CYTSA

Política de Seguridad de la Información

Código: PO-TI-01
Versión: 1.1
Fecha: Julio 2026
Estado: Vigente
Clasificación: Público

Control de Versiones

Versión	Fecha	Descripción	Responsable
1.0	Junio 2026	Adaptación y actualización de la Política de Seguridad conforme al ENS y al modelo documental corporativo	Responsable de Seguridad
1.1	Julio 2026	Actualización de roles, estructura documental y revisión del contenido conforme al ENS Medio.	Responsable de Seguridad

Tabla de Contenido

1. Introducción 4
1.1. Objetivo 4
1.2. Alcance 4
1.3. Marco de Referencia 4
2. Principios de Seguridad 5
2.1. Principios generales 5
2.2. Gestión de Riesgos 5
2.3. Mejora continua 5
3. Objetivos de la Seguridad de la Información 6
4. Marco Legal y Regulatorio 7
5. Organización de la Seguridad 8
5.1. Roles y Responsables 8
5.2. Comité de la Seguridad 8
5.3. Designación y renovación de responsables 8
6. Gestión de la Seguridad 9
6.1. Gestión del Riesgo 9
6.2. Gestión de incidentes 9
6.3. Continuidad 9
6.4. Formación y concienciación 9
7. Sistema Documental de Seguridad 10
7.1. Política de Seguridad 10
7.2. Normativa de Seguridad 10
7.3. Procedimientos 10
7.4. Guías 10
7.5. Informes y registros 10
7.6. Gestión y acceso a la documentación 10
8. Revisión y aprobación de la política 11
8.1. Revisión periódica 11
8.2. Aprobación 11
8.3. Control de versiones 11

1. Introducción

La presente Política de Seguridad establece el marco general de gobierno, organización y gestión de la seguridad de la información aplicable a los sistemas de información de CYTSA. Este documento recoge los principios, responsabilidades y directrices básicas que deben orientar la protección de la información, los servicios y los recursos tecnológicos utilizados por la organización en el desarrollo de su actividad.

1.1. Objetivo

El objetivo de esta Política de Seguridad es definir, de forma clara y proporcionada al tamaño, actividad y modelo operativo de CYTSA, las directrices generales para la protección de la información y de los sistemas que la soportan. La política tiene como finalidad asegurar que la seguridad se gestione de manera continua, basada en riesgos, integrada en la operativa diaria y alineada con los requisitos del Esquema Nacional de Seguridad.

Esta política permite establecer los objetivos de seguridad de la organización, el marco legal y regulatorio aplicable, la asignación de roles y responsabilidades, la estructura de coordinación de la seguridad y las directrices para la gestión de la documentación de seguridad del sistema.

1.2. Alcance

El alcance de esta Política de Seguridad comprende los sistemas de información, servicios, usuarios, dispositivos, aplicaciones, plataformas en la nube, comunicaciones, repositorios documentales y procesos tecnológicos utilizados por CYTSA para el desarrollo de su actividad corporativa y para la prestación de servicios a sus clientes.

Está política se aplica a todos los sistemas TIC de la entidad y a todos los miembros de la organización, implicados en Servicios y Proyectos destinados al sector público, que requieran la aplicación de ENS, sin excepciones.

1.3. Marco de Referencia

Esta Política de Seguridad se establece conforme al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y toma como referencia las guías y criterios de verificación del Centro Criptológico Nacional, en particular los requisitos aplicables a la medida org.1 relativa a la política de seguridad.

El marco legal y regulatorio aplicable incluye la normativa española y europea relacionada con la ciberseguridad, la protección de datos, la prestación de servicios digitales, la administración electrónica cuando resulte aplicable por relación contractual con entidades del sector público, y cualquier otra obligación legal, contractual o regulatoria que afecte a la información y a los servicios gestionados por CYTSA.

CYTSA mantiene la identificación y revisión de la normativa aplicable mediante un registro o relación de referencias legales y regulatorias, que permite controlar las obligaciones relevantes y mantener actualizada la documentación de seguridad cuando se produzcan cambios significativos en el marco normativo, contractual u operativo.

2. Principios de Seguridad

La seguridad de la información en CYTSA se fundamenta en un conjunto de principios generales orientados a proteger la información y los servicios corporativos de forma proporcionada, continua y alineada con la actividad real de la organización. Estos principios sirven de base para la definición de controles, procedimientos y responsabilidades en materia de seguridad.

