

# Política de Seguridad - Sistema ERP Completo

## Versiones Soportadas

Actualmente proporcionamos actualizaciones de seguridad para las siguientes versiones:

Versión	Soportada
4.0.x	 Sí
3.0.x	 Sí
2.0.x	 No
1.0.x	 No

## Reportar Vulnerabilidades de Seguridad

La seguridad de nuestro sistema ERP es una prioridad máxima. Si descubres una vulnerabilidad de seguridad, te pedimos que nos ayudes a mantener seguros a nuestros usuarios siguiendo estos pasos:

### Reporte Responsable

**Por favor NO reportes vulnerabilidades de seguridad a través de issues públicos de GitHub.**

En su lugar, envía un email a: **security@tu-empresa.com** con la siguiente información:

- Descripción detallada de la vulnerabilidad
- Pasos para reproducir el problema
- Posible impacto y severidad
- Cualquier información adicional que pueda ayudar

### Información a Incluir

Para acelerar la resolución, incluye:

1. **Tipo de vulnerabilidad** (XSS, SQL injection, etc.)
2. **Componente afectado** (módulo específico)
3. **Versión del sistema** donde encontraste el problema
4. **Entorno** (desarrollo, producción, etc.)
5. **Proof of Concept** (si es aplicable)
6. **Sugerencias de remediación** (si las tienes)

### Tiempo de Respuesta

Nos comprometemos a:

- **24 horas:** Confirmación de recepción del reporte

- **72 horas:** Evaluación inicial y clasificación de severidad
- **7 días:** Plan de acción para vulnerabilidades críticas
- **30 días:** Resolución para vulnerabilidades de severidad media/alta

## Programa de Reconocimiento







Valoramos enormemente las contribuciones de seguridad responsables:

- **Reconocimiento público** (con tu permiso) en nuestro changelog
- **Crédito en la documentación** de seguridad
- **Badge de colaborador** en el repositorio
- **Acceso early** a nuevas versiones para testing







## Medidas de Seguridad Implementadas

---






### Autenticación y Autorización

-  **NextAuth.js** para autenticación robusta
-  **Session management** seguro
-  **Role-based access control** (RBAC)
-  **Password hashing** con bcrypt
-  **CSRF protection** habilitada
-  **Rate limiting** en APIs






### Protección de Datos

-  **Input validation** en todos los endpoints
-  **SQL injection prevention** con Prisma ORM
-  **XSS protection** con sanitización
-  **Data encryption** para datos sensibles
-  **Secure headers** configurados
-  **HTTPS enforcement** en producción

### Auditoría y Monitoreo

-  **Audit logs** completos
-  **Security events** monitoreados
-  **Failed login attempts** rastreados
-  **Data changes** registrados
-  **Access patterns** analizados

### Base de Datos

-  **Encrypted connections** (SSL/TLS)
-  **Parameterized queries** exclusivamente
-  **Database user permissions** mínimos
-  **Backup encryption** habilitado
-  **Connection pooling** seguro

## Vulnerabilidades Conocidas

---

Actualmente **no hay vulnerabilidades conocidas** en la versión 4.0.x.

## Historial de Vulnerabilidades

ID	Fecha	Severidad	Estado	Descripción
-	-	-	-	No se han reportado vulnerabilidades



## Configuración de Seguridad Recomendada

### Variables de Entorno

```
# Generar un NEXTAUTH_SECRET fuerte
NEXTAUTH_SECRET="[64+ caracteres aleatorios]"

# Usar HTTPS en producción
NEXTAUTH_URL="https://tudominio.com"

# Configurar base de datos segura
DATABASE_URL="postgresql://user:pass@host:5432/db?sslmode=require"
```

### Headers de Seguridad

```
// next.config.js
const securityHeaders = [
  {
    key: 'X-DNS-Prefetch-Control',
    value: 'on'
  },
  {
    key: 'Strict-Transport-Security',
    value: 'max-age=63072000; includeSubDomains; preload'
  },
  {
    key: 'X-Frame-Options',
    value: 'DENY'
  },
  {
    key: 'X-Content-Type-Options',
    value: 'nosniff'
  },
  {
    key: 'Referrer-Policy',
    value: 'origin-when-cross-origin'
  }
]
```

## Configuración de Base de Datos

```
-- Crear usuario con permisos mínimos
CREATE USER erp_app WITH PASSWORD 'strong_password';
GRANT CONNECT ON DATABASE erp_db TO erp_app;
GRANT USAGE ON SCHEMA public TO erp_app;
GRANT SELECT, INSERT, UPDATE, DELETE ON ALL TABLES IN SCHEMA public TO erp_app;

-- Habilitar SSL
ssl = on
ssl_cert_file = 'server.crt'
ssl_key_file = 'server.key'
```

## Checklist de Seguridad

### Para Desarrolladores

- ☐ ☒ Validar toda entrada de usuario
- ☐ ☒ Usar consultas parametrizadas
- ☐ ☒ Sanitizar salida HTML
- ☐ ☒ Implementar rate limiting
- ☐ ☒ Manejar errores sin exponer información
- ☐ ☒ Usar HTTPS en todas las comunicaciones
- ☐ ☒ Implementar logs de auditoría
- ☐ ☒ Realizar pruebas de penetración

### Para Administradores

- ☐ ☒ Mantener dependencias actualizadas
- ☐ ☒ Configurar backups cifrados
- ☐ ☒ Implementar monitoreo de seguridad
- ☐ ☒ Revisar logs regularmente
- ☐ ☒ Configurar alertas de seguridad
- ☐ ☒ Mantener certificados SSL actualizados
- ☐ ☒ Implementar políticas de contraseñas
- ☐ ☒ Capacitar al equipo en seguridad

## Actualizaciones de Seguridad

### Suscribirse a Alertas

Para recibir notificaciones de actualizaciones de seguridad:

1. **Watch** este repositorio en GitHub
2. Suscribirse a **security advisories**
3. Seguir nuestro **changelog** de seguridad

## Aplicar Actualizaciones

```
# Verificar versión actual
npm list sistema-erp-completo

# Actualizar a la última versión
npm update sistema-erp-completo

# Verificar vulnerabilidades conocidas
npm audit

# Arreglar automáticamente vulnerabilidades menores
npm audit fix
```

## Contacto de Seguridad

- **Email Principal:** security@tu-empresa.com
- **Email Alternativo:** admin@tu-empresa.com
- **Tiempo de Respuesta:** 24 horas máximo
- **Idiomas:** Español, Inglés

## Agradecimientos

Agradecemos a todos los investigadores de seguridad y desarrolladores que han contribuido a mejorar la seguridad de este sistema:

- [Lista de colaboradores será actualizada según reportes]

---

**La seguridad es responsabilidad de todos. Gracias por ayudarnos a mantener seguro nuestro Sistema ERP. **

Desarrollado con  y  usando DeepAgent de Abacus.AI