Misión y Alcance

Establecer las directrices y principios que regirán el modo en que **Instrumentación y Control del Sur, S.L., S.L. (Surcontrol)** gestionará y protegerá su información y sus servicios, a través de la implantación, mantenimiento y mejora de los requisitos dentro del marco regulatorio legal y vigente del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, siendo su aplicación en el ámbito de desarrollo de sus actividades de consultoría, asistencia técnica, desarrollo e integración en ingeniería en automatización y robótica.

Principios de Seguridad

Surcontrol protegerá la información en todas las fases de su ciclo de vida —creación/recepción, uso y procesamiento, comunicación y transporte, almacenamiento y difusión autorizada, y borrado o destrucción— garantizando su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Esta protección se aplicará sobre medios físicos y lógicos, propios y de terceros (incluida nube), mediante controles organizativos, técnicos y físicos proporcionales a su clasificación (p. ej., control de accesos, cifrado, registro y monitorización, y destrucción certificada cuando proceda)..

Por ello, se establecen los siguientes principios mínimos:

a) Seguridad como proceso integral (art.6)

La seguridad se concibe como un proceso integral y continuo que abarca los elementos humanos, materiales, técnicos, jurídicos y organizativos del sistema de información. Todo tratamiento de la información se regirá por este principio, evitando actuaciones puntuales o coyunturales.

La Dirección y los responsables (RSI, RS, RI, RSE) asegurarán la coordinación efectiva, la definición de responsabilidades y la dotación de recursos necesarios. Se promoverá la concienciación y formación de todas las personas implicadas, de modo que la falta de conocimiento, organización, coordinación o instrucciones no se convierta en fuente de riesgo.

La seguridad se implementará bajo un enfoque de mejora continua (PDCA), con controles preventivos, detectivos y correctivos, documentados y medibles.

b) Gestión de la seguridad basada en los riesgos (art. 7).

El análisis y la gestión de riesgos es un proceso esencial, continuo y actualizado que sustenta la seguridad. Su objetivo es mantener un entorno controlado, reduciendo los riesgos a niveles aceptables definidos por la Dirección (apetito de riesgo).

La reducción del riesgo se logrará mediante la aplicación proporcionada y equilibrada de medidas de seguridad (organizativas, operativas y técnicas) acordes con la clasificación de la información, los servicios prestados y la exposición a amenazas.

Los riesgos identificados se registrarán y tratarán conforme a una metodología de análisis de riesgos, aplicando tratamientos de mitigar, transferir, evitar o aceptar, con responsables, plazos y evidencias definidos.

c) Prevención, detección, respuesta y conservación (art. 8).

La seguridad del sistema se implementará como un ciclo continuo de prevención, detección y respuesta, con el fin de minimizar vulnerabilidades, disuadir y reducir la superficie de exposición, y lograr que las amenazas no se materialicen o, si lo hacen, limitar su impacto sobre la información y los servicios.

Las medidas de prevención eliminarán o reducirán la probabilidad de materialización (hardening, parches, control de accesos, segmentación, cifrado, principios de mínimo privilegio y Zero Trust).
Las medidas de detección permitirán descubrir y cualificar ciberincidentes en tiempo oportuno (registro y correlación de eventos, alertas y umbrales definidos).

Las medidas de respuesta restaurarán la información y los servicios afectados de acuerdo con el tiempo máximo para restablecer el servicio y la antigüedad máxima de datos que se acepta perder, incluyendo contención, erradicación, recuperación y lecciones aprendidas.

Sin merma de los principios del ENS, el sistema garantizará la conservación y autenticidad de los datos electrónicos y la disponibilidad de los servicios durante todo el ciclo de vida de la información.

d) Existencia de líneas de defensa (art. 9).

El sistema contará con una estrategia de protección en múltiples capas. Si una capa se ve comprometida, las restantes permitirán reaccionar de forma adecuada y contener el incidente, reduciendo la probabilidad de compromiso total y minimizando el impacto sobre la información y los servicios.

Estas líneas de defensa incluirán medidas de naturaleza organizativa, física y lógica/tecnológica coordinadas entre sí.

e) Vigilancia continua y reevaluación periódica. (art. 10).

La vigilancia continua del sistema permitirá detectar actividades o comportamientos anómalos y responder a tiempo para contenerlos.

La evaluación permanente de la seguridad de los activos medirá su evolución, identificando vulnerabilidades y desviaciones de configuración.

Las medidas de seguridad se revisarán y actualizarán periódicamente, ajustando su eficacia a la evolución de los riesgos, amenazas y tecnologías de protección, pudiendo replantear el enfoque de seguridad cuando sea necesario.

f) Diferenciación de responsabilidades. (art. 11).

