PABE Methodology - Exploitation-Based Threat Prioritization (PABE) Method

Rubén Darío Aybar[1]

[1]Universidad de Buenos Aires, Buenos Aires, Argentina
r4yb4r@gmail.com

Abstract. The contemporary cybersecurity landscape is characterized by a relentless influx of threats and vulnerabilities. Organizations face an overwhelming volume of exposures, with more than 20,000 new vulnerabilities cataloged each year (Balbix, 2023). This deluge of data has led to security team fatigue and analysis paralysis, where disproportionate time is spent identifying issues, but little is achieved in terms of practical, actionable results. The traditional approach, based almost exclusively on severity scores, often leads to inefficient remediation strategies, dedicating resources to vulnerabilities with "critical" scores that are never actually exploited, while neglecting more relevant and urgent risks.

In response to this strategic imperative, the new Exploitation-Based Threat Prioritization (PABE) method is introduced. This cybersecurity framework is designed to optimize defense efforts by integrating theoretical risk analysis (threat modeling) with real-time threat intelligence. This method focuses on answering the critical question: "Of all the possible weaknesses, which are most likely to be exploited by actual attackers right now?"

PABE formalizes a sequence of steps from business strategy to tactical action, using widely recognized industry tools and databases to ensure that mitigation resources are directed toward the most imminent threats.

By adopting the PABE methodology, organizations can overcome the limitations of traditional systems, optimize resource allocation, and strengthen their security posture against the most relevant and active threats in today's landscape.

Keywords: Threat Modeling, Vulnerability Prioritization, EPSS, CISA KEV, Risk Based Vulnerability Management

Metodología PABE - Método de Priorización de Amenazas Basado en Explotación (PABE)

Resumen. El panorama de la ciberseguridad contemporánea se caracteriza por una incesante marea de amenazas y vulnerabilidades. Las organizaciones se enfrentan a un volumen abrumador de exposiciones, con más de 20,000 nuevas vulnerabilidades catalogadas cada año (Balbix, 2023). Este diluvio de datos ha provocado la fatiga de los equipos de seguridad y una parálisis del análisis, donde se dedica un tiempo desproporcionado a la identificación de problemas, pero se logra poco en términos de resultados prácticos y accionables. El enfoque tradicional, basado casi exclusivamente en la puntuación de gravedad, a menudo conduce a estrategias de remediación ineficientes, dedicando recursos a vulnerabilidades con puntajes "críticos" que en realidad nunca se explotan, mientras que se descuidan riesgos más relevantes y urgentes.

En respuesta a este imperativo estratégico, se presenta el nuevo Método de Priorización de Amenazas Basado en Explotación (PABE) que es un framework de ciberseguridad diseñado para optimizar los esfuerzos de defensa al integrar el análisis de riesgo teórico (modelado de amenazas) con la inteligencia de amenazas en tiempo real. Este método se enfoca en responder a la pregunta crítica: "¿De todas las posibles debilidades, ¿cuáles tienen la mayor probabilidad de ser explotadas por atacantes reales ahora?"

PABE formaliza una secuencia de pasos que van desde la estrategia de negocio hasta la acción táctica, utilizando herramientas y bases de datos ampliamente reconocidas en la industria para garantizar que los recursos de mitigación se dirijan a las amenazas más inminentes.

Al adoptar la metodología PABE, las organizaciones pueden superar las limitaciones de los sistemas tradicionales, optimizar la asignación de recursos y fortalecer su postura de seguridad contra las amenazas más relevantes y activas en el panorama actual.

Palabras clave: Modelado de Amenazas, Priorización de Vulnerabilidades, EPSS, CISA KEV, Gestión de Vulnerabilidades Basada en el Riesgo.

1 Introducción

1.1 De la Reacción a la Proactividad Estratégica

La ciberseguridad, como disciplina, ha evolucionado rápidamente, pero los desafíos que enfrentan los equipos de defensa han crecido a un ritmo aún más vertiginoso. El contexto de la amenaza actual se define por un crecimiento exponencial del volumen de vulnerabilidades. Los catálogos públicos como el de Common Vulnerabilities and Exposures (CVE) se actualizan diariamente, y cada año se añaden más de 20,000 nuevas entradas (Fortinet, 2023c). Este volumen de datos no solo es difícil de manejar, sino que ha llevado a una incapacidad general para convertir la "montaña de datos de vulnerabilidad en información procesable" (Mell et al., 2007). Las organizaciones se encuentran atrapadas en un ciclo interminable de escaneos y parches, lidiando con una "fatiga de alerta" que reduce la moral del equipo y aumenta el riesgo de que se pasen por alto las amenazas críticas (Indusface, 2023).

La raíz del problema radica en una dependencia excesiva de los enfoques tradicionales. La priorización impulsada únicamente por la gravedad, como la que se basa en el Common Vulnerability Scoring System (CVSS), a menudo conduce a prioridades ineficientes (Software Secured, 2021). Se ha observado que las organizaciones gastan una cantidad significativa de tiempo y recursos en corregir vulnerabilidades con una puntuación CVSS alta o crítica que, en la práctica, no están siendo explotadas por los atacantes (Balbix, 2023). Mientras tanto, los riesgos reales, que pueden ser menos graves en papel, pero más probables de ser atacados, se descuidan, dejando a la organización expuesta a una explotación real.

