

Servicio de Pruebas de Penetración



INTRODUCCIÓN

Visión y Objetivos

Las pruebas de Seguridad propuestas tienen la visión y objetivos:

Visión: Dar tratamiento de manera eficaz a las posibles vulnerabilidades y/o brechas de seguridad presentes en los componentes mencionados en el alcance de esta propuesta.



Objetivos:

- Ejecutar pruebas de penetración que permitan identificar brechas de seguridad en los componentes de seguridad definidos en el alcance de esta propuesta.
- Determinar el nivel de criticidad y explotabilidad de las mismas.
- Emitir recomendaciones para el tratamiento de las brechas identificadas.

Beneficios

- **Reducir el riesgo**
 - Certeza de las brechas identificadas eliminando falsos-positivos.
 - Identificar líneas de acción para controlar el riesgo mediante la mitigación de brechas críticas y altas.
- **Productividad**
 - Evita las interrupciones de operación en el negocio, derivadas de la materialización de riesgos tecnológicos previamente identificados.
 - Menores retrasos al tratar de mitigar de forma empírica e individual algunas de estas brechas.
- **Eficiencia**
 - Habilita al negocio a recibir información relacionada con sus brechas de seguridad en un mínimo de tiempo.
 - Se tienen recomendaciones de mitigación de forma rápida, permitiendo tomar decisiones en los tiempos adecuados.

Mejores Prácticas Base

Para la ejecución de nuestros proyectos de gestión de vulnerabilidades nos basamos en las mejores prácticas y estándares de la industria.

Entre ellos se cuentan los siguientes:

- NIST 800-115
- OSSTMM (Open Source Security Testing Methodology Manual)
- ISSAF (Information System Security Assessment Framework)
- PTES
- OWASP Top Ten

Propuesta de Valor



METODOLOGÍA



Metodología



Para los ejercicios de pruebas de penetración se debe entregar el inventario de objetivos y definir el tipo de prueba (caja negra, caja blanca o caja gris).

Caja negra – Perspectiva de atacante externo para la cual no se requieren detalles técnicos de los objetivos, más que las URL's y/o direcciones homologadas objetivo.

Caja gris – Direccionamiento IP homologado y un punto de acceso físico/virtual dentro de la infraestructura del cliente.

Caja blanca – Inventario con direccionamiento IP no homologado de los activos dentro del alcance que contemple las mismas características técnicas definidas para el escaneo de vulnerabilidades.

Metodología

Metodología para la valoración de riesgos

La valoración del riesgo para las vulnerabilidades encontradas se calculó mediante información de las normas ISO/IEC 27005 e ISO/IEC 31000, ambos definen sistemas de Gestión de Riesgos. Se considera la siguiente fórmula:

| Categoría de Impacto | Valor | Sistemas/Información | Procesos (Tabla 1) |
|----------------------|-------|--|--|
| Mínimo | 1 | Caída o degradación de rendimiento de un sistema no crítico. Corrupción de información interna. | Proceso no crítico afectado totalmente sin impacto a clientes externos. |
| Bajo | 2 | Caída o degradación de rendimiento de un sistema crítico. Corrupción de información confidencial. Descubrimiento no autorizado de información interna. | Proceso crítico afectado parcialmente con impacto a clientes externos. |
| Medio | 3 | Caída de sistemas que imposibilita totalmente la operación de un área crítica. Corrupción de información privilegiada. Descubrimiento no autorizado de información confidencial. | Proceso crítico afectado totalmente con impacto a clientes externos. |
| Alto | 4 | Caída de sistemas que imposibilita totalmente la operación de más de un área crítica. Descubrimiento no autorizado de información privilegiada. | Más de un proceso crítico afectado totalmente con impacto a clientes externos. |
| Crítico | 5 | Caída de la totalidad de los sistemas críticos. | Todos los procesos críticos son interrumpidos. |

Riesgo = Impacto x Probabilidad

Los valores de Impacto se resumen en la siguiente tabla:

Tabla 1. Categoría de impacto

La descripción de las categorías de probabilidad se muestra en la siguiente tabla:

Tabla 2. Categoría de probabilidad

Tabla 3. Descripción del nivel de riesgo

| Categoría de Probabilidad | Valor | Definición del criterio (Tabla 2) |
|---------------------------|-------|---|
| Improbable | 1 | Raro |
| Poco probable | 2 | Improbable; podría ocurrir en algún momento |
| Probable | 3 | Posible; puede ocurrir en algún momento |
| Muy probable | 4 | Probable; probablemente ocurrirá |
| Altamente probable | 5 | Casi seguro; se espera que ocurra |

| Nivel de Riesgo | Descripción | Tolerancia Recomendada (Tabla 3) |
|-----------------|---|----------------------------------|
| Crítico | El nivel de riesgo genera una afectación que puede provocar la interrupción o cierre de la organización | No aceptable |
| Alto | El nivel de riesgo genera una afectación severa a la organización | No aceptable |
| Medio | El nivel de riesgo genera una afectación importante a la organización | Evaluar plan de tratamiento |
| Bajo | El nivel de riesgo no genera una afectación considerable a la organización | Aceptable |
| Mínimo | El nivel de riesgo no genera una afectación relevante a la organización | Aceptable |

Actividades Clave



Propuesta de Valor

Plan de ejecución



X semanas

4 Meses

X
Semanas

Levantamiento de información

Pruebas de penetración y código

Identificación de Brechas

Validación de Explotabilidad

Identificación de Riesgos

Priorización y Generación de Recomendaciones

Reporte Técnico y Ejecutivo

Mitigación

Re-evaluación

Para la ejecución de las pruebas se requiere el siguiente esfuerzo (promedio) por ejercicio:

- Pruebas de penetración
- Generación de reporte (Simultaneo):
- Re-test ambos ambientes:

Se considera un periodo de 4 meses para la aplicación de remediaciones al menos para las brechas más críticas identificadas, después del cual se ejecutarán de nuevo pruebas para validar el correcto cierre de las mismas.

Detalle De Las Actividades

- **Contextualización:**
 - Identificar los activos objetivos de las pruebas de seguridad.
 - Acordar las ventanas de tiempo (días y horarios) para la ejecución de las pruebas.
 - Establecer la dinámica de trabajo para la comunicación durante las pruebas
- **Identificación de Vulnerabilidades y Brechas:**
 - Ejecución de escaneos y actividades de identificación de brechas de seguridad.
 - Ejecución de pruebas de penetración de caja negra.
- **Evaluación de Brechas:**
 - Validación de las brechas.
 - Validación y o ajustes de criticidad intrínseca de las brechas.
 - Generación de reportes “crudos” directamente por las herramientas utilizadas.
- **Priorización:**
 - Contextualización de los resultados identificados para asignación real de criticidad (riesgo para la organización).
 - Generación de reporte contextualizado y priorizado de brechas.
 - Generación de recomendaciones de atención a los resultados identificados (en conjunto con la organización).
- **Remediación:**
 - Aplicación de las remediaciones (por parte de personal de la organización).
- **Validación:**
 - Ejecución de tareas de evaluación posteriores a las remediaciones.
 - Generación de reportes de reevaluación.

Entregables

El análisis de seguridad mediante la ejecución de pruebas de penetración considera los siguientes entregables:

- Reportes de brechas detallado conteniendo al menos:
 - Total de activos analizados.
 - Datos de los activos analizados.
 - Total de brechas detectadas y agrupadas por tipo.
 - Principales amenazas detectadas.
 - Desviaciones detectadas (Puertos, vulnerabilidades, huecos de seguridad, entre otros).
 - Clasificación de las brechas detectadas, así como las posibles formas de explotación de las mismas.
 - Recomendaciones para la remediación de las desviaciones detectadas
- Reporte ejecutivo conteniendo al menos:
 - Cantidad de brechas totales
 - Cantidad de brechas agrupadas por categoría de severidad, tipo de infraestructura y activo
 - Matriz de riesgos, analizando la probabilidad de ocurrencia y el impacto.
 - Principales vulnerabilidades con su descripción y recomendaciones de remediación.
- Reportes generados por las herramientas utilizadas
- Planes de mitigación conteniendo al menos:
 - Agrupamiento por tipo de activo.
 - Priorización por tipo de amenazas y riesgos.
 - Agrupamiento por facilidad de remediación
- Reporte de re-test para validar el correcto cierre de las vulnerabilidades identificadas

