5.11 Propósito del Punto de Vista de Seguridad

Este viewpoint detalla las medidas de protección del sistema contra amenazas internas/externas, cubriendo:

- Autenticación y autorización
- Protección de datos en tránsito/reposo
- Gestión de vulnerabilidades
- Cumplimiento normativo

Objetivos clave:

1. Garantizar confidencialidad, integridad y disponibilidad (CID)
2. Mitigar riesgos OWASP Top 10
3. Cumplir con GDPR, HIPAA (si aplica)

Modelo de Amenazas

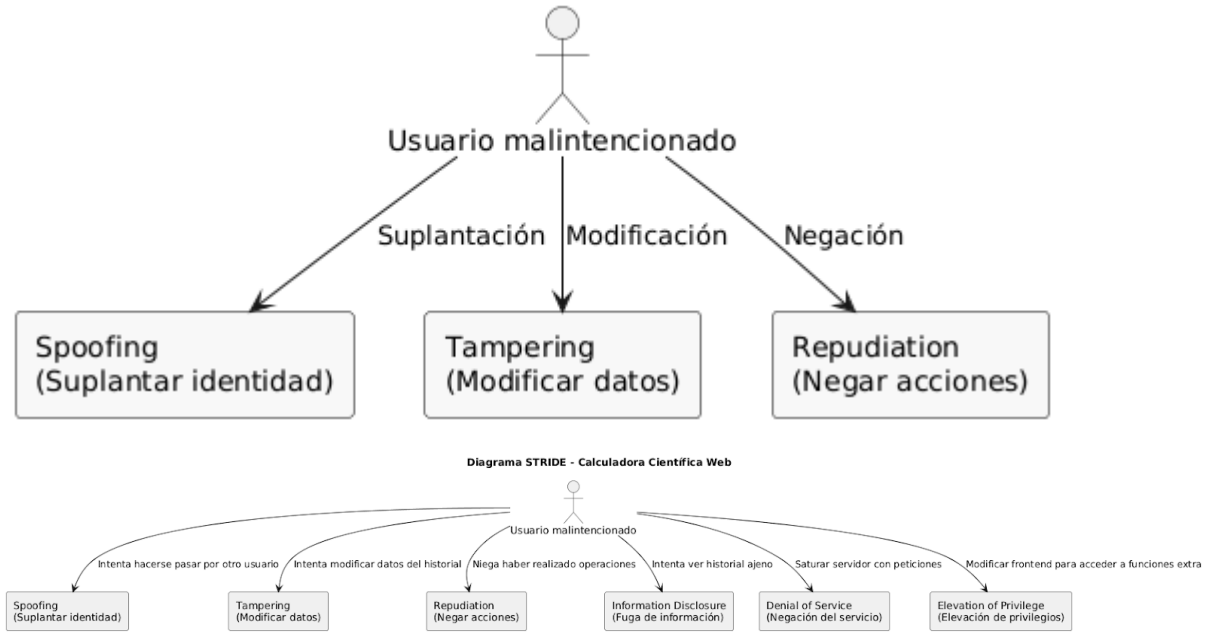
Top 5 Riesgos Identificados

Amenaza	Impacto	Probabilidad	Mitigación
Inyección SQL	Alto	Media	Prepared Statements + ORM
XSS	Medio	Alta	Sanitización con DOMPurify
Exposición de APIs	Crítico	Media	Rate Limiting + OAuth 2.0

Diagrama STRIDE

Letra	Amenaza	Descripción
S	Spoofing	Suplantación de identidad
T	Tampering	Alteración o modificación de datos o código
R	Repudiation	Negación de acciones por parte del usuario

I	Information Disclosure	Exposición de datos sensibles
D	Denial of Service	Interrupción del servicio
E	Elevation of Privilege	Escalada de privilegios para acceder a funcionalidades no autorizadas



Spoofing
Tampering
Repudiation
Usuario malintencionado
Suplantar identidad
Modificar datos
Negar acciones

Arquitectura Segura

Capas de Defensa

1. Perímetro: WAF (Cloudflare)
2. Aplicación: Validación entrada/salida
3. Datos: Encriptación AES-256

Segmentación de Red

bash

```
# Reglas firewall (ejemplo)
ufw allow 443/tcp  # HTTPS
ufw deny 22/tcp    # SSH expuesto
```

Control de Accesos

Modelo RBAC

Rol	Permisos
Usuario	Leer/escribir sus operaciones
Admin	CRUD usuarios + ver logs

JWT Implementation

```
javascript
// Ejemplo Node.js
const token = jwt.sign(
  { userId: 123 },
  process.env.JWT_SECRET,
  { expiresIn: '1h' }
);
```

Protección de Datos

Encriptación

Tipo	Tecnología	Uso
Tránsito	TLS 1.3	Todas las comunicaciones
Reposo	AWS KMS	Datos sensibles

Máscara de Datos

```
sql
-- PostgreSQL
CREATE VIEW masked_users AS
SELECT id,
       regexp_replace(email, '(.).*(.@)', '\1***\2') AS email
FROM users;
```

Gestión de Vulnerabilidades

Proceso de Parcheo

1. Escaneo semanal (Trivy + Snyk)
2. Priorización CVSS > 7.0
3. Parches en 72 horas (críticos)

Cumplimiento

Checklist GDPR

- [ ] Consentimiento explícito
- [ ] Derecho al olvido
- [ ] DPO asignado

Logs de Seguridad

```
json
{
  "timestamp": "2024-06-20T12:00:00Z",
  "event": "failed_login",
  "ip": "192.168.1.100",
  "userAgent": "Chrome/114"
}
```

Hardening

Configuración Segura

```
docker
# Dockerfile
USER node  # No root
RUN apt-get update && apt-get upgrade -y
```

Headers HTTP

```
nginx
Copy
Download
add_header X-Content-Type-Options "nosniff";
add_header X-Frame-Options "DENY";
```

Respuesta a Incidentes

Playbook Ejemplo

1. Contención: Aislar sistemas afectados
2. Erradicación: Eliminar malware
3. Recuperación: Restaurar backups

Contactos Clave

Rol	Teléfono
CSIRT	+34 900 000 000

con esto garantizamos:

Protección proactiva contra amenazas. Detección temprana de anomalías.

Cumplimiento regulatorio