Para contrarrestar este problema, es imperativo que la seguridad cibernética se desplace de un modelo reactivo, basado en la remediación, a un modelo proactivo, basado en la predicción y el contexto. En este informe, se conceptualiza la metodología PABE como la respuesta estratégica a este desafío. La metodología PABE se presenta como un marco integrado que no solo identifica vulnerabilidades, sino que las contextualiza con la inteligencia de amenazas en tiempo real y la criticidad de los activos del negocio. La acuñación del nombre PABE se basa en cuatro principios fundamentales que trascienden las limitaciones de los sistemas tradicionales: Proactividad, al actuar en las fases de diseño y desarrollo; Alineación con los atacantes, al considerar sus motivaciones y tácticas; Basada en el negocio, al priorizar los activos que son de mayor valor para la organización; y priorizando la Explotabilidad, al enfocarse en las vulnerabilidades que tienen la mayor probabilidad de ser explotadas.

2 Marco Teórico de la Metodología PABE - La Fusión de Disciplinas de Seguridad

2.1 El Fundamento Proactivo: El Modelado de Amenazas como Piedra Angular

La piedra angular de la metodología PABE es el modelado de amenazas, una disciplina de seguridad que va más allá de la simple detección de fallos. El modelado de amenazas es un enfoque estructurado para identificar posibles amenazas, vectores de ataque y vulnerabilidades en un sistema antes de que ocurran los incidentes (Imperva, 2023; Palo Alto Networks, 2023a). A diferencia del escaneo de vulnerabilidades o las pruebas de penetración, que evalúan los sistemas ya desplegados, el modelado de amenazas opera en fases más tempranas del ciclo de vida del desarrollo de software (SDLC). Esta medida proactiva permite a los arquitectos e ingenieros de seguridad diseñar defensas de manera más inteligente, reduciendo los costos de remediación y disminuyendo la superficie de ataque antes de que se escriba una sola línea de código en producción (Black Duck, 2023).

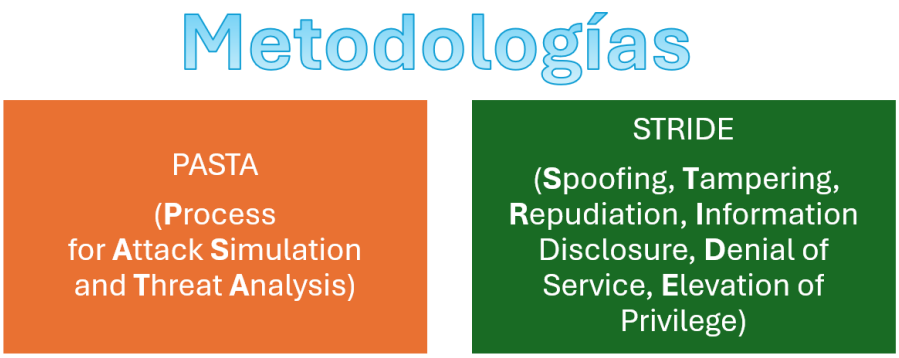
La metodología PABE adopta el Proceso para la Simulación de Ataques y Análisis de Amenazas (PASTA) como su marco estratégico principal. PASTA se distingue por su enfoque holístico y orientado al riesgo, que comienza por alinear los requisitos de seguridad con los objetivos empresariales (Pure Storage, 2023a). Esta alineación inicial garantiza que las iniciativas de seguridad apoyen directamente las metas organizacionales, a diferencia de otros marcos que pueden centrarse únicamente en los riesgos técnicos. La naturaleza adaptable e iterativa de PASTA, que se puede

personalizar para adaptarse a las necesidades específicas de una organización, la convierte en un pilar fundamental para PABE (VerSprite, 2012).

El proceso de PASTA consta de siete etapas bien definidas:

1. Definición de Objetivos de Negocio: Identificar los objetivos críticos de la organización y sus implicaciones de seguridad para establecer una base estratégica.
2. Definición del Alcance Técnico: Documentar los componentes del sistema, los flujos de datos y los límites de confianza para establecer el alcance del análisis.
3. Análisis de Amenazas: Identificar a los posibles actores de amenazas y sus motivaciones, analizando los patrones de ataque para crear perfiles de amenaza.
4. Análisis de Vulnerabilidades y Debilidades: Realizar evaluaciones exhaustivas de las vulnerabilidades y los fallos de diseño, mapeándolos a las amenazas identificadas.
5. Modelado de Ataques: Simular escenarios de ataque detallados para probar los controles de seguridad y validar la efectividad de las defensas existentes.
6. Análisis de Riesgos: Evaluar el daño potencial y la probabilidad de cada riesgo, priorizándolos en función del impacto en el negocio.
7. Desarrollo y Gestión de Contramedidas: Desarrollar e implementar estrategias para mitigar los riesgos, que se pueden adaptar al ciclo de vida del desarrollo de software (SDLC).

