



CryptoBlack LTD

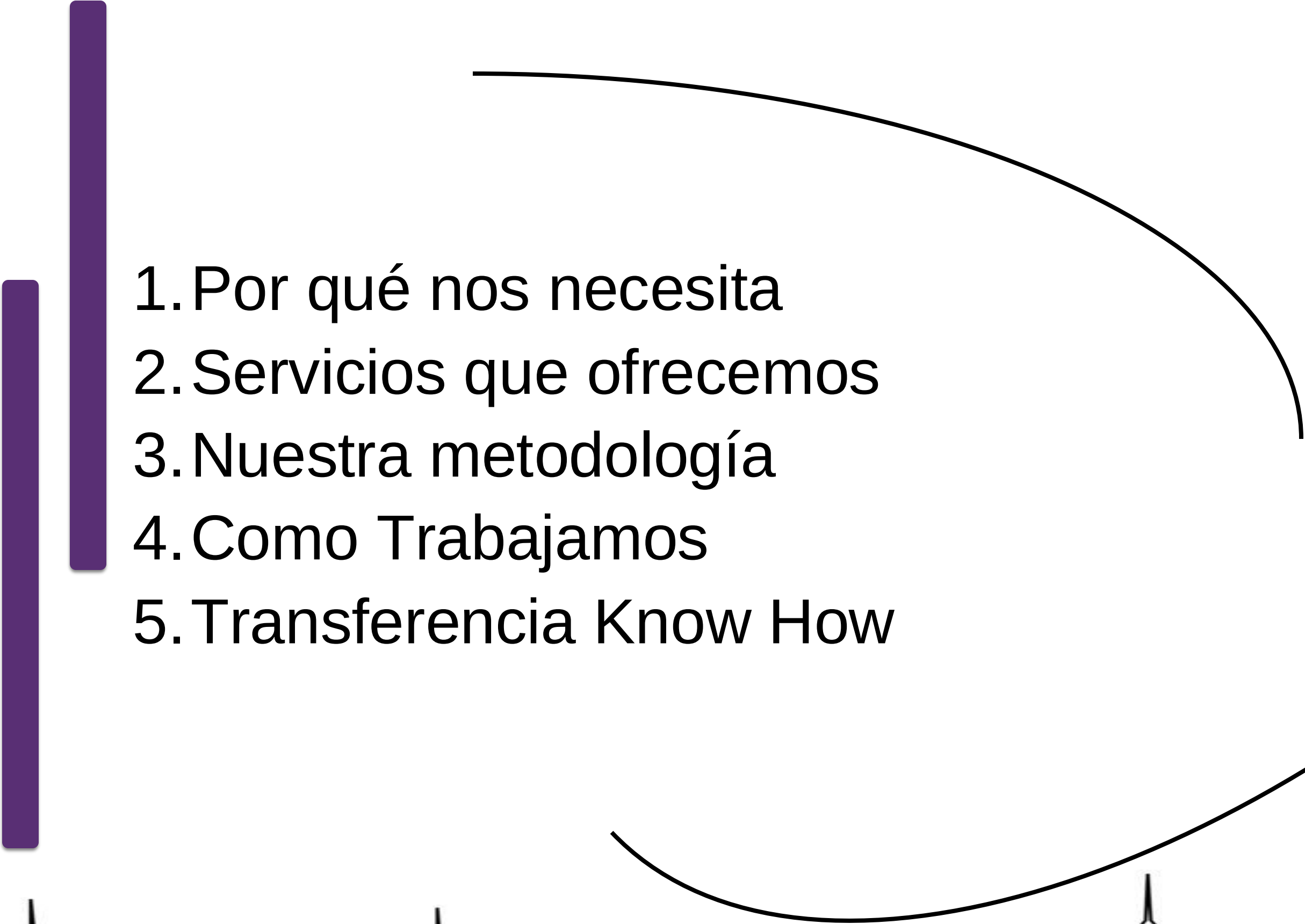
Contacto: [info@cryptoblack.com](mailto:info@cryptoblack.com)