2.1. Principios generales

CYTSA adopta como principios generales la protección de la información frente a accesos no autorizados, modificaciones indebidas, pérdida de disponibilidad, uso inadecuado o divulgación no autorizada. Para ello, la organización aplica medidas técnicas, organizativas y operativas adecuadas a sus riesgos, a sus recursos y al tipo de información tratada.

La seguridad está integrada en la gestión ordinaria de los sistemas y servicios, desde la planificación y adquisición de nuevos componentes hasta su operación, mantenimiento, supervisión y retirada. Las decisiones relacionadas con la seguridad deberán considerar la criticidad de los activos, las obligaciones legales y contractuales, la continuidad del servicio y la capacidad operativa de la organización.

Las actuaciones de seguridad se rigen por criterios de prevención, detección, respuesta, recuperación y mejora continua, evitando enfoques meramente reactivos y procurando que los controles implantados sean sostenibles, verificables y útiles para la operación diaria.

2.2. Gestión de Riesgos

La gestión de la seguridad en CYTSA se realiza mediante un enfoque basado en riesgos, de forma que las medidas de protección se definan y prioricen atendiendo al impacto que una amenaza o incidente pueda tener sobre la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y de los servicios.

El análisis y tratamiento de riesgos permite identificar los activos relevantes, valorar las amenazas y vulnerabilidades que puedan afectarles, determinar los riesgos asumibles y establecer las medidas necesarias para reducirlos a niveles aceptables para la organización.

La gestión de riesgos se revisa de forma periódica y cuando se produzcan cambios significativos en los sistemas, servicios, proveedores, tecnologías utilizadas, requisitos legales o condiciones de prestación de los servicios.

2.3. Mejora continua

CYTSA asume la mejora continua como principio básico de su sistema de seguridad de la información. La seguridad no se considera una actuación puntual, sino un proceso permanente de revisión, adaptación y evolución de las medidas implantadas.

La mejora se apoya en la revisión periódica de controles, el seguimiento de incidencias, la evaluación de cambios tecnológicos, los resultados de auditorías, las recomendaciones recibidas y las necesidades detectadas durante la operación diaria del sistema.

Las acciones de mejora deben ser proporcionadas, priorizadas y trazables, permitiendo evidenciar la evolución del sistema de seguridad sin introducir cargas documentales u operativas innecesarias para la organización.

3. Objetivos de la Seguridad de la Información

Los objetivos de la seguridad de la información en CYTSA se orientan a garantizar que la información corporativa, los servicios tecnológicos y los sistemas que los soportan se protejan de forma adecuada durante todo su ciclo de vida, conforme a las necesidades de la organización, los compromisos adquiridos con clientes y las obligaciones legales y contractuales aplicables. Con carácter general, CYTSA establece como objetivos de seguridad los siguientes:

- Proteger la confidencialidad de la información corporativa, de clientes y de terceros, evitando accesos, usos o divulgaciones no autorizadas.
- Preservar la integridad de la información y de los sistemas, evitando alteraciones indebidas, errores no controlados o modificaciones no autorizadas.
- Garantizar la disponibilidad de los servicios y recursos tecnológicos necesarios para el desarrollo de la actividad de CYTSA y la prestación de servicios a sus clientes.
- Asegurar la autenticidad, trazabilidad y control de las actuaciones realizadas sobre los sistemas, servicios e información gestionada por la organización.
- Aplicar controles de acceso basados en la necesidad de uso, el principio de mínimo privilegio y la adecuada segregación de funciones cuando resulte aplicable.
- Mantener los sistemas, dispositivos y servicios corporativos actualizados, gestionados y protegidos frente a amenazas, vulnerabilidades y usos no autorizados.
- Disponer de mecanismos de registro, supervisión y detección que permitan identificar eventos relevantes de seguridad y facilitar la respuesta ante incidentes.
- Promover el uso responsable de los recursos tecnológicos por parte del personal, colaboradores y terceros autorizados.
- Mantener evidencias, registros y documentación que permitan demostrar la aplicación efectiva de las medidas de seguridad implantadas.
- Revisar periódicamente el estado de la seguridad y adoptar acciones de mejora cuando se identifiquen cambios, desviaciones, incidentes o necesidades de refuerzo.

Estos objetivos se desarrollan mediante la normativa interna, los procedimientos operativos, los controles técnicos y organizativos, y las revisiones periódicas definidas por CYTSA dentro de su sistema de gestión de la seguridad.

