

Vector Cybersecurity

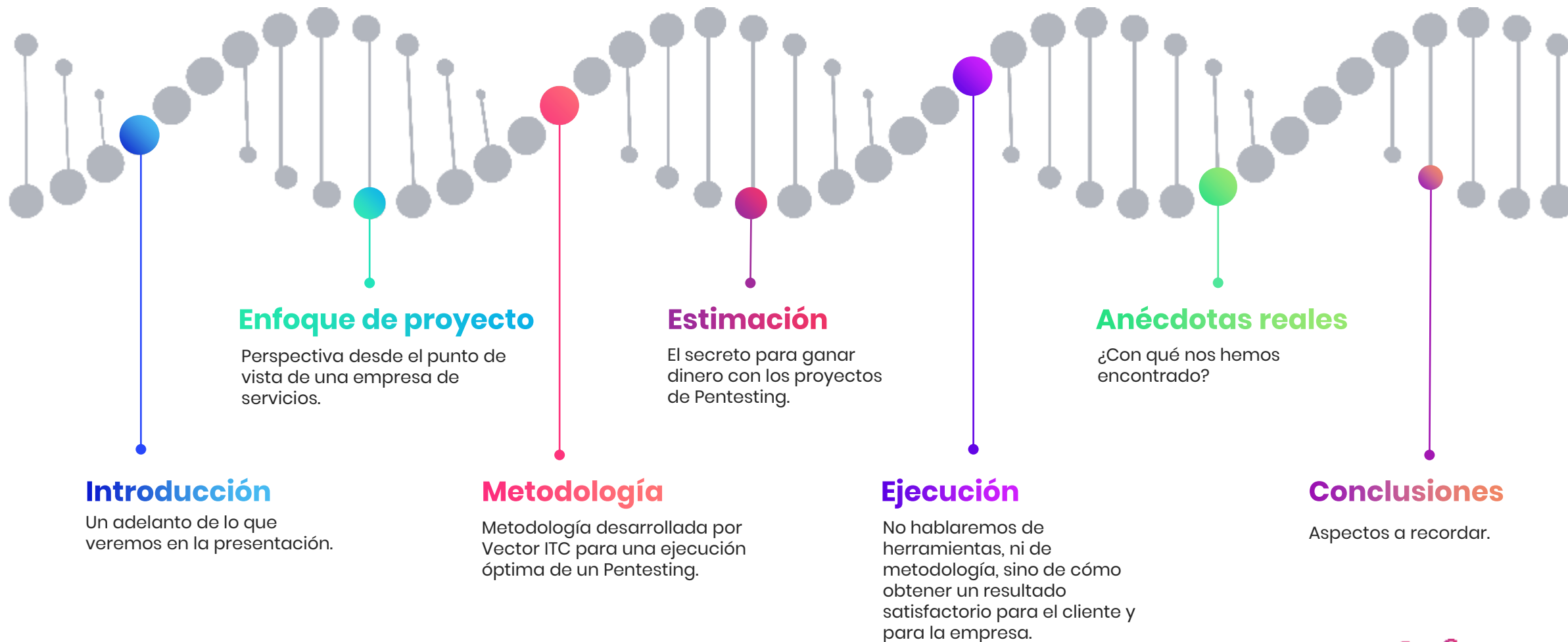
¿Cómo ganar dinero con un pentesting?.

corporate approaches to red team exercises

www.vectoritcgroup.com



ÍNDICE



Introducción



Introducción.

VECTOR ITC

Vector es una empresa de servicios de TI. Ofrecemos servicios que abarcan el ciclo completo del software de nuestros clientes: consultoría tecnológica y de negocio, UX, desarrollo, mantenimiento, sistemas, ciberseguridad, innovación, outsourcing, y un largo etcétera.

MÁXIMA EXPERIENCIA

Llevamos desde el año 2002 acompañando a nuestros clientes, algunos de ellos muy grandes como Banco Santander o Inditex, en toda su amplitud tecnológica. La adopción de nuevas tecnologías y metodologías nos ha permitido evolucionar, siendo hoy día más de 2.500 personas en 9 países.

TECNOLOGÍA DE VANGUARDIA

Utilizamos la última tecnología en cada área de actuación para poder aportar al cliente el máximo valor en el desarrollo de sus soluciones. Invertimos más de un 5% de nuestros ingresos en I+D+i para poder experimentar con las nuevas tendencias.