Para la tercera etapa de PASTA, PABE integra herramientas tácticas, en particular el modelo STRIDE. STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) es una mnemónica desarrollada por Microsoft para categorizar los tipos de amenazas de seguridad (Wikipedia, 2024a). STRIDE es particularmente útil cuando se aplica a los diagramas de flujo de datos (DFDs) creados en la etapa 2 de PASTA. Por ejemplo, se puede utilizar STRIDE para auditar los flujos de datos y los límites de confianza en un DFD, identificando amenazas como la divulgación de información o la suplantación de identidad (Wikipedia, 2024a). La integración de PASTA y STRIDE no es opcional, sino una relación simbiótica que proporciona un puente crucial entre la estrategia y la táctica. PASTA ofrece el marco estratégico de alto nivel, basado en el negocio, mientras que STRIDE proporciona la lente táctica y categórica para identificar los tipos específicos de amenazas durante la descomposición de la aplicación, lo que demuestra una integración fluida que va más allá de la simple enumeración de herramientas.



2.2 El Lenguaje Común de las Debilidades y los Patrones de Ataque

Para que el análisis de amenazas sea efectivo, PABE se basa en un lenguaje estandarizado para describir las debilidades y los patrones de ataque. Este lenguaje es proporcionado por catálogos mantenidos por organizaciones de seguridad líderes.

El Common Weakness Enumeration (CWE) es un catálogo de debilidades de software y hardware que representan las causas raíz de las vulnerabilidades de seguridad (Orca Security, 2023). A diferencia de CVE, que documenta instancias específicas de vulnerabilidades del mundo real, CWE se enfoca en los tipos de fallos subyacentes, como la validación de entrada incorrecta o los desbordamientos de búfer. Esta naturaleza proactiva de CWE es fundamental para PABE, ya que ayuda a los desarrolladores y arquitectos a prevenir errores en las etapas de diseño y codificación, en lugar de reaccionar a los incidentes después de que se hayan divulgado. El uso de CWE en la educación de codificación segura, las herramientas de análisis de seguridad y la evaluación de software de terceros es un componente clave de una estrategia de seguridad madura (Bugcrowd, 2023).

El Common Attack Pattern Enumeration and Classification (CAPEC), por su parte, es un catálogo de patrones de ataque conocidos que los atacantes utilizan comúnmente para explotar aplicaciones y sistemas de TI (Wikipedia, 2024b). CAPEC es una herramienta invaluable para comprender la mentalidad de los adversarios, ya que describe los pasos comunes involucrados en un ataque (por ejemplo, los pasos de una inyección SQL). Esta comprensión permite a los defensores anticipar las acciones de los atacantes y desarrollar contramedidas más efectivas (Threat Modeling, 2023). CAPEC se vincula directamente con las debilidades de CWE, ya que un patrón de ataque (CAPEC) describe el método para explotar una debilidad (CWE).

La metodología PABE capitaliza la relación inherente entre estos catálogos para una comprensión profunda de la anatomía de las amenazas. Se entiende que una debilidad genérica de CWE (por ejemplo, una "falla en la validación de la entrada") puede ser explotada a través de un patrón de ataque CAPEC (por ejemplo, "Inyección SQL") para dar lugar a una vulnerabilidad específica de CVE (Common Vulnerabilities and Exposures), que es una instancia particular encontrada en un sistema (Fortinet, 2023c; Threat Modeling, 2023). PABE aprovecha esta cadena de conocimiento para una comprensión profunda, permitiendo a los equipos de seguridad no solo parchear, sino también abordar la causa raíz de las vulnerabilidades. Al fusionar estos conceptos en la metodología PABE, se crea un bucle de retroalimentación de inteligencia: el modelado

de amenazas identifica las amenazas (con STRIDE), los catálogos (CAPEC/CWE) proporcionan el "cómo" y el "por qué" de los ataques, y la priorización posterior se basa en la instancia específica del CVE.

3 Marco Conceptual de la Priorización en PABE - Más Allá de la Gravedad

3.1 La Evolución de la Puntuación de Vulnerabilidades: El Fin del Reinado del CVSS

Durante casi dos décadas, el Common Vulnerability Scoring System (CVSS) ha sido el estándar de facto para calificar la gravedad de las vulnerabilidades de seguridad de TI en una escala de 0 a 10 (Wikipedia, 2024c). CVSS se compone de tres grupos de métricas (Mell et al., 2007; Fortinet, 2023b):

Base: Representa las cualidades intrínsecas de una vulnerabilidad, como el vector de ataque, la complejidad del ataque y el impacto en la confidencialidad, integridad y disponibilidad.

Temporal: Refleja las características de una vulnerabilidad que cambian con el tiempo, como la existencia de código de explotación o la disponibilidad de soluciones de remediación.

Ambiental: Representa las características de una vulnerabilidad que son únicas para el entorno del usuario, como la criticidad de los activos o la presencia de controles compensatorios.