En el sistema de información se mantendrá una segregación clara de responsabilidades:

Responsable de la Información (RI): Define la clasificación y los requisitos de seguridad de la información tratada.

Responsable del Servicio (RSE): Establece los requisitos de seguridad del servicio y vela por que se cumplan en la operación.

Responsable del Sistema (RS): Es responsable de la implantación y operación técnica que soporta los servicios (infraestructura, aplicaciones, redes).

Responsable de Seguridad de la Información (RSI): Orienta y decide en materia de seguridad para satisfacer los requisitos definidos, coordina la gestión de riesgos y la respuesta a incidentes.

Cuando exista tratamiento de datos personales, se identificarán además las figuras del Responsable del Tratamiento y, en su caso, el Encargado del Tratamiento, conforme a RGPD/LOPDGDD, asegurando la coherencia entre estas funciones y las responsabilidades anteriores.

Marco Normativo

Surcontrol se encuentra sujeto a la siguiente normativa en la provisión de los servicios prestados a sus clientes:

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad

Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad

Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información

Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

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 (reglamento General de Protección de Datos), de aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

Guías CCN-STIC de Seguridad

Prevención de Riesgos Laborales Ley 31/1995 de 8 de noviembre y Real Decreto 39/1997 de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención.

Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE).

RD-ley 13/2012 de 30 de marzo, ley de cookies.

Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

El marco de referencia que da cobertura legal a este documento se establece en las siguientes secciones del Real Decreto 311/2022 de 22 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS):

ENS. Artículo 12. Política de Seguridad y requisitos mínimos de seguridad La seguridad deberá comprometer a todos los miembros de la organización. La política de seguridad según se detalla en el Anexo II, sección 3.1, deberá identificar unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la empresa.
ENS. Anexo II. Medidas de Seguridad Marco organizativo [org] Política de seguridad [org.1]

Organización de la Seguridad. Roles y Funciones de Seguridad

Los diferentes roles determinados junto con sus respectivas funciones y responsabilidades son:

RSI — Responsable de la Seguridad de la Información

Funciones y responsabilidades

- Diseñar, implantar y mantener el SGSI conforme al ENS (gobierno, riesgos, controles).
- Mantener Análisis y Tratamiento de Riesgos, determinación de acciones y plan de formación/concienciación.
- Establecer normas/procedimientos (accesos, cambios, incidentes, copias, registros, continuidad).
- Coordinar incidentes de seguridad.
- Medir y reportar indicadores (cumplimiento de controles, parches, copias, eventos, vulnerabilidades).

Autoridad

- Proponer políticas y normas; requerir su cumplimiento a RS/RSE/RI.
- Acceso a evidencias y registros necesarios para verificar el cumplimiento.

RSE — Responsable del Servicio

Funciones y responsabilidades

- Ser dueño funcional del servicio (p. ej., Nóminas, ERP, Sede electrónica).
- Definir, integrar y mantener requisitos de seguridad en contratos, con proveedores y revisar su desempeño
- Alinear la operación con necesidades de negocio y con el ENS.
- Priorizar cambios y correcciones según impacto en el servicio.

Autoridad

- Exigir a proveedores el cumplimiento de requisitos ENS y penalizaciones/planes de mejora.
- Escalar a Dirección riesgos/impactos que exceden su mandato.

RS — Responsable del Sistema

Funciones y responsabilidades

- Ser dueño técnico de la plataforma/sistema: arquitectura, hardening, parches, copias, registros.
- Gestionar la configuración e inventario, vulnerabilidades, monitorización y capacidad.
- Ejecutar (o supervisar) la operación diaria: accesos, despliegues, continuidad técnica.

Autoridad

- Aprobar diseños técnicos, estándares y guías de bastionado dentro de su ámbito.
- Rechazar despliegues/cambios que incumplan requisitos de seguridad/operatividad.
- Priorizar tareas técnicas (parches críticos, refuerzos, mejoras de capacidad).
- Solicitar recursos (herramientas, licencias) para mantener el nivel de seguridad.

RI — Responsable de la Información

Funciones y responsabilidades

- Establecer criterios de acceso y autorizar accesos a sus datos.
- Definir retención y destrucción de la información (conservación legal y negocio).
- Verificar que los procesos (envíos, publicación, portabilidad, eliminación) cumplen las normas.
- Participar en evaluaciones de impacto y en la gestión de incidentes que afecten a “sus” datos.

