

# Plan de Seguridad para Semas, SL



IVANA SÁNCHEZ PÉREZ

Plan de Seguridad para Semas, SL

## Contenido

<b>1. RESUMEN EJECUTIVO Y CONTEXTO DE LA EMPRESA</b>	3
<b>2. PLAN DE ACTIVIDADES DETALLADO</b>	3
Fase 1 – Análisis y Diagnóstico (40h)	3
Fase 2 – Desarrollo e Implementación (55h)	3
Fase 3 – Informe y Propuesta de Mejoras (30h)	3
<b>3. CRONOGRAMA DE TRABAJO (DIAGRAMA DE GANTT)</b>	4
<b>4. APORTACIÓN DE VALOR A LA EMPRESA</b>	4
<b>5. EJECUCIÓN DEL PROYECTO</b>	4
FASE 1 – Análisis y Diagnóstico (40h)	4
Reunión de kickoff con tutor/a (2h)	5
Revisión de la infraestructura de Dolibarr (8h)	5
Identificación de activos críticos (6h)	5
Revisión OSINT y análisis pasivo (8h)	5
Autodiagnóstico de ciberseguridad (8h)	5
Entrevistas con personal clave (8h)	5
FASE 2 – Desarrollo e Implementación (55h)	6
Políticas de acceso seguro (10h)	6
Implementación de cabeceras de seguridad (8h)	6
Revisión y optimización de copias de seguridad (10h)	6
Procedimiento de gestión de incidentes (8h)	6
Pruebas técnicas no intrusivas (8h)	7
Redacción de procedimientos internos (11h)	7
FASE 3 – Informe y Propuesta de Mejoras (30h)	7
Consolidación de hallazgos (6h)	7
Redacción del protocolo de seguridad Dolibarr (10h)	7
Propuesta de mejoras a corto, medio y largo plazo (7h)	7
Presentación de resultados (5h)	7
Valor añadido del Kit Consulting (2h):	7
<b>6. Plantillas</b>	8
Plantilla para Identificación de Activos Críticos (Fase 1)	8
Plantilla para Autodiagnóstico de Ciberseguridad (Basado en OWASP Top 10)	10
Plantilla para Matriz de Riesgos (Fase 3)	12
Plantilla para Procedimiento de Gestión de Incidentes (Fase 2)	14
Plantilla para Protocolo de Seguridad de Dolibarr (Fase 3)	14
Plantilla para entrevistas al personal	14
Plantilla para Cronograma de Mejoras (Corto, Medio, Largo Plazo)	15

## 1. RESUMEN EJECUTIVO Y CONTEXTO DE LA EMPRESA

El presente documento tiene como propósito establecer un plan de trabajo personalizado para las prácticas profesionales en SEMÁS SL, con foco en la seguridad informática aplicada a su ERP/CRM ([dolibarr.knowbiz.es](https://dolibarr.knowbiz.es)). El objetivo es aportar valor real a la organización mediante el análisis, implementación y documentación de medidas de ciberseguridad que fortalezcan sus procesos de digitalización.

SEMÁS SL es una consultoría especializada en sostenibilidad, innovación y digitalización, que ofrece servicios a entidades públicas y privadas. Sus principales activos de información son el ERP/CRM Dolibarr, los datos sensibles de clientes y proyectos, y la infraestructura digital interna. El Producto Mínimo Viable (MVP) consiste en definir e implementar un protocolo básico de seguridad informática para Dolibarr, incluyendo diagnóstico, medidas preventivas, controles de acceso y documentación de buenas prácticas.

## 2. PLAN DE ACTIVIDADES DETALLADO

### Fase 1 – Análisis y Diagnóstico (40h)

- Reunión de kickoff con tutor/a.
- Revisión de la infraestructura de Dolibarr.
- Identificación de activos críticos.
- Revisión OSINT y análisis pasivo.
- Autodiagnóstico de ciberseguridad.
- Entrevistas con personal clave.

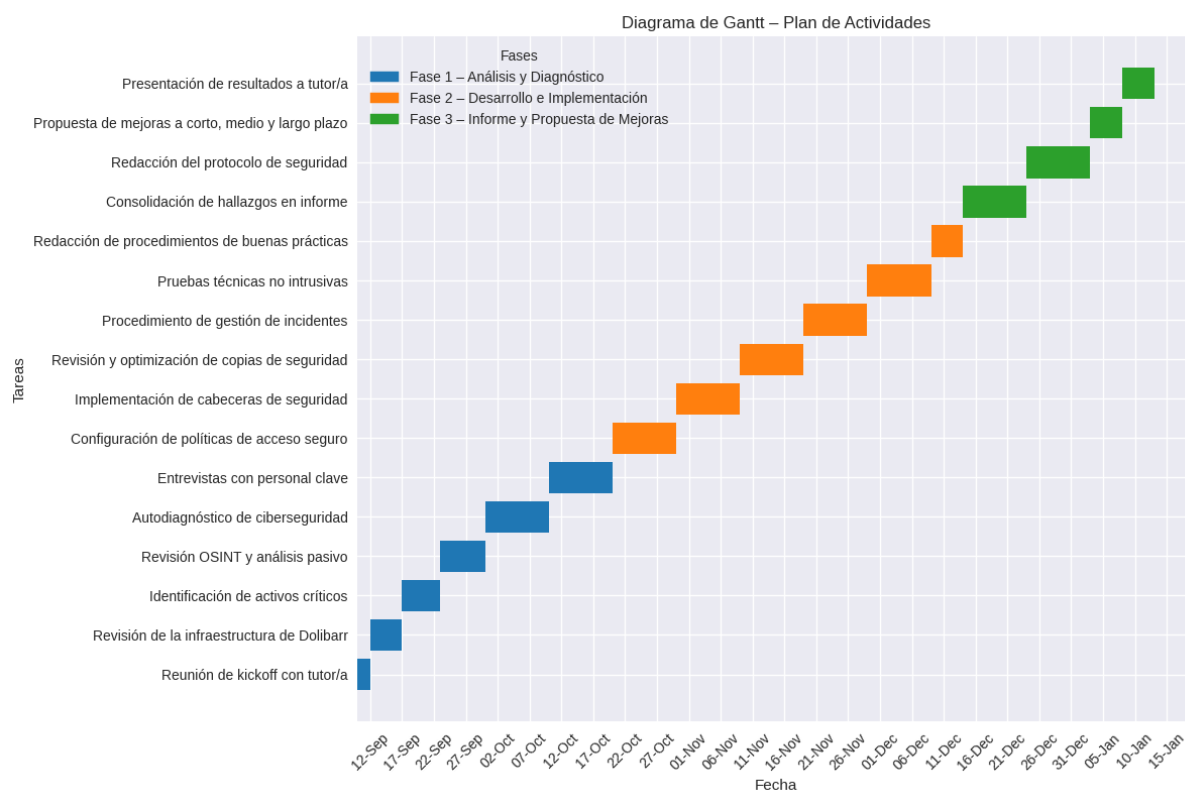
### Fase 2 – Desarrollo e Implementación (55h)

- Configuración de políticas de acceso seguro.
- Implementación de cabeceras de seguridad.
- Revisión y optimización de copias de seguridad.
- Procedimiento de gestión de incidentes.
- Pruebas técnicas no intrusivas.
- Redacción de procedimientos de buenas prácticas.

### Fase 3 – Informe y Propuesta de Mejoras (30h)

- Consolidación de hallazgos en informe.
- Redacción del protocolo de seguridad.
- Propuesta de mejoras a corto, medio y largo plazo.
- Presentación de resultados a tutor/a.

### 3. CRONOGRAMA DE TRABAJO (DIAGRAMA DE GANTT)



### 4. APORTACIÓN DE VALOR A LA EMPRESA

**Fase 1** – El diagnóstico permitirá a SEMÁS SL tener una fotografía clara de su postura de seguridad actual, identificando riesgos en Dolibarr y priorizando acciones. Esto da confianza a clientes y garantiza el cumplimiento normativo.

**Fase 2** – La implementación de medidas prácticas aportará valor tangible en la protección de datos sensibles y en la continuidad del negocio. Además, dotará al personal de guías claras para un uso seguro del ERP/CRM.

**Fase 3** – El informe final y el protocolo documentado quedarán como activo interno, permitiendo a SEMÁS SL seguir mejorando su seguridad, responder a auditorías y ofrecer garantías adicionales de confianza.

### 5. EJECUCIÓN DEL PROYECTO

#### FASE 1 – Análisis y Diagnóstico (40h)

Objetivo: conocer la situación actual de la empresa y detectar posibles riesgos de seguridad en Dolibarr.

## **Reunión de kickoff con tutor/a (2h)**

- Herramientas: Google Meet, Teams o presencial.
- Explicación: es una reunión inicial para entender qué espera la empresa de mí, acordar prioridades y definir los activos más importantes (ejemplo: datos de clientes, facturación, proyectos).

## **Revisión de la infraestructura de Dolibarr (8h)**

- Herramientas: Acceso al ERP Dolibarr como usuario autorizado, documentación interna.
- Explicación: entrar en Dolibarr, revisar qué módulos están activos, qué roles existen (administrador, usuarios normales, externos) y cómo se gestiona actualmente la información. Documentar con capturas de pantalla y un esquema sencillo.

## **Identificación de activos críticos (6h)**

- Herramienta: Excel o Google Sheets para listar.
- Explicación: elaborar una tabla con los datos más sensibles (ejemplo: base de datos de clientes, facturación, proyectos, usuarios con privilegios). Preguntar al personal qué información consideran más delicada (ejemplo: ayudas públicas, subvenciones).

## **Revisión OSINT y análisis pasivo (8h)**

- Herramientas:
  - [SecurityHeaders.com](https://securityheaders.com) para revisar cabeceras de seguridad.
  - SSL Labs para comprobar el certificado HTTPS.
  - Wappalyzer para identificar tecnologías usadas.
- Explicación: estas herramientas permiten revisar desde fuera cómo está configurada la seguridad de la web, sin hacer intrusiones.

## **Autodiagnóstico de ciberseguridad (8h)**

- Herramientas:
  - Checklist OWASP Top 10 (para aplicaciones web).
  - Guía básica del Esquema Nacional de Seguridad (ENS).
- Explicación: marcar en una tabla si Dolibarr cumple con buenas prácticas (contraseñas seguras, protección contra inyecciones, backups actualizados, etc.).

## **Entrevistas con personal clave (8h)**

- Herramienta: Cuestionario en Google Forms o entrevistas cortas.
- Explicación: preguntar cómo acceden al ERP (desde oficina, móvil, remoto), si comparten contraseñas, si usan medidas como VPN.

## **FASE 2 – Desarrollo e Implementación (55h)**

Objetivo: aplicar medidas prácticas para reforzar la seguridad de Dolibarr y los procesos internos.

### **Políticas de acceso seguro (10h)**

- Herramientas: Panel de administración de Dolibarr.
- Pasos:
  1. Revisar contraseñas → exigir mínimo 12 caracteres con números y símbolos.
  2. Eliminar cuentas inactivas o duplicadas.
  3. Activar autenticación en dos pasos (2FA) si es posible o, en su defecto, cambio obligatorio de contraseñas cada 90 días.

### **Implementación de cabeceras de seguridad (8h)**

- Herramientas: Servidor Apache/Nginx donde esté Dolibarr.
- Cabeceras a configurar:
  - Strict-Transport-Security → obliga a usar HTTPS.
  - X-Frame-Options → evita que la web se cargue en marcos externos (clickjacking).
  - X-Content-Type-Options → protege contra interpretaciones erróneas de archivos.
- Explicación: estas configuraciones son líneas que se añaden en el servidor web y fortalecen la seguridad de acceso.

### **Revisión y optimización de copias de seguridad (10h)**

- Herramientas: módulo de backup de Dolibarr + almacenamiento en nube (ej. Google Drive Business, Nextcloud).
- Pasos:
  1. Verificar si las copias se realizan automáticamente.
  2. Confirmar la frecuencia (idealmente diaria).
  3. Probar restaurar una copia en un entorno de prueba.
  4. Recomendar cifrado en copias sensibles.

### **Procedimiento de gestión de incidentes (8h)**

- Herramienta: Google Docs o Word.
- Pasos: redactar un documento sencillo que explique:
  - Qué hacer si hay un acceso sospechoso.
  - A quién avisar internamente.
  - Cómo restaurar un backup.

## **Pruebas técnicas no intrusivas (8h)**

- Herramientas:
  - Nmap (para detectar puertos abiertos).
  - Shodan.io (para revisar exposición de servicios).
- Explicación: comprobar que solo los servicios necesarios están expuestos en Internet.

## **Redacción de procedimientos internos (11h)**

- Herramienta: Word o PDF.
- Ejemplo de contenidos:
  - Cómo crear una contraseña segura.
  - No compartir credenciales.
  - Acceso remoto seguro mediante VPN.
  - Uso responsable del correo electrónico corporativo.

## **FASE 3 – Informe y Propuesta de Mejoras (30h)**

Objetivo: dejar documentación y propuestas que la empresa pueda usar a futuro.

## **Consolidación de hallazgos (6h)**

- Herramienta: Excel con tabla de riesgos (Bajo, Medio, Alto).

## **Redacción del protocolo de seguridad Dolibarr (10h)**

- Documento en PDF con políticas claras de acceso, copias de seguridad, actualizaciones y gestión de incidentes.

## **Propuesta de mejoras a corto, medio y largo plazo (7h)**

- Corto plazo: eliminar cuentas inactivas, contraseñas seguras.
- Medio plazo: activar 2FA, mejorar backup externo.
- Largo plazo: auditoría externa, certificación ENS.

## **Presentación de resultados (5h)**

- Herramienta: PowerPoint o Canva.
- Explicación: presentación visual para explicar lo que se hizo, los beneficios y próximos pasos.

## **Valor añadido del Kit Consulting (2h):**

- Elaboración de un **plan de respuesta detallado** ante brechas de seguridad.
- Definir una **estrategia personalizada a corto y medio plazo**.
- Dejar preparada la documentación básica para avanzar hacia un **SGSI (ISO27001 y ENS media-alta)**.

## 6. Plantillas

### Plantilla para Identificación de Activos Críticos (Fase 1)

#### SENSIBILIDAD ALTA

- **Impacto por pérdida o acceso no autorizado: Crítico o irreversible** para la empresa.
- **Ejemplos típicos:**
  - **Datos:** Información personal de clientes (RGPD), datos financieros (facturas, balances), proyectos con subvenciones públicas, secretos comerciales.
  - **Sistemas:** Servidor principal de Dolibarr, sistema de copias de seguridad, servidor de correo corporativo.
  - **Accesos:** Cuentas de administrador con permisos totales.

#### SENSIBILIDAD MEDIA

- **Impacto por pérdida o acceso no autorizado: Significativo pero manejable**, con posibles daños operativos o económicos.
- **Ejemplos típicos:**
  - **Datos:** Documentación interna de proyectos ya finalizados, correos electrónicos no críticos.
  - **Sistemas:** Herramientas de comunicación interna (ej. Slack), almacenamiento en la nube para documentos no sensibles.
  - **Accesos:** Cuentas de usuario con permisos para editar pero no eliminar información crítica.

#### SENSIBILIDAD BAJA

- **Impacto por pérdida o acceso no autorizado: Mínimo o nulo.** Su disponibilidad no afecta a las operaciones principales.
- **Ejemplos típicos:**
  - **Datos:** Información pública de la empresa, boletines informativos, documentación ya obsoleta.
  - **Sistemas:** Webs corporativas de solo lectura, folletos digitales.
  - **Accesos:** Cuentas de invitado o de solo lectura en sistemas no críticos.

<b>Activo</b>	<b>Tipo (Dato/Sistema/Usuario)</b>	<b>Sensibilidad (Baja/Media/Alta)</b>	<b>Responsable</b>	<b>Observaciones</b>
Base de datos clientes	Datos	Alta		
Módulo de facturación	Sistema	Alta		
Usuario Admin Dolibarr	Usuario	Alta		
Correos corporativos	Comunicación	Media		
Documentación de proyectos	Datos	Alta		
Backup Dolibarr	Copia de seguridad	Alta		
VPN de acceso remoto	Infraestructura	Media		

## Plantilla para Autodiagnóstico de Ciberseguridad (Basado en OWASP Top 10)

Control de Seguridad	Cumple (Sí/No/Parcial)	Observaciones	Prioridad
Contraseñas seguras			
Autenticación en dos factores (2FA)			
Cabeceras de seguridad implementadas			
Copias de seguridad automatizadas y cifradas			
Actualizaciones del sistema al día			
Protección contra inyecciones SQL			
Control de Acceso por roles			
Protección contra Cross-Site Scripting			
Registro y monitorización de logs de acceso y seguridad			
Política de bloquear cuentas tras intentos fallidos			
Certificados SSL/TSSL válido y configurado correctamente			
Acceso administrativo restringido por IP o VPN			

<b>Control de Seguridad</b>	<b>Cumple (Sí/No/Parcial)</b>	<b>Observaciones</b>	<b>Prioridad</b>
Separación de entornos (Producción, Pruebas, Desarrollo)			
Procedimiento de gestión de incidentes documentado			
Cifrado de datos sensibles en reposo (ej. En base de datos)			
Formación básica en ciberseguridad para usuarios			
Análisis de vulnerabilidades periódico			
Política de retirada de cuentas de usuarios inactivos			
Uso de conexiones seguras (HTTPS, SFP, VPN)			
Configuración segura del servidor web (Apache/Ngnix)			

## Plantilla para Matriz de Riesgos (Fase 3)

### Guía para rellenar la matriz:

- **Probabilidad (1-5):**
  - 1: Muy improbable
  - 2: Improbable
  - 3: Probable
  - 4: Muy probable
  - 5: Casi seguro
- **Impacto (1-5):**
  - 1: Insignificante
  - 2: Menor
  - 3: Moderado
  - 4: Mayor
  - 5: Crítico
- **Nivel de Riesgo (Calculado: Prob x Impact):**
  - 1-5: Bajo
  - 6-12: Medio
  - 13-25: Alto

<b>Riesgo Identificado</b>	<b>Probabilidad (1-5)</b>	<b>Impacto (1-5)</b>	<b>Nivel de Riesgo</b>	<b>Acción Recomendada</b>
Acceso sin 2FA	4	5	Alto	Implementar 2FA
Backup no cifrado	3	4	Medio	Cifrar backups
Contraseñas débiles	4	4	Alto	Establecer política de contraseñas
Dolibarr desactualizado	3	5	Alto	Actualizar la última versión estable
Cabeceras de seguridad faltantes	4	3	Medio	Configurar HSTS, etc

