

<b>AENOR</b>	<b>AENOR</b>	<b>AENOR</b>	<b>AENOR</b>	<b>AENOR</b>
GESTIÓN DE LA CALIDAD	GESTIÓN AMBIENTAL	SEGURIDAD Y SALUD EN EL TRABAJO	PROYECTO I+D+i	GESTIÓN ENERGÉTICA
ISO 9001	ISO 14001	ISO 45001	EN 15160:2010	ISO 50001
<small>L-29610-001</small>	<small>GA-30300047</small>	<small>201 1022-2399</small>		<small>17-361 10233</small>



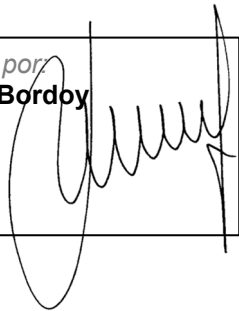
# POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN

**SGSI**

**CONTROL DE EDICIONES**


EDICIÓN	FECHA	OBSERVACIONES
01	31/03/2023	Primera redacción

Aprobado por:  
**Joaquim Bordoy**




31/03/23

Revisado por:  
**Jaume Cucurella**



31/03/23

Editado por:  
**Oliver Jimeno**



31/03/23

<b>1 CARACTERÍSTICAS GENERALES .....</b>	<b>4</b>
<b>2 ALCANCE .....</b>	<b>4</b>
<b>3 DESARROLLO .....</b>	<b>4</b>
<b>3.1 DEFINICIONES .....</b>	<b>6</b>
<b>3.2. MARCO LEGAL Y REGULATORIO .....</b>	<b>7</b>
<b>3.3. LIDERAZGO Y COMPROMISO DE LA DIRECCIÓN. ....</b>	<b>7</b>
<b>3.4. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN .....</b>	<b>8</b>
<b>3.5 ESTABLECIMIENTO, IMPLANTACIÓN, MANTENIMIENTO Y MEJORA .....</b>	<b>9</b>
<b>3.6 FUNCIONES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN .....</b>	<b>10</b>
<b>3.7 REVISIÓN DE LA POLÍTICA .....</b>	<b>11</b>
<b>3.8 APROBACIÓN, DIFUSIÓN Y APLICACIÓN .....</b>	<b>11</b>

## 1 CARACTERÍSTICAS GENERALES

La Política de Seguridad de la Información es el conjunto de directrices que rigen la forma en que *Construcciones Rubau, S.A.* gestiona y protege la información que trata y los servicios que presta. En el desarrollo de sus actividades Rubau utiliza tecnologías y sistemas de gestión de la información de naturaleza diversa.

Sea cual sea el uso de las tecnologías, y el sistema de información, debe garantizarse en todo momento la seguridad de la información evitando, en la medida que sea posible, el acceso, uso o alteración no autorizada, ya que las incidencias pueden afectar a los legítimos intereses de Rubau.

Al mismo tiempo, deben garantizarse los derechos de los trabajadores de Rubau, de sus clientes, de sus proveedores y de otras personas físicas o jurídicas con los que se establezca relación. Entre estos derechos figuran el secreto industrial y comercial y el derecho fundamental a la protección de los datos personales.

Con esta finalidad Rubau ha elaborado y aprobado esta Política de Seguridad de la Información de obligado cumplimiento para todos los trabajadores. Con ella se promueve un uso óptimo de los sistemas de información, garantizando los derechos de las personas que los utilizan.

Esta política es entendida, implantada y mantenida al día en todos los niveles de la empresa y cuenta con el total compromiso y apoyo de la Dirección de Rubau, quien la establece, desarrolla y aplica por medio de su Sistema de Gestión Integrado (en adelante, S.G.I.) conforme a lo establecido en la norma UNE-ISO/IEC 27001:2014.

## 2 ALCANCE

Esta Política se aplica dentro del alcance interno de la norma ISO 27001, siendo de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios a la compañía.