LA CIBERSEGURIDAD NO DEBE SER UNA EXCEPCIÓN

Como empresa de servicios TI, hacemos uso de las últimas metodologías para servicios y proyectos, con el fin de obtener los mejores resultados con la máxima rentabilidad. En el área de Ciberseguridad desarrollamos proyectos y servicios, por lo que aunque siendo bastante peculiares, debemos buscar también los mismos resultados: satisfacción de cliente y rentabilidad para la compañía.




Introducción.

TEST DE SEGURIDAD

- Siguen siendo proyectos peculiares
- Cada vez sistemas más complejos
- Nuevas herramientas y métodos
- No hay una guía estándar de cómo ejecutarse, aunque sí procedimientos/esquemas que ayudan a ejecutarlos:
 - Kill Chain
 - OSSTMM
 - OWASP
 - PTES





Enfoque de proyecto

Enfoque de proyecto

PREMISAS INICIALES

- *Una empresa debe ganar dinero, ser rentable.*
- *El cliente debe quedar satisfecho con el resultado.*

1. Un proyecto más

- Para una empresa prestadora de servicios, un proyecto de pentesting, es un proyecto más.
- Es un proyecto que tiene un presupuesto, un alcance, un tiempo de ejecución y unos recursos asignados.
- Genera unos ingresos, y tiene una serie de costes.
- Está sujeto a las mismas condiciones que el resto de proyectos en cuanto al margen de beneficio.

2. Algunas excepciones

Al ser la ciberseguridad un área en auge en el entorno, y ser además bastante notoria, sí que se pueden establecer políticas para hacer alguna excepción en este tipo de proyectos, encaminadas a asumir más riesgos como bajada del margen comercial, e incluso asumir margen 0% o más costes, en alguna de estas situaciones:

- *Potenciar el área de ciberseguridad.*
- *Usarlo como acción de marketing*
- *Consecución de nuevo cliente.*
- *Conseguir una referencia importante (o la primera si es el caso)*

3. Aún así, se intenta ganar dinero..

- Una empresa de servicios es más cara que un freelance por estructura y márgenes, y es más barata que una empresa de nicho, pero con menos presencia y especificación. Se ha de adelantar a la empresa de nicho por calidad y precio, y al freelance por confianza y precio.
- No se pueden inflar las tarifas, ni hinchar las horas de proyectos.
- Por tanto, por muchas excepciones que haya, finalmente se va a exigir intentar dar beneficios.
- Y, una vez en marcha el proyecto, sólo nos queda maximizar la productividad para conseguirlo, visto que no se debe sobrestimar.
- ¿Cómo? → Productividad

4. El secreto, una buena planificación

- Maximizar la productividad → Una cuidada planificación.
- Teniendo en cuenta el equipo, la metodología, al cliente, otros proyectos, sinergias, plazos, partners, colaboradores, etc.
- Se debe planificar la ejecución con respecto a estos condicionantes, para obtener el mejor rendimiento.



Metodología

Metodología

PREMISAS INICIALES

- *No hay una metodología mejor que otra.*
- *Se debe hacer uso de la experiencia para mejorar la ejecución.*

1. La mejor metodología, la que funciona

- Los proyectos de pentesting también tienen metodologías específicas: OWASP, OSSTMM, PTES, etc. como hemos visto en la introducción.
- Depende del tipo de proyecto, del cliente, de la madurez del mismo y de los proyectos, de los equipos participantes, etc.
- Por tanto, no hay una metodología específica que asegure el éxito de un proyecto de este tipo.
- Conforme se ejecutan proyectos, se afina la metodología.

2. Aspectos a tener en cuenta

- ¿Es un nuevo cliente?
- ¿Voy a contar con equipo nuevo, o un freelance o partner?
- ¿Vamos apretados en presupuesto o fechas?
- ¿Tenemos un equipo formado en metodologías, sean cuales sean?
- Otros

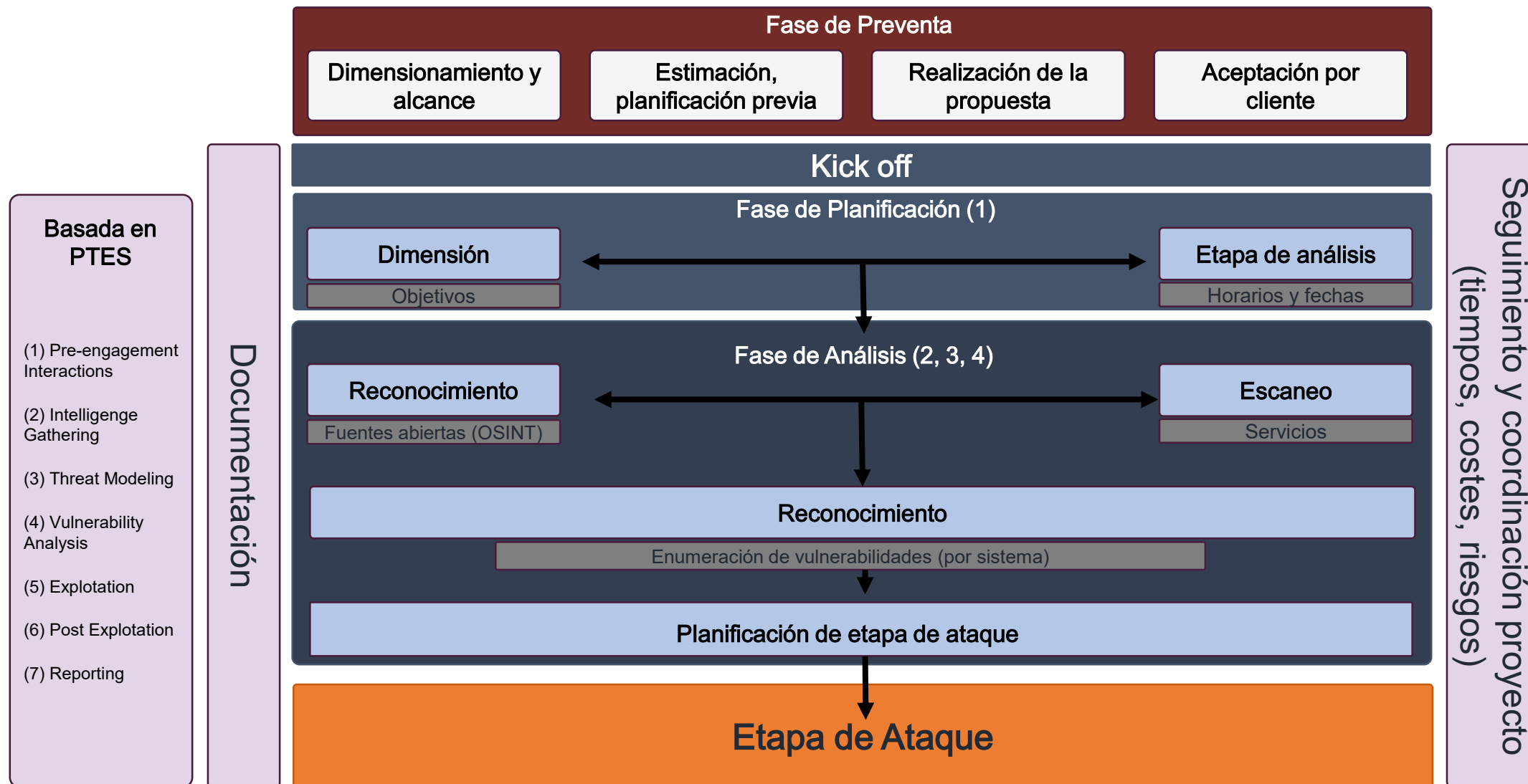
3. Objetivos de una buena metodología

- Sea cual sea la metodología usada (waterfall, agile, mixta, específica por tipologías, etc.) los objetivos son comunes: mejora de los procesos y satisfacción del cliente.
- Mismos objetivos que con otros proyectos: productividad y satisfacción.
- Algunas además (y es una buena práctica) buscan ayudar en el bienestar de los equipos. Un equipo contento es un equipo más productivo.
- Aprovechamiento al máximo de los recursos: composición del equipo, localizaciones, usos horarios, herramientas, conocimiento, coordinación, etc.
- Prever riesgos, anticipar incidencias o contingencias, detectar desviaciones, acciones correctivas o previsoras, etc.

