



# POLÍTICA DE PREVENCIÓN DE RIESGOS PENALES

1. OBJETO Y ÁMBITO DE APLICACIÓN .....	1
2. RIESGOS .....	2
3. ÓRGANOS DE CONTROL .....	3
4. CONTROL PREVENTIVO DE LOS PRINCIPALES RIEGOS DE SEGURISA.....	5
5. CANAL DE DENUNCIAS.....	7
6. FORMACIÓN .....	8
7. OBLIGACIONES.....	8
8. RÉGIMEN DISCIPLINARIO .....	9

## 1. OBJETO Y ÁMBITO DE APLICACIÓN

El sector de la vigilancia y seguridad privada busca generar a sus clientes la tranquilidad y confianza de contar con entidades que identifiquen y generen controles del riesgo de seguridad física.

La Política de Prevención de Riesgos Penales de SEGURISA (en adelante PPRP), se establece para evitar la responsabilidad de las personas jurídicas por delitos cometidos por personal de la organización, pudiendo derivar en la imposición de sanciones penales.

Las personas físicas que pueden transferir responsabilidad penal son:

- Representantes legales o aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control.
- Empleados o colaboradores, que han podido realizar hechos delictivos por haberse incumplido los procesos de supervisión, vigilancia y control por parte de los representantes legales de la organización.

El objeto de esta política es el de identificar las prácticas inadecuadas en el control y supervisión de los diferentes puestos en la prestación del servicio de seguridad y vigilancia privada, para la generación de recomendaciones óptimas en la prestación de dicho servicio.



## 2. RIESGOS

En el Código Penal se establecen los supuestos delictivos de los que pueden ser responsables las personas jurídicas. A continuación se relacionan los riesgos que deben ser objeto de supervisión, vigilancia y control de prevención, y que se encuentran comprendidos en el Código Penal:

- Tráfico ilegal de órganos
- Trata de seres humanos
- Delitos relativos a la prostitución, explotación sexual y corrupción de menores
- Delitos contra la intimidad personal e informática
- Delitos de estafas
- Frustración de la ejecución
- Insolvencias punibles
- Daños informáticos
- Delitos relativos a la propiedad intelectual
- Delitos relativos a la propiedad industrial
- Acceso ilegítimo y revelación de secretos empresariales
- Delitos contra el mercado y los consumidores
- Corrupción en los negocios/corrupción entre particulares
- Blanqueo de capitales
- Financiación ilegal de partidos políticos
- Delitos contra la Hacienda Pública y la Seguridad Social
- Delitos contra los derechos de los ciudadanos extranjeros
- Delitos sobre la ordenación del territorio y el urbanismo
- Delitos contra los recursos naturales y el medio ambiente
- Delitos de riesgo catastrófico
- Delitos contra la salud pública
- Falsificación de tarjetas de crédito y débito y cheques de viaje
- Cohecho
- Tráfico de influencias
- Delitos de odio y enaltecimiento
- Financiación del terrorismo
- Manipulación genética
- Alteración de precios en concursos y subastas públicas
- Obstaculización de la labor inspectora o supervisora de la Administración
- Delitos contra los derechos de los trabajadores



- Falsificación de moneda y efectos timbrados
- Asociación ilícita
- Organización y grupo criminal
- Acoso laboral
- Acoso sexual
- Revelación de secretos
- Allanamiento del domicilio de personas jurídicas
- Delitos contra el honor
- Delitos de suposición de parto y de alteración de la paternidad, estado o condición del menor
- Delitos de riesgo provocados por explosivos y otros agentes
- Tenencia, tráfico y depósitos de armas, municiones o explosivos

SEGURISA realiza de forma periódica (mínimo una vez al año) una evaluación de los riesgos por corrupción en el formato “Análisis de riesgos por corrupción”, estableciendo una valoración de los riesgos identificados a partir de una matriz de evaluación que consta de:

RIESGOS DE GESTIÓN	VALORACIÓN
<b>Valor: PROBABILIDAD</b>	
1 = poco probable	1
2 = probabilidad media	2
3 = muy probables	3
<b>Valor: IMPACTO</b>	
1 = poco impacto para la organización	1
2 = impacto medio	2
3 = mucho impacto para la organización	3
<b>Valor = 9. Riesgo crítico. Debe ser abordado. Deben establecerse planes de mitigación</b>	
<b>Valor = 6. Riesgo medio. Debe ser considerado y aplicar planes de mitigación o no a criterio de la empresa.</b>	
<b>Valor &lt; 6. Riesgo bajo. Debe reevaluarse a lo largo del tiempo. No es necesario establecer planes de mitigación.</b>	

Con los riesgos identificados como naranja (valor 6) y rojo (valor 9) SEGURISA confeccionará planes de acción para mitigar los impactos y posibles consecuencias.