## 3 DESARROLLO

La calidad y la seguridad de los servicios son objetivos estratégicos para Rubau, y la información relacionada con ellos constituye un activo fundamental para la toma de decisiones eficientes. Por estas razones la Dirección declara su compromiso expreso con la mejora continua de su Sistema de Gestión de Seguridad de la Información (en adelante, S.G.S.I.) como pilar de una estrategia orientada a la gestión de los riesgos y la consolidación de una cultura basada en la seguridad.

El alcance de nuestro S.G.S.I. es el siguiente:

Los sistemas de información y documentación de obras con especiales requerimientos de seguridad ubicados en obras, delegaciones y servicios centrales relacionados con:

La construcción de los tipos de obra de Movimiento de tierras y perforaciones. Puentes, viaductos y grandes estructuras. Edificaciones incluyendo su conservación y mantenimiento. Ferrocarriles (obra de ferrocarriles sin cualificación específica), incluyendo su conservación y mantenimiento de vías férreas, hidráulicas (abastecimiento y saneamiento. Canales. Acequias y desagües. Defensas de márgenes y encauzamiento. Conducciones con tubería de presión de gran diámetro. Obras hidráulicas sin cualificación específica). marítimas (escolleras. Con bloques de hormigón. Con pilotes y tablestacas. Obras marítimas sin cualificación específica. Emisarios submarinos). Viales y pistas (con firmes de hormigón armado. Con firmes de mezclas bituminosas) incluyendo la conservación y mantenimiento de carreteras, autopistas, autovías y calzadas. Señalizaciones y balizamientos viales. Obras viales sin cualificación específica). transporte de productos petrolíferos y gaseosos. Instalaciones eléctricas (alumbrados. Iluminaciones y balizamientos luminosos. Centros de transformación y distribución en alta tensión. Distribución en baja tensión. Telecomunicaciones e instalaciones radioeléctricas. Instalaciones eléctricas sin cualificación específica). Instalaciones mecánicas especiales (cimentaciones especiales, sondeos. Inyecciones y pilotajes. Pinturas y metalizaciones. Jardinería y plantaciones. Restauración de bienes inmuebles histórico-artísticos. Estaciones de tratamiento de aguas, redes de agua y alcantarillado, incluyendo su conservación y mantenimiento. instalaciones contra incendios). La explotación de concesiones de: edificios, parkings, carreteras, autopistas, autovías y puertos. El diseño, la construcción y la explotación de: Infraestructuras hidráulicas, como la captación, redes de abastecimiento y alcantarillado; canales, acequias y desagües; Conducciones con tubería de presión de gran diámetro; Plantas de tratamiento de aguas (residuales, potables, lixiviados y desaladoras); Plantas de tratamiento de fangos y residuos sólidos urbanos para su valorización energética.

Según la declaración de aplicabilidad vigente a la fecha de emisión del certificado.

### 3.1 DEFINICIONES

Activo de información: se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Parte interesada: Persona o grupo que tiene un interés en el desempeño o éxito de la organización.

Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

Confidencialidad: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

Integridad: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a una persona o entidad.

Disponibilidad: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

Vulnerabilidad: Debilidad que puede ser explotada por una amenaza.

Amenaza: Causa potencial de un incidente no deseado que puede provocar daños a un sistema o a la organización.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Tratamiento de riesgos: Proceso de modificar el riesgo mediante la implementación de controles.

Datos personales: Cualquier información relacionada con una persona que permita identificarla o pueda servir para identificarla.

### **3.2. MARCO LEGAL Y REGULATORIO**

Con la implantación de un S.G.S.I. bajo la Norma UNE ISO/IEC 27001 integrado en nuestro S.G.I. se fortalece la seguridad de nuestros servicios, así como de la información y datos que incluyen y que son necesarios para su correcta y adecuada prestación.