Equipo de Trabajo y Certificaciones

El equipo de trabajo para la ejecución de pruebas de penetración cuenta con las siguientes certificaciones:

| Certificaciones |
|--|
| |
| <ul style="list-style-type: none">• Certificado Hacking Etico por la OIHEC Organización Internacional de Hackers y Expertos en Ciberseguridad• AHSPL1 (Accredited Hacking & Security Pentester Level 1) |
| <ul style="list-style-type: none">• CompTIA CySA+• CRISC• ECC-CEH |
| <ul style="list-style-type: none">• ECC-CEH• CISSP |

Certificaciones Cybolt

CERTIFICADO



| | | | |
|-------------------------|------------|-------------------------|------------|
| Núm. Certificado | 1694-3/21 | Auditoría de renovación | 19/06/2024 |
| Emisión inicial | 06/08/2021 | Renovación | 06/08/2024 |
| Expiración último ciclo | 05/08/2024 | Expiración | 05/08/2027 |

Certificado Sistema de Gestión de la Calidad

ISO 9001:2015

IVAC-INSTITUTO DE CERTIFICACIÓN, S.L. certifica, tras el acuerdo de la Comisión 31694/1R3/2024 revisión 2.0 que la organización

CYBER TEAM SAPI de C.V.
NOVITECH, S.A. de C.V.
CKC CONSULTORES, S.A. de C.V.
CYBOLT MANAGED SERVICES S.A. de C.V.
INFORMACIÓN SEGURA, S.A. de C.V.
TAGSEC GROUP, S.A. de C.V.
CYBOLT S.A.S.

Dispone de un sistema de gestión de la calidad conforme con la norma ISO 9001:2015 para la siguiente actividad:

Documentación y entregables del servicio de alojamiento y colocado en el centro de datos, del servicio de consultoría y del servicio de SOC y NOC.

Director IVAC-INSTITUTO DE CERTIFICACION, S.L.
 Juan Cardona Estrli

Firmado digitalmente por 79070092W JUAN CARDONA B87986746 IVAC-INSTITUTO DE CERTIFICACIÓN, S.L. J. Paterna 2024.07.08 11:42:35+0200

Sede principal
 IVAC-INSTITUTO DE CERTIFICACIÓN, S.L.
 C/ Carretera Aguila Escudosa
 Sección, nº 8, P.O. 46001 Paterna (Valencia)
 Spain
 Tel: +34 963 943 905
 ES.alfonso@kiwa.com
 www.kiwa.es

ENAC
 CERTIFICACIÓN
 ISO 9001
 ISO 9004

IAF

El presente certificado es válido hasta la fecha indicada, salvo rebote o suspensión. Su validez está sujeta a los seguimientos realizados con periodicidad anual.
 Para cualquier aclaración sobre el certificado puede contactar a través de nuestra página web.

Este certificado es completo con los emplacements indicados en su anexo técnico cuyo número coincide con el de este certificado. Página 1 de 1

CERTIFICADO



| | | | |
|-------------------------|------------|-------------------------|------------|
| Núm. Certificado | 1694-W/21 | Auditoría de renovación | 07/06/2024 |
| Emisión inicial | 06/08/2021 | Renovación | 06/08/2024 |
| Expiración último ciclo | 05/08/2024 | Expiración | 05/08/2027 |

Certificado Sistema de Gestión de Servicios de Tecnologías de la Información

ISO 20000-1:2018

IVAC-INSTITUTO DE CERTIFICACIÓN, S.L. certifica, tras el acuerdo de la Comisión W1694/1R3/2024 revisión 2.0 que la organización

CYBER TEAM SAPI de C.V.
NOVITECH, S.A. de C.V.
CKC CONSULTORES, S.A. de C.V.
CYBOLT MANAGED SERVICES S.A. de C.V.
INFORMACIÓN SEGURA, S.A. de C.V.
TAGSEC GROUP, S.A. de C.V.
CYBOLT S.A.S.