Autoridad

Aprobar/Vetar solicitudes de acceso y usos de la información.
Exigir medidas de protección acordes a la clasificación
Ordenar la destrucción segura o anonimización al final de la retención.

Concienciación y Formación

Todos los trabajadores de **Surcontrol** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información, siendo responsabilidad del Comité de la Seguridad de la Información de disponer de los medios necesarios para que la información llegue a los afectados.

Todos los trabajadores de **Surcontrol** asistirán 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 todo el personal, 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.

Documentación de Seguridad del Sistema (art. 12.1.e)

Surcontrol tiene un sistema de gestión documental mediante el cual se editan, revisan y aprueban los documentos, y se publican a los usuarios correspondientes según la naturaleza y alcance del documento.

La documentación está estructurada de la siguiente manera, con la siguiente estructura de documentación: Política de SI, Manual, Procedimientos y Políticas

Gestión de Riesgos (art. 12.1.f)

Todos los sistemas sujetos a esta Política estarán incluidos en un análisis de riesgos que evalúe amenazas, vulnerabilidades e impactos. Este análisis se repetirá:

- De forma periódica, al menos anualmente.
- Cuando cambie la información tratada (volumen, sensibilidad, nuevos datos personales, etc.).
- Cuando cambien los servicios prestados o su criticidad.
- Tras un incidente grave de seguridad.
- Ante vulnerabilidades graves o nuevas amenazas relevantes.

El Comité de Seguridad de la Información definirá valoraciones de referencia por tipos de información y servicios (criterios comunes de impacto/probabilidad) para homogeneizar el análisis en toda la organización. Asimismo, priorizará y dinamizará recursos para atender las necesidades de seguridad de los distintos sistemas, promoviendo inversiones transversales cuando aporten mayor reducción de riesgo.

Controles Organizativos, Operacionales y de Protección (ENS) (art. 12.6)

Se establecen los principios y requisitos que rigen la seguridad de la información en **Surcontrol**, alineados con el ENS, y que deben aplicarse de forma proporcional al riesgo en todos los servicios, activos y personas implicadas

a) Organización e implantación del proceso de seguridad

La seguridad se gestiona de forma integral bajo la dirección del Comité de Seguridad y el liderazgo del RSI, con roles definidos (RI, RSE, RS) y segregación de funciones. La implantación se realiza mediante políticas, normas y procedimientos aprobados, evidencias de cumplimiento y un plan anual de trabajo alineado con los riesgos.

b) Análisis y gestión de los riesgos

Todos los servicios y activos se someten a análisis de riesgos continuo. Los riesgos se registran, tratan y aceptan formalmente, aplicando medidas proporcionales a la criticidad. El riesgo residual y las excepciones se documentan, se aprueban por los responsables y se revisan periódicamente.

c) Gestión de personal

El personal y terceros con acceso a información o sistemas deberá firmar compromisos de confidencialidad y recibir formación específica por rol. Se aplican controles en el ciclo de vida (incorporación, cambios, desvinculación) y revisiones de accesos.

d) Profesionalidad

Las funciones de seguridad serán desempeñadas por personal con competencia acreditada y formación actualizada. La organización promoverá certificaciones y capacitación continua, y asignará recursos adecuados para garantizar la eficacia de los controles.

e) Autorización y control de los accesos

Se exigirá identidad única, autenticación fuerte y autorización por rol con revisiones periódicas. Los accesos privilegiados se gestionarán mediante sistemática de control de cuentas privilegiadas y se registrarán para su trazabilidad. Todo acceso será concedido, modificado y revocado conforme a procedimiento.

f) Protección de las instalaciones

Las instalaciones y espacios técnicos aplicarán controles físicos (acceso, vigilancia, zonas seguras) y medidas ambientales (energía, incendio, inundación). Los soportes serán custodiados y destruidos de forma segura; las visitas se registrarán.

g) Adquisición de productos de seguridad y contratación de servicios de seguridad

Las compras y contrataciones incluirán requisitos de seguridad (técnicos, organizativos y legales), evaluación de proveedores por criticidad y cláusulas de cumplimiento, auditoría y continuidad. No se pondrán en producción productos/servicios sin validación de seguridad.

h) Mínimo privilegio

El acceso a información y sistemas se limitará al mínimo necesario, por el tiempo imprescindible y con justificación. Se evitarán cuentas compartidas; se aplicarán controles temporales y registros de uso.

i) Integridad y actualización del sistema

Se mantendrán configuraciones de seguridad mínimas obligatorias en todos los equipos y servidores, y aplicaremos las actualizaciones de seguridad dentro de los plazos máximos acordados según su criticidad y control de cambios. La integridad se protege con configuraciones seguras, supervisión de cambios, firmas cuando proceda y verificación posterior a actualizaciones.

