Marco Normativo

Política de Seguridad de la Información

SALCAI UTINSA S.A.

Documento:	Política de Seguridad de la Información

Tipo de documento:	Marco Normativo
Clasificación:	Uso Oficial
Empresas	SALCAI UTINSA S.A.
Finalidad	Establecer la política de seguridad de los sistemas de información
Autor	SALCAI UTINSA S.A.

Revisión y aprobación

Revisión y aprobación		**Fecha**
Revisado por:	Responsable de Seguridad / Responsable del Sistema	24/12/2025
Aprobado por:	Comité de Seguridad	24/12/2025
Aprobado por:	Comité de Seguridad	28/10/2026

Control de Cambios

Versión	**Fecha**	**Autor**	**Descripción del Cambio**	**Estado**
1.0	24/12/2025	Consultores Telefónica; Responsable de Seguridad; Responsable del Sistema;	Versión Inicial	Definitivo
2.0	28/10/2026	Responsable del Sistema	Cambio de RSI	Definitivo

ÍNDICE

1. Introducción 4
2. Alcance 4
3. Misión y Objetivos 5
4. Principios Rectores de la Política 6
5. Marco Normativo 6
6. Organización de la Seguridad 7
6.1. Definición de Roles y Responsabilidades asociados al ENS 7
6.1.1. Responsable de la Información (rinf) y Servicios (RSERV) 7
6.1.2. Responsable de Seguridad (RSEG) 7
6.1.3. Responsable del Sistema (RSIS) 8
6.1.4. Delegado de Protección de Datos (DPD) 9
6.2. Comité de Seguridad de la Información 10
6.2.1. Roles del Comité de Seguridad 10
6.2.2. Atribuciones del Comité de Seguridad 11
6.2.3. Periodicidad de la reuniones y adopción de acuerdos 11
6.3. Designación y resolución de conflictos 12
7. Tratamiento de datos personales 12
8. Gestión de Riesgos 12
9. Desarrollo de la Política de Seguridad de la Información 13
10. Obligaciones del personal 13
11. Terceras partes 14
12. Gestión de incidentes de seguridad 15
13. Aprobación y entrada en vigor 15

1. Introducción

SALCAI UTINSA S.A. depende de los sistemas de información para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas, en función del riesgo, para protegerlos frente a daños accidentales o deliberados que puedan afectar a la autenticidad, trazabilidad, integridad o confidencialidad de la información tratada o la disponibilidad de los servicios prestados.

El objetivo último de la seguridad de la información es garantizar que la entidad pueda cumplir con sus objetivos, desarrollar sus funciones o competencias y prestar los servicios para la cual ha sido constituida la calidad de la información y la prestación continuada de los servicios, actuando previamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

SALCAI UTINSA S.A. debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificables e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos donde se traten datos personales, se adquieran servicios TIC o se presten servicios que afecten a los sistemas de información.

2. Alcance

Esta política se aplica a todos los sistemas de información de **SALCAI UTINSA S.A.** a las personas que conforman la organización y a los prestadores de servicios o proveedores de soluciones TIC de **SALCAI UTINSA S.A.**.

3. Misión y Objetivos

SALCAI UTINSA S.A. tiene como misión proporcionar un servicio público de transporte interurbano insular de viajeros, seguro, eficiente, sostenible, y de calidad, que contribuya a la mejora de la movilidad y de la calidad de vida de la ciudadanía de Gran Canaria y de las personas que la visitan.

La organización presta este servicio conectando municipios, promoviendo la accesibilidad, el respeto al medio ambiente, el compromiso social y operando bajo criterios de viabilidad técnica y económica, garantizando la continuidad y fiabilidad de los servicios que soporta su actividad.

Los objetivos en materia de seguridad que **SALCAI UTINSA S.A.** pretende garantizar con la presente Política son:

