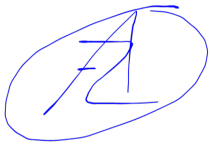
ID Proceso de firma electrónica avanzada: 09c249ad-c1e1-4030-a5e8-7099154bc862
Documento firmado electrónicamente a través de Signaturit Solutions, S.L.U. en 30/06/2025 08:41:45 UTC

Política de Seguridad de la Información

Aprobación del documento		
Cargo	Nombre	Firma
Dirección	Agustín Izzo Díaz	 4a3d6d3d-88c9-3535-a32e-d17fe02779de 2025-06-30 08:39:27 UTC
Responsable de Seguridad	Adolfo Trocolí Naranjo	 e618cc9f-ca93-37dd-b34a-558ae36fae7f 2025-06-30 08:41:41 UTC

Control de versiones			
Versión	Fecha	Responsable	Cambios
01	22/11/2024	Adolfo Trocolí	Versión inicial del documento.
02	18/02/2025	Adolfo Trocolí	Adecuación ENS.
03	26/06/2025	Adolfo Trocolí	Adición de sociedades.

ID Proceso de firma electrónica avanzada: 09c249ad-c1e1-4030-a5e8-7099154bc862
Documento firmado electrónicamente a través de Signaturit Solutions, S.L.U. en 30/06/2025 08:41:45 UTC

Índice de contenidos

ID Proceso de firma electrónica avanzada: 09c249ad-c1e1-4030-a5e8-7099154bc862
Documento firmado electrónicamente a través de Signaturit Solutions, S.L.U. en 30/06/2025 08:41:45 UTC

1 Introducción

La presente Política de Seguridad de la Información (en adelante, Política) persigue la adopción de un conjunto de medidas destinadas a preservar la confidencialidad, integridad, y disponibilidad de la información.

Tiene como objetivo definir los principios en base a los que deberán diseñarse los Sistemas de Gestión de Seguridad de la Información (en adelante SGSIs) para TUCA BIDCO S.L. y sus sociedades participadas, excluyendo a CENTAURUS BIDCO S.L., cuya política será acordada con el resto de socios (en adelante, "Olin Group" o "el grupo").

Esta Política de Seguridad también sigue los requisitos del Esquema Nacional de Seguridad (en adelante ENS) y de la guía CCN-STIC-805 del Centro Criptológico Nacional (CCN), centro adscrito al Centro Nacional de Inteligencia (CNI).

Los principios básicos por los cuales se rige esta política son los especificados en los siguientes apartados.

1.1 Prevención

Olin Group debe 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 implementará las medidas mínimas de seguridad determinadas por el 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, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, se debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

1.2 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

ID Proceso de firma electrónica avanzada: 09c249ad-c1e1-4030-a5e8-7099154bc862
Documento firmado electrónicamente a través de Signaturit Solutions, S.L.U. en 30/06/2025 08:41:45 UTC

la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.

La monitorización es especialmente relevante cuando se establecen líneas de defensa. 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.

1.3 Respuesta

Con respecto a la respuesta ante incidentes, Olin Group:

- Establecerá mecanismos para responder eficazmente a los incidentes de seguridad.
- Designará un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecerá protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

1.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, Olin Group dispondrá de planes de continuidad de los sistemas TIC como parte de su plan general de continuidad del servicio y actividades de recuperación.

2 Misión

La misión de Olin Group es consolidar y hacer crecer operadores locales de telecomunicaciones, ofreciendo conexiones de alta velocidad con un enfoque en la proximidad, calidad del servicio y simplicidad. Buscamos proporcionar soluciones mayoristas y minoristas que permitan a nuestros clientes acceder a servicios de telecomunicaciones eficientes y competitivos.

3 Alcance

La Política es aplicable para Olin Group, que deberá cumplir esta especificación sin perjuicio de tener políticas propias más restrictivas en cada sociedad participada.

ID Proceso de firma electrónica avanzada: 09c249ad-c1e1-4030-a5e8-7099154bc862
Documento firmado electrónicamente a través de Signaturit Solutions, S.L.U. en 30/06/2025 08:41:45 UTC

Este cumplimiento deberá ser reportado y coordinado con la matriz del grupo. El alcance de la presente Política abarca toda la información de las empresas del grupo con independencia de cómo sea almacenada, procesada, y de si el formato es físico o electrónico.