Versión 1.2d 3q-2022

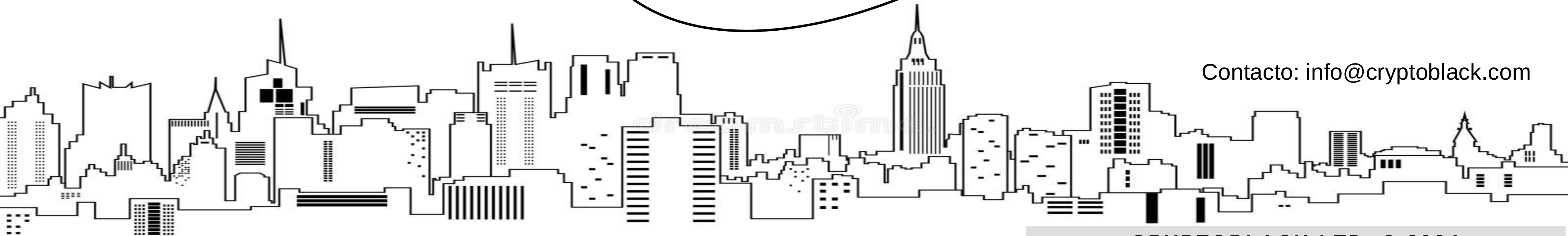
# CiberSeguridad En Aplicaciones

SERVICIOS AUDITORIA PERSONALIZADOS



- 
1. Por qué nos necesita
  2. Servicios que ofrecemos
  3. Nuestra metodología
  4. Como Trabajamos
  5. Transferencia Know How

Contacto: [info@cryptoblack.com](mailto:info@cryptoblack.com)





# 1.

## Por qué Nos Necesita.

- El desarrollo seguro de software y aplicaciones supone tener en cuenta la seguridad desde el inicio del ciclo de vida de los mismos.
- Las vulnerabilidades de seguridad en el software generalmente son causadas por programadores o equipos con habilidades inadecuadas en el desarrollo de software seguro.
- Desafortunadamente, miles de diseñadores y expertos de TI en todo el mundo carecen de habilidades de seguridad precisamente porque la Ciberseguridad no era parte del programa de estudio que siguieron en la universidad.
- La infraestructura de TIC en expansión en todo el mundo está siendo construida por expertos en TI con una comprensión y experiencia de seguridad insuficientes.
- Esta es una situación que pone en riesgo a sus clientes y a los activos desarrollados en su empresa.
- A pesar de sus grandes habilidades en programación y diseño de TI, sin habilidades en seguridad, sus equipos de TI necesariamente construirán soluciones de TI vulnerables.
- Las auditorías sobre su software y la implementación del conocimiento adecuado, dentro de un ciclo de vida de desarrollo de software seguro (SDLC) es ahora mas importante que nunca.



## 2.

# Servicios Que Ofrecemos

### **Recopilación de información**

En esta fase se realizan pruebas de reconocimiento, metarchivos, enumeración de aplicaciones identificación de puntos de entrada, mapeo de rutas, mapa de arquitectura, etc.

### **Proceso de autenticación**

Esta es una de las fases más importantes, se realiza la revisión de credenciales predeterminadas, bloqueo, bypass de autenticación, proceso de recordatorio de contraseña, pruebas de cache, fortaleza de contraseñas y recuperación, etc.

### **Pruebas de validación**

Pruebas de Cross Site Scripting Reflejado, Cross Site Scripting almacenado, manipulación de archivos, SQL Injection, LDAP, XML, Xpath, IMAP/SMTP, inclusión de archivos locales, inclusión de archivos remotos, desbordamiento de buffer, etc.

### **Configuración y pruebas de despliegue**

Entre otras se revisa la prueba de configuración de respuesta, extensiones de archivo, revisión de contenido antiguo u oculto, métodos http, pruebas de http strict transport security, políticas de dominio, etc.

### **Pruebas de autorización**

Pruebas de recorrido en directorio, realización de bypass a esquema de autorización, escalamiento de privilegios, pruebas de inseguridad en referencias a objetos directos, etc.

### **Control de errores**

Análisis de código de errores, verificación de errores por default, errores de programación, errores de despliegue, etc.

### **Gestión de identidad**

Pruebas de identidad de la aplicación, proceso de registro de usuarios, aprovisionamiento de cuentas, enumeración de cuentas, usuarios por default, políticas de asignación, etc.

### **Gestión de sesiones**

Verificación de omisión de sesiones, atributos de cookies, fijación de sesión, variables de sesiones, pruebas de Cross Site Request, funcionalidad en cierre de sesión, espera de sesión, sesión aleatoria y cifrado.



## 2.

## Servicios Que Ofrecemos



### Cifrado de aplicación

Pruebas de cifrado y transporte de datos por canal seguro, validación suplantación de ssl, prueba de relleno, validación de envío de información por canales no cifrados, etc.



