



BLACK HAT ARCHETYPE
Desmantelando al Hacker

Ciberseguridad



bha news



bha_cybersecurity



black-hat-archetype



bha - black hat archetype

¿Visitantes de tu sitio web van visto alertas sobre “Su conexión no es segura”? ¿Tus usuarios están seguros al realizar transacciones web? ¿Sabes la fecha de vencimiento de tus certificados digitales? ¿Sabes quien solicita certificados digitales a tu compañía? ¿Quieres prevenir la falsificación de documentos físicos de tu compañía?’

- ▶ La nueva era tecnológica ha permitido que empresas y organizaciones puedan ofrecer más servicios y transacciones en línea, sin embargo se debe priorizar la seguridad de las transacciones e información confidencial de nuestros clientes cumpliendo con los estándares PCI DSS (Payment Card Industry Data Security Standard) y con la legislación de protección de datos. por eso los certificados SSL (Secure Sockets Layer) son tan importantes y obligatorios, estos nos garantizan que un sitio web tenga autenticación de identidad y manejo de la información cifrada. Por eso vamos hablar de:



Entrust Datacard™

- ▶ Es una compañía estadounidense fundada en 1969 que ofrece diferentes soluciones enfocadas en herramientas de certificación, autenticación y seguridad.



EV Este tipo de certificado verifica el dominio, la ubicación física y permite un rastreo detallado en caso de fraude mientras se realiza una transacción en el sitio web. Los certificados EV se distinguen con un candado bloqueado, el nombre de la organización y, a veces, la identificación del país en la barra de direcciones web en la mayoría de los principales navegadores.

OV Los certificados OV, además de la propiedad del dominio, la organización se valida y los detalles del certificado se pueden ver en la mayoría de los principales navegadores web, lo que brinda a los usuarios en línea la oportunidad de determinar si el sitio en el que están es legítimo.

► ¿Cómo funcionan los certificados SSL?

1. Un navegador o servidor intenta conectarse a un sitio web (es decir, un servidor web) protegido con SSL. El navegador / servidor solicita que el servidor web se identifique.
2. El servidor web envía al navegador / servidor una copia de su certificado SSL.
3. El navegador / servidor verifica si confía o no en el certificado SSL. Si es así, envía un mensaje al servidor web.
4. El servidor web devuelve un acuse de recibo firmado digitalmente para iniciar una sesión cifrada SSL.
5. Los datos cifrados se comparten entre el navegador / servidor y el servidor web.



CERTIFICADOS SSL



Seguridad en aplicaciones móviles y en la nube

Experiencias más seguras para tus clientes

Protección de datos internos y del cliente

Ranking más fuerte de Google

CERTIFICADOS DIGITALES

Si quieres adquirir las herramientas ENTRUST DATACARD no dudes en contactarnos somos BLACK HAT ARCHETYPE

**Tel: (BOG) + 57 1 805 32 07 /
(MDE)+ 57 4 231 55 24**

