POLÍTICA DE **SEGURIDAD DE LA INFORMACIÓN**

ALEA SOLUCIONES SL, empresa dedicada a:

Desarrollo de soluciones y sistemas para el operador de telecomunicaciones, soporte técnico para la gestión y mantenimiento de sus redes FTTH y comercialización de equipamiento IP y transmisión y acceso.

ha decidido implantar un Sistema de Gestión de la Seguridad de la Información basado en la norma **ISO 27001:2022** y el **Esquema Nacional de Seguridad (ENS)** con el objetivo de preservar la confidencialidad, integridad, disponibilidad, uso previsto, valor de la información y los servicios de la información, y protegerla de un amplio grupo de amenazas. Este Sistema de Gestión está destinado a asegurar la continuidad de las líneas de negocio, minimizar los daños ante actos de intrusión y la mejora continua.

La Dirección de **ALEA SOLUCIONES SL** es consciente de que la información es un activo que tiene un elevado valor para la organización y requiere por tanto una protección adecuada. Por ello establece como objetivos estratégicos y principios para la seguridad de la información los siguientes:

- La protección de los datos de carácter personal y la intimidad de las personas
- La salvaguarda de los registros de la organización
- La protección de los derechos de propiedad intelectual
- La documentación de la política de seguridad de la información
- La asignación de responsabilidades de seguridad
- La formación, capacitación y concienciación para la seguridad de la información
- El registro de las incidencias de seguridad
- La gestión de la continuidad del negocio
- La gestión de los cambios que pudieran darse en la empresa relativos a la seguridad.

La Dirección de **ALEA SOLUCIONES SL**, mediante la elaboración e implantación del presente Sistema de Gestión de Seguridad de la Información adquiere los siguientes compromisos:

- Desarrollar productos y servicios conforme con los requisitos legales, identificando para ello las legislaciones de aplicación a las líneas de negocio desarrolladas por la organización e incluidas en el alcance del Sistema de Gestión de la Seguridad de la Información.
- Establecer y cumplir los requisitos contractuales con las partes interesadas.
- Definir los requisitos de formación en seguridad y proporcionar la formación necesaria en dicha materia a las partes interesadas mediante el establecimiento de planes de formación.
- Prevenir y detectar software malicioso mediante el desarrollo de políticas específicas y el establecimiento de acuerdos contractuales con organizaciones especializadas.
- Gestionar la continuidad del negocio, desarrollando planes de continuidad conforme a metodologías de aceptación general.
- Establecer las consecuencias de las violaciones de la política de seguridad, las cuales serán reflejadas en los contratos firmados con las partes interesadas.
- Actuar en todo momento dentro de la más estricta ética profesional.

Esta Política proporciona el marco de referencia para la mejora continua y para establecer y revisar los objetivos del Sistema de Gestión de Seguridad de la Información. Es comunicada a toda la

Organización a través del gestor documental instalado en **ALEA SOLUCIONES SL** y su publicación en paneles informativos, siendo revisada anualmente para su adecuación y extraordinariamente cuando concurran situaciones especiales y/o cambios sustanciales en la Gestión de la Seguridad de la Información, estando a disposición público en general.

Con esta declaración de Política de Seguridad de la Información, **ALEA SOLUCIONES SL,** reconoce que los diferentes departamentos de la empresa deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema. En este sentido las áreas organizativas deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, según se indica a continuación:

Prevención: Las áreas organizativas deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por las normas **ISO 27001:2022** y el **Esquema Nacional de Seguridad (ENS)**, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados. Para garantizar el cumplimiento de la política, las áreas deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad.
- Solicitar la revisión periódica independiente por parte de terceros.

Detección: Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

Respuesta: Las áreas organizativas deben:

- 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 o en partes interesadas.
- 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).

Recuperación: Para garantizar la disponibilidad de los servicios críticos, los áreas deben seguir los planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

ALCANCE DE APLICACIÓN DE LA POLÍTICA: Esta política se aplica a todos los sistemas TIC de **ALEA SOLUCIONES SL** y a todos los miembros de la organización, sin excepciones. Toma en cuenta la misión y visión de la empresa, a las cuales da protección; a su marco normativo y organización.

> **MISIÓN: ALEA Soluciones SL,** es una empresa especializada en automatizar, optimizar y rentabilizar los despliegues de red de acceso y networking de nuestros clientes dotándolos, no solo del mejor equipamiento proveniente de nuestros partners, sino también de soluciones in-house que permitan la gestión y optimización de sus redes, de forma agregada, focalizada y amigable; así como la automatización de sus procesos.

VISIÓN: En **ALEA Soluciones SL,** creemos en un mundo hiperconectado, optimizado en recursos de red de usuario y libre de fallos. Creemos en sistemas amigables y eficientes que minimicen la intervención humana automatizando al máximo los procesos.

MARCO NORMATIVO RELACIONADO A LA SEGURIDAD DE LA INFORMACIÓN

- Ley 11/2022, de 28 de junio, General de Telecomunicaciones. *Boletín Oficial del Estado* (BOE núm. 154, de 29 de junio de 2022).
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (transposición de la Directiva NIS).
- Reglamento (UE) 2019/881, de 17 de abril de 2019 (Reglamento de Ciberseguridad de la UE).
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a medidas para un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifica el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y se deroga la Directiva (UE) 2016/1148 (Directiva NIS 2). En proceso de trasposición mediante anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad.

FUNCIONES Y RESPONSABILIDADES EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

Comité

El Comité de Seguridad TIC, reportará a la dirección y estará formado por el responsable del sistema de gestión de seguridad de la información, el representante del área de operaciones, el representante de sistemas, el representante de desarrollo, el representante del negocio, el responsable de soporte de TI.