Con respecto a las entidades del grupo, las actividades de seguridad serán coordinadas desde la sociedad matriz, quien deberá atender a las necesidades específicas de cada empresa.

La firma de este documento implica la puesta en marcha de las actividades de planificación y coordinación de las actividades necesarias para que todas las sociedades del grupo se adapten al nivel de seguridad requerido en esta Política.

3.1 Alcance de certificación ENS

Sistemas de información de que dan soporte a los servicios de:

- Internet fibra óptica.
- Internet radio.
- Telefonía móvil.
- Telefonía fija.
- Televisión.
- Comercialización de servicios de alarma y vigilancia.
- Servicios de despliegue y gestión de red.
- Servicio mayorista de fibra óptica.

4 Marco Normativo

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- 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).
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.

ID Proceso de firma electrónica avanzada: 09c249ad-c1e1-4030-a5e8-7099154bc862
Documento firmado electrónicamente a través de Signaturit Solutions, S.L.U. en 30/06/2025 08:41:45 UTC

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).

5 Organización de la seguridad

En los siguientes apartados se especifican los miembros del Comité de Seguridad, así como las funciones atribuidas a cada uno de sus roles.

5.1 Miembros del Comité de Seguridad

El Comité de Seguridad coordina la seguridad de la información en Olin Group y está formado por:

- **Responsable de la Información:** Enrique Gurrea-Nozaleda Hörnlein.
- **Responsable del Servicio**: Enrique Gurrea-Nozaleda Hörnlein.
- **Responsable de Seguridad:** Adolfo Trocolí Naranjo.
- **Responsable del Sistema:** Miguel Alcón Vargas.

Además, existirán perfiles con rol operativo en las sociedades participadas, con título de Responsable del Sistema Delegado:

- **Olin:** Juan Giménez García.
- **Fibranet:** Raúl Leal Hernández.
- **XTA:** Joan Llopart Cudié.
- **Cartago Telecom:** Lorenzo García Martínez.
- **ClubTV:** Lorenzo García Martínez.
- **Comenersol:** Javier Rico Albert.
- **Mowitel:** Javier Macías Sánchez.
- **Conecta-T:** Víctor Hugo Romero Martín.
- **AIONQTALON:** Jose Antonio Montero Navarro.
- **Fibralink:** Ricard Cloquells Rivero.
- **Telecable Almonte:** Fernando Torres Llanos.
- **Waytel:** Álvaro Vargas Marín.

ID Proceso de firma electrónica avanzada: 09c249ad-c1e1-4030-a5e8-7099154bc862
Documento firmado electrónicamente a través de Signaturit Solutions, S.L.U. en 30/06/2025 08:41:45 UTC

- **Youtel:** Jerónimo Jesús Rodríguez Macías.
- **Giganet:** Pepe Moreno.
- **Netcan:** Javier Gracia.

5.2 Responsable de la Información

Será el responsable de:

- Los activos esenciales de tipo información, es decir, el responsable de las decisiones relativas a la información.
- Velar por el buen uso de la información y, por tanto, de su protección.
- Cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Establecer los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información.

5.3 Responsable del Servicio

Será el responsable de:

- Es el responsable de los activos esenciales de tipo servicio, es decir, el responsable de las decisiones relativas a los servicios.
- Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
- Determinar los niveles de seguridad de los servicios.

5.4 Responsable de Seguridad

Es el Responsable de Seguridad de la Información de acuerdo al Esquema Nacional de Seguridad, y tiene las siguientes responsabilidades:

- Asegura que los procesos del Sistema de Gestión están establecidos, implantados y mantenidos, de acuerdo con los requisitos de las normas aplicables.
- Informa a la Dirección del funcionamiento y eficacia del sistema para que ésta lleve a cabo la revisión, y como base para la mejora de la gestión de la empresa.
- Promueve el conocimiento de los requisitos de los clientes en materia de Seguridad de la Información a todos los niveles de la organización.

