AYUNTAMIENTO DE COSLADA

PLS-GLB-001

Política General de Seguridad de la Información

DOCUMENTO PÚBLICO

Esquema Nacional de Seguridad

CONTROL DEL DOCUMENTO

Nombre del documento:**COSLADA-PLS-GLB-001-Política General de Seguridad de la Informacion-V01** Número de Páginas: **20**	
Autor: DEPARTAMENTO DE INFORMATICA	Fecha creación: 23-5-2022
Clasificación de la información: **PÚBLICO**	DATOS PERSONALES: DP_0
Lista de Distribución: PUBLICO	

Este documento está dirigido EXCLUSIVAMENTE a las personas nombradas en la lista de distribución, las cuales podrán, en base a su criterio, divulgarlo a quienes consideren oportuno. Se recomienda encarecidamente una divulgación controlada en la que todos los cesionarios del documento conozcan inequívocamente su CLASIFICACIÓN y se comprometan a mantener la consecuente confidencialidad en todo el ciclo de uso y, en su caso, archivo y/o destrucción.

CONTROL DE VERSIONES

Nº Versión	Autor	Fecha	Cambios realizados	Comentarios

ÍNDICE

1 Contenido y Objetivos del presente documento.

Este documento contiene la Política General de Seguridad de la Información (PGSI en adelante) del Ayuntamiento de Coslada ("la Organización" o "el Ayuntamiento", en adelante).

El objetivo fundamental de esta Política se centra en definir las estructuras organizativas, roles, responsabilidades, criterios e iniciativas de esta organización respecto a la Seguridad de la Información que almacena y gestiona, así como el cumplimiento de los diferentes marcos normativos que la regulan.

2 Justificación de una política general de seguridad de la información.

Los marcos normativos vigentes en materia de seguridad de la información requieren la disponibilidad de una política de seguridad corporativa que, aprobada por el llamado "Órgano Superior Competente", representado en el caso del Ayuntamiento de Coslada por su Alcalde, y adecuadamente difundida entre el personal y todas las entidades afectadas, implemente los requerimientos de estos Marcos para preservar los derechos y libertades de los interlocutores sociales con los que interactúa el Ayuntamiento de Coslada, englobados en adelante bajo la denominación genérica" interlocutores", "interlocutores sociales", "terceros" o "partes interesadas".

La diversidad de marcos normativos, sus distintos ámbitos objetivos y subjetivos, así como la evolución permanente de los mismos, aconsejan desarrollar una PGSI unificada y permitir con ello eliminar redundancias en actividades, documentos y controles, optimizando con ello las actuaciones corporativas y el nivel de cumplimiento normativo.

3 Ámbito objetivo de la PGSI.

La PGSI abarca todos los medios, automatizados o no, que el Ayuntamiento de Coslada utiliza para el desarrollo de sus actividades, así como todos los medios por los que opera internamente con otras entidades, públicas y/o privadas. Las actividades incluyen:

(1). Las relaciones de carácter jurídico-económico-administrativo entre los interlocutores sociales y el Ayuntamiento de Coslada

(2). La realización de las funciones de negocio/servicio por parte del Ayuntamiento de Coslada, tanto los desarrollados por medios electrónicos como los manuales.

(3). El tratamiento de la información gestionada por el Ayuntamiento de Coslada en el ejercicio de sus competencias, especialmente aquella relacionada con datos personales.

(4). Las relaciones del Ayuntamiento de Coslada con las administraciones públicas.

4 Ámbito subjetivo de la PGSI.

La PGSI será aplicada por todos los servicios, informaciones, departamentos, áreas, unidades administrativas de la Organización y, en general, por todas las entidades internas y externas de

cualquier tipo vinculadas a esta entidad mediante cualquier modelo de relación. Para unificar la terminología, las estructuras organizativas internas serán llamadas “departamentos” en adelante.

La PGSI afecta a todo el personal del Ayuntamiento de Coslada, sea cual sea su relación laboral con ésta. Asimismo, la PGSI afecta a todo el personal que presta servicios a la Organización a través de empresas externas y que, por razón de esta relación, acceda, almacene y/o trate información cuya competencia y/o responsabilidad recaiga sobre la Organización.

La PGSI será aplicada en las relaciones del Ayuntamiento de Coslada con los interlocutores sociales, empresas y entidades públicas y/o privadas con las que interactúe, por lo que las personas que intervengan en estas relaciones están incluidas en los sujetos a quienes resulta de aplicación esa política.

