# 📘 Glosario: Principios Básicos de Mitigación y Prevención

---

## 🔐 1. Mitigación

Acción reactiva destinada a **reducir el impacto de una vulnerabilidad o ataque ya ocurrido**. No elimina la causa raíz, pero permite contener daños y mantener la continuidad operativa.

---

## 🛡️ 2. Prevención

Conjunto de prácticas y medidas **proactivas** cuyo objetivo es **evitar la aparición de vulnerabilidades** o la ejecución exitosa de ataques.

---

## 📈 3. Ciclo de Vida del Desarrollo de Software (SDLC)

Modelo estructurado que define las fases necesarias para el desarrollo de una aplicación, desde su planificación hasta el mantenimiento. Integrar seguridad en cada fase es clave para la prevención.

---

## ⚠️ 4. Vulnerabilidad

Debilidad o error en un sistema, aplicación o configuración que puede ser explotado para comprometer la seguridad de la información.

---

## 🔓 5. Amenaza

Potencial de un agente (humano o no) de explotar una vulnerabilidad y causar daño a los activos de una organización.

---

## 📊 6. Riesgo

Probabilidad de que una amenaza explote una vulnerabilidad y cause un impacto negativo. Es el resultado de la ecuación: **Riesgo = Amenaza × Vulnerabilidad × Impacto**.

---

## 🧩 7. Web Application Firewall (WAF)

Sistema que filtra, monitorea y bloquea tráfico HTTP malicioso dirigido a aplicaciones web. Ayuda a mitigar ataques como XSS, SQLi y CSRF.

---

## 🔐 8. Security by Design

Principio que establece que la **seguridad debe incorporarse desde el diseño inicial del software**, y no como un agregado posterior.

---

## 👥 9. Defensa en Profundidad

Estrategia de seguridad que **implementa múltiples capas de controles defensivos** para proteger los activos, reduciendo la posibilidad de compromiso total.

---

## ⚙️ 10. Lista Blanca (Whitelist)

Lista de entradas explícitamente autorizadas. En validación de inputs, restringe el contenido a valores previamente definidos como seguros.

---

## 🔐 11. Validación de Entrada

Proceso mediante el cual se verifica que los datos introducidos por el usuario cumplan los requisitos esperados (formato, longitud, tipo, etc.). Previene inyecciones y errores lógicos.

---

## 🧪 12. Análisis Estático de Código (SAST)

Revisión automatizada del código fuente sin ejecutarlo. Permite detectar vulnerabilidades de seguridad antes de que la aplicación entre en producción.

---

## 🧪 13. Análisis Dinámico de Seguridad (DAST)

Proceso que evalúa la aplicación **en tiempo de ejecución**, simulando ataques reales para detectar vulnerabilidades desde el exterior.

---

## 💥 14. Cross-Site Scripting (XSS)

Vulnerabilidad que permite la **inyección de scripts maliciosos** en páginas web vistas por otros usuarios, generalmente por falta de validación o escape de contenido.

---

## 🔄 15. Cross-Site Request Forgery (CSRF)

Ataque que fuerza al navegador de un usuario autenticado a **realizar una acción no autorizada** en una aplicación en la que está autenticado.

---

## 📌 16. Token CSRF

Valor único y secreto incluido en formularios o solicitudes sensibles, que permite validar la legitimidad de la acción y prevenir ataques CSRF.

---

## 📊 17. MTTR (Mean Time To Respond/Remediate)

Tiempo promedio que transcurre entre la detección de un incidente y su resolución. Es un indicador clave de eficiencia en respuesta ante incidentes.

---

## 📋 18. Auditoría de Seguridad

Revisión formal y sistemática de las políticas, configuraciones, procesos y controles de seguridad de una organización. Identifica debilidades estructurales.

---

## 🔁 19. Mejora Continua

Ciclo iterativo de evaluación y ajuste que busca optimizar progresivamente los sistemas de defensa y gestión de riesgos en una organización.

---

## 🧠 20. Conciencia de Seguridad

Grado en que los miembros de una organización comprenden las amenazas de ciberseguridad y actúan con responsabilidad frente a ellas.

---