- Garantizar la confidencialidad, integridad, autenticidad de la información y la continuidad en la prestación de los servicios.
- Implementar medidas de seguridad en función del riesgo.
- Formar y concienciar a los integrantes de **SALCAI UTINSA S.A.** respecto a la seguridad de la información.
- Implementar medidas de seguridad que permitan la trazabilidad de los accesos y respetar, entre otros, el principio de mínimo privilegio, reforzando también el deber de confidencialidad de las personas usuarias en relación con la información que conocen en el desempeño de sus funciones.
- Desplegar y controlar la seguridad física haciendo que los activos de información se encuentren en áreas seguras, protegidos por controles de acceso, atendiendo a los riesgos detectados.
- Establecer la seguridad en la gestión de comunicaciones mediante los procedimientos necesarios, logrando que la información que se transmita a través de redes de comunicaciones sea adecuadamente protegida.
- Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Controlar el cumplimiento de las medidas de seguridad en la prestación de los servicios, manteniendo el control en la adquisición, e incorporación de nuevos componentes del sistema.
- Gestionar los incidentes de seguridad para la correcta detección, contención, mitigación y resolución de estos, adoptando las medidas necesarias para que los mismos no vuelvan a producirse.
- Proteger la información personal, adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación en materia de protección de datos.
- Supervisar de forma continuada el sistema de gestión de la seguridad, mejorando y corrigiendo las ineficiencias detectadas.

4. Principios Rectores de la Política

- Alcance estratégico: la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles de la entidad y deberá coordinarse e integrarse con el resto de las iniciativas estratégicas de forma coherente.
- Seguridad integral: la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de la información, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.
- Gestión de la seguridad basada en el riesgo: la gestión de la seguridad basada en los riesgos identificados permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a que esté sujeta la información y sus sistemas y serán proporcionales al riesgo que tratan, debiendo estar justificadas. Se tendrán también en cuenta los riesgos identificados en el tratamiento de los datos personales.
- Prevención, detección, respuesta y conservación con la implementación de acciones preventivas de incidentes, minimizando las vulnerabilidades detectadas, evitando la materialización de las amenazas y, cuando estas se produzcan, dando una respuesta ágil para restaurar la información o servicios prestados, garantizando una conservación segura de la información.
- Existencia de líneas de defensa, la estrategia de seguridad de la entidad se diseña e implementa en capas de seguridad.
- Vigilancia continua y reevaluación periódica: la entidad implementa medios de detección y respuesta a actividades o comportamientos anómalos. Además, de otros que permitan una evaluación continuada del estado de seguridad de los activos. Existirá, también, un proceso de mejora continua para la revisión y actualización de las medidas de seguridad, de manera periódica, conforme a su eficacia y evolución de los riesgos y sistemas de protección.
- Seguridad por defecto y desde el diseño: los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.
- Diferenciación de responsabilidades, en aplicación de este principio las funciones del Responsable de Seguridad y del Responsable del Sistema estarán diferenciadas.

5. Marco Normativo

Las principales normas que afectan a esta Política son:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley 13/2007, de 17 de mayo, de Ordenación del Transporte por Carretera de Canarias.
- Asimismo, será de aplicación toda aquella normativa de carácter legal, sectorial u organizativo, que resulte de obligado cumplimiento en el ámbito del servicio prestado por la organización.

6. Organización de la Seguridad

La organización, teniendo en cuenta los artículos que describe el ENS, establece las siguientes acciones para organizar la Seguridad de la Información:

i. Designará roles de seguridad: Responsable del Servicio o Servicios, Responsable de la Información, Responsable de la Seguridad, Responsable del Sistema y Delegado de Protección de Datos.
ii. Constituirá un órgano consultivo y estratégico para la toma de decisiones en materia de Seguridad de la Información. Este órgano se denominará Comité de Seguridad de la Información.

6.1. Definición de Roles y Responsabilidades asociados al ENS

6.1.1. RESPONSABLE DE LA INFORMACIÓN (RINF) Y SERVICIOS (RSERV)

Serán funciones de los Responsable de la Información y de los Servicios:

- Establecer los requisitos de seguridad aplicables a la información (niveles de seguridad de la información) y a los Servicios (niveles de seguridad de los servicios), dentro del marco establecido en el Anexo I del RD ENS, pudiendo recabar una propuesta del Responsable de Seguridad y teniendo en cuenta la opinión del Responsable del Sistema.
- Dictaminar respecto a los derechos de acceso a la información y los servicios.
- Aceptar los niveles de riesgo residual que afectan a la información y los servicios.
- Poner en comunicación del Responsable de Seguridad cualquier variación respecto a la Información y los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios o Información a su cargo. El cual dará traslado de dichos cambios, al Comité de Seguridad de la Información, en su próxima reunión.
- Tiene la responsabilidad última del uso que se haga de determinados servicios e información y, por tanto, de su protección.

6.1.2. Responsable de Seguridad (RSEG)

Serán funciones del Responsable de Seguridad:

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los Servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la Declaración de Aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias y elaborar documentación del sistema.