Si bien el CVSS ha sido una herramienta valiosa para proporcionar un lenguaje estandarizado para comunicar la gravedad de una vulnerabilidad, tiene limitaciones fundamentales que lo hacen inadecuado como único motor de priorización en un entorno de amenazas moderno. La principal crítica es que el CVSS se centra en la gravedad, no en el riesgo (Software Secured, 2021). Una puntuación base alta simplemente indica el daño potencial que podría causar la vulnerabilidad, pero no considera si los atacantes la están explotando activamente en el mundo real o si representa un riesgo real para un entorno específico.
Además, la puntuación base del CVSS es estática y no evoluciona con el panorama de amenazas. Esto puede llevar a situaciones en las que una vulnerabilidad "crítica" con un puntaje de 9. puede ser menos importante para una organización que una vulnerabilidad con un puntaje de 6. que está siendo explotada activamente (Wiz, 2023).
A esto se suma la subjetividad en la puntuación de las métricas. Diferentes evaluadores pueden interpretar la "complejidad del ataque" de manera diferente, lo que conduce a inconsistencias y a una falta de confianza en el sistema (Software Secured, 2021). Por estas razones, la dependencia exclusiva del CVSS en la priorización se ha demostrado ineficaz, perpetuando el problema del volumen y la fatiga del equipo.

3.2 La Irrupción de la Probabilidad: EPSS como el Nuevo Motor de Priorización

Para abordar las deficiencias del CVSS, la metodología PABE integra el Exploit Prediction Scoring System (EPSS). EPSS es un esfuerzo impulsado por datos que utiliza un modelo de aprendizaje automático para predecir la probabilidad de que una vulnerabilidad sea explotada en los próximos 30 días (FIRST, 2023). Su puntuación oscila entre 0 y 1 (o 0% y 100%), donde un puntaje más alto indica una mayor probabilidad de explotación.

EPSS se basa en una amplia variedad de fuentes de datos dinámicas, lo que le permite proporcionar una visión más precisa del panorama de amenazas en tiempo real (Balbix, 2024). Estas fuentes incluyen la edad de una CVE, la existencia de código de explotación publicado en repositorios como Metasploit y GitHub, los datos de escáneres de seguridad y los vectores CVSS v3. A diferencia del CVSS, que se centra en el daño potencial, el EPSS se enfoca en la probabilidad de que ese daño ocurra, lo que lo convierte en una herramienta invaluable para la priorización (Fortinet, 2023a; Orca Security, 2024).

La fortaleza de PABE reside en la complementariedad de CVSS y EPSS. Un enfoque dual permite tomar decisiones más inteligentes. El CVSS proporciona la información sobre la gravedad potencial, mientras que el EPSS añade el contexto de la probabilidad de explotación (Brinqa, 2023; Xygeni, 2024). La combinación de ambos permite a las organizaciones optimizar la asignación de recursos de manera significativa. Se ha demostrado que menos del 2% de las vulnerabilidades conocidas tienen una puntuación alta de EPSS, lo que contrasta con el gran número de vulnerabilidades "críticas" de CVSS que nunca se tocan por los ciberdelincuentes (Brinqa, 2023; Xygeni, 2024). La integración de EPSS en la priorización de PABE es una respuesta directa al problema de la fatiga del equipo y la escasez de recursos, ya que permite a las organizaciones reducir drásticamente el volumen de parches requeridos sin sacrificar la cobertura de las amenazas más relevantes (FOSSA, 2023; ZeroFox, 2023).

3.3 La Integración de la Inteligencia de Amenazas y el Contexto Empresarial

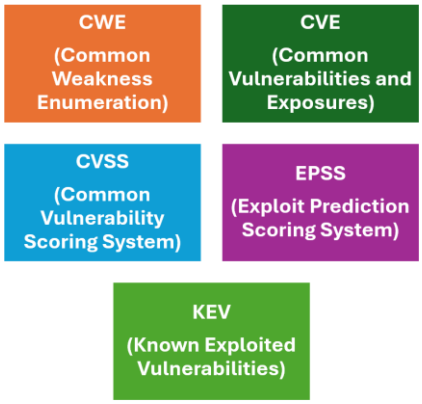
Una priorización efectiva no puede depender únicamente de los puntajes técnicos. La inteligencia de amenazas y el contexto del negocio son componentes cruciales que PABE integra a través del Catálogo de Vulnerabilidades Explotadas Conocidas (KEV) de CISA y el marco de Gestión de Vulnerabilidades Basada en el Riesgo (RBVM).

El Catálogo KEV es una fuente de inteligencia de amenazas "autoritativa" mantenida por la Cybersecurity and Infrastructure Security Agency (CISA) de EE. UU.. Este catálogo enumera las vulnerabilidades que tienen evidencia de haber sido explotadas activamente en el mundo real (Cybersecurity and Infrastructure Security Agency, 2023). El KEV actúa como una señal de peligro binaria: una vulnerabilidad está en la lista o no lo está. Su inclusión en el KEV es un indicador de que una vulnerabilidad requiere una remediación inmediata, ya que las agencias federales de EE. UU. están obligadas a parchearlas en un plazo específico (Cybersecurity and Infrastructure Security Agency, 2025). Si bien el KEV es una herramienta poderosa, no es una lista exhaustiva de todas las vulnerabilidades explotadas, y un análisis muestra que hasta el 94% de las vulnerabilidades explotadas pueden no estar en el catálogo (Perkal, 2023; Zest Security, 2023).