5 Misión, visión y servicios prestados.

El Ayuntamiento de Coslada tiene como principal misión impulsar la calidad de vida en el municipio a través de la mejora en la prestación de los servicios para conseguir una mayor sostenibilidad, participación e integración tanto social como territorialmente y, consecuentemente, una mayor eficiencia en la gestión de los recursos.

La visión del Ayuntamiento de Coslada es impulsar la transformación digital y consolidar la Sede Electrónica como punto de contacto digital entre el ciudadano y la entidad. De esta forma, en su propio entorno laboral, proporcionar a sus empleados un ambiente agradable que les permita sentirse realizados y a gusto en el trabajo.

Como consecuencia, los ciudadanos encontrarán un Ayuntamiento con respuestas a los problemas de gestión ciudadana, consolidada en su aspecto administrativo y servicios.

6 Marcos normativos referenciales de la PGSI.

Los marcos normativos referenciales se encuentran en el Registro Corporativo de Marcos Normativos:

COSLADA-RGS-GLB-610-Marco Normativo

Conteniendo los marcos normativos aplicables al Ayuntamiento de Coslada.

7 Órgano Superior Competente.

A los efectos de las actuaciones previstas en el SGSI y encomendadas al llamado “Órgano Superior Competente”, este Órgano, en el Ayuntamiento de Coslada, será su Alcalde y, en su caso, en quien se establezca la oportuna delegación.

8 Organización de la seguridad.

8.1 Definición de roles.

Tal y como indican las normas de referencia, la seguridad debe comprometer a todos los miembros de la organización. La Política de Seguridad debe identificar a unos responsables claros para velar por su cumplimiento y ser conocida por todos los miembros de la Organización.

Adicionalmente, otros marcos normativos requieren asimismo la creación de roles específicos, como el rol Delegado de Protección de Datos en el RGPD-LOPDGDD.

Se establecen por tanto los siguientes roles en la Organización relacionados con la Seguridad de la Información:

8.2 Responsable de la Información (RINF)

El Responsable de la Información será el encargado de llevar a cabo en relación con el Esquema Nacional de Seguridad las siguientes tareas:

- Establecer y aprobar los requisitos de seguridad aplicables a la información dentro del marco establecido en el anexo I de Real Decreto 311/2022, de 3 de mayo, previa propuesta al responsable de seguridad y/o Comité de Seguridad de la Información.
- Aceptar los niveles de riesgo residual que afecten a la información.

8.3 Responsable del Servicio (RSERV)

El Responsable del Servicio será el encargado de llevar a cabo en relación con el Esquema Nacional de Seguridad las siguientes tareas:

- Establecer y aprobar los requisitos de seguridad aplicables al servicio dentro del marco establecido en el anexo I de Real Decreto 311/2022, de 3 de mayo, previa propuesta al responsable de seguridad y/o Comité de Seguridad de la Información.
- Aceptar los niveles de riesgo residual que afecten al servicio.

8.4 Responsable de seguridad de la información. (RSEG o CIS).

El rol de Responsable de Seguridad debe asumir las siguientes funciones:

- Mantener y verificar el adecuado nivel de seguridad de la Información gestionados y de los servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar a responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación de sistema.
- Proporcionar asesoramiento para la determinación de la categoría de sistema, en colaboración con el responsable del Sistema y/o Comité de Seguridad de la Información.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.

- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos de sistema.
- Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones.
- Monitorizar el ejercicio de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto a los mismos. En particular, velar por la coordinación de las distintas áreas de seguridad en la gestión de incidentes de seguridad de la información.

8.5 Responsable de sistema (RSIS o CIO).

Las funciones del Responsable del Sistema (o Responsables de Sistemas si así se establece) son:

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que éstos presentan deficiencias graves de seguridad.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
- Elaborar los procedimientos operativos necesarios.
- Definir la topología y gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Asegurarse de que las medidas específicas de seguridad se integren adecuadamente en el marco general de seguridad.
- Prestar a el responsable de seguridad de la Información y/o el Comité de Seguridad asesoramiento para la determinación de la Categoría del Sistema.
- Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, en su caso, en los planes de continuidad.
- Llevar a cabo las funciones del administrador de la seguridad de sistema:
    - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
    - La gestión de las autorizaciones concedidas a los usuarios de sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo que autoriza.
    - Aprobar los cambios en la configuración vigente del sistema de información.
    - Hay que asegurar que los controles de seguridad establecidos son estrictamente cumplidos.
    - Asegurarse que se aplican los procedimientos aprobados para gestionar el Sistema de Información.
    - Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajusten a las autorizaciones pertinentes.
    - Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