- Aprobar la Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS, todo ello lugar aparte a este documento.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad TIC.
- 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 del sistema.
- Aprobar los procedimientos de seguridad que forman parte del Marco Normativo (y no sean competencia del Comité) y poner en conocimiento al Comité de las modificaciones que se hayan realizado a lo largo del periodo en curso.
- Participará en la elaboración, en el marco del Comité de Seguridad de la Información, la Política de Seguridad de la Información, para su aprobación por Dirección.
- Actuará como Secretario del Comité de Seguridad de la Información, realizando las siguientes funciones:
    - 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.
    - Es responsable de la ejecución directa o delegada de las decisiones del Comité.

6.1.3. Responsable del Sistema (RSIS)

Serán funciones del Responsable del Sistema:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, elaborando los procedimientos operativos necesarios.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Detener el acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable de Seguridad y/o Comité de Seguridad de la Información 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.
- Coordinar las funciones del administrador de la seguridad del 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 del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
    - Aprobar los cambios en la configuración vigente del Sistema de Información.

- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar 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 ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.
- Informar al Responsable de Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

6.1.4. Delegado de Protección de Datos (DPD)

Serán funciones del Delegado de Protección de Datos:

- Informar y asesorar a la organización, y a los usuarios que se ocupen del tratamiento, de las obligaciones que les incumben en virtud de la normativa vigente en materia de Protección de Datos.
- Supervisar el cumplimiento de lo dispuesto en normativa de seguridad y de las políticas internas de la organización, en materia de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisará su aplicación.
- Cooperar con la Agencia Española de Protección de Datos cuando ésta lo requiera, actuando como punto de contacto con ésta para cuestiones relativas al tratamiento de datos.
- El Delegado de Protección de datos desempeñará sus funciones prestando atención a los riesgos asociados a las operaciones de tratamiento. Para ello debe ser capaz de:
    - Recabar información para determinar las actividades de tratamiento.
    - Analizar y comprobar la conformidad de las actividades de tratamiento.
    - Informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
    - Recabar información para supervisar el registro de las operaciones de
    - tratamiento.
    - Asesorar en el principio de la protección de datos por diseño y por defecto.
    - Asesorar sobre si se lleva a cabo o no las evaluaciones de impacto, metodología, salvaguardas a aplicar, etc.
    - Priorizar actividades en base a los riesgos.
    - Asesorar al Responsable de Tratamiento sobre áreas a cometer a auditorías, actividades de formación a realizar y operaciones de tratamiento a dedicar más tiempo y recursos.

6.2. Comité de Seguridad de la Información

En la organización, se ha creado el Comité de Seguridad de la Información que estará compuesto por los siguientes miembros:

- Presidencia
- Secretario
- Vocales

Estos miembros se clasificarán en permanentes o no permanentes ateniendo a la obligatoriedad de la participación en el Comité de Seguridad de la Información:

Miembros permanentes:

- Presidencia.
- Responsable de Seguridad.
- Responsable del Sistema.

Miembros no permanentes:

- Responsables del Servicio.
- Responsable de la Información
- Delegado de Protección de datos.
- Representantes de la organización, especialistas externos de los sectores público, privado, cuya presencia, por razón de su experiencia o vinculación con los asuntos tratados, sea necesaria o aconsejable.
- Asesores que se consideren oportunos para los temas en cuestión (con voz, pero sin voto).

Los Responsables de la Información y los Servicios serán convocados por la presidencia en función de los asuntos a tratar, en representación de los distintos ámbitos o áreas de seguridad TIC. Cada área estará representada por un vocal con voto, sin perjuicio de que acudan varios representantes de esta.

El Delegado de Protección de Datos participará con voz, pero sin voto en las reuniones del Comité de seguridad de la información cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiese a votación, se hará constar siempre en acta la opinión del Delegado de Protección de Datos.

El Secretario/a del Comité realizará las convocatorias y levantará actas de las reuniones del Comité de Seguridad. A las sesiones del Comité de Seguridad podrán asistir en calidad de asesores las personas que en cada caso estime pertinentes su Presidente.

6.2.1. Roles del Comité de Seguridad

- **Presidencia**: Sub-Director.
- **Secretario:** Responsable de Asesoría Jurídica
- **Vocales**: Recursos Humanos, Finanza, Taller, Comercial.
- **Responsable del Sistema**: Administrador de Sistema.
- **Responsable de Seguridad**: Externo.
- **Delegado de Protección de Datos**: Externo.