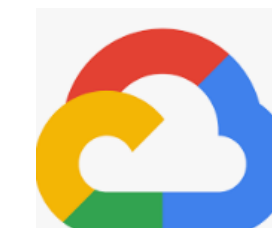
### Pruebas del lado del cliente

Pruebas de DOM basado en Cross Site Scripting, ejecución de código malicioso JavaScript, inyección de código HTML, redireccionamiento a sitios maliciosos, inyección de CSS, pruebas de manipulación, pruebas de Cross Site FLASH, clickjacking, websockets, etc.



### Auditoria en aplicaciones móviles

Ingeniería inversa código, comprobación ofuscación, seguridad en los endpoints, comunicación segura con backend, gestión del almacenamiento local, pruebas OWASP



### Auditoria Cloud

Pruebas tradicionales bajo Cloud, consola, portal, cuentas de usuario, permisos IAM, lista de control y acceso, almacenamiento Cloud, Monitorización, Configuración de los despliegues, respuesta de los SIEM, IPS, IDS, Balanceadores, HIDS, HIPS, NIDS, NIPS, etc.

### Adicionalmente

- Black-box & White-box
- Informes detallados de vulnerabilidades
- Asistencia en la remediación
- Asistencia en la toma de decisiones
- Implementación Pentesting OnPremise
- Formación SDLC OnPremise



### 3.

## Nuestra metodología

### Estándares y Frameworks

- Information Systems Security Assessment Framework (ISSAF)
- Open Source Security Testing Methodology Manual (OSSTMM)
- Open Web Application Security Project (OWASP)
- Penetration Testing Execution Standard (PTES)
- Technical Guide to Information Security Testing and Assessment 800-115(NIST)
- Open Source Intelligence (OSINT)



### Informe y Seguimiento

- Informe ejecutivo detallado donde se ofrece un resumen de nivel y en contexto.
- Resumen gráfico que muestra el número de vulnerabilidades altas, medias y bajas, medidas contra las categorías de riesgo o impacto y probabilidad.
- Pruebas de concepto y documentación técnica detallada que le permite recrear las vulnerabilidades
- Análisis técnico ordenado por riesgo, detallando la ruta de explotación, muestra de existencia y recomendación para su solución.
- Consejos claros de remediación para una mejora inmediata
- Recomendaciones estratégicas para una mejora a corto y largo plazo
- Cumplimiento regulatorio, medición de riesgos y costes.





### 3.

## Nuestra metodología

Nuestro equipo posee las certificaciones mas importantes de la industria para un correcto desempeño de su trabajo.



Certified Cloud  
Security Professional





## 4.

# Como trabajamos

### Pasos Habituales en nuestras auditorias

- Recopilación de las necesidades de auditoria.
- Estimación inicial de costes y tiempos de realización.
- Toma de contacto con entornos y aplicaciones a auditar.
- Estimación final de costes y tiempos de realización.
- Inicio de la auditoria.
- Presentación de informe inicial.
- Soporte y acompañamiento en la remediación.
- Auditoria Post Remediación.
- Presentación de informe final y conclusiones.

***Trabajar con nosotros es fácil y claro. Se comienza al acordar un documento de alcance que resume exactamente qué debe ser testeado de modo que podamos ofrecer una estimación de coste y propuesta completa, identificando metas y áreas, así como cualquier tiempo de inicio y finalización que se requieran. Nuestro equipo trabajara codo con codo con su Dpto. de TI para definir sus necesidades y establecer el enfoque adecuado.***



## 5. Servicios De Transferencia Know How

Creemos que nadie como Ud. conoce su software y su negocio, por ello ofrecemos un servicio de transferencia de conocimiento destinado a Dptos. TI para que su equipo pueda realizar por si mismo sus futuras auditorias.

Ofrecemos los siguientes pasos de implantación y formativos:

- Identificación de necesidades formativas
- Formación en las áreas con carencias
- Implementación de herramientas TI
- Formación en la realización de auditorias internas
- Acompañamiento y soporte tras la implantación
- Formación adicional para la obtención de certificaciones.



CryptoBlack LTD

"My message to companies that think they haven't been attacked is:  
'You're not looking hard enough.'"

James Snook, Deputy Director, UK Office for Cyber Security

Contacto: [info@cryptoblack.com](mailto:info@cryptoblack.com)