El marco de Gestión de Vulnerabilidades Basada en el Riesgo (RBVM) es el componente que unifica todos los elementos de la metodología PABE (ConnectWise, 2023; Palo Alto Networks, 2023b). El RBVM es la filosofía que transforma los datos de vulnerabilidad sin procesar en inteligencia procesable, ya que considera el contexto único del entorno de la organización. Sus principios son:

- **Descubrimiento y Clasificación de Activos**: La base de cualquier programa de RBVM es el conocimiento de lo que se debe proteger. Esto implica el descubrimiento continuo de activos y la clasificación de los mismos en función de su criticidad para el negocio, la sensibilidad de los datos que manejan y su exposición a amenazas externas (GitHub, 2023; Palo Alto Networks, 2023c).
- **Análisis de Riesgo Contextual**: El RBVM va más allá de las puntuaciones de CVSS y EPSS al tener en cuenta factores como la presencia de controles compensatorios, la segmentación de la red y el impacto potencial en los sistemas interconectados.
- **Análisis de la Trayectoria de Ataque:** Este paso refuerza la priorización al visualizar cómo un atacante podría moverse lateralmente dentro de la infraestructura y escalar privilegios (Palo Alto Networks, 2023d).

Bases de Datos e Indicadores de explotabilidad



El RBVM es el "cerebro" de la metodología PABE, ya que es el componente que sintetiza la probabilidad de explotación (EPSS), la confirmación de la explotación (KEV) y la gravedad potencial (CVSS) con la capa crucial de la criticidad del activo definida en las primeras etapas de PASTA (Palo Alto Networks, 2023b). Esta síntesis permite a las organizaciones tomar decisiones informadas, como despriorizar una vulnerabilidad de alta gravedad en un sistema de prueba de bajo valor, mientras se prioriza una vulnerabilidad de gravedad moderada en una aplicación de misión crítica. El RBVM previene la "fatiga de alerta" y la "parálisis de análisis" al proporcionar un método claro para pasar de los datos brutos a las acciones priorizadas.

4 La Metodología PABE en la Práctica - Un Flujo de Trabajo Unificado y Operacional

4.1 Estructura y Fases del Framework PABE

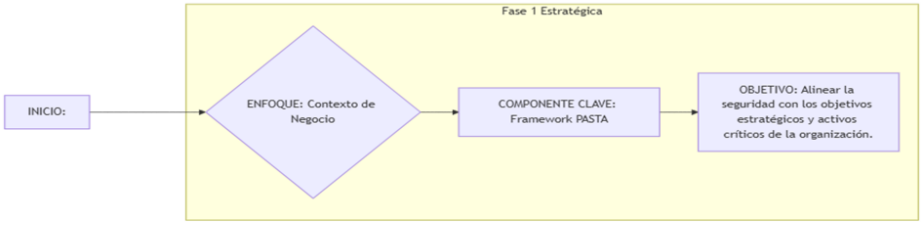
El framework se divide en cuatro fases progresivas y conceptuales, cada una con un propósito claro y un conjunto de herramientas asociadas.

Fase	Enfoque Principal	Componentes Clave	Objetivo de la Fase
Fase 1: Estratégica	**Contexto de Negocio**	PASTA	Alinear la seguridad con los objetivos estratégicos y activos críticos de la organización.
Fase 2: Analítica	**Riesgo Potencial**	STRIDE, DREAD	Identificar sistemáticamente las amenazas en el diseño del sistema y cuantificar su riesgo.
Fase 3: Forense	**Mecánica del Ataque**	CAPEC, CWE	Comprender cómo se explota una amenaza y cuál es la debilidad de código subyacente.
Fase 4: Táctica	**Urgencia de Explotación**	CVE, CVSS, EPSS, KEV	Priorizar las vulnerabilidades basándose en su probabilidad y confirmación de explotación activa.

Tabla. 1. Estructura y Fases del Framework PABE

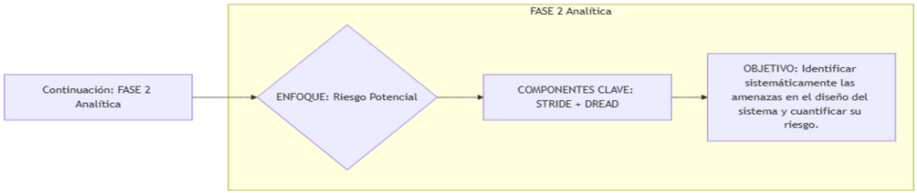
4.2 Fases Detalladas y Aplicación

Fase 1: Definición y Análisis Estratégico
Esta fase establece el contexto, los activos críticos y el punto de vista del atacante, utilizando PASTA como la columna vertebral de la metodología.



1. **Herramienta Principal:** PASTA (Process for Attack Simulation and Threat Analysis).
2. **Actividades:**
   - **Definición del Alcance:** Identificar los límites del sistema (por ejemplo, microservicios, APIs, interfaz de usuario).
   - **Identificación de Activos:** Determinar qué datos son más valiosos (por ejemplo, PII (Información de Identificación Personal), datos de transacciones, secretos de negocio) y los activos que los gestionan.
   - **Objetivos de Seguridad:** Establecer los requisitos de confidencialidad, integridad y disponibilidad (CIA) y los objetivos de cumplimiento normativo.