Cuando la complejidad del sistema lo justifique, el responsable de Sistema podrá designar a los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el

mismo. Del mismo modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

8.6 Delegado de Protección de Datos (DPD).

El rol de Delegado de Protección de Datos (DPD) es requerido por el RGPD en base a su arte. 37:

> *Artículo 37 Designación del delegado de protección de datos*
> *1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:*
>
> *a) El tratamiento se llevará a cabo por una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial.*
> *b) Las principales actividades del responsable o del encargado consistan en operaciones de tratamiento que, por razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala.*
> c) *Las principales actividades del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales de acuerdo con el artículo 9 RGPD y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10 RGPD .*

Adicionalmente, la LOPDGDD, en su artículo 76. Sanciones y medidas correctivas incluye como punto a considerar en un posible procedimiento sancionador:

> *g) Disponer, cuando no sea obligatorio, un delegado de protección de datos.*

En base a estas consideraciones, el Ayuntamiento de Coslada asume la necesidad de disponer del rol delegado de protección de datos.

Por tanto, identifica y nombra un delegado de protección de datos corporativo.

La titularidad concreta del DPD corporativo se determina mediante designación del Órgano Superior Competente.

Las funciones del DPD están definidas en el RGPD.

8.7 Comité de Seguridad de la Información.

8.7.1 Composición.

Se crea el Comité de Seguridad de la Información, que estará compuesto por los siguientes miembros:

Cargo en Comité	**Cargo Corporativo**
Presidencia	Alcalde
Vocal-Secretaría	Técnica de Informática-Responsable de Seguridad
Vocal 1	Secretaria General
Vocal 2	Técnico Adjunto a Intervención General

Vocal 3	Intendente de Policía
Vocal 4	Archivera
Vocal 5	Técnica de Relaciones Laborales

El Comité de Seguridad de la Información podrá convocar a responsables departamentales y/u otras personas cuya intervención sea requerida para el desarrollo de las actuaciones del Comité. Es obligatoria la asistencia de las personas convocadas, la aportación de toda la información que les sea solicitada y el cumplimiento de las instrucciones recibidas del Comité de Seguridad de la Información.

Corresponde al secretario/a del Comité de Seguridad de la Información:

- Convocar las reuniones del Comité de Seguridad de la Información.
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el acta de las reuniones.
- La responsabilidad de la ejecución directa o delegada de las decisiones del Comité.

Todos los miembros del Comité actuarán con voz y voto y sus acuerdos requerirán, al menos, el voto de la mayoría simple de los miembros.

8.7.2 Funciones del Comité de Seguridad de la Información.

Las funciones del Comité de Seguridad de la Información son las siguientes:

- Atender a los requerimientos, objetivos y necesidades de información del Órgano Superior Competente y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información en el Órgano Superior Competente.
- Determinar la categoría del Sistema en base a las valoraciones de servicios e información soportados por el sistema de información que han realizado sus responsables con el soporte del Responsable de la Seguridad de la Información y Responsable del Sistema.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia devolución de la Organización en lo que respecta a la Seguridad de la Información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, evitando duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por el Órgano competente.
- Elaborar y aprobar los requisitos de formación y cualificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
- Aprobar planes de mejora de la seguridad de la información de la organización. En particular, velará por la coordinación de diferentes planes que se puedan realizar en diferentes áreas.
- Asegurar que la Seguridad de la Información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación, incluyendo el principio de

"Privacidad por diseño y por defecto" requerido por el RGPD. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Pedir regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones.
- Obtener asesoramiento sobre los temas que deba decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y modos:
  - Grupos de trabajo especializados internos, externos o mixtos.
  - Asesoría interna y/o externa.
  - Asistencia a cursos u otros tipos de entornos formativos o de intercambio de experiencias.
- Aprobar el Plan de Mejora de la Seguridad, con la dotación presupuestaria correspondiente, para su presentación al Órgano Superior Competente y su correspondiente aprobación formal.
- Asumir los roles de Responsable de Servicio y Responsable de Información especificados en el ENS.