Dispone de un sistema de gestión de servicios de tecnologías de la información conforme con la norma ISO 20000-1:2018 para la siguiente actividad:

El Sistema de Gestión de Servicios para la gestión de servicios de T.I del servicio de alojamiento y colocado en el centro de datos y del servicio de SOC y NOC, que se encuentran definidos en el Catálogo de Servicios para todos los Clientes.

Director IVAC-INSTITUTO DE CERTIFICACION, S.L.
 Juan Cardona Estrli

Firmado digitalmente por 79070092W JUAN CARDONA B87986746 IVAC-INSTITUTO DE CERTIFICACIÓN, S.L. J. Paterna 2024.07.08 11:38:56+0200

Sede principal
 IVAC-INSTITUTO DE CERTIFICACIÓN, S.L.
 C/ Carretera Aguila Escudosa
 Sección, nº 8, P.O. 46001 Paterna (Valencia)
 Spain
 Tel: +34 963 943 905
 ES.alfonso@kiwa.com
 www.kiwa.es

ENAC
 CERTIFICACIÓN
 ISO 20000-1

IAF

El presente certificado es válido hasta la fecha indicada, salvo rebote o suspensión. Su validez está sujeta a los seguimientos realizados con periodicidad anual.
 Para cualquier aclaración sobre el certificado puede contactar a través de nuestra página web.

Este certificado es completo con los emplacements indicados en su anexo técnico cuyo número coincide con el de este certificado. Página 1 de 1

CERTIFICADO



| | | | |
|-------------------------|------------|-------------------------|------------|
| Núm. Certificado | 1694-5/21 | Auditoría de renovación | 04/08/2023 |
| Emisión inicial | 15/01/2021 | Renovación | 15/01/2024 |
| Expiración último ciclo | 14/01/2024 | Expiración | 14/01/2027 |
| | | Modificación | 07/04/2025 |

Certificado Sistema de Gestión de Seguridad de la Información

ISO 27001:2022

IVAC-INSTITUTO DE CERTIFICACIÓN, S.L. certifica, tras el acuerdo de la Comisión 51694/2AE1/2025 revisión 2.1 que la organización

CYBER TEAM SAPI de C.V.
CKC CONSULTORES, S.A. de C.V.
CYBOLT MANAGED SERVICES S.A. de C.V.
INFORMACIÓN SEGURA, S.A. de C.V.
TAGSEC GROUP, S.A. de C.V.
CYBOLT, S.A.S.

Dispone de un sistema de gestión de seguridad de la información conforme con la norma ISO 27001:2022 para la siguiente actividad:

El Sistema de Gestión de Seguridad de la Información protegerá la confidencialidad, integridad y disponibilidad de la información para la prestación de servicio de alojamiento y colocado en el centro de datos, de la entrega de servicios de consultoría y del servicio del SOC y NOC, según la declaración de aplicabilidad en vigor a fecha de la última actualización del certificado.

Director IVAC-INSTITUTO DE CERTIFICACION, S.L.
 Juan Cardona Estrli

Firmado digitalmente por 79070092W JUAN CARDONA B87986746 IVAC-INSTITUTO DE CERTIFICACIÓN, S.L. J. Paterna 2025.04.08 17:10:34+0200

Sede principal:
 Perfil Blvd. Manuel Ávila Camacho 5
 Torre B, Piso 23, Oficina B-2301,
 Lomas de Soltero
 C.P. 53390 - Naucalpan de Juárez,
 Estado de México, México

Centro:
 Antonio Caso 108
 Col. Colinas de San Jerónimo
 C.P. 54600 - Monterrey, Nuevo León,
 México

Centro:
 Adolfo López Mateos #1956 Oriente
 Col. Bella Vista
 C.P. 52172 - Metepec,
 Estado de México, México

ENAC
 CERTIFICACIÓN
 ISO 27001
 ISO 27002

IAF

El presente certificado es válido hasta la fecha indicada, salvo rebote o suspensión. Su validez está sujeta a los seguimientos realizados con periodicidad anual.
 Para cualquier aclaración sobre el certificado puede contactar a través de nuestra página web.