Secretario del Comité de Seguridad TIC

El secretario del Comité de Seguridad TIC será el responsable de los sistemas de información y tendrá como funciones:

1. Mantener actualizado al comité de los cambios en las tecnologías que sean aplicables. La información deberá considerar el impacto que las nuevas tecnologías tendrán en los procesos de negocio.

2. Implementar los procedimientos de uso de los servicios TIC. Los procedimientos deben estar aprobados por el Comité de seguridad.
3. Ejecutar las instrucciones emanadas de seguridad informática y del Comité de Seguridad de TI.
4. Presentar regularmente informes sobre el estado de seguridad de los servicios TIC.
5. Preparar informes sobre incidentes graves de seguridad de la información y presentarlos a la alta dirección **ALEA SOLUCIONES SL**, las instancias definidas y al Comité de Seguridad.
6. Realizar el análisis de riesgos de los sistemas TIC, presentarlo a la Alta Dirección y al Comité de Seguridad. El análisis deberá realizarse al menos una vez al año con independencia de las actividades específicas de inteligencia de amenazas y otras medidas tomadas para la gestión del riesgo.
7. Realizar regularmente verificaciones de seguridad según un plan determinado y aprobado por el Comité de Seguridad. Tomando las medidas correctivas y preventivas cuando sea necesario.
8. Verifica que se mantengan los principios de segregación de tareas, mínimos privilegios y seguridad en los accesos.
9. Coordinar la respuesta ante incidentes, la investigación forense y la causa raíz, presentando las acciones correctivas y las lecciones aprendidas.

El Comité de Seguridad TIC tendrá las siguientes funciones:

1. Definir, aprobar y publicar la política de seguridad de la información conforme al Esquema Nacional de Seguridad y los requisitos establecidos en la norma ISO 27001:2022.
2. Validar los nombramientos de los roles clave para la seguridad de la información, asignando responsabilidades.
3. Actuar como coordinador entre diferentes áreas y normativas implicadas en la seguridad de las operaciones, sistemas de TI, compliance, protección de datos, entre otras aplicables.
4. Supervisar la implantación del Sistema de Gestión de Seguridad de la Información (SGSI) y su efectividad técnica y de cumplimiento del Esquema Nacional de Seguridad (ENS).
5. Aprobar los criterios para el análisis y tratamiento de riesgos en los sistemas TIC.
6. Revisar y aprobar la documentación de seguridad: políticas, normativa interna, directrices operativas.

Funciones y Responsabilidades del Responsable de la Seguridad de la Información

1. Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en esta Política de Seguridad de la Información.
2. Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
3. Determinar los niveles de seguridad requeridos en la dimensión alta del Esquema Nacional de Seguridad (ENS).
4. Verificar la satisfacción de los requisitos establecidos en la Norma ISO 27001:2022 y su anexo A: Declaración de Aplicabilidad.
5. Realizar el análisis de riesgo y aceptar el riesgo residual.
6. Gestionar la configuración de la seguridad.
7. Gestionar la documentación de seguridad del sistema
8. Informar al Comité de seguridad y a la alta dirección de la gestión realizada.

9. Atender revisiones y auditorías de la seguridad de la información.

ROLES: Funciones y Responsabilidades del Responsable de los Sistemas de TI

1. Atender los requerimientos de seguridad en la prestación del servicio de TI
2. Notificar las incidencias de seguridad.
3. Implementar las medidas de resiliencia y continuidad del servicio cuando se encuentre bajo ataque o haya superado una acción de intrusión indebida.

ROLES: Funciones y Responsabilidades del Responsable de las Operaciones

1. Atender los requerimientos de seguridad en las operaciones
2. Notificar las incidencias de seguridad.
3. Implementar las medidas de resiliencia y continuidad del servicio cuando se encuentre bajo ataque o haya superado una acción de intrusión indebida.

PROCEDIMIENTOS DE DESIGNACIÓN: El Responsable de Seguridad de la Información será nombrado por el Director a propuesta del Comité de Seguridad TIC. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN: Será misión del Comité de Seguridad TIC la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la Dirección y difundida para que la conozcan todas las partes afectadas.

DATOS DE CARÁCTER PERSONAL: ALEA SOLUCIONES SL trata datos de carácter personal. El Registro de Actividades de Tratamiento, al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de **ALEA SOLUCIONES SL** se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

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 cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

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

DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN: Esta Política de Seguridad de la Información complementa las políticas de seguridad de **ALEA SOLUCIONES SL** implementadas dentro del marco de gobernanza establecido.

Esta Política se desarrollará por medio de normativas de seguridad que afronten aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. La política de seguridad estará disponible impresa en el tablón de anuncios y en la página web de la empresa.

OBLIGACIONES DEL PERSONAL: Todos los miembros de **ALEA SOLUCIONES SL** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de **ALEA SOLUCIONES SL** atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de **ALEA SOLUCIONES SL,** 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 asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo

TERCERAS PARTES: Cuando **ALEA SOLUCIONES SL** preste servicios a otras organizaciones o maneje información de otros, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando **ALEA SOLUCIONES SL** 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. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se solicitará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un 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 de la información y los servicios afectados antes de seguir adelante.

En Madrid, 01 de diciembre 2025

Dirección

Firmado Digitalmente por - Francisco Bonachela Lorente en representación de ALEA SOLUCIONES SL ***2300** FRANCISCO BONACHELA (R: ****9863*) el día 18/12/2025 con un certificado emitido por AC Representación