8.8 Estructura en el proceso de decisiones y mecanismos de coordinación.

Los distintos roles de Seguridad de la Información (autoridad principal y posibles delegadas) se limitan a una estructura simple:

8.8.1 Comité de Seguridad de la Información.

El Comité de Seguridad de la Información da instrucciones al Responsable de Seguridad de la Información, que se encarga de su cumplimentación, supervisando que administradores y operadores implementan las medidas de seguridad según lo establecido en esta PGSI.

8.8.2 Responsable de seguridad de la información.

El Responsable de la Seguridad de la Información:

1. Informa al Responsable de la Información de las decisiones e incidentes en materia de seguridad que afecten a la información que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto a los márgenes aprobados.
2. Informa al Responsable del Servicio de las decisiones e incidentes en materia de seguridad que afecten al servicio que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto a los márgenes aprobados.
3. Rinde cuentas en el Comité de Seguridad de la Información, como secretario:
   - Resumen consolidado de actuaciones en materia de seguridad.
   - Resumen consolidado de incidentes relativos a la seguridad de la información.
   - Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

4. Rinde cuentas al Órgano Superior Competente, según lo acordado por el Comité de Seguridad de la Información.
   - Resumen consolidado de actuaciones en materia de seguridad.
   - Resumen consolidado de incidentes relativos a la seguridad de la información.
   - Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

8.8.3 Responsable del sistema.

El Responsable del Sistema:

1. Informa al Responsable de la Información de las incidencias funcionales relativas a la información que le compete.
2. Informa al Responsable de Servicio de las incidencias funcionales relativas al servicio que le compete.
3. Da cuenta al Responsable de la Seguridad:
   - Actuaciones en materia de seguridad, en particular en lo que se refiere a decisiones de arquitectura del sistema.
   - Resumen consolidado de los incidentes de seguridad.
   - Medidas de la eficacia de las medidas de protección a implantar.

8.9 Procedimientos de designación de personas.

El Órgano Superior Competente nombrará formalmente, mediante las resoluciones pertinentes:

- Comité de Seguridad de la Información.
- Delegado de protección de datos.
- Responsable/s de la Seguridad.
- Responsable/s de los sistemas de información.
- Administrador/es de Seguridad del Sistema, a propuesta del Responsable del Sistema o del Responsable de Seguridad de la Información.

8.10 Segregación de funciones.

El ENS recoge el principio de "seguridad como función diferenciada". Este principio exige:

- Responsable de Seguridad debe ser independiente del Responsable del sistema.
- Responsable de Servicio o de información debe ser independiente del Responsable del Sistema.
- Las personas asignadas a funciones de desarrollo deben ser independientes de las personas asignadas a los pases a producción.
- Las personas asignadas a la operación de sistemas tendrán que ser independientes de las personas asignadas al mantenimiento de sistemas.
- Delegado de Protección de Datos debe ser independiente de toda influencia que pudiera condicionar sus actuaciones, en base a lo que requiere el RGPD.

La asignación de roles y responsabilidades tendrá en cuenta la preceptiva segregación de funciones, de forma que las actuaciones de las personas titulares de los mismos no comprometan la seguridad

de informaciones y servicios en cualquiera de sus dimensiones (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad).

En casos excepcionales, sobre todo cuando no están disponibles los recursos necesarios, pueden exceptuarse estas reglas de segregación de funciones y establecer las medidas compensatorias apropiadas para la resolución de los conflictos de intereses que puedan surgir.

En caso de que exista relación jerárquica en la Estructura de la RPT entre el Responsable de Seguridad y el Responsable del Sistema se entenderá como dependencia orgánica, pero no afectará al concreto desempeño de los roles de cada uno de los responsables, ejerciendo éste último las tareas con independencia funcional.

8.11 Suplencias y delegaciones.

Los roles requeridos por los marcos normativos referenciales de esta PGSI deben estar permanentemente operativos. La Organización establecerá un procedimiento formal de suplencias y/o delegaciones de modo que la ausencia de una persona, por cualquier motivo, no cause carencia de las funciones y/o competencias que desarrolla.

9 Datos de carácter personal.

9.1 Tratamiento.

Para la prestación de los servicios corporativos deben ser recabados, tratados y almacenados datos de carácter personal. Es compromiso del Ayuntamiento de Coslada respetar y proteger los derechos recogidos en la Constitución Española respecto a la intimidad, privacidad, imagen y honor de las personas, por lo que el cumplimiento de los marcos normativos que los regulan y, por tanto, la implementación de las medidas de seguridad y control requeridas constituye un objetivo prioritario de esta Organización.

El cumplimiento de RGPD, LOPDGDD y sus marcos normativos que los desarrollen será una iniciativa prioritaria. Se adoptarán las medidas necesarias para que esta Organización cumpla en las fechas de entrada en vigor todos los preceptos de los nuevos marcos, siendo uno de los puntos más importantes el nombramiento de la figura DPO/DPD (Data Protection Officer/Delegado de Protección de Datos).

Asimismo, se realizarán los ciclos de formación y concienciación específicos para que el personal conozca las medidas que deben aplicar en sus puestos de trabajo y los medios disponibles para la resolución de dudas, problemas e incidentes relacionados.

Será prioritario implementar las medidas organizativas y técnicas apropiadas para proteger los derechos y libertades de las personas físicas afectadas por los tratamientos de datos personales realizados por la Organización.

9.2 Videovigilancia.

La Organización observará en todo momento la normativa vigente en materia de videovigilancia, respetando los derechos de las personas captadas y suprimiendo las imágenes en los plazos establecidos por este ordenamiento.

10 Gestión de riesgos.

Todos los sistemas sujetos a esta PGSI deberán realizar un análisis de riesgos, evaluando las amenazas a las que están expuestos, sus vulnerabilidades, el impacto que supondría la materialización de las amenazas y, por tanto, el nivel de riesgo que supone.

En cuanto a todos los sistemas de información comprendidos al alcance de esta Política, será necesario realizar análisis de riesgos periódicos, evaluando las amenazas y los riesgos a los que están expuestos.

El análisis de riesgos será una de las bases fundamentales para determinar las medidas de seguridad a adoptar, así como para los requerimientos del RGPD relacionados sobre Análisis de Riesgos y Evaluaciones de Impacto sobre Protección de Datos (EIPD), cuando procedan.

El proceso de gestión de riesgos comprenderá las siguientes fases:

- Categorización de los sistemas.
- Análisis de riesgos.
- El Comité de Seguridad de la Información procederá a la selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos y estar justificadas.

Las fases de este proceso se realizarán según lo dispuesto en los anexos I y II del ENS y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.

10.1 Criterios de evaluación de riesgos.

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los distintos tipos de información manejados y los distintos servicios prestados.

Los criterios de evaluación de riesgos detallados se especificarán en la metodología de evaluación de riesgos que adoptará la Organización, basándose en estándares y buenas prácticas reconocidas. Esta metodología será MAGERIT V3 y las actualizaciones que pueda incorporar en el futuro.

Se tratarán, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la Organización, en base al impacto que los eventos analizados supongan sobre éstos, así como aquéllos que afecten los derechos y libertades de las personas físicas afectadas por los tratamientos de datos personales.

Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios a los interlocutores sociales y asociados a los tratamientos de datos de carácter personal.

10.2 Directrices de tratamiento.

El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, documentando, justificando y promoviendo las inversiones adecuadas para la aprobación del Órgano Superior Competente.

10.3 Proceso de aceptación del riesgo residual.

Los riesgos residuales serán determinados por el Responsable de Seguridad de la Información.

Los niveles de riesgo residual esperados sobre servicios e informaciones después de la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad contenidas en el Anexo II del ENS, ISO 27001 y aquellas complementarias que sean necesarias para el cumplimiento de LOPDGDD) deben ser aprobados por el Comité de Seguridad de la Información, del que forma parte el Alcalde del Ayuntamiento de Coslada, su Órgano Superior Competente.

10.4 Necesidad de realizar o actualizar las evaluaciones de riesgos.

El análisis de los riesgos y su tratamiento serán una actividad repetida regularmente, según lo establecido en el ENS y este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando se produzcan cambios significativos en la información manejada.
- Cuando se produzcan cambios significativos en los servicios prestados.
- Cuando se produzcan cambios significativos en los sistemas que traten la información e intervienen en la prestación de los servicios.
- Cuando se produzca un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.
- Cuando se produzcan cambios normativos que así lo exijan o lo hagan conveniente.

11 Gestión de incidentes de seguridad

11.1 Prevención.

El Ayuntamiento de Coslada debe evitar, o, al menos, prevenir en la medida de lo posible, que la información o los servicios se vean afectados por incidentes de seguridad. Por ello, es necesario implementar las medidas de seguridad determinadas por las normativas corporativas, así como cualquier control adicional identificado a través de una evaluación de riesgos.

Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados, existiendo una caracterización de puestos de trabajo donde se incluyan las cuestiones relacionadas con la seguridad.

Para garantizar el cumplimiento de la política, y bajo la supervisión del Comité de Seguridad de la Información, los departamentos deben:

- Autorizar a los sistemas antes de entrar en producción desde el prisma de las prestaciones,

funcional y legal.

- Evaluar regularmente la seguridad, incluyendo apreciaciones de riesgos, impulsando las iniciativas necesarias para resolver las situaciones no conformes o fuera de los márgenes de riesgo aceptables.
- Solicitar la revisión periódica por parte de terceros para obtener una evaluación independiente.
- Desarrollar Planes de Formación para el personal, así como reciclaje periódico y acciones de concienciación.

11.2 Detección.

Dado que los servicios se pueden degradar rápidamente a causa de incidentes, pudiendo incluso provocar su detención, el Responsable de Sistema y los Administradores de Seguridad del Sistema deben monitorizar la operación de forma continua para detectar anomalías en los niveles de prestación de los servicios y actuar a consecuencia, según lo que establece el ENS y la norma ISO 27001.

La monitorización es especialmente relevante cuando se establecen líneas de defensa, práctica requerida por las normativas de referencia y el ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

11.3 Respuesta.

La respuesta ante incidentes debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos u otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT), autoridades competentes y, en su caso, a los afectados. Este precepto está recogido explícitamente en el ENS y en el RGPD (en este último caso, cuando el incidente afecte a datos de carácter personal).

11.4 Recuperación.

Para garantizar la disponibilidad de los servicios y las informaciones corporativas, el Ayuntamiento de Coslada desarrolla y mantiene iniciativas de continuidad de los sistemas de información como parte del plan general de continuidad de servicio, así como actividades de recuperación en caso de caída total o parcial, afectando tanto al ENS como a los preceptos de disponibilidad y resiliencia de RGPD-LOPDGDD.

Estas iniciativas de continuidad serán desarrolladas teniendo en cuenta la categorización de los sistemas de información corporativos, según lo preceptuado en el Anexo I – Categoría de los sistemas, del ENS, y aplicar las medidas correspondientes de su Anexo II.

11.5 Aprendizaje.

Los incidentes serán analizados para determinar su causa raíz, las actuaciones desarrolladas en su resolución y recuperación y se extraerán las conclusiones apropiadas para prevenir su recurrencia.

12 Gestión de personal.

12.1 Obligaciones del personal.

El personal del Ayuntamiento de Coslada tiene la obligación de conocer y cumplir esta Política General de Seguridad de la Información y las Normativas y Procedimientos de Seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la PGSI llegue a los afectados.

El personal de la organización asistirá a sesiones de formación y concienciación en materia de seguridad de la información al menos una vez al año, o cuando se realicen cambios significativos en medios y/o métodos relacionados. Se establecerá un programa de formación/concienciación continua para atender al personal, en particular en los casos de nueva incorporación.

El cumplimiento de la presente Política de Seguridad es obligatorio por parte de todo el personal interno o externo que intervenga en los procesos de la Organización, constituyendo su incumplimiento una infracción a efectos de posibles procedimientos sancionadores, la cual será calificada en función del grado de incumplimiento y el impacto que éste haya generado sobre los servicios corporativos.

Asimismo, y sin perjuicio del procedimiento sancionador, la Organización denunciará ante las autoridades competentes las acciones que pudieran ser constitutivas de cualquier tipo de presunto delito.

12.2 Caracterización del puesto de trabajo.

El Ayuntamiento de Coslada incluirá en la descripción de puestos de trabajo los perfiles, titulaciones, acreditaciones y experiencia requeridos para aquellos puestos dedicados a tareas relacionadas con la Seguridad de la Información. Los procesos de selección tendrán en cuenta esta caracterización.

El Ayuntamiento de Coslada incluirá en la descripción de puestos de trabajo las funciones y responsabilidades en materia de seguridad de cada uno de estos puestos.

12.3 Formación.

Las personas con responsabilidad en el uso, operación o administración de sistemas de información recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La asistencia a las sesiones de formación es obligatoria y su aprovechamiento podrá ser evaluado.

El Ayuntamiento de Coslada elaborará anualmente un Plan de Formación, sobre el que se hará un seguimiento detallado, registrando todas las personas asistentes a los ciclos formativos.

12.4 Concienciación.

El Ayuntamiento de Coslada realizará actividades periódicas de concienciación hacia el personal, implementando mecanismos de comunicación de reglas de seguridad, cambios normativos, incidentes, resoluciones de Autoridades y, en general, toda información relevante para mejorar la conciencia del personal en cuanto a seguridad de la información y el cumplimiento de los marcos normativos aplicables.

13 Terceras partes.

Cuando se presten servicios o gestione información de otras organizaciones, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales para reportar y coordinar los respectivos Comités de Seguridad de la Información u órganos equivalentes, y se establecerán procedimientos de actuación para la reacción frente a incidentes de seguridad.

Cuando se utilicen servicios de terceros o se ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que corresponda a estos servicios o información. Esta tercera parte queda sujeta a las obligaciones establecidas en esta normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

La contratación de servicios de terceras partes incluirá, en la medida de lo posible, el establecimiento de acuerdos de nivel de servicio, los cuales deberán ser controlados por parte de las personas responsables de dichos servicios y, en su caso, entablar las reclamaciones pertinentes en caso de incumplimiento, eventos que deberán ser comunicados al Responsable de Seguridad en caso de afectar a la disponibilidad, confidencialidad, integridad, autenticidad o trazabilidad de los servicios y/o informaciones del Ayuntamiento de Coslada, y el Delegado de Protección de Datos cuando se vieran afectados datos de carácter personal.

Las entidades terceras deben seleccionarse atendiendo a los principios de idoneidad y cumplimiento de los marcos normativos exigibles, además del resto de criterios aplicables a su contratación.

Se establecerán procedimientos específicos de reporte y resolución de incidencias.

Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que lo establecido en esta Política.

En caso de que algún aspecto de la Política no pueda ser satisfecho por una tercera parte, según se requiere en los párrafos anteriores, se requerirá informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables departamentales afectados antes de seguir adelante con la contratación.

En caso de que los tratamientos desarrollados por terceras partes involucren datos de carácter personal, se realizarán todas las actuaciones requeridas por el RGPD y LOPDGDD. En este último caso, se evaluará la idoneidad de los proveedores, tal y como requiere el RGPD, y se firmarán los correspondientes contratos de “encargado de tratamiento” o “corresponsabilidad” con todo proveedor que desarrolle sus tareas tratando datos personales o “compromisos de confidencialidad y seguridad de la información cuando los tratamientos de datos personales sean incidentales.

14 Revisión y aprobación de la Política de Seguridad

La Política General de Seguridad de la Información será revisada por el Comité de Seguridad de la Información a intervalos planificados, que no podrán exceder del año de duración, o siempre que se produzcan cambios significativos, para asegurar que se mantenga su idoneidad, adecuación y eficacia.

Los cambios sobre la Política de Seguridad de la Información deben ser aprobados por el Órgano Superior Competente.

Cualquier cambio sobre la Política de Seguridad de la Información deberá ser difundido en todas las partes afectadas y, en su caso, objeto de reciclaje en la formación para el personal afectado.

15 Documentación complementaria.

La Política de Seguridad de la Información se complementará con documentos más detallados que ayuden a materializar sus preceptos teniendo en cuenta los principios básicos de seguridad definidos en el artículo 12 apartado 6 del RD 311/2022:

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

Por eso se utilizarán:

15.1 Normativas de seguridad.

Las normas uniformizan el uso de aspectos concretos del sistema, como son la mínima funcionalidad, seguridad por defecto, actividades de los usuarios, uso de dispositivos portátiles y móviles, Protección de la información almacenada y en tránsito. Indican el uso correcto y las responsabilidades de los usuarios. Serán aprobadas por el órgano superior y tendrán carácter obligatorio.

15.2 Procedimientos de seguridad.

Los procedimientos de seguridad detallan tareas concretas, indicando claramente su operativa.

15.3 Instrucciones de seguridad.

Las instrucciones de seguridad desarrollan la operativa descrita en los procedimientos, explicando a nivel técnico su implementación.

16 APROBACIÓN Y ENTRADA EN VIGOR.

Esta Política General de Seguridad de la Información es efectiva desde la fecha de su aprobación y será válida hasta que sea reemplazada por una nueva Política o sea derogada por resolución del Órgano Superior Competente del Ayuntamiento de Coslada

Este texto anula cualquier Política de Seguridad de la Información vigente hasta la fecha de aprobación de la presente.