j) Protección de la información almacenada y en tránsito

La información se clasificará y etiquetará; se aplicará cifrado proporcional a su nivel, controles para prevenir la fuga de información, copias de seguridad verificadas y segregación de entornos. Las transmisiones usarán canales seguros y políticas de compartición controladas.

k) Prevención ante otros sistemas de información interconectados

Las interconexiones se autorizarán y documentarán, con segmentación, controles de frontera, filtrado y acuerdos de nivel de seguridad. Se limitará la exposición, se aplicarán principios de Zero Trust y se monitorizarán las comunicaciones.

l) Registro de la actividad y detección de código dañino

Se registrarán eventos relevantes (accesos, cambios, fallos, actividad administrativa) con retención definida y correlación. Se desplegarán medidas anti-malware, sistemas de detección y respuesta en los equipos y detección en red para identificar comportamiento malicioso y responder oportunamente.

m) Incidentes de seguridad

Existirá un procedimiento de gestión de incidentes que cubra detección, clasificación, contención, erradicación, recuperación, comunicación (incluidas obligaciones regulatorias) y lecciones aprendidas. Se conservarán evidencias y se informará al Comité.

n) Continuidad de la actividad

La continuidad se asegurará mediante la definición del tiempo máximo para restablecer el servicio y del límite de pérdida de datos permitido, planes de continuidad/recuperación, pruebas periódicas y mejora sobre resultados reales.

ñ) Mejora continua del proceso de seguridad

La organización aplicará PDCA: planificar, implantar, verificar y mejorar. Se usarán auditorías internas/externas y revisiones por la Dirección para ajustar controles, recursos y prioridades, manteniendo la adecuación al riesgo y a la normativa.

Datos de Carácter Personal

Surcontrol trata datos de carácter personal y garantizará su protección conforme al RGPD/LOPDGDD y al ENS.

El acceso a la documentación de cumplimiento estará restringido a personas autorizadas.

Todos los sistemas de información que traten datos personales aplicarán medidas técnicas y organizativas adecuadas al riesgo, teniendo en cuenta la naturaleza y finalidad del tratamiento, y respetando los principios de minimización, integridad/confidencialidad, limitación de acceso y trazabilidad.

Terceras Partes (Proveedores y Clientes)

Cuando prestemos servicios o tratemos información de otras organizaciones, o cuando usemos servicios de terceros o cedamos información, dichas partes conocerán y aceptarán esta Política de Seguridad y la normativa asociada aplicable al servicio/ información.

Se establecerán canales formales de coordinación y procedimientos de respuesta a incidentes.

Las terceras partes quedarán sujetas a obligaciones contractuales de seguridad y podrán definir procedimientos operativos propios, siempre que cumplan los requisitos acordados.

El personal de terceros deberá acreditar concienciación y formación en seguridad equivalente al nivel exigido por esta Política.

Prevención, Detección, Respuesta y Recuperación

Surcontrol estará preparada para prevenir, detectar, responder y recuperarse de incidentes de seguridad, con responsabilidades definidas (RSI, RS, RSE, RI) y coordinación del Comité de Seguridad (Art. 8 ENS).

Prevención

Surcontrol reducirá la probabilidad de incidentes y su impacto mediante controles mínimos del ENS y controles adicionales derivados del análisis de amenazas y riesgos.

Detección

Dado que los servicios pueden degradarse rápidamente, se realizará monitorización continua para detectar anomalías y actuar con prontitud.

Respuesta

Los distintos departamentos que integran **Surcontrol** deberán contener, erradicar y comunicar los incidentes de forma coordinada.

Recuperación

Para garantizar la disponibilidad de los servicios, **Surcontrol** mantendrá planes de continuidad y recuperación como parte del Plan de Continuidad de negocio.

Revisión Política de Seguridad de la Información

El Comité de Seguridad de la Información elaborará la Política de Seguridad de la Información (PSI) conforme al art. 12 del ENS y al control ORG.1 del Anexo II. Asimismo, realizará su revisión al menos anual y propondrá su actualización o mantenimiento cuando proceda.

La PSI será aprobada por la Dirección (CEO de Surcontrol) y comunicada a todas las partes afectadas para asegurar su conocimiento y cumplimiento.

FIRMADO JESÚS RODRÍGUEZ VARGAS

surcontrol

Fdo.: Dirección - CEO

Jesús Rodríguez Vargas
12 octubre 2025 – Rev. 1