- **Responsable de la Información**:
    - Información 1: Producción.
    - Información 2: Producción.
- **Responsable del Servicio**:
    - Servicio 1: Producción.
    - Servicio 2: Producción.

6.2.2. Atribuciones del Comité de Seguridad

Serán funciones del Comité de Seguridad:

- Atender las inquietudes de la Alta Dirección y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Alta Dirección.
- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la estrategia de evolución en lo que respecta a la seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar documentación de seguridad de la información.
- Estar permanentemente informado de la normativa que regula la Certificación de Conformidad con el ENS, incluyendo sus normas de acreditación, certificación, guías, manuales, procedimientos e instrucciones técnicas.
- Estar permanentemente informado de la relación de Entidades de Certificación acreditadas y organizaciones, públicas y privadas, certificadas.
- Estar perm000anentemente informado de la relación de esquemas de certificación de la seguridad con los que la Administración Pública tiene establecidos arreglos o acuerdos de reconocimiento mutuo de certificados.
- Proponer directrices y recomendaciones, que serán recogidas en las correspondientes actas de las reuniones del Comité, a las que su presidente, deberá dar cumplida respuesta.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Atender las inquietudes, en materia de Seguridad de la Información, de la Administración y de las diferentes áreas, informando regularmente del estado de la seguridad de la información a la Dirección.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes Departamentos, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Asesorar en materia de seguridad de la información, siempre y cuando le sea requerido.
- Revisar la Política de Seguridad de la Información previa aprobación por el Órgano Superior.

6.2.3. Periodicidad de la reuniones y adopción de acuerdos

- El Comité de Seguridad de la Información se reunirá, al menos, una vez al año, sin perjuicio de que, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera de una mayor frecuencia en las reuniones.

- En cualquier caso, las reuniones se convocarán por su Presidencia, a través del Secretario, a su iniciativa o por mayoría de sus miembros permanentes.
- Las decisiones se adoptarán por consenso de los miembros permanentes.

6.3. Designación y resolución de conflictos

- La creación del Comité de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta Política, se realizará a través de un acta de constitución inicial.
- Los roles nombrados se renovarán anualmente de forma automática. Las bajas o modificaciones en los roles designados, se comunicarán al Comité y se seguirán los cauces establecidos para la designación del nuevo responsable.
- Tal y como se regula en el artículo 13.3 del RD del ENS, se estipula que no puede existir dependencia jerárquica entre el RSEG y el RSIS, salvo excepciones justificadas, lo que conllevará a disponer de medidas compensatorias para garantizar la finalizad del principio de diferenciación de responsabilidades.

7. Tratamiento de datos personales

SALCAI UTINSA S.A. trata datos de carácter personal, según se describe en el Registro de Actividades del Tratamiento. **SALCAI UTINSA S.A.** deberá evaluar los riesgos relacionados con los datos personales tratados proponiendo un plan de actuación para la corrección de aquellos riesgos que superen el umbral autorizado.

El análisis de riesgos será reevaluado de forma periódica, contando con el asesoramiento y supervisión que realice el Delegado de Protección de Datos, y, en todo caso, cuando se detecte un tratamiento de alto riesgo, debiendo realizar, en su caso, una evaluación de impacto. La implementación del plan de tratamiento del riesgo se coordinará con el del ENS, así como el resto de procedimientos o normas de seguridad con las derivadas de las obligaciones en materia de protección de datos, especialmente en el control de los prestadores de servicios o la respuesta a incidentes y/o brechas de seguridad.

8. Gestión de Riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando se produzcan cambios en la información manejada.
- Cuando se produzcan cambios en los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.
- Cuando se produzcan modificaciones en el análisis de riesgos de protección de datos o en las evaluaciones de impacto.

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

Se tendrán en cuenta los riesgos en protección de datos, contando con la opinión del Delegado de Protección de Datos, además se coordinarán los planes del tratamiento del riesgo.

9. Desarrollo de la Política de Seguridad de la Información

La presente Política de Seguridad de la Información será complementada con documentos más precisos (normas, procedimientos de seguridad e instrucciones técnicas) que ayudan a llevar a cabo lo propuesto.