ID Proceso de firma electrónica avanzada: 09c249ad-c1e1-4030-a5e8-7099154bc862
Documento firmado electrónicamente a través de Signaturit Solutions, S.L.U. en 30/06/2025 08:41:45 UTC

- Colabora con la Dirección en la definición e implantación de Políticas y Normativas de forma que sean fiel reflejo de la estrategia de la empresa.
- Planifica, programa y participa, cuando proceda, en las auditorías internas y externas.
- Controla la elaboración, actualización, aprobación y distribución de la documentación del Sistema de Gestión.
- Actúa como interlocutor con partes externas (clientes, proveedores, Administración, y demás partes interesadas) sobre aspectos del sistema de gestión.
- Controla la ejecución y eficacia de las acciones emprendidas para prevenir y gestionar No Conformidades, y valora las acciones a realizar tras la comunicación de una sugerencia de mejora.

5.5 Responsable del Sistema

Será el responsable de:

- Los activos no esenciales, es decir, la persona que es responsable de las decisiones relativas a todos los elementos del sistema de información de Olin Group salvo los servicios e información esenciales.
- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- La administración y gestión de las cuentas de los usuarios.
- Asegurarse de que sólo las personas autorizadas a tener acceso cuentan con él.
- Asegurarse de que los sistemas tienen los niveles de disponibilidad requeridos por la Organización.
- Incluir en los requisitos para nuevos desarrollos los aspectos de seguridad que apliquen.

ID Proceso de firma electrónica avanzada: 09c249ad-c1e1-4030-a5e8-7099154bc862
Documento firmado electrónicamente a través de Signaturit Solutions, S.L.U. en 30/06/2025 08:41:45 UTC

5.6 Procedimiento de designación

El desempeño de las responsabilidades definidas en esta Política de Seguridad vendrá determinado por el acceso a los diferentes cargos que se le hayan vinculado. En el caso de que alguno de estos puestos desaparezca o cambie de nombre, será responsabilidad del CEO de Olin Group asignar el nuevo puesto al que se vinculará la figura.

5.7 Procedimientos de resolución de conflictos

En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Comité de Seguridad.

6 Información documentada

Para desarrollar este Sistema de Gestión se dispone de una estructura documental compuesta por:

- Política de Seguridad, la presente política: documento donde se establecen las bases del Sistema de Gestión de la empresa.
- Normativa, documentación donde se definen los usos permitidos o prohibidos en la organización.
- Procedimientos: describen las actividades requeridas para implementar el Sistema de Gestión para dar cumplimiento a requisitos exigidos por alguna de las normas aplicables.
- Instrucciones Técnicas: cualquier procedimiento que precise la intervención necesaria de determinados elementos y que requiera indicaciones específicas relacionadas con actividades críticas para satisfacer un objetivo se desarrollará en una instrucción técnica o de trabajo.

Los diferentes documentos tienen la extensión adecuada para asegurar el funcionamiento efectivo del Sistema y de la organización y el control de los procesos, en función de la complejidad del proceso, la interacción de los distintos procesos y la competencia del personal que intervenga.

ID Proceso de firma electrónica avanzada: 09c249ad-c1e1-4030-a5e8-7099154bc862
Documento firmado electrónicamente a través de Signaturit Solutions, S.L.U. en 30/06/2025 08:41:45 UTC

6.1 Control de la documentación del Sistema de Gestión

Olin Group tiene establecido, y mantiene al día, el procedimiento PS.12 Gestión del SGSI donde se describe cómo debe realizarse el control de la documentación del Sistema, donde se describen los criterios y responsabilidades asociadas al control de los documentos necesarios para el funcionamiento del Sistema de Gestión.

7 Desarrollo de la política de gestión de seguridad de la información

7.1 Requisitos mínimos de seguridad

A continuación, se enuncian los principios básicos relacionados con la seguridad de la información (art. 11 ENS), que rigen la política de seguridad de la información de la organización:

- Resolución de conflictos. Ver apartado "Procedimientos de resolución de conflictos" de este documento.
- Organización e implantación del proceso de seguridad. Ver apartado "Organización de la Seguridad" de la presente política.
- Análisis y gestión de los riesgos. Ver procedimiento "Análisis de riesgos".
- Gestión de personal. Ver procedimiento "Gestión del Personal".
- Profesionalidad. Ver apartado "Obligaciones del Personal" de la presente política.
- Autorización y control de los accesos. Ver procedimiento "Autorización".
- Protección de las instalaciones. Ver procedimiento "Seguridad Física".
- Adquisición de productos. Ver procedimiento "Gestión de proveedores".
- Mínimo privilegio. Ver procedimiento "Seguridad Lógica".
- Integridad y actualización del sistema. Ver procedimiento "Seguridad Lógica".
- Protección de la información almacenada y en tránsito. Ver procedimiento "Control de accesos".
- Prevención ante otros sistemas de información interconectados. Ver procedimiento "Seguridad Lógica".
- Registro de actividad. Ver procedimiento "Seguridad Lógica".

