

**Empresa Ejemplo S.L.**

NIF B00000000 · Calle Ficticia 0, 00000 Ciudad Ejemplo

EJEMPLO DE ENTREGABLE · EXTRACTOS

Sistema de seguridad de la información conforme al Esquema Nacional de Seguridad

Categoría MEDIA · Real Decreto 311/2022 · Sistema en alcance: Servicio de Cita Previa (SCP) que la empresa presta a entidades locales

1. Índice del conjunto documental (23 documentos)	pág. 2
2. Política de Seguridad de la Información (PSI-01), extracto	págs. 3–5
3. Declaración de Aplicabilidad (DA-01), extracto de 12 de las 73 medidas del anexo II	pág. 6

Documento ficticio. Empresa Ejemplo S.L., su sistema, sus responsables, sus fechas y sus datos son inventados para mostrar el formato y el nivel de detalle de los entregables. No es un documento de ningún cliente ni procede de ninguno. Cualquier parecido con una organización real es casual.

En un proyecto real, el contenido de cada documento sale del cuestionario inicial, del análisis de riesgos y de la información de la empresa, y la Dirección y los responsables de seguridad de la empresa lo aprueban y lo firman.

Índice del conjunto documental

Documentos del sistema de seguridad del SCP, con las medidas del anexo II del RD 311/2022 que cubre cada uno. Versión del conjunto 1.0 · 30/09/2026. ● = incluido como extracto en este ejemplo.

Código	Documento	Medidas que cubre	Responsable	Estado
NIVEL 1 · POLÍTICA Y MARCO				
PSI-01	● Política de Seguridad de la Información (aprobada por la Dirección General)	org.1	Dirección General	Aprobado v1.0
CAT-01	Categorización del sistema (anexo I) y valoración de las dimensiones C, I, T, A, D	Base de todo el sistema	Resp. Información y Servicio	Aprobado v1.0
AR-01	Análisis de riesgos (MAGERIT) y aceptación del riesgo residual	op.pl.1	Resp. Seguridad	Aprobado v1.0
DA-01	● Declaración de Aplicabilidad (firmada por el Responsable de la Seguridad)	Las 73 medidas	Resp. Seguridad	Aprobado v1.0
ARQ-01	Arquitectura de seguridad y diagrama de red y sistemas	op.pl.2	Resp. Sistema	Aprobado v1.0
NIVEL 2 · NORMATIVA				
NOR-01	Normativa de seguridad: uso de equipos, correo, internet y teletrabajo	org.2	Resp. Seguridad	Aprobado v1.0
PER-01	Deberes y obligaciones del personal (firmados por cada persona)	mp.per.1, mp.per.2	Dirección General	Aprobado v1.0
NIVEL 3 · PROCEDIMIENTOS, GUÍAS Y PLANES				
PRO-00	Marco de procedimientos de seguridad y relación de procedimientos	org.3	Resp. Seguridad	Aprobado v1.0
AUT-01	Proceso de autorización: sistemas, cambios y accesos	org.4	Resp. Seguridad	Aprobado v1.0
PRO-01	Gestión de identidades y derechos de acceso	op.acc.1 – op.acc.6	Resp. Sistema	Aprobado v1.0
GUI-01	Guías de configuración segura (bastionado) de nube, puestos y suite ofimática	op.exp.2, op.exp.3	Resp. Sistema	Aprobado v1.0
PRO-02	Actualizaciones de seguridad y gestión de cambios	op.exp.4, op.exp.5	Resp. Sistema	Aprobado v1.0
PRO-03	Gestión de incidentes y registro de incidentes	op.exp.7, op.exp.9	Resp. Seguridad	Aprobado v1.0
PRO-04	Registro de la actividad (logs) y su revisión	op.exp.8	Resp. Sistema	Aprobado v1.0
PRO-05	Gestión de claves criptográficas	op.exp.10, mp.si.2	Resp. Sistema	Aprobado v1.0
PRO-06	Copias de seguridad y pruebas de restauración	mp.info.6	Resp. Sistema	Aprobado v1.0
PRO-07	Desarrollo seguro y paso a producción	mp.sw.1, mp.sw.2	Resp. Sistema	Aprobado v1.0
PRV-01	Registro de proveedores, contratos y acuerdos de nivel de servicio	op.ext.1 – op.ext.4, op.nub.1	Resp. Información y Servicio	Aprobado v1.0
CON-01	Análisis de impacto (en MEDIA no se exige plan de continuidad)	op.cont.1	Resp. Información y Servicio	Aprobado v1.0
MON-01	Plan de monitorización y sistema de métricas	op.mon.1 – op.mon.3	Resp. Seguridad	Aprobado v1.0
FOR-01	Plan de formación y concienciación	mp.per.3, mp.per.4	Resp. Seguridad	Aprobado v1.0
NIVEL 4 · REGISTROS Y EVIDENCIAS				
INV-01	Inventario de activos	op.exp.1	Resp. Sistema	Vigente 3T 2026
EVI-01	Índice de evidencias para la auditoría de certificación	Las 73 medidas	Resp. Seguridad	Vigente 3T 2026

Además del conjunto documental, el proyecto entrega el informe de preauditoría con sus hallazgos y el plan para cerrarlos antes de la auditoría de certificación. Los registros operativos (actas del Comité, registro de incidentes, informes de revisión de logs, pruebas de restauración) se generan durante la operación y se enlazan desde EVI-01.

Política de Seguridad de la Información

Conforme al artículo 12 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad · Extracto

Código PSI-01	Versión 1.0	Clasificación Uso interno
Elaborada por Responsable de la Seguridad	Revisada por Comité de Seguridad (acta 2026/03)	Aprobada por Dirección General
Fecha de aprobación 15/09/2026	Próxima revisión septiembre de 2027	Distribución Todo el personal y proveedores con acceso

1. Aprobación y entrada en vigor

Esta Política de Seguridad de la Información ha sido aprobada por la Dirección General de Empresa Ejemplo S.L. el 15 de septiembre de 2026. Es efectiva desde esa fecha hasta que la sustituya una nueva versión, y deja sin efecto cualquier política anterior sobre la misma materia.

2. Misión y objetivos (art. 12.1.a)

Empresa Ejemplo S.L. desarrolla y presta a entidades locales el Servicio de Cita Previa (SCP), una aplicación en la nube con la que la ciudadanía reserva citas para trámites municipales. Al prestar este servicio a entidades del sector público, el sistema que lo sustenta está incluido en el ámbito de aplicación del Esquema Nacional de Seguridad (art. 2.3 del RD 311/2022). La seguridad de la información forma parte de la misión de la empresa, y sus objetivos son:

- Garantizar la confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad de la información que trata el SCP y del propio servicio, en el nivel que exige su categoría.
- Proteger los datos personales que la empresa trata por cuenta de las entidades contratantes.
- Cumplir los requisitos de seguridad de los pliegos y contratos y mantener vigente la certificación de conformidad con el ENS.
- Prevenir los incidentes, detectarlos pronto, responder a ellos y recuperar el servicio en los plazos acordados.
- Mejorar de forma continua el proceso de seguridad a partir de las revisiones, las auditorías y los incidentes.

3. Alcance

Esta política se aplica al sistema de información que sustenta el SCP: la aplicación y sus entornos de producción y preproducción, alojados en un proveedor de servicios en la nube con certificación de conformidad con el ENS de categoría ALTA; los puestos de trabajo y dispositivos con los que se desarrolla y administra; la suite ofimática en la nube; y los procesos de desarrollo, soporte y administración. Obliga a todo el personal de la empresa y a los proveedores con acceso al sistema.

Categoría del sistema: **MEDIA**, según la valoración de las dimensiones de seguridad del anexo I documentada en CAT-01:

Confidencialidad MEDIO	Integridad MEDIO	Trazabilidad MEDIO	Autenticidad MEDIO	Disponibilidad MEDIO
-------------------------------	-------------------------	---------------------------	---------------------------	-----------------------------

4. Marco normativo (art. 12.1.b)

Las actividades de seguridad se desarrollan dentro del siguiente marco, cuyo registro actualizado mantiene el Responsable de la Seguridad (anexo A, no incluido en este extracto):

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Reglamento (UE) 2016/679, General de Protección de Datos, y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (art. 156), y Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, y los pliegos y contratos de cada entidad contratante.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.
- Como referencia técnica, las guías CCN-STIC de la serie 800 publicadas por el Centro Criptológico Nacional.

5. Principios de seguridad

La empresa aplica los principios básicos del artículo 5 del RD 311/2022: la seguridad como proceso integral; la gestión de la seguridad basada en los riesgos; la prevención, detección, respuesta y conservación; la existencia de líneas de defensa; la vigilancia continua; la reevaluación periódica; y la diferenciación de responsabilidades.

6. Organización de la seguridad: funciones y responsabilidades (art. 12.1.c y art. 13)

Función	Quién la ejerce	Deberes y responsabilidades
Dirección General	Director/a General	Aprueba esta política, asigna los recursos necesarios, designa a los responsables y preside el Comité de Seguridad.
Responsable de la Información y del Servicio	Director/a de Operaciones	Determina los requisitos de la información tratada y del servicio prestado, propone la valoración de las dimensiones de seguridad y acepta formalmente el riesgo residual. En una empresa de este tamaño ambas funciones recaen en la misma persona.
Responsable de la Seguridad	Responsable de Calidad y Seguridad	Determina las decisiones para satisfacer los requisitos de seguridad; mantiene la documentación y el análisis de riesgos; supervisa el cumplimiento; coordina la gestión de incidentes; firma la Declaración de Aplicabilidad (art. 28); y es el punto de contacto (POC) de seguridad ante las entidades contratantes.
Responsable del Sistema	Responsable Técnico	Desarrolla la forma concreta de implementar la seguridad en el sistema y supervisa su operación diaria. Puede delegar tareas en los administradores, bajo su responsabilidad.
Administradores del sistema	Equipo técnico (3 personas)	Aplican las configuraciones, gestionan cuentas, copias y actualizaciones y revisan los registros según los procedimientos.
Personal y proveedores	Todas las personas con acceso	Cumplen la normativa de seguridad, protegen sus credenciales y comunican de inmediato cualquier incidente o debilidad.

Diferenciación de responsabilidades. La responsabilidad de la seguridad está diferenciada de la explotación del sistema: el Responsable de la Seguridad no depende jerárquicamente del Responsable del Sistema, informa directamente a la Dirección General y no tiene privilegios de administración en producción.

Designación y renovación. La Dirección General designa por escrito a cada responsable por dos años renovables, y revisa la designación al vencer el plazo, si el puesto queda vacante o si cambia la estructura de la empresa. Los cambios se comunican al personal y, si afectan al POC de seguridad, a las entidades contratantes. Nombramientos vigentes: anexo B.

7. Comité de Seguridad de la Información (art. 12.1.d)

Composición. Director/a General, que lo preside; Responsable de la Información y del Servicio; Responsable de la Seguridad, que ejerce la secretaría; Responsable del Sistema; y el asesor externo de protección de datos, con voz y sin voto.

Ámbito de responsabilidad. El Comité revisa el estado de la seguridad; aprueba la normativa de seguridad; propone a la Dirección General la revisión de esta política; hace el seguimiento de los riesgos, los incidentes, las auditorías y los planes de mejora; y resuelve los conflictos entre responsables.

Funcionamiento. Se reúne al menos una vez por semestre y, con carácter extraordinario, tras un incidente grave o un cambio relevante del sistema. Levanta acta de cada reunión.

Relación con el resto de la organización. Informa a la Dirección General y se coordina con las áreas de Desarrollo, Soporte y Administración para que la seguridad se integre en sus procesos desde el diseño.

8. Riesgos derivados del tratamiento de datos personales (art. 12.1.f)

En el SCP, la empresa actúa como encargada del tratamiento de cada entidad contratante (art. 28 del RGPD) y trata datos identificativos y de contacto de la ciudadanía y el motivo de cada cita. Los riesgos para los derechos y libertades de las personas se analizan con los del sistema en AR-01, y la empresa facilita a cada entidad la información que necesite para su evaluación de impacto. Las medidas del ENS se aplican también al tratamiento, que se hace solo con instrucciones documentadas de cada entidad; al terminar el contrato, los datos se devuelven o se suprimen.

9. Gestión de riesgos (art. 14)

El Responsable de la Seguridad realiza el análisis de riesgos con la metodología MAGERIT y lo revisa al menos una vez al año, ante cambios relevantes del sistema y tras cualquier incidente grave. El Responsable de la Información y del Servicio acepta formalmente el riesgo residual. El análisis justifica la selección de medidas recogida en la Declaración de Aplicabilidad (DA-01).

10. Estructura, gestión y acceso a la documentación de seguridad (art. 12.1.e)

Nivel	Contenido	Aprueba	Acceso
1 · Política	Esta política (PSI-01), la categorización (CAT-01), el análisis de riesgos (AR-01), la arquitectura de seguridad (ARQ-01) y la Declaración de Aplicabilidad (DA-01).	Dirección General; DA-01 la firma el Resp. de la Seguridad	PSI-01: todo el personal. Resto: responsables
2 · Normativa	Normas de uso de equipos, correo, internet y teletrabajo (NOR-01) y deberes del personal (PER-01).	Comité de Seguridad	Todo el personal
3 · Procedimientos	Procedimientos, guías y planes (PRO-, GUI-, AUT-, PRV-, CON-, MON-, FOR-).	Responsable de la Seguridad	Personal afectado
4 · Registros	Inventario, registros de actividad, actas, incidentes y evidencias (INV-01, EVI-01).	Los mantienen sus responsables	Restringido

La documentación se guarda en el repositorio documental de la empresa con control de versiones y de acceso; cada documento indica código, versión, fecha, aprobador y clasificación, y las versiones obsoletas se marcan como tales. Esta política se publica en la intranet y se entrega a los proveedores con acceso.

11. Requisitos mínimos de seguridad (art. 12 y arts. 13 a 27)

La política se desarrolla aplicando los requisitos mínimos del ENS, que se concretan en las medidas del anexo II seleccionadas en la Declaración de Aplicabilidad:

- | | |
|---|--|
| a) Organización e implantación del proceso de seguridad. | h) Mínimo privilegio. |
| b) Análisis y gestión de los riesgos. | i) Integridad y actualización del sistema. |
| c) Gestión de personal. | j) Protección de la información almacenada y en tránsito. |
| d) Profesionalidad. | k) Prevención ante otros sistemas de información interconectados. |
| e) Autorización y control de los accesos. | l) Registro de la actividad y detección de código dañino. |
| f) Protección de las instalaciones. | m) Incidentes de seguridad. |
| g) Adquisición de productos de seguridad y contratación de servicios de seguridad. | n) Continuidad de la actividad. |
| | ñ) Mejora continua del proceso de seguridad. |

12. Obligaciones del personal

Todas las personas con acceso al sistema conocen y cumplen esta política y la normativa de seguridad, firman sus deberes y obligaciones (PER-01) y reciben formación y concienciación en seguridad al menos una vez al año (FOR-01). El incumplimiento puede dar lugar a las medidas que prevea la legislación laboral aplicable.

13. Terceras partes

Los proveedores que prestan servicios relacionados con el SCP o acceden al sistema quedan sujetos a esta política por contrato. La empresa exige a los proveedores de servicios en la nube que intervienen en el SCP una certificación de conformidad con el ENS de categoría igual o superior a la del sistema, y lo registra en PRV-01.

14. Revisión

El Comité de Seguridad revisa esta política al menos una vez al año y siempre que cambien la normativa aplicable, el alcance del sistema o la organización. Las modificaciones las aprueba la Dirección General.

[...] Se omiten en este extracto el anexo A (registro de normativa aplicable) y el anexo B (nombramientos vigentes).

Aprobado por la Dirección General de Empresa Ejemplo S.L.
Firma y fecha: 15/09/2026

Revisado por el Comité de Seguridad de la Información
Acta 2026/03

Declaración de Aplicabilidad · art. 28 del RD 311/2022 · Extracto: 12 de las 73 medidas del anexo II

Sistema: **Servicio de Cita Previa (SCP)** Categoría: **MEDIA** Dimensiones: **C MEDIO · I MEDIO · T MEDIO · A MEDIO · D MEDIO** Medidas que aplican: **68 de 73**

No exigidas en MEDIA: **op.ext.3, op.cont.2, op.cont.3, op.cont.4, mp.info.4** Medidas compensatorias: **ninguna** v1.0 · 22/09/2026

Código	Medida	Se determina por	Requisito en MEDIA (anexo II)	¿Aplica?	Cómo se cumple	Documento / evidencia
org.1	Política de seguridad	Categoría	aplica	Sí	Política aprobada por la Dirección General con el contenido mínimo del art. 12.1, revisada cada año por el Comité y comunicada al personal y a los proveedores con acceso.	PSI-01 v1.0 firmada; acta del Comité 2026/03; registro de comunicación al personal.
op.pl.1	Análisis de riesgos	Categoría	+ R1	Sí	Análisis semiformal con metodología MAGERIT: activos valorados, catálogo de amenazas y salvaguardas, y riesgo residual aceptado por el Responsable de la Información y del Servicio. Revisión anual y ante cambios relevantes.	AR-01 v1.0; acta de aceptación del riesgo residual (10/09/2026).
op.acc.3	Segregación de funciones y tareas	C · I · T · A	aplica	Sí	Desarrollo, aprobación de cambios y paso a producción los realizan personas distintas; los desarrolladores no tienen acceso de escritura a producción; el Responsable de la Seguridad no administra el sistema.	PRO-01 §4 (matriz de funciones); permisos del flujo de despliegue; revisión trimestral de accesos.
op.acc.6	Mecanismo de autenticación (usuarios de la organización)	C · I · T · A	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	Sí	Doble factor obligatorio para el acceso remoto, la consola del proveedor de nube y las cuentas con privilegios; contraseñas de al menos 12 caracteres; bloqueo tras intentos fallidos; caducidad de sesiones; credenciales personales e intransferibles.	PRO-01 §6; GUI-01 §2 (acceso condicional); exportación del estado del doble factor por usuario.
op.exp.1	Inventario de activos	Categoría	aplica	Sí	Inventario de equipos, servicios en la nube, aplicaciones y datos, con responsable y ubicación de cada activo. Se actualiza con cada alta o baja y se revisa cada trimestre.	INV-01 (revisión 3T 2026).
op.exp.4	Mantenimiento y actualizaciones de seguridad	Categoría	+ R1	Sí	Seguimiento de los avisos de seguridad de fabricantes y del CCN-CERT; actualizaciones probadas en preproducción antes de pasar a producción, con plazos máximos según su criticidad.	PRO-02 §3; registro de actualizaciones aplicadas; informe mensual de estado de parches.
op.exp.7	Gestión de incidentes	Categoría	+ R1 + R2	Sí	Procedimiento de detección, clasificación, respuesta y cierre; comunicación a la entidad contratante según lo acordado en el contrato y, cuando proceda, al CCN-CERT; lecciones aprendidas revisadas por el Comité.	PRO-03; registro de incidentes; informe del ejercicio de respuesta del 2T 2026.
op.exp.8	Registro de la actividad	Trazabilidad	+ R1 + R2 + R3 + R4	Sí	Registro centralizado de accesos y acciones de administración (usuario, fecha y hora, acción y resultado) con relojes sincronizados; revisión semanal por el Responsable del Sistema; conservación de 12 meses con acceso restringido.	PRO-04; configuración del servicio de registros; informes semanales de revisión.
op.cont.1	Análisis de impacto	Disponibilidad	aplica	Sí	Análisis de impacto del SCP: interrupción máxima aceptable de 24 horas y pérdida máxima de datos de 4 horas, acordadas con el Responsable de la Información y del Servicio.	CON-01 §2.
op.cont.2	Plan de continuidad	Disponibilidad	n.a.	No	No exigida para el nivel MEDIO de disponibilidad (se exige en ALTO). La recuperación ante fallos se cubre con las copias y el procedimiento de restauración (mp.info.6).	CON-01 §1 (justificación).
mp.info.1	Datos personales	Categoría	aplica	Sí	La empresa es encargada del tratamiento: contrato de encargo con cada entidad (art. 28 RGPD), registro de actividades como encargada y medidas del ENS aplicadas también al tratamiento de datos personales.	Contratos de encargo; registro de actividades (art. 30.2 RGPD); PSI-01 §8.
mp.info.6	Copias de seguridad	Disponibilidad	+ R1	Sí	Copias cifradas de la base de datos cada 4 horas y de la configuración cada día, en una región distinta del mismo proveedor, conservadas 30 días; prueba de restauración trimestral documentada.	PRO-06; informe de la prueba de restauración del 3T 2026; configuración de la política de copias.

La columna «Requisito en MEDIA» reproduce la aplicabilidad del anexo II del RD 311/2022 para la categoría MEDIA o, en las medidas que dependen de una dimensión, para su nivel MEDIO: «aplica» = requisitos base; «+ R1» = requisitos base más el refuerzo R1; «n.a.» = no exigida. La Declaración completa recoge las 73 medidas.

Firmado: Responsable de la Seguridad de Empresa Ejemplo S.L. · 22/09/2026