4. Marco Legal y Regulatorio

La seguridad de la información en CYTSA se desarrolla dentro del marco legal, regulatorio y contractual aplicable a su actividad, especialmente en aquellos servicios relacionados con clientes del sector público, gestión de información corporativa, prestación de servicios tecnológicos, protección de datos personales y uso de medios electrónicos.

Este marco no se limita a una relación cerrada de normas, sino que comprende las disposiciones españolas y europeas que resulten aplicables en cada momento, así como los requisitos derivados de contratos, pliegos, acuerdos de confidencialidad, obligaciones con clientes y compromisos internos asumidos por la organización.

Como referencias principales, CYTSA considera el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad; la normativa europea y española en materia de protección de datos personales, incluyendo el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018; y, cuando resulte aplicable por la naturaleza de los servicios prestados, la normativa relacionada con procedimiento administrativo, régimen jurídico del sector público y administración electrónica.

Asimismo, se tienen en cuenta las guías, instrucciones técnicas, criterios de conformidad y recomendaciones emitidas por organismos competentes en materia de seguridad de la información y ciberseguridad, en la medida en que resulten aplicables al sistema de información y al contexto operativo de CYTSA.

La identificación, revisión y actualización de la normativa aplicable se realiza mediante un registro o relación de referencias legales, regulatorias y contractuales relevantes, en el que se conservará la información necesaria para conocer su vigencia, ámbito de aplicación y posible impacto sobre la seguridad de la información.

Cuando se identifiquen cambios normativos, contractuales u organizativos que puedan afectar al sistema de información, CYTSA valorará su impacto y, en su caso, actualizará la documentación, los controles, los procedimientos o las responsabilidades que resulten necesarios.

5. Organización de la Seguridad

CYTSA establece una organización de la seguridad basada en la asignación clara de funciones, responsabilidades y mecanismos de coordinación, de forma proporcionada a su estructura interna y al alcance de los sistemas de información gestionados.

5.1. Roles y Responsables

La organización de la seguridad contempla los roles necesarios para asegurar la adecuada gestión, operación y supervisión de la seguridad de la información. Entre estos roles se incluyen, según corresponda, el Responsable de la Información, el Responsable del Servicio, el Responsable de Seguridad, el Responsable del Sistema y las funciones técnicas o administrativas necesarias para la gestión diaria de los sistemas.

Cada rol tiene asignadas funciones acordes con su ámbito de responsabilidad, incluyendo la definición de requisitos de seguridad, la supervisión del cumplimiento, la administración técnica de los sistemas, la gestión de accesos, el seguimiento de riesgos, la coordinación de actuaciones y la conservación de evidencias cuando proceda.

5.2. Comité de la Seguridad

El Comité de Seguridad constituye el órgano de coordinación y seguimiento de la seguridad de la información en CYTSA. Su finalidad es facilitar la toma de decisiones, revisar el estado general de la seguridad, valorar riesgos relevantes, realizar seguimiento de incidencias significativas y promover las acciones de mejora necesarias.

La composición del Comité de Seguridad, sus integrantes nominales, ámbito de responsabilidad y posibles cambios de composición se documentan mediante las correspondientes actas o registros internos. El Comité puede apoyarse en personal técnico, responsables internos o asesoramiento externo cuando la materia tratada lo requiera.

El Comité celebra sesiones ordinarias como mínimo una vez al año con el fin de actualizar su designación, renovar a sus miembros y aprobar las revisiones pertinentes en la documentación oficial de seguridad de la información.

5.3. Designación y renovación de responsables

La designación de los responsables de seguridad se realiza por la Dirección, quedando documentada mediante acta, registro de designación o documento equivalente. La designación deberá identificar el rol asignado, la persona designada, sus principales responsabilidades y la fecha de efectos.

Las designaciones se revisarán cuando se produzcan cambios organizativos, cambios en las funciones desempeñadas, altas o bajas de personal, modificaciones relevantes en el sistema de información o cuando así lo determine la Dirección. Las personas designadas deberán conocer y aceptar las responsabilidades asociadas a su función.

6. Gestión de la Seguridad

La gestión de la seguridad en CYTSA se apoya en procesos operativos orientados a mantener los riesgos bajo control, responder ante incidentes, asegurar la continuidad razonable de los servicios y promover el conocimiento de las obligaciones de seguridad por parte de las personas usuarias.

6.1. Gestión del Riesgo

La gestión del riesgo se realiza mediante la identificación de activos, amenazas, vulnerabilidades e impactos potenciales, así como mediante la definición de medidas de tratamiento proporcionadas a la criticidad de los sistemas y servicios afectados.