<b>Riesgo Identificado</b>	<b>Probabilidad (1-5)</b>	<b>Impacto (1-5)</b>	<b>Nivel de Riesgo</b>	<b>Acción Recomendada</b>
Cuentas inactivas no eliminadas	3	3	Medio	Revisar y eliminar cuentas inactivas periódicamente
Permisos excesivos a usuarios	3	4	Medio	Revisar y ajustar permisos
No hay registro de logs de acceso	2	3	Bajo	Implementar sistema de logging y monitorización
Acceso administrativo sin restricción IP	3	5	Alto	Restringir acceso por IP/VPN
Datos sensibles no cifrados en BD	2	5	Medio	Evaluar implementar cifrado de datos en reposo
No hay procedimiento de incidentes	3	4	Medio	Documentar procedimiento de respuesta a incidentes
No se realizan pruebas de restauración	3	5	Alto	Programar pruebas trimestrales de restauración
Uso de servicios con vulnerabilidades conocidas	2	4	Medio	Actualizar/Parchear servicios del servidor

## Plantilla para Procedimiento de Gestión de Incidentes (Fase 2)

**Título:** Procedimiento de Respuesta ante Incidentes de Seguridad

**Versión:** 1.0

**Fecha:** [fecha]

### Pasos a seguir:

1. **Detección:** ¿Quién detecta el incidente?
2. **Comunicación:** Contactar con [persona responsable].
3. **Contención:** Medidas inmediatas (ej.: desconectar sistema).
4. **Análisis:** Investigar causa y alcance.
5. **Eliminación:** Eliminar la causa (ej.: malware).
6. **Recuperación:** Restaurar desde backup.
7. **Lecciones aprendidas:** Documentar y mejorar.

## Plantilla para Protocolo de Seguridad de Dolibarr (Fase 3)

**Título:** Protocolo de Seguridad para Dolibarr

**Ámbito:** Todos los usuarios del sistema

### Políticas:

- **Contraseñas:** Mínimo 12 caracteres, con números y símbolos.
- **Accesos:** No compartir credenciales. Uso de 2FA recomendado.
- **Backups:** Diarios, cifrados, con prueba de restauración mensual.
- **Actualizaciones:** Revisión mensual de parches de seguridad.
- **Incidentes:** Seguir procedimiento [nombre del documento].

## Plantilla para entrevistas al personal

**Fecha:** [Fecha]

**Entrevistado:** [Nombre y Cargo]

1. **¿Qué tipo de información maneja en Dolibarr?**
2. **¿Cómo accede al sistema? (Oficina, remoto, móvil)**
3. **¿Utiliza alguna medida de seguridad adicional? (VPN, 2FA)**
4. **¿Ha recibido formación sobre cómo proteger sus credenciales?**
5. **¿Sabe qué hacer en caso de detectar un acceso sospechoso?**
6. **Observaciones generales:**

## Plantilla para Cronograma de Mejoras (Corto, Medio, Largo Plazo)

Mejora	Plazo	Responsable	Estado	Fecha Límite
Eliminar cuentas inactivas	Corto			
Implementar 2FA	Medio			
Auditoría externa de seguridad	Largo			
Configurar cabeceras de seguridad (HSTS, X-FRAME-OPTIONS, etc)	Corto			
Establecer política de contraseñas robusta (más de 12 caracteres)	Corto			
Implementar cifrado para las copias de seguridad	Medio			
Realizar pruebas de restauración de backups	Medio			
Definir y documentar procedimiento de gestión de incidentes	Corto			
Restringir acceso administrativo por IP/VPN	Medio			
Actualizar Dolibarr y extensiones a la última versión estable.	Corto			
Realizar formación básica en ciberseguridad para usuarios	Medio			

<b>Mejora</b>	<b>Plazo</b>	<b>Responsable</b>	<b>Estado</b>	<b>Fecha Límite</b>
Implementar monitorización de logs de acceso	Largo			
Evaluar y ajustar permisos de usuarios (principio de mínimo privilegio)	Medio			
Configurar bloqueo de cuentas tras múltiples intentos fallidos	Corto			
Planificar ejercicio de simulacro de incidente	Largo			