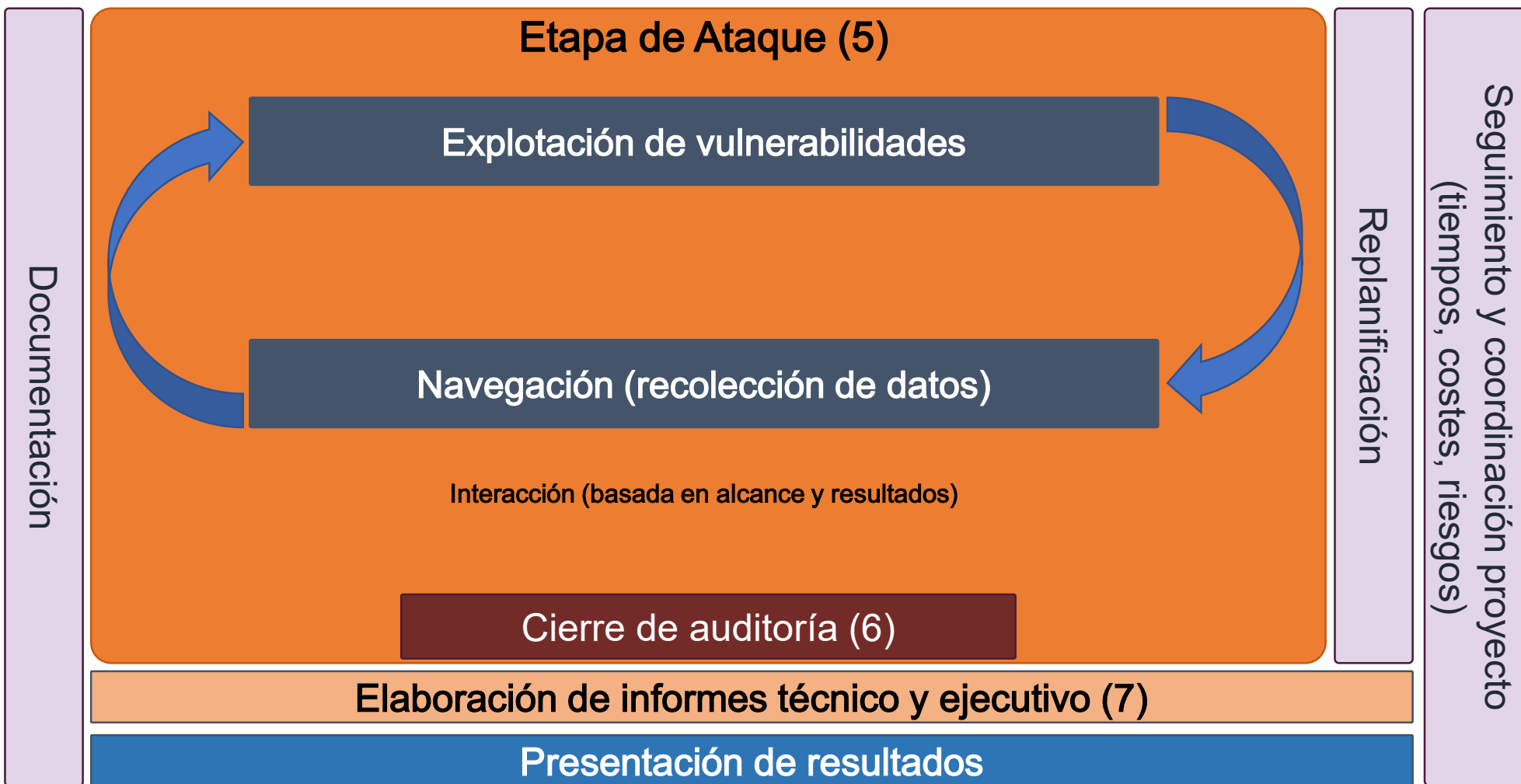
4. Metodología Vector ITC

- Teniendo esto en cuenta, en Vector ITC hemos desarrollado nuestra propia metodología para proyectos específicos de pentesting.
- Partimos de una metodología específica para proyectos de Pentesting, debidamente adaptada a las necesidades de una compañía de Servicios que debe controlar costes, tiempos y satisfacción del cliente.
- Aplicamos principios ágiles como filosofía para el día a día.