El resultado del análisis de riesgos servirá de base para priorizar controles, justificar decisiones de seguridad, planificar mejoras y mantener evidencias de la evolución del sistema de seguridad.

6.2. Gestión de incidentes

CYTSA dispone de mecanismos para la identificación, comunicación, análisis, tratamiento y seguimiento de incidentes de seguridad que puedan afectar a la información, los sistemas, los servicios o los usuarios.

Los incidentes se registrarán con la información necesaria para permitir su trazabilidad, valorar su impacto, adoptar medidas correctivas y conservar evidencias de las actuaciones realizadas. Cuando proceda, se aplicarán los canales de comunicación o notificación exigidos por la normativa, los contratos o los procedimientos internos.

6.3. Continuidad

CYTSA establece medidas orientadas a preservar la continuidad de los servicios y la recuperación de la información ante fallos, incidentes, indisponibilidades o pérdida de datos, considerando la criticidad de los activos y servicios afectados.

Estas medidas incluirán, entre otras, la gestión de copias de seguridad, la revisión de la disponibilidad de servicios esenciales, la documentación de actuaciones de recuperación y la evaluación de mejoras cuando se detecten debilidades o cambios relevantes.

6.4. Formación y concienciación

El personal de CYTSA y los terceros autorizados debe conocer las normas básicas de uso seguro de los sistemas, protección de la información, gestión de credenciales, tratamiento de datos y comunicación de incidencias.

Las acciones de formación y concienciación se adaptarán a las necesidades de la organización y podrán realizarse mediante comunicaciones internas, instrucciones operativas, recordatorios, sesiones formativas o difusión de normativa interna aplicable.

7. Sistema Documental de Seguridad

CYTSA estructura la documentación de seguridad de forma ordenada y proporcional, con el objetivo de facilitar su elaboración, aprobación, consulta, mantenimiento y conservación como evidencia del sistema de seguridad.

7.1. Política de Seguridad

La Política de Seguridad constituye el documento principal que define el marco general, los principios, los objetivos, la organización, las responsabilidades y las directrices básicas de seguridad de la información.

7.2. Normativa de Seguridad

La normativa de seguridad desarrolla las reglas internas de uso, comportamiento, responsabilidades del personal, obligaciones de protección de la información y criterios generales aplicables al uso de los recursos tecnológicos.

7.3. Procedimientos

Los procedimientos describen la forma en que se ejecutan actividades concretas de seguridad, administración, operación, control, revisión o respuesta ante eventos e incidentes, permitiendo asegurar una gestión homogénea y trazable.

7.4. Guías

Las guías e instrucciones técnicas proporcionan criterios prácticos para la aplicación de controles, configuración de sistemas, uso de herramientas, gestión de evidencias o realización de tareas operativas específicas.

7.5. Informes y registros

Los informes y registros constituyen evidencias de la aplicación de controles, revisiones, incidencias, auditorías, cambios, designaciones, aprobaciones y demás actuaciones relevantes en materia de seguridad.

7.6. Gestión y acceso a la documentación

La documentación de seguridad se conserva en repositorios corporativos autorizados, con acceso restringido según la necesidad de uso y las responsabilidades asignadas. La gestión documental deberá contemplar criterios de elaboración, revisión, aprobación, actualización, conservación, trazabilidad y control de versiones.

8. Revisión y aprobación de la política

La Política de Seguridad debe mantenerse actualizada, aprobada y disponible para las personas que deban conocerla o aplicarla, de forma que refleje adecuadamente la organización de la seguridad y el contexto operativo de CYTSA.

8.1. Revisión periódica

La Política de Seguridad es revisada a intervalos planificados, al menos una vez al año y, adicionalmente, cuando se producen cambios relevantes en la organización, en los sistemas de información, en el marco legal o contractual, en los riesgos identificados o en los requisitos aplicables.

8.2. Aprobación

La aprobación de la Política de Seguridad corresponde a la Dirección de CYTSA, quedando documentada mediante acta o registro formal de aprobación, dejando constancia documental de la versión aprobada, fecha de aprobación y responsable correspondiente.

8.3. Control de versiones

Las versiones de la Política de Seguridad se controlan mediante el registro de versión, fecha, descripción de cambios y responsable de la actualización. Las versiones anteriores se conservarán cuando resulte necesario para mantener trazabilidad documental y evidenciar la evolución del sistema de seguridad.