquea el torniquete.



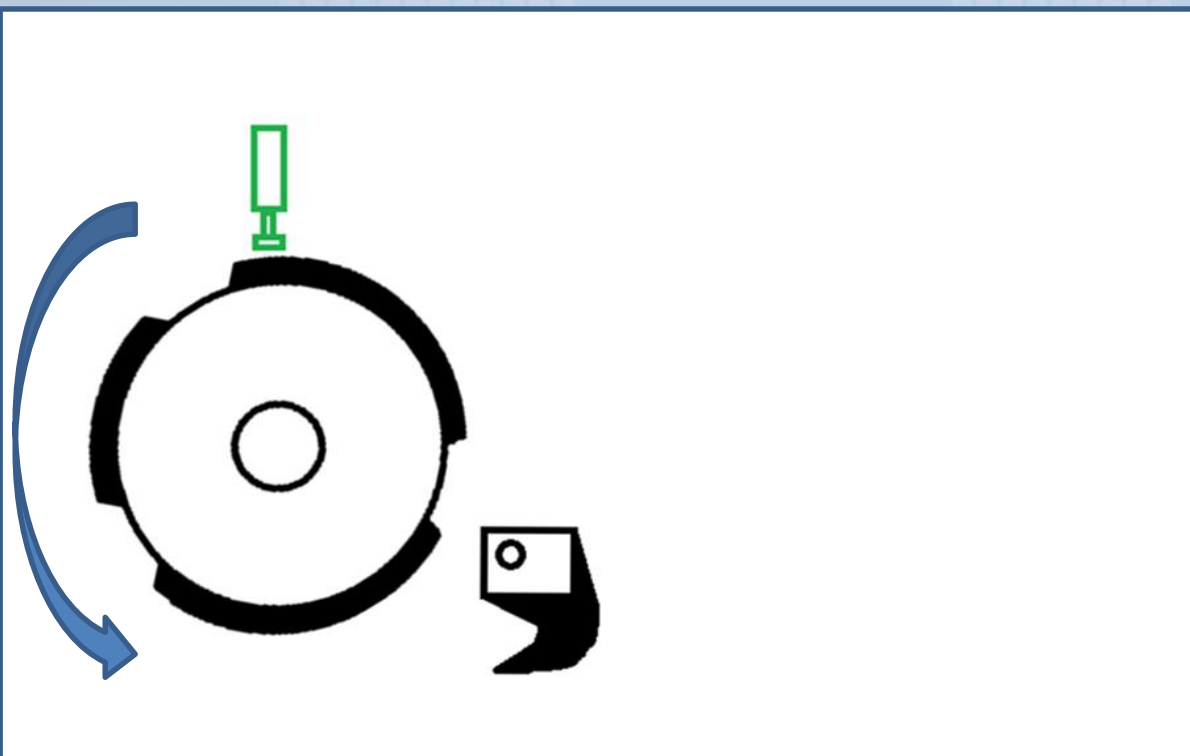
Torniquete en Modo Desbloqueado



OWASP

Open Web Application
Security Project

Girar las aspas de forma invertida, forzando el rotor hacia atrás. Una persona delgada caminando no de forma frontal, puede pasar por el torniquete antes de activar el modo bloqueo.



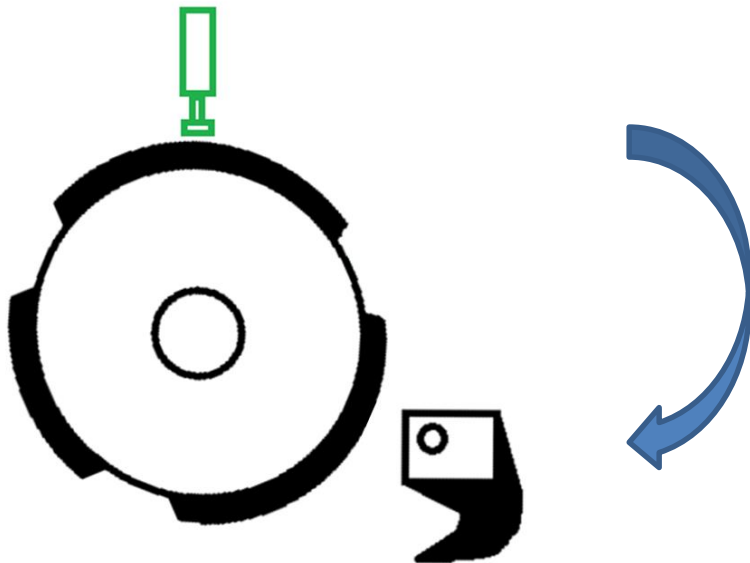
Torniquete en Modo Desbloqueado

Podemos ver el pistilo retraído y la cuña o pasador en modo de desbloqueo. Acá la luz del Torniquete continúa en verde.



OWASP

Open Web Application
Security Project



Contramedidas



OWASP

Open Web Application
Security Project

El personal que verifica los seriales de los equipos debe poseer conocimientos de hardware básicos.

La verificación de los equipos debe hacerse de forma detallada: Stickers, marcas físicas, etc. Encendido del Equipo.

Realización del mantenimiento a las Cámaras para evitar fallos.

Realización de mantenimiento a los mecanismos de los Torniquetes. (*)

Etiquetas RFI a equipos de la Institución o Empresa.





OWASP

Open Web Application
Security Project

Gracias ...

Jonathan_Maderos@hotmail.com

 @JTMaderos