El cuerpo normativo se desarrollará en tres niveles:

i. **Primer nivel normativo**: constituido por la presente Política de Seguridad de la Información.
ii. **Segundo nivel normativo**: constituido por las normas de seguridad derivadas de las anteriores con el objetivo de indicar el uso correcto de aspectos concretos del sistema de gestión de seguridad de la información.
iii. **Tercer nivel normativo**: constituido por procedimientos de seguridad, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la Política de Seguridad de la Información, determinan las acciones o tareas a realizar en el desempeño de un proceso.

Corresponde a la dirección, la aprobación de la Política de Seguridad de la Información y siendo el Comité de Seguridad de la Información el órgano responsable de la aprobación y difusión de los restantes documentos propios de la organización, todo ello tal y como se establece en el artículo 12 del RD ENS.

Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas.

10. Obligaciones del personal

Todos los miembros de **SALCAI UTINSA S.A.** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y las normas, procedimientos o guías que la desarrollen, siendo responsabilidad de **SALCAI UTINSA S.A.** a través del Comité de Seguridad y del área de personal de disponer de los medios necesarios para que la información llegue a los afectados.

Todos los miembros de **SALCAI UTINSA S.A.** atenderán a una sesión de concienciación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de **SALCAI UTINSA S.A.**, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para

realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera designación o si se trata de un cambio de puesto de trabajo o de responsabilidad en el mismo.

11. Terceras partes

Cuando **SALCAI UTINSA S.A.** preste servicios a otras entidades o maneje información de otras, se les hará partícipes de esta Política de Seguridad de la Información, sin perjuicio de respetar las obligaciones de la normativa de protección de datos si actúa como encargado del tratamiento en la prestación de los citados servicios, y se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y procedimientos de actuación para la reacción ante incidentes de seguridad. Además, el Responsable de Seguridad (o persona en quien delegue) será el Punto de Contacto (POC).

Cuando **SALCAI UTINSA S.A.** utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información, sin perjuicio del cumplimiento de otras obligaciones en materia de protección de datos. En la contratación de prestados de servicios o adquisición de productos se tendrá en cuenta la obligación del adjudicatario de cumplir con el ENS.

En la adquisición de derechos de uso de los activos en la nube tendrá en cuenta los requisitos establecidos en las medidas de seguridad del Anexo II y las Guías de desarrollo.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla, de modo que **SALCAI UTINSA S.A.** pueda supervisarlos o solicitar evidencias del cumplimiento de estos, incluso auditorías de segunda o tercera parte. Se establecerán procedimientos específicos de reporte y resolución de incidencias que deberán ser canalizados por el POC de los terceros implicados y, además, cuando se afecte a datos personales por el Delegado de Protección de datos. Los terceros garantizarán que su personal está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política o el que específicamente se pueda exigir en el contrato.

Cuando algún aspecto de la Política no pueda ser satisfecho por un tercero según se requiere en los párrafos anteriores, el Responsable de Seguridad emitirá un informe que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los Responsables de la Información y los Servicios afectados antes del inicio de la contratación o, en su caso, la adjudicación. El informe se trasladará al representante de la organización que deberá autorizar la continuación con la tramitación de contratación del tercero, asumiendo los riesgos detectados.

Cuando la organización adquiera, desarrolle o implante un sistema de Inteligencia Artificial, además de cumplir con lo establecido en la normativa vigente en la materia, deberá contar con el informe del Responsable de Seguridad, que consultará al Responsable de la Información y los Servicios y, cuando sea necesario, al del Sistema, debiendo también el Delegado de Protección de Datos emitir su parecer.

12. Gestión de incidentes de seguridad

SALCAI UTINSA S.A. dispondrá de un procedimiento para la gestión ágil de los eventos e incidentes de seguridad que supongan una amenaza para la información y los servicios.

Este procedimiento se integrará con otros relacionados con los incidentes de seguridad de otras normas sectoriales como la de protección de datos personales u otra que afecte al organismo para coordinar la respuesta desde los diferentes enfoques y comunicar a los diferentes organismos de control sin dilaciones indebidas y, cuando sea preciso, a las Fuerzas y Cuerpos de Seguridad del Estado o los juzgados.

13. Aprobación y entrada en vigor

Esta Política de Seguridad de la Información, será efectiva desde su fecha de aprobación y hasta que sea reemplazada por una nueva Política.

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

Texto aprobado el día 24 de diciembre de 2025 mediante firma del acta 001/2025 por **SALCAI UTINSA S.A.**.