Metodología



Metodología





Estimación

Estimación

PREMISAS

- *Por ética y competencia:*
 - *No se puede sobrestimar en horas.*
 - *No se pueden incrementar las tarifas.*

¿CÓMO SE ABORDA UNA ESTIMACIÓN SI NO QUIERO PERDER PASTA?

1. Acotando debidamente el alcance

Analizando y dejando claro el alcance, y que todo lo que se salga de ahí es un cambio que debe ser gestionado. Análogamente a cualquier proyecto.

4. Responsable de proyecto experto

Es tarea del responsable del proyecto identificar los riesgos, tareas ajenas al desarrollo, planificar los seguimientos etc. Y todo esto suma a la hora de hacer una estimación, y es crucial tenerlo en cuenta.

Asimismo debe ser capaz de identificar si habrá que realizar horas extras, viajes, etc. Ya que impacta en el presupuesto.

2. Disponiendo de toda la información

Insistiendo al cliente en disponer de toda la información posible sobre sistemas, hw, sw, accesos, políticas, etc.

Realizando reuniones si es necesario, en casa del cliente.

5. Aprovechando la experiencia de Vector

La experiencia en otros servicios/proyectos con ese cliente que nos ha contratado el pentesting es fundamental para anticipar riesgos que sabemos que van a surgir, debido a lo que ya hemos vivido con ese cliente en otros proyectos.