Este certificado es completo con los emplacements indicados en su anexo técnico cuyo número coincide con el de este certificado. Página 1 de 1

CERTIFICADO



| | | | |
|------------------|------------|--------------|------------|
| Núm. Certificado | 1694-J/22 | Modificación | 21/07/2023 |
| Emisión inicial | 28/06/2022 | Expiración | 27/06/2025 |

Certificado Sistema de Gestión de la Continuidad de Negocio

ISO 22301:2019

IVAC-INSTITUTO DE CERTIFICACIÓN, S.L. certifica, tras el acuerdo de la Comisión J1694/2023 revisión 1.3 que la organización

CYBER TEAM SAPI de CV
NOVITECH, S.A. de C.V.
CKC CONSULTORES, S.A. de C.V.
CYBOLT MANAGED SERVICES S.A. de C.V.
INFORMACIÓN SEGURA, S.A. de C.V.
TAGSEC GROUP, S.A. de C.V.
CYBOLT, S.A.S.

Dispone de un sistema de gestión de la continuidad de negocio conforme con la norma ISO 22301:2019 para la siguiente actividad:

El Sistema de Gestión de Continuidad del Negocio para los procesos de alojamiento y colocado en el centro de datos, del servicio de consultoría, servicios administrados y de los servicios del SOC y NOC.

Director IVAC-INSTITUTO DE CERTIFICACION, S.L.
 Juan Cardona Estrli

Firmado digitalmente por 79070092W JUAN CARDONA B87986746 IVAC-INSTITUTO DE CERTIFICACIÓN, S.L. J. Paterna 2023.07.24 17:55:15+0200

Sede principal
 Calle Boulevard Manuel Ávila Camacho No. 5
 Torre B, Piso 23, Oficina B-2301,
 Fraccionamiento Lomas de Soltero
 C.P. 53390 - Naucalpan de Juárez, Estado de México
 México

Centro:
 Adolfo López Mateo #1956 Oriente,
 Col. Bella Vista
 C.P. 52172 - Metepec, Estado de México
 México

ENAC
 CERTIFICACIÓN
 ISO 22301

IAF

El presente certificado es válido hasta la fecha indicada, salvo rebote o suspensión. Su validez está sujeta a los seguimientos realizados con periodicidad anual.
 Para cualquier aclaración sobre el certificado puede contactar a través de nuestra página web.

Este certificado es completo con los emplacements indicados en su anexo técnico cuyo número coincide con el de este certificado. Página 1 de 1

Propuesta Económica

| Descripción | Cant. | Importe |
|-----------------------------------|---------|-------------|
| Pruebas de penetración caja negra | 1 URL | \$2,650.00 |
| Pruebas de penetración caja negra | 10 URLs | \$21,200.00 |

Condiciones comerciales

- La propuesta se encuentra expresada en Dólares americanos.
- A los importes deberá agregárseles el impuesto aplicable.

Forma de pago sugerida:

- 50% Anticipo.
- 35% a la entrega del primer ciclo de pruebas.
- 15% contra la entrega del reporte de re-ejecución de pruebas.

Referencias de Clientes

En Cybolt tenemos amplia experiencia en este tipo de ejercicios, entre los clientes que podemos mencionar de referencia se encuentran los siguientes:

- Intercam
- Afirme
- Grupo Pecuário Porres
- Seguros HDI
- Viva Aerobús
- SPIN
- Banreservas (Rep. Dominicana)
- Ferromex
- Florida East Cost Railroad
- SOLUFI
- BTG

CYBOLT

Security Innovation