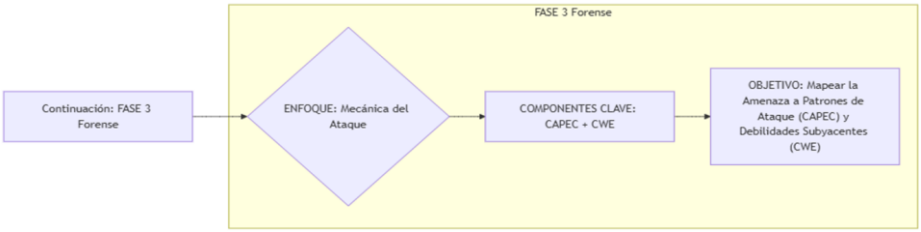
Fase 2: Identificación y Evaluación de Riesgos
El objetivo es crear una lista de amenazas priorizadas basadas en el diseño del sistema, incluso antes de que existan vulnerabilidades conocidas.



1. **Herramientas:** STRIDE y DREAD.
2. **Actividades:**
   - **Modelado del Sistema:** Crear Diagramas de Flujo de Datos (DFD) para visualizar las fronteras de confianza y los flujos de información del sistema.
   - **Identificación de Amenazas (STRIDE):** Aplicar las categorías (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) a cada elemento del DFD para identificar las posibles amenazas.

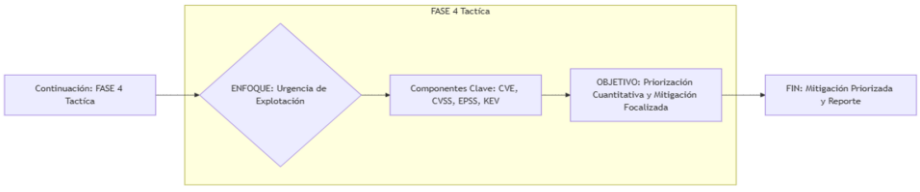
- **Cuantificación del Riesgo (DREAD):** Evaluar cada amenaza identificada con el modelo DREAD (Daño, Reproducibilidad, Explotabilidad, Usuarios Afectados, Detectabilidad) para obtener una puntuación de riesgo potencial y ordenar la lista (Pure Storage, 2023b).

Fase 3: Análisis Forense de Ataque
Para las amenazas de alto riesgo (según el puntaje DREAD), esta fase detalla la mecánica del ataque y la debilidad del código.



1. **Herramientas:** CAPEC y CWE.
2. **Actividades:**
   - **Construcción de Casos de Abuso:** Desarrollar narrativas detalladas sobre cómo un atacante explotaría las amenazas priorizadas (por ejemplo, "Un atacante manipula los privilegios de un usuario para obtener acceso de administrador").
   - **Patrón de Ataque (CAPEC):** Identificar el patrón de ataque que corresponde al caso de abuso (por ejemplo, CAPEC-241: Privilege Escalation).
   - **Causa Raíz (CWE):** Identificar la debilidad de código o diseño subyacente que lo permite (por ejemplo, CWE-269: Improper Privilege Management).

Fase 4: Priorización Basada en Explotación Activa
Esta es la fase de inteligencia de amenazas que proporciona la justificación final para la mitigación.



1. **Herramientas:** CVE, CVSS, EPSS y KEV.
2. **Actividades:**
   - **Identificación de Vulnerabilidad (CVE):** Si la debilidad es una vulnerabilidad conocida en un componente de terceros, buscar su

identificador CVE.

- **Severidad Técnica (CVSS):** Consultar el puntaje CVSS para obtener la severidad técnica de la vulnerabilidad (impacto y métricas de explotabilidad).
- **Probabilidad de Explotación (EPSS):** Utilizar el puntaje EPSS (Exploit Prediction Scoring System) para estimar la probabilidad de que la CVE sea explotada activamente en los próximos 30 días.
- **Confirmación de Explotación (KEV):** Consultar el Catálogo KEV (Known Exploited Vulnerabilities) de CISA para verificar si la vulnerabilidad ya está siendo explotada por atacantes.

4.3 Priorización Final y Toma de Decisiones

El **framework PABE** establece una jerarquía de priorización de mitigación que va más allá de la simple severidad técnica.

1. **Prioridad Máxima y Urgente:** Si la vulnerabilidad se encuentra en el **Catálogo KEV**, la mitigación es **inmediata**.
2. **Prioridad Alta:** Si no está en KEV, pero tiene un puntaje **EPSS > 0.8** (80% de probabilidad de ser explotada en los próximos 30 días), la mitigación es **crítica**.
3. **Prioridad Estándar:** Las vulnerabilidades con puntaje **CVSS >= 8.0** se gestionan según los procesos de mitigación **estándar de la organización**.

Lógica de Priorización	Acción Recomendada	Justificación (Análisis PABE)	Fuentes de Datos Clave
CVSS Alto + EPSS Alto + KEV	Prioridad máxima e inmediata	La vulnerabilidad tiene un alto impacto, una alta probabilidad de explotación y ya se está explotando activamente. Representa un riesgo inminente.	CVSS, EPSS, Catálogo KEV.
CVSS Alto + EPSS Bajo	Monitoreo cercano, pero despriorizar	La vulnerabilidad tiene un alto impacto potencial, pero es poco probable que sea explotada en el futuro cercano. Los recursos pueden dirigirse a amenazas más probables.	CVSS, EPSS.

CVSS Medio/Bajo + EPSS Alto	Investigar rápidamente	La puntuación de gravedad es baja, pero los datos de amenazas indican que es un objetivo activo. Podría ser un componente de una cadena de ataque.	CVSS, EPSS, Inteligencia de Amenazas.