Rubau trata datos personales que deberán mantenerse inventariados por tratamiento, con el objeto de facilitar el control, la gestión y la protección de los mismos, aplicando medidas para cumplir con el 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), equivalente a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, que se creó para facilitar su aplicación y cumplimiento en España.

El S.G.I de Rubau se mantendrá cumpliendo y respetando la Ley de Propiedad Intelectual en lo que se refiere al uso del software, obteniendo las licencias correspondientes y llevando un registro y control de estas para el empleo adecuado de éstas en el desarrollo de las actividades. Por lo tanto, el marco legal antes indicado estará en consonancia con el S.G.S.I de Rubau, ya que uno de los grupos de controles de seguridad de este, es el Cumplimiento de la Legislación Aplicable.

### **3.3. LIDERAZGO Y COMPROMISO DE LA DIRECCIÓN.**

La Dirección de Rubau se compromete a facilitar y proporcionar los recursos necesarios para el establecimiento, implantación, mantenimiento y mejora de su S.G.S.I., así como a demostrar liderazgo y compromiso respecto a éste, a través de la constitución del Comité de Seguridad de la Información que tendrá la responsabilidad de:

- Asegurar el establecimiento de la presente política y los objetivos de seguridad de la información, y que estos sean compatibles con la estrategia de Rubau.
- Asegurar la integración y el cumplimiento de los requisitos aplicables del S.G.S.I. en los servicios y procesos de la entidad.
- Asegurar que los recursos necesarios para el S.G.S.I. estén disponibles.
- Comunicar la importancia de una gestión de la seguridad eficaz y conforme con los requisitos del S.G.S.I.
- Asegurar que el S.G.S.I. consigue los resultados previstos.
- Dirigir y apoyar a las personas para contribuir a la eficacia del S.G.S.I.
- Promover la mejora continua.
- Apoyar otros roles pertinentes de la Dirección, liderando a sus áreas de responsabilidad en seguridad de la información. El detalle de las funciones específicas del Comité de Seguridad de la Información, se describen en su acta de constitución.

### 3.4. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Los objetivos de seguridad de la información se establecerán en las funciones y niveles pertinentes, enfocados a la mejora y utilizando como marco de referencia:

- Cambios en las necesidades de las partes interesadas que lleven a una mejora del alcance del sistema.
- Requisitos de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos para garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información, así como la protección de los datos personales.
- Factores internos como la aplicación de técnicas organizativas que mejoren el seguimiento de la tramitación y resolución de incidentes de seguridad.
- Factores externos como los avances tecnológicos, cuya aplicación mejore la eficacia del tratamiento de los riesgos.
- La mejora de la eficacia de la formación y concienciación del personal que trabaja en la entidad y afecta a su desempeño en seguridad de la información.

Así mismo, la planificación para la consecución de los objetivos de seguridad de la información establecidos se realizará tomando en cuenta los siguientes elementos:



- Lo que se va a hacer.
- Los recursos necesarios
- El responsable.
- Plazo de consecución.
- Indicadores para evaluar el resultado/cumplimiento.

### 3.5 ESTABLECIMIENTO, IMPLANTACIÓN, MANTENIMIENTO Y MEJORA

El despliegue del S.G.S.I. de Rubau se inicia a partir del análisis de riesgos que permite determinar el nivel de riesgo de seguridad de la información en que se encuentra la entidad e identificar los controles de seguridad necesarios, así como las oportunidades de mejora para el tratamiento del riesgo para llevarlo a un nivel aceptable, tomando en cuenta el contexto de la Organización.

Los controles de seguridad deberán implantarse, mantenerse y mejorarse continuamente y estar disponibles como información documentada que deberá ser revisada y aprobada por el Comité de Seguridad de la Información en representación de la Dirección General.

La presente Política de Seguridad se desarrollará aplicando los siguientes requisitos mínimos e incluirse en la documentación del sistema:

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.
- Profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos.
- Seguridad por defecto.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de actividad.
- Incidentes de seguridad.
- Continuidad de la actividad.

- Mejora continua del proceso de seguridad.

Se deberá comunicar la información documentada de los controles de seguridad al personal que trabaja en la entidad (personal interno y externo) que tendrá la obligación de aplicarla en la realización de sus actividades laborales.

La información documentada será clasificada como Pública, Interna, Restringida y Confidencial, dándole un uso adecuado de acuerdo con dicha clasificación y según el criterio que se establezca en el Procedimiento de Clasificación y Etiquetado de la Información.

Se realizarán auditorías que revisen y verifiquen el cumplimiento del S.G.S.I. de Rubau respecto a los requisitos de la Norma ISO/IEC 27001, por lo que el personal afectado por el alcance de dichas auditorías deberá ser colaborativo para la eficacia de las mismas, así como en la aplicación de las acciones correctivas que se deriven para su mejoramiento continuo.

### 3.6 FUNCIONES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

- El **Comité de Seguridad** procederá a revisar y a proponer la aprobación de la presente Política de Seguridad de la Información a la Dirección General de Rubau, que será la **Responsable de la Información**. Además, centralizará los mecanismos de coordinación y resolución de conflictos entre los responsables que se indican a continuación, que se tratarán mediante debate durante las reuniones de los miembros de dicho comité y que serán moderados por la Dirección General. Actuando en representación de la Dirección General de Rubau, será el órgano encargado de aprobar la Política, de la autorización de sus modificaciones, así como de toda la información documentada del S.G.S.I. de la entidad.
- El **Responsable de Seguridad de la Información** será el encargado de notificar la presente Política al personal de la entidad y de los cambios que en ella se produzcan, así como de coordinar las acciones de implantación, mantenimiento y mejora del S.G.S.I. de la entidad (incluyendo la firma de la Declaración de Aplicabilidad que formaliza la relación de medidas de seguridad aplicables derivadas del análisis de riesgos), y de sus auditorías.
- El **Responsable de Sistemas** se encargará de gestionar los requisitos técnicos de seguridad de los sistemas de información.
- El **Responsable del Servicio**, cuya figura recae en los directores de las áreas de la entidad, se encargará de gestionar los requisitos de seguridad de las actividades de su área para la prestación de los servicios. El Responsable de cada información y/o del servicio se indicará en el Mapa de Riesgos de Rubau, que recogerá los criterios que determinarán el nivel de seguridad requerido para cada uno.

- El **Responsable de Protección de Datos** será el encargado de garantizar que los datos personales se tratan y se protegen conforme al Reglamento General de Protección de Datos (RGPD UE 2016/679), por lo que trabajará en coordinación con el Responsable de Seguridad de la Información y con el Responsable de Sistemas.
- Todo el **personal de la organización**, tanto interno como externo, será responsable de cumplir con la presente Política de Seguridad de la Información dentro de su área de trabajo, así como de aplicar toda la información documentada de los controles y medidas de seguridad del S.G.S.I. de Rubau en sus actividades.

### 3.7 REVISIÓN DE LA POLÍTICA

La presente Política de Seguridad de la Información será examinada en las revisiones del sistema por la Dirección, a través del Comité de Seguridad de la Información, siempre que se produzcan cambios significativos y, como mínimo, una vez al año.

### 3.8 APROBACIÓN, DIFUSIÓN Y APLICACIÓN

La presente Política de Seguridad de la Información será aprobada por la Dirección General de RUBAU mediante firma, y difundida a las partes interesadas.

Así mismo, la Dirección General de Rubau dotará de los recursos necesarios para la aplicación efectiva de esta política, y para su buen desarrollo, tanto en las actividades de implantación como en el posterior mantenimiento y mejora de todo el S.G.S.I. de la entidad.



**Aprobado por:**

**Joaquim Bordoy Colomer**

.....Barcelona, 31 de marzo de 2023