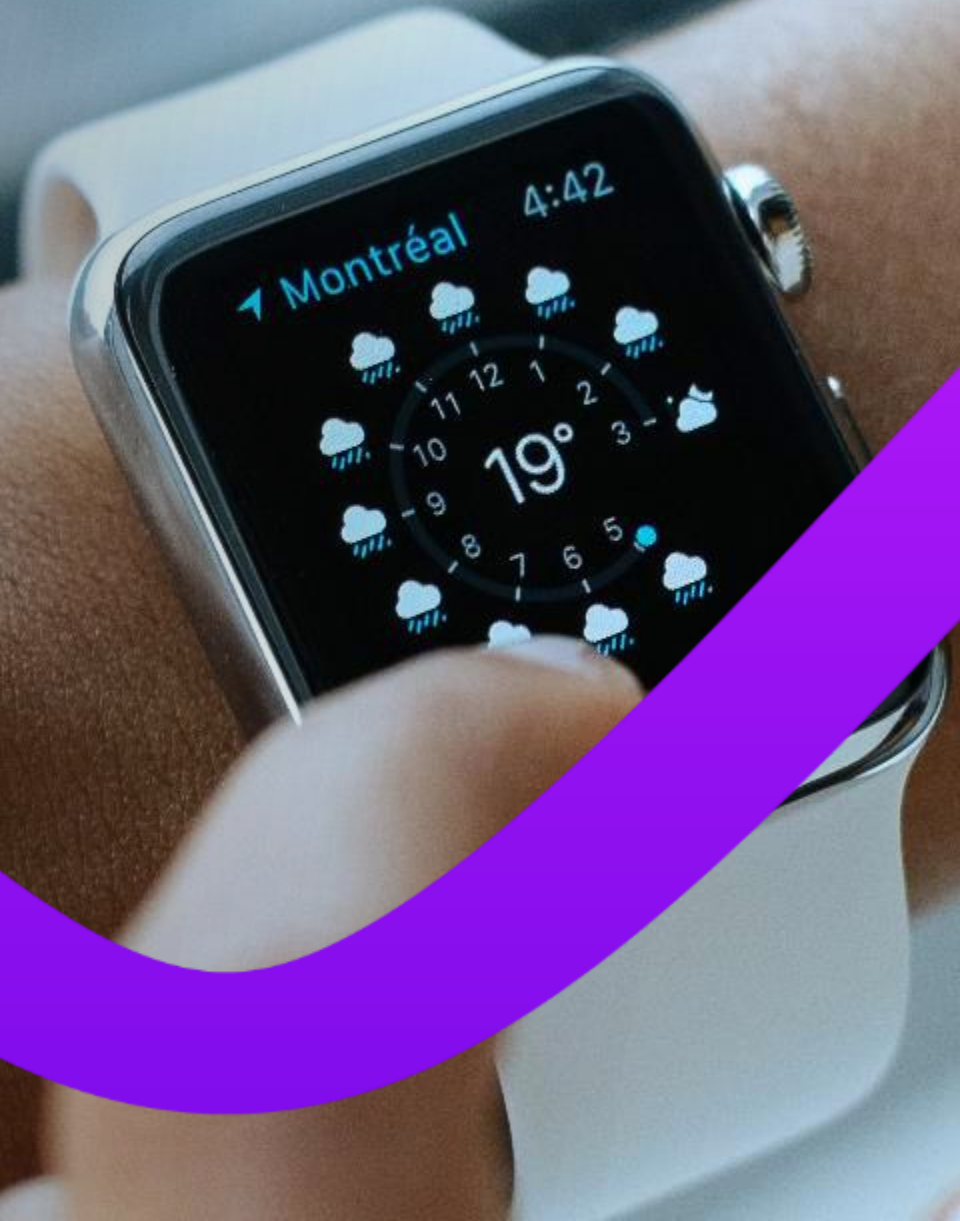
3. Contar con un buen equipo técnico

El equipo técnico, que será quien ejecute las tareas del pentesting, es fundamental a la hora de realizar una buena estimación temporal, debido a que conoce mejor que nadie las dificultades de cada tarea.

6. Realizar una estimación justa.

No se puede pretender aprovecharse de los clientes, eso no funciona. Se debe realizar una estimación justa, tanto por ética profesional, como por necesidad de mercado, puesto que también es cierto que al existir tanta competencia entre otras empresas de servicios, empresas de nicho y freelance, estas prácticas no resultan.

Ejecución



Ejecución

PREMISAS INICIALES

- *Objetivos:*
 - *Satisfacción del cliente.*
 - *Maximizar la productividad.*
- *Existen aspectos específicos a tener en cuenta.*

1. No voy a hablar de herramientas

- Primero porque sabéis mucho más que yo de temas técnicos.
- Y segundo porque no es la idea de la charla.
- Pero también influye en la ejecución: una buena selección de las herramientas más óptimas para cada caso nos puede hacer ganar tiempo y por ende, dinero...

2. Sino de maximizar la productividad. ¿Cómo?

- La fuerza comercial de una empresa de servicios nos debe hacer ganar más proyectos, por tanto debemos conseguir que el equipo pueda atender más de un proyecto a la vez, con lo que evitaremos tiempos muertos aprovecharemos sinergias.
- Tenemos la opción de contar con áreas de la compañía que nos apoyen en aspectos puntuales que nos puedan ahorrar tiempo. P.e. nos pueden ahorrar en buscar algo si otro ya lo sabe.
- Ojo con las horas extra. Ídem para fines.
- Más proyectos, más equipo y mejor pirámide de costes.
- Colaboración con partners, freelance etc. Si no nos salen las cuentas o si hay picos de trabajo.

3. Orientación a cliente

- Ojo, no nos puede cegar el hecho de ganar dinero sí o sí...
- El cliente debe quedar satisfecho con el trabajo: por tanto se debe trabajar con ese objetivo en mente.
- Buscar la diferenciación con respecto a empresas de nicho y freelance. Por un lado el tema económico no puede ser un escollo, pero el tema de calidad es básico también.
- Algunos puntos diferenciadores:
 - Atención prioritaria y constante al cliente. Reportes constantes.
 - Informes adaptados al público: informe ejecutivo e informe técnico.

4. Aspectos a tener en cuenta con respecto a otros proyectos “estándar”

- El cliente debe ser consciente de que podemos colarnos en sus sistemas, tirar una aplicación en producción, quedarse sin servicio, etc. Se debe por tanto tener avisado al cliente, y que sea consciente de que sus usuarios pueden verse afectados.
- Se deben firmar consentimientos y buscar el mejor momento.
- Se debe mantener avisado al proveedor de infraestructura. Si es un cloud (AWS, Google, etc.) hay procedimientos a seguir para dar aviso de los test.
- Se debe tener muy en cuenta la LOPD/GDRP porque tendremos acceso (ese es el objetivo) a información sensible.
- Otros

A person's hands are shown holding a white smartphone. The screen displays a blue-themed interface with a list of items and a keyboard at the bottom. A thick, bright green wave graphic curves across the lower half of the image, partially obscuring the person's arms and the phone. The background is a blurred, warm-toned surface, possibly a wooden floor or wall.