Tabla. 2. Flujo de Trabajo PABE: La Lógica de Priorización Integrada

PABE asegura que los recursos se centren en mitigar las vulnerabilidades que no solo son severas, sino que representan una amenaza **inminente y confirmada**.

La metodología PABE no es una simple suma de disciplinas de seguridad, sino una arquitectura de seguridad coherente que fusiona el modelado de amenazas proactivo con una gestión de vulnerabilidades reactiva pero inteligente. El resultado es un flujo de trabajo unificado y operativo que garantiza que la seguridad no sea un proceso aislado, sino una parte intrínseca y continua de las operaciones empresariales.

5 Desafíos y Consideraciones para la Implementación

A pesar de sus beneficios, la adopción de la metodología PABE conlleva ciertos desafíos que deben ser abordados de manera proactiva:

- **Complejidad y Fatiga:** La integración de múltiples fuentes de datos (CVSS, EPSS, KEV, datos de activos) puede ser un proceso abrumador si no se automatiza. Sin las herramientas adecuadas, la gestión manual de este volumen de información podría provocar la misma "parálisis de análisis" que PABE busca resolver.
- **Limitaciones de los Datos:** Las fuentes de datos, aunque valiosas, tienen sus propias limitaciones. La puntuación DREAD, por ejemplo, puede ser subjetiva y simplificar en exceso amenazas complejas. El Catálogo KEV de CISA no es una lista exhaustiva de todas las vulnerabilidades explotadas. De manera similar, los puntajes de EPSS pueden fluctuar y no reflejar con precisión el panorama de amenazas en el caso de vulnerabilidades muy recientes o de día cero. La aplicación madura de PABE requiere que los equipos reconozcan y compensen estas limitaciones.
- **Necesidad de Contexto Único:** Ni el CVSS ni el EPSS tienen en cuenta el contexto único de una organización. La implementación exitosa de PABE depende de la capacidad de la organización para integrar la criticidad de sus propios activos, la segmentación de su red y sus controles de seguridad existentes en la lógica de priorización.
- **Brecha entre Equipos:** Si no existe una alineación cultural y de procesos entre los equipos de seguridad y de TI, los esfuerzos de PABE pueden fracasar.

La falta de comunicación puede sabotear la mitigación de vulnerabilidades, incluso cuando la priorización es clara.

6 Conclusiones y Recomendaciones

La ciberseguridad se encuentra en un punto de inflexión. El enfoque tradicional de la gestión de vulnerabilidades, impulsado por la gravedad, se ha vuelto insostenible ante el volumen de amenazas y la escasez de recursos. La metodología PABE se erige como una solución estratégica que trasciende este paradigma obsoleto. PABE no es un producto ni una herramienta individual, sino un cambio de mentalidad fundamental en la forma en que una organización aborda el riesgo de ciberseguridad. Es una arquitectura de seguridad que integra el pensamiento proactivo del modelado de amenazas, el contexto dinámico de la inteligencia de amenazas y la toma de decisiones informada del RBVM.

Se recomienda a los líderes y profesionales de la seguridad cibernética considerar las siguientes acciones para adoptar los principios de PABE:

- **Adoptar la mentalidad RBVM:** Guíe la estrategia de seguridad reconociendo que el riesgo es una función del impacto y la probabilidad. Priorice los esfuerzos de seguridad basándose en la criticidad de los activos y la exposición real a amenazas, no solo en la gravedad teórica de una vulnerabilidad.
- **Invertir en herramientas integradas:** Seleccione soluciones de seguridad que combinen los datos de EPSS, el Catálogo KEV y la inteligencia de activos. La automatización de la correlación de datos es crucial para evitar la sobrecarga del equipo y permitir una priorización eficiente a escala.
- **Fomentar la colaboración:** Promueva una cultura de seguridad "desplazada a la izquierda" (shifting left) a través de la integración del modelado de amenazas en el SDLC. Fomente una comunicación fluida entre los equipos de seguridad, desarrollo y TI para garantizar que la mitigación sea un proceso colaborativo y sin fricciones.
- **Entender que PABE es un proceso cíclico y en constante evolución:** El panorama de amenazas cambia a diario. La metodología PABE requiere un monitoreo continuo, una reevaluación regular de los riesgos y una adaptación constante a medida que emergen nuevas amenazas y los sistemas de la organización evolucionan.

Referencias

Balbix. (2023). *Is your vulnerability management strategy doing more harm than good?* https://www.balbix.com/blog/is-your-vulnerability-management-strategy-doing-more-harm-than-good/

Balbix. (2024). *What is the Exploit Prediction Scoring System (EPSS)?* https://www.balbix.com/insights/what-is-epss-epss-vs-cvss/

Black Duck. (2023). *What is threat modeling and how does it work?* https://www.blackduck.com/glossary/what-is-threat-modeling.html

Brinqa. (2023). *EPSS vs. CVSS: Understanding the differences and use cases*. https://www.brinqa.com/blog/epss-vs-cvss

Bugcrowd. (2023). *Common Weakness Enumeration (CWE)*. https://www.bugcrowd.com/glossary/common-weakness-enumeration-cwe/