### 3. ÓRGANOS DE CONTROL

Los órganos de control interno del cumplimiento normativo penal en SEGURISA son los responsables de la implantación del PRRP a nivel operativo y funcional y de la implementación, seguimiento y evaluación del cumplimiento, determinando las medidas correctivas y de mejora del mismo en caso de ineficacia, así como de realizar el análisis y seguimiento de las medidas propuestas de los diferentes sucesos ocurridos. Los órganos de control en SEGURISA son:



- Dirección General
- Comité de Certificación

### 3.1 Comité de Control normativo

El Comité se constituye como un órgano con poderes autónomos de iniciativa y de control, de conformidad con lo establecido en el Código Penal (artículo 31 bis). El Comité de Control Normativo está compuesto por:

- Director General Corporativo (Responsable de Control Normativo).
- Comité de Certificación

El Comité de Control Normativo es el órgano de control en materia de prevención de riesgos penales del SEGURISA, cuya función es definir y supervisar la eficacia de los controles establecidos, con la finalidad de evitar sucesos con responsabilidad penal, y, en su caso, minimizar las consecuencias e impacto derivados.

En concreto, se confía al Comité de Control Normativo la supervisión del funcionamiento y del cumplimiento del PPRP, con poderes autónomos de iniciativa y control.

Sus miembros, en el ejercicio de su función, son autónomos, independientes e imparciales, actúan bajo el principio de responsabilidad personal, y no están sujetos a órdenes ni instrucciones de la propiedad, ni de la alta dirección del grupo, garantizando de esta manera la indemnidad de sus opiniones, actuaciones y decisiones en las que intervengan en el seno del Comité salvo que sea algún miembro del Comité quien incurra en algún acto con responsabilidad para el SEGURISA.

El Comité de Control Normativo se reunirá con una frecuencia semestral, y siempre que sea requerido por algún miembro del mismo, siendo convocadas dichas reuniones por correo electrónico, determinando la fecha y hora de la reunión, y la programación de los temas a tratar.

Se levantará acta de las reuniones del Comité de Control Normativo, registrando todos los temas tratados, así como las votaciones y acuerdos alcanzados, siendo firmadas en señal de conocimiento y conformidad por todos los miembros que componen el Comité. Los acuerdos se tomarán por mayoría simple, es decir, cuando existan más votos a favor que en contra, siendo el voto del Responsable de Control Normativo el voto de calidad en caso de empate.



### 3.2 Responsable de Control Normativo

El puesto de Responsable de Control Normativo recae en el Director General Corporativo, siendo sus funciones:

- Velar por la aplicación y cumplimiento de la Política de Prevención de Riesgos Penales, así como de su desarrollo, supervisión y mejora.
- Informar al Comité de Control Normativo sobre cualquier tema relacionado con la Política de Prevención de Riesgos Penales, sometiendo a votación las propuestas de mejora, revisión, control o seguimiento que considere oportunas.
- Asegurar la implantación de un sistema de recepción y gestión de denuncias, y que éstas son respondidas y tratadas.
- Aplicar las medidas que se consideren necesarias para evitar y, en su caso, reducir las consecuencias de cualquier comportamiento ilícito o del que pueda derivar un supuesto de responsabilidad penal.
- Promover la implantación del PPRP en SEGURISA, definiendo planes de formación, información y de difusión del mismo para su conocimiento por los empleados.
- Cualquier otra función que se acuerde por los miembros del Comité de Control Normativo.

## 4. CONTROL PREVENTIVO DE LOS PRINCIPALES RIEGOS DE SEGURISA

Con anterioridad se han relacionado los diferentes supuestos delictivos a los que a los que pueden estar expuestas las organizaciones y que eventualmente podrían dar lugar a responsabilidad penal atribuible a las mismