



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.**



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 disuención de intrusos en instalaciones especialmente sensibles.



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

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

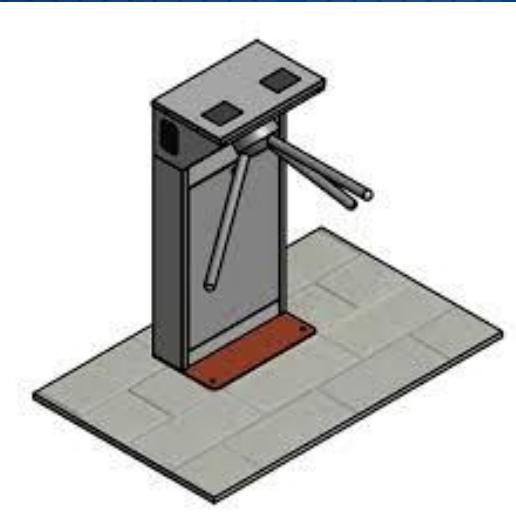
007





OWASP
Open Web Application
Security Project

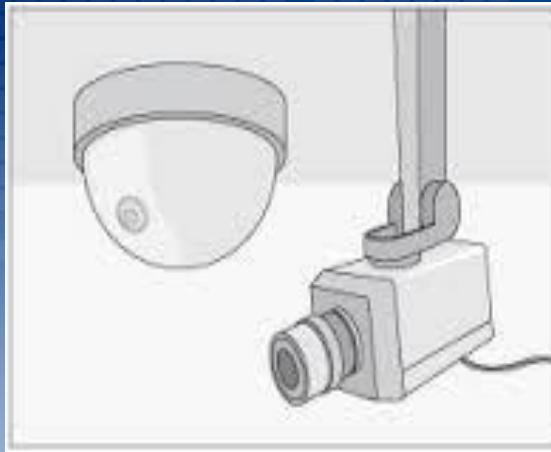
Control de Chequeo Manual el cual incluía un personal Militar (2) ó más, armados con fusiles y/o armas cortas ,un personal Civil (2) ó más, distribuidos uno en Recepción y el resto para Revisiones y registro de Equipos.



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.

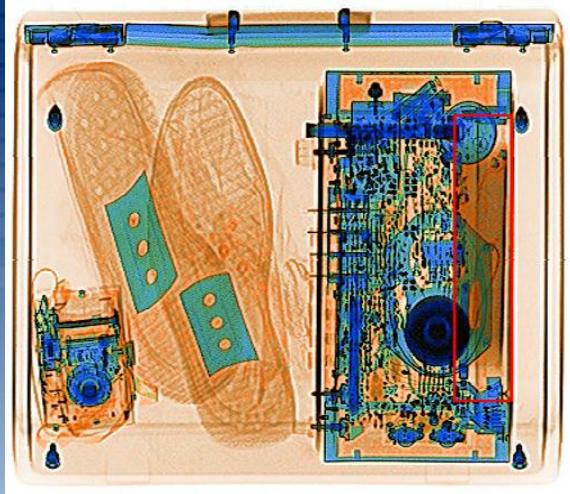




OWASP
Open Web Application
Security Project

Por cada nivel había 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



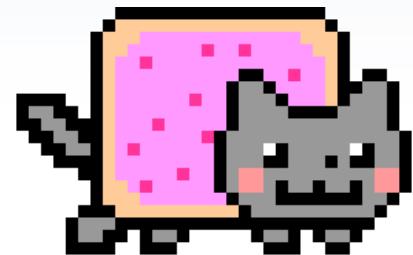


BIG BROTHER IS
WATCHING YOU



OWASP
Open Web Application
Security Project

*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

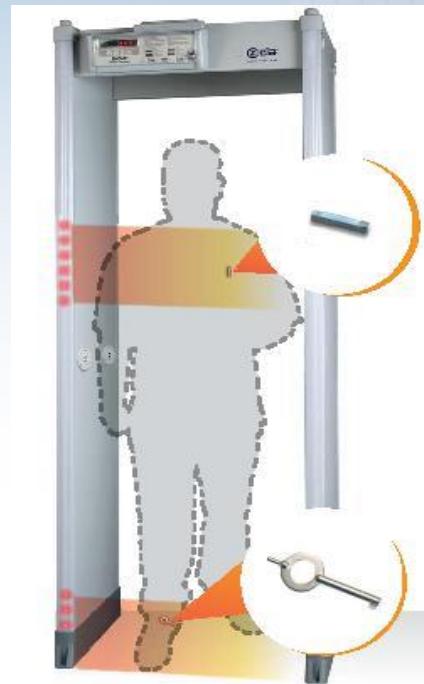
¿ Cómo lo Lograron ?





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***





OWASP
Open Web Application
Security Project

SIPass Integrated de Siemens tanto para el video como el acceso a las puertas.

The screenshot shows a software interface for managing access control and video surveillance. The top menu includes: Aplikácia, Zobrazit, Archív, Snímáče, Uživatelia, Systém, Okno, Pomocník. The sidebar on the left lists 'Snímáče' (Cameras) with icons for HK II, 5680, and SCR100, and 'Stánice' (Stations) with icons for Server (100) and Patrol (1). The main window displays a table of transactions with columns: Počet transakcií (14429), Filter, and Upozriť. The table lists various transactions such as Recepčia, Administratívna, and Patrol, along with details like Užívateľ meno, Čas, and Transakcia. The bottom of the window shows tabs for Všetky aktívne transakcie, Dočasného k., Technické k., Stavové k., Obslužné k., and Archív. The status bar at the bottom right shows: Prezernom stav F1, NUM, and 24.8.2011 8:35:56.

Consideraciones



- ✓ 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/>

Applikácia Zobrazit Archív Snímáteľa Systém Okno Pomocník

Snímáteľa HK II 5680 SCR100

Stanicie Server (100) (** APIS ***)
Patrol (1) (** APIS ***)

Snímáteľa Usílateľa Čísleky

Počet transakcií: 14429 Filter: Upraviť filtre

Typ transakcie	Zdroj mena	Δt	Δs	Datum	Δt	Čas	Δt	Užívateľ ID	Δt	Užívateľ meno	Transakcia	Δt	Činnosť	Δt	Prenumešenie / Identifik.	Δt	Priestor	Δt	Staní
B Recepčia	1	09.02.2011	07:04:08	67						Šandorová Viera	Overeň		Odhod	0	> 0	100			
E Administratívna	3	09.02.2011	07:04:58	179						Matúša Marcel	Overeň		Prichod	0	> 0	100			
E Administratívna	3	09.02.2011	07:05:58	343						Bohdáková Jana	Overeň		Odhod	2	> 0	100			
Patrol	0	09.02.2011	07:06:58	0							Obrnenová komunikácia	Obrnenová komunikácia	Odhod	2	> 0	100			
B Urgent	2	09.02.2011	07:10:12	164						Pálenčík Adrián	Overeň		Prichod	0	> 0	100			
B Recepčia	1	09.02.2011	07:10:36	189						Cabánová Alena	Overeň		Prichod	0	> 0	100			
E Administratívna	1	09.02.2011	07:14:44	121						Babušková Viera	Overeň		Odhod	0	> 0	100			
B Recepčia	1	09.02.2011	07:14:10	97						Pántíková Eva	Overeň		Odhod	0	> 0	100			
B Recepčia	1	09.02.2011	07:16:20	311						Lesková Zuzana	Overeň		Odhod	0	> 0	100			
B Recepčia	1	09.02.2011	07:19:42	228						Mesák Branislav	Overeň		Odhod	0	> 0	100			
BL Recepčia	2	09.02.2011	07:20:24	204						Foltinová Stáťka	Overeň		Prichod	0	> 0	100			
Patrol	0	09.02.2011	08:03:10	0							Obrnenová komunikácia	Obrnenová komunikácia	Prichod	1	-	100			
Patrol	0	09.02.2011	08:04:10	0								Obrnenová komunikácia	Obrnenová komunikácia	Prichod	1	-	100		
B Urgent	2	09.02.2011	08:06:48	205						Riedloška Alena	Overeň		Prichod z prenúšenia	2	- Vyšetroenie zamestnanc...	100			
E Administratívna	0	09.02.2011	08:29:24	169						Waldmannová Andrea	Overeň		Prichod	0	> 0	100			
B Recepčia	1	09.02.2011	09:14:28	104						Stachová Beata	Overeň		Odhod	0	> 0	100			
Patrol	0	16.03.2011	16:08:07	0								Prihlásenie do systému		0	-	0			
Patrol	0	16.03.2011	16:10:17	0								Spustenie programu PA...		0	-	1			
Patrol	0	16.03.2011	16:10:28	0								Prihlásenie do systému		0	-	1			
Patrol	0	16.03.2011	16:15:03	0								Bruháčovského Ľubomíra			0	> 0	100		

Všetky aktuálne transakcie: Dozdravkova Ir. Technické Ir. Stavovce Ir. Obsluha Ir. Archiv

Pre pomocné stáť F1

NUM 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.

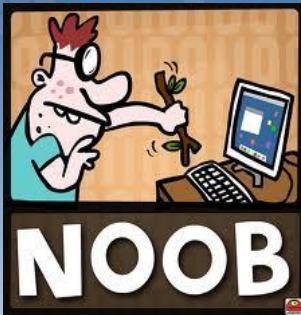
Los equipos no eran revisados de forma correcta

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.



OWASP
Open Web Application
Security Project



Verificación de los seriales



Verificación de los Equipos



Verificación de las Personas

Acceso a Equipo No Autorizado



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

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

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

Acceso a Equipo No Autorizado



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

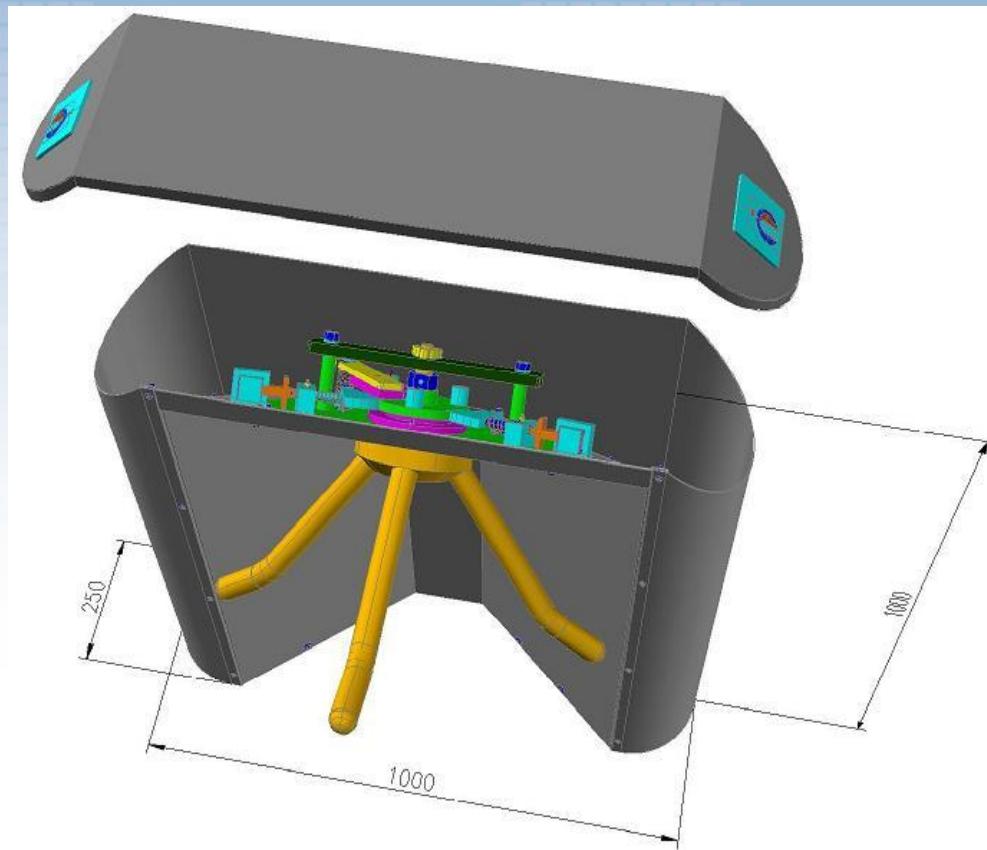
Análisis del Hardware





OWASP
Open Web Application
Security Project

Torniquete de Seguridad





OWASP
Open Web Application
Security Project

Vista Interna de los Mecanismos



Verificando . . .



OWASP
Open Web Application
Security Project

Revisión de los Equipos y verificación de Serials 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.

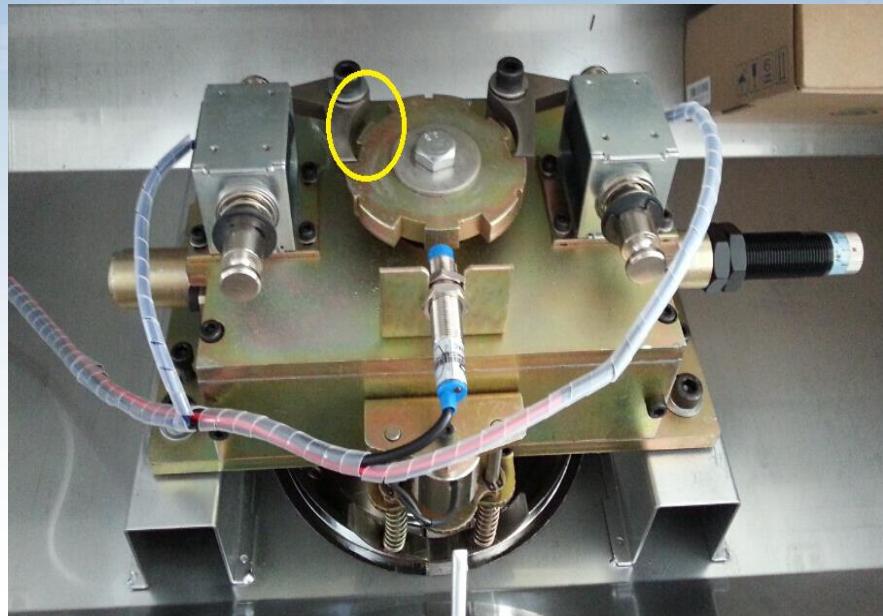
Revisión de la Cámaras para observar coincidencias en el acceso y la salida de personas en pares.



0 Day de Hardware ?



OWASP
Open Web Application
Security Project

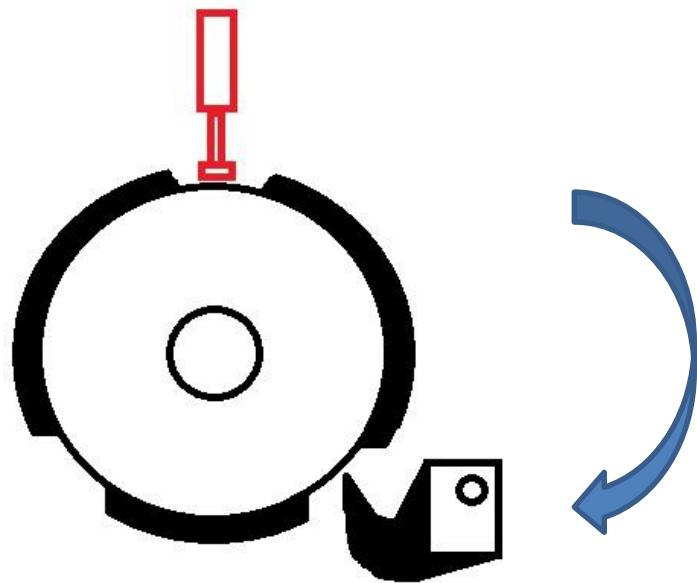


Torniquete en Modo Bloqueado



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

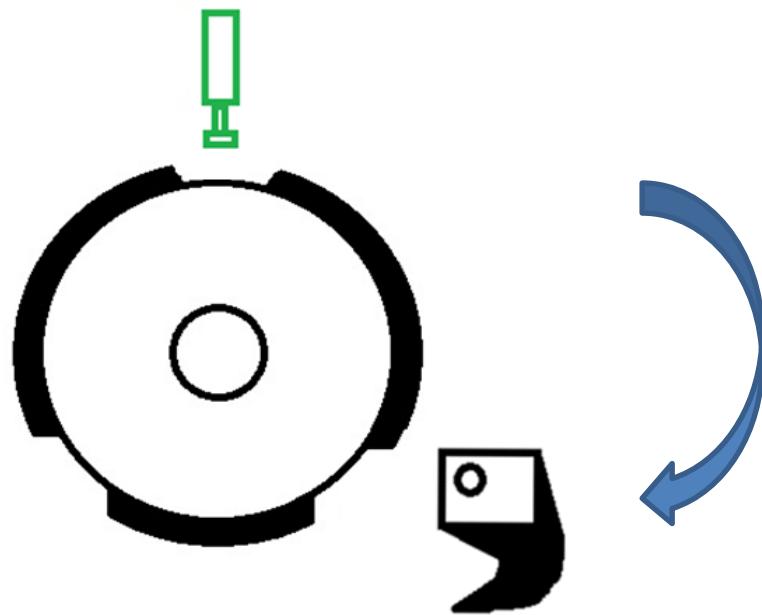


Torniquete en Modo Desbloqueado



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.

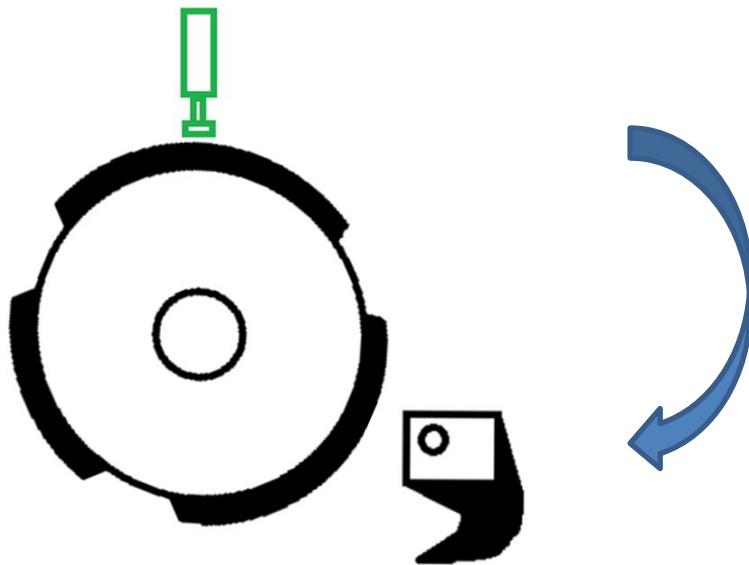


Torniquete en Modo Desbloqueado

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.



OWASP
Open Web Application
Security Project

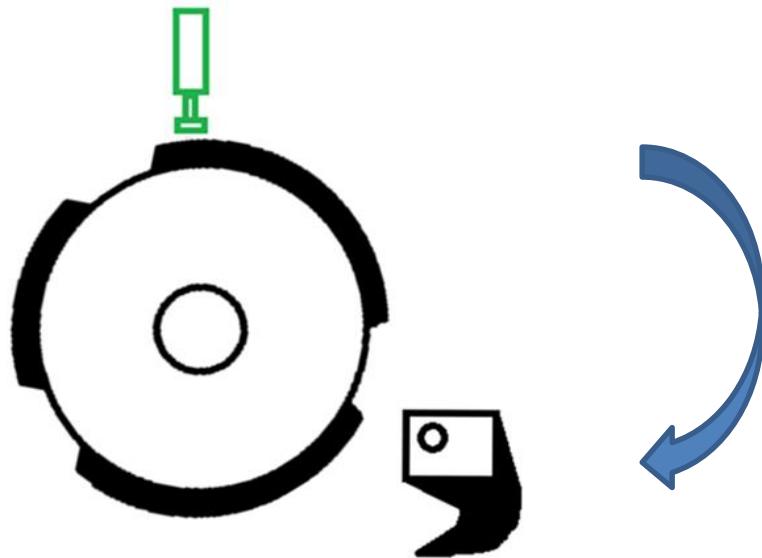


Torniquete en Modo Desbloqueado



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.

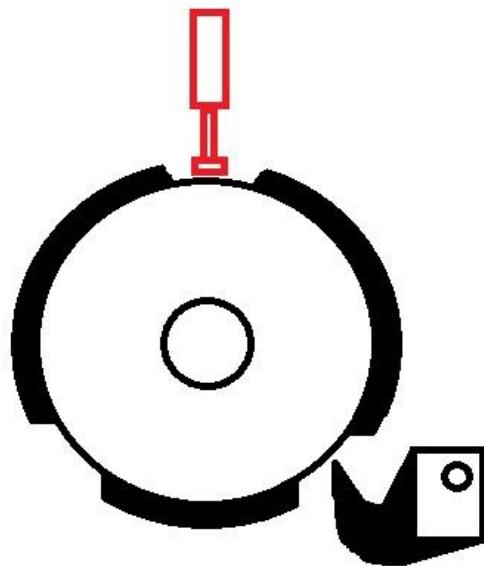


Torniquete en Modo Bloqueado



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.

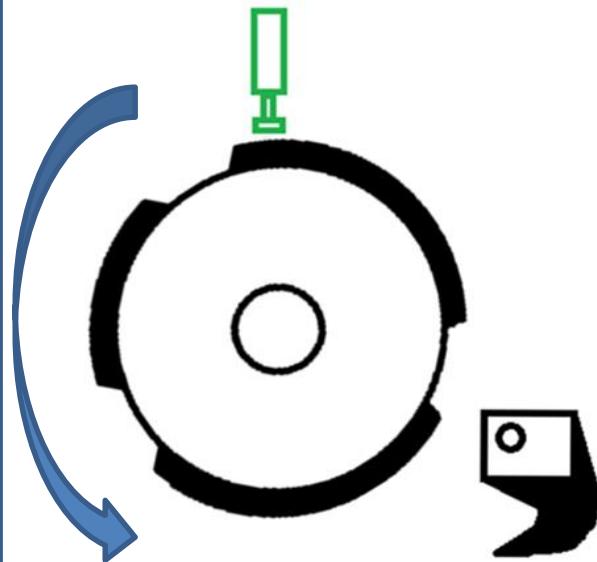


Torniquete en Modo Desbloqueado



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.

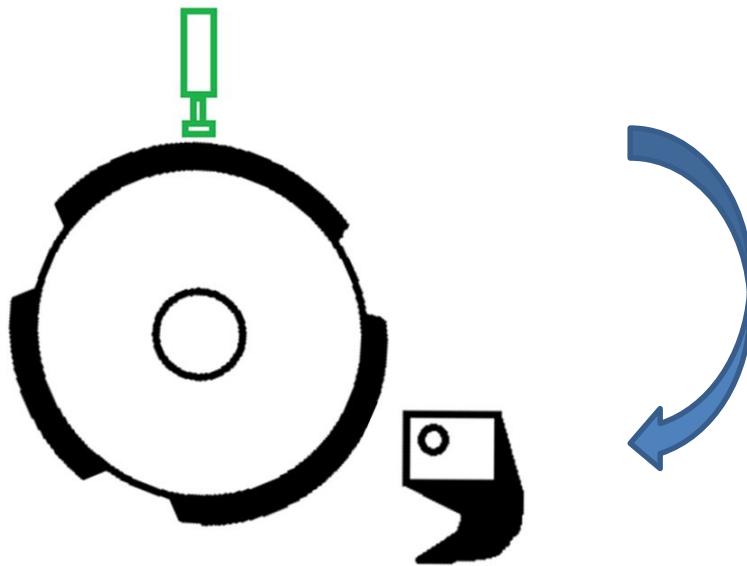


Torniquete en Modo Desbloqueado

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