ConnectWise. (2023). *Risk-based vulnerability management & what you need to know*. https://www.connectwise.com/blog/risk-based-vulnerability-management

Cybersecurity and Infrastructure Security Agency. (2023). *Known Exploited Vulnerabilities catalog*. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Cybersecurity and Infrastructure Security Agency. (2025). *CISA adds one known exploited vulnerability to catalog*. https://www.cisa.gov/news-events/alerts/2025/09/11/cisa-adds-one-known-exploited-vulnerability-catalog

FIRST. (2023). *EPSS user guide*. Forum of Incident Response and Security Teams. https://www.first.org/epss/user-guide

Fortinet. (2023a). *Using EPSS to predict threats and secure your network*. FortiGuard Labs. https://www.fortinet.com/blog/threat-research/predict-threats-and-secure-networks-with-epss

Fortinet. (2023b). *What is Common Vulnerability Scoring System (CVSS)?* https://www.fortinet.com/resources/cyberglossary/common-vulnerability-scoring-system

Fortinet. (2023c). *What is a CVE? Common Vulnerabilities and Exposures defined*. https://www.fortinet.com/resources/cyberglossary/cve

FOSSA. (2023). *Understanding and using the EPSS scoring system*. https://fossa.com/blog/understanding-using-epss-scoring-system/

GitHub. (2023). *What is Risk-Based Vulnerability Management (RBVM)?* https://github.com/resources/articles/security/what-is-risk-based-vulnerability-management

Imperva. (2023). *What is threat modeling: Guide to security risk management*. https://www.imperva.com/learn/application-security/threat-modeling/

Indusface. (2023). *Vulnerability management: 8 key challenges - Don't ignore!* https://www.indusface.com/blog/8-common-recurring-vulnerability-management-challenges-dont-ignore-them/

Mell, P., Scarfone, K., & Romanosky, S. (2007). *A complete guide to the Common Vulnerability Scoring System (CVSS) version 2.0*. National Institute of Standards and Technology. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=51198

Orca Security. (2023). *CWE: Understanding Common Weakness Enumeration in cloud security*. https://orca.security/glossary/cwe/

Orca Security. (2024). *How the EPSS scoring system works*. https://orca.security/resources/blog/epss-scoring-system-explained/

Palo Alto Networks. (2023a). *What is threat modeling?* https://www.paloaltonetworks.com/cyberpedia/threat-modeling

Palo Alto Networks. (2023b). *What is risk-based vulnerability management?* https://www.paloaltonetworks.com/cyberpedia/risk-based-vulnerability-management

Palo Alto Networks. (2023c). *What is risk-based vulnerability management?* Palo Alto Networks Australia. https://www.paloaltonetworks.com.au/cyberpedia/risk-based-vulnerability-management

Palo Alto Networks. (2023d). *What is threat and vulnerability management?* https://www.paloaltonetworks.com/cyberpedia/threat-and-vulnerability-management

Perkal, Y. (2023). *CISA KEV — A balanced perspective*. Medium. https://medium.com/@yotamperkal/cisa-kev-a-balanced-perspective-ff3856e69ba9

Pure Storage. (2023a). *What is the PASTA threat model?* https://www.purestorage.com/knowledge/pasta-threat-modeling.html

Pure Storage. (2023b). *What is the DREAD threat model?* https://www.purestorage.com/knowledge/dread-threat-model.html

Software Secured. (2021). *Why Common Vulnerability Scoring Systems (CVSS) suck*. https://www.softwaresecured.com/post/why-common-vulnerability-scoring-systems-suck

Strobes. (2023). *Smarter vulnerability prioritization: A Strobes guide*. https://strobes.co/blog/what-is-vulnerability-prioritization-strobes-guide/

Threat Modeling. (2023). *CAPEC threat modeling*. https://threat-modeling.com/capec-threat-modeling/

VerSprite. (2012). *Process for Attack Simulation & Threat Analysis*. HubSpot. https://cdn2.hubspot.net/hubfs/4598121/Content%20PDFs/VerSprite-PASTA-Threat-Modeling-Process-for-Attack-Simulation-Threat-Analysis.pdf

Wikipedia. (2024a). *STRIDE model*. https://en.wikipedia.org/wiki/STRIDE_model

Wikipedia. (2024b). *Common Attack Pattern Enumeration and Classification*. https://en.wikipedia.org/wiki/Common_Attack_Pattern_Enumeration_and_Classification

Wikipedia. (2024c). *Common Vulnerability Scoring System*. https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System

Wiz. (2023). *Vulnerability prioritization: Building a maximum security strategy*. https://www.wiz.io/academy/vulnerability-prioritization

Xygeni. (2024). *EPSS vs CVSS: What's the difference?* https://xygeni.io/blog/epss-vs-cvss-whats-the-difference/

Zest Security. (2023). *Beyond CVSS: Why EPSS and KEV are game-changers for prioritizing vulnerabilities*. https://www.zestsecurity.io/resources/content/beyond-cvss-why-epss-and-kev-are-game-changers-for-prioritizing-vulnerabilities

ZeroFox. (2023). *EPSS explained: How to strengthen your vulnerability management strategy*. https://www.zerofox.com/blog/epss-explained-how-to-strengthen-your-vulnerability-management-strategy/