ID Proceso de firma electrónica avanzada: 09c249ad-c1e1-4030-a5e8-7099154bc862
Documento firmado electrónicamente a través de Signaturit Solutions, S.L.U. en 30/06/2025 08:41:45 UTC

- Incidentes de seguridad. Ver procedimiento "Gestión de Incidentes".
- Continuidad de la actividad. Ver procedimiento "Gestión de la continuidad".
- Mejora continua del proceso de seguridad. Tal como se especifica en esta política, el Comité de Seguridad y los responsables promoverán la mejora continua, de forma que se planifiquen y realicen objetivos y acciones de mejora (Apartado "Organización de la Seguridad").

7.2 Política de clasificación de datos

El sistema de clasificación de datos se puede aplicar a toda la información en posesión de Olin Group. El uso coherente del sistema de clasificación de datos es esencial para proteger adecuadamente la información y los sistemas de información.

7.3 Gestión de riesgos

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

- Regularmente, al menos una vez al año.
- Cuando la información que se maneja cambia.
- Cuando cambian los servicios prestados.
- Cuando ocurre un incidente de seguridad grave.
- Cuando se informa de vulnerabilidades graves.

Para la armonización del análisis de riesgos, el Comité de Seguridad establecerá una evaluación de referencia para los diferentes tipos de información gestionada y los diferentes servicios prestados.

7.4 Obligaciones del Personal

Todo el personal de Olin Group tiene la obligación de conocer y cumplir esta Política de Seguridad de la Información y las otras normativas de seguridad desarrolladas, siendo responsabilidad del Comité de Seguridad brindar los medios necesarios para que la información llegue a los afectados.

Todo el personal de Olin Group bajo el alcance del ENS recibirá concienciación y formación en materia de seguridad de la información.

ID Proceso de firma electrónica avanzada: 09c249ad-c1e1-4030-a5e8-7099154bc862
Documento firmado electrónicamente a través de Signaturit Solutions, S.L.U. en 30/06/2025 08:41:45 UTC

En su caso, si se requiere formación específica para la gestión segura de los sistemas, las personas responsables de la operación o administración de los sistemas de información la recibirán según sea necesario para realizar su trabajo.

Dentro de la relación laboral o contractual, los empleados deberán desempeñar siempre las funciones asignadas con profesionalidad, es decir, realizar un ejercicio adecuado de la profesión con capacidad y eficacia.

7.5 Terceras Partes

Cuando Olin Group preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. Para ello, se establecerán canales de reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para reaccionar ante incidentes de seguridad.

Cuando Olin Group utilice servicios de terceros o ceda información a terceros, se les hará partícipe de los requisitos de seguridad que deben cumplir. Además, el proveedor debe garantizar que su personal esté adecuadamente capacitado en materia de seguridad de acuerdo con los requisitos de Olin Group.

Se ha desarrollado un procedimiento específico en relación con la gestión de proveedores y donde se documentan las consideraciones en materia de seguridad de la información en cuanto a la adquisición de nuevos componentes, la contratación de proveedores y la gestión de dichos contratos.

8 Compromiso de la dirección

La dirección de Olin Group conoce la relevancia de la seguridad de la información en el contexto actual. Es por ello que ha desarrollado un SGSI apropiado a las necesidades del grupo, y que se compromete a implementarlo, mantenerlo y mejorarlo de forma continua, empleando los recursos necesarios para tal fin.

La dirección de Olin Group expresa explícitamente su conocimiento y aprobación de esta Política, a partir de la cual se desarrollan el resto de los procedimientos, normas y controles. Todo ello será coherente con lo aquí especificado, y tendrá la finalidad de ofrecer las mejores condiciones de protección para la información de los clientes, de los empleados, y del negocio.