Anécdotas

Anécdotas

¿ALGO QUE RESEÑAR?

- *Ejemplos de situaciones no esperadas en nuestro día a día en el marco de proyectos de ciberseguridad.*

1. Situaciones no esperadas

- No esperas que un sw para un proceso crítico tenga vulnerabilidades del tipo contraseñas hardcodedas.
- Tampoco esperas que un sistema que se utiliza en un servicio en producción que todos usamos a diario, tenga un código de tan poca calidad y tan vulnerable que haya que rescribirlo si se quiere pasar una mínima auditoría.
- O el descubrir el que causante de introducir un malware en la compañía fue un antiguo empleado mosqueado por un despido. Aunque es una situación bastante usual sobre todo en latinoamérica.

2. Situaciones comprometidas

- Cuando te toca certificar el trabajo realizado por otra empresa o grupo y ves que no han hecho su trabajo... son compañeros (de empresa o de profesión), pero el trabajo hay que hacerlo por ética y profesionalidad, y el cliente debe tener constancia de lo que ha pagado.
- Nos tiene pedido un cliente "suavizar" el informe para que sus responsables y jefes no se mosqueen, cosa que va en contra de nuestro buen hacer.

3. Situaciones divertidas

- Que nos indique el cliente que obviemos algún aviso por contenido a páginas comprometidas (contenido sexual, armas, etc.) porque el usuario/IP es la del Jefe.
- Que se nos pida crear una regla ad hoc en el IDS para obviar cualquier acción si viene de una MAC, una IP o USER determinado. Y suele ser del jefe.
- Descubrir contenido "poco apropiado" en alguna auditoría de infraestructuras.

4. Otras situaciones

- Nos ha pasado descubrir que el personal de mantenimiento, el señor que cambiaba la bombilla, había metido un malware en un pendrive. Es una actuación bastante habitual en Latinoamérica, el utilizar a personas de mantenimiento para este tipo de fraudes.
- Nos ha pasado que un cliente nos llama para pedir un presupuesto para la realización de un pentesting, se lo enviamos y lo considera caro. A los pocos días, reciben un ataque DDoS que tira su sistema en PRO, y pierden 50.000€ en sólo unas horas que estuvieron sin servicio. Su CEO decidió que era más importante invertir el importe del proyecto en modificar el diseño de los membretes de las cartas en papel... la concienciación es muy importante. Algunos lo aprenden a golpes...

Conclusiones



Conclusiones

PARA FINALIZAR

Un pentesting no deja de ser un Proyecto que persigue los mismos objetivos que cualquier otro proyecto: obtener una rentabilidad, ofreciendo satisfacción al cliente.

- *Ojo a la estimación y el alcance.*
 - *Maximizar la productividad.*
 - *Adaptar la metodología.*
 - *Identificar riesgos y tratar de anticiparlos.*
 - *Y no dejemos de divertirnos.*
- *The Penetration Test Execution Standard:*
http://www.pentest-standard.org/index.php/Main_Page
 - *OWASP:* <https://www.owasp.org>
 - *The Cyber Kill Chain:*
<https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>
 - *OSSTMM:* <http://www.isecom.org/research/osstmm.html>

Un Aún así se debe tener en cuenta que los test de seguridad son proyectos peculiares, y hay que estar al tanto de nuevas herramientas y procedimientos para mejora continua. Así que el entusiasmo y las ganas siempre son bien recibidas 😊

Iván Lastra Quintana

Responsable de Ciberseguridad en
Vector ITC

ilastra@vectoritcgroup.com

@ilastraq

Sobre Vector ITC

Con un equipo humano de **más de 2.500 profesionales**, tenemos presencia a nivel nacional e internacional, con sedes en EE.UU., Perú, Brasil, Chile, México, Colombia, Paraguay, Reino Unido y Alemania.

¿Nuestra misión?: generar el mayor valor a nuestros clientes, a los sectores económicos y al conjunto de la sociedad, mediante el diseño y desarrollo de **iniciativas basadas en tecnología de vanguardia**, con el objetivo de accionar el cambio digital de una manera disruptiva.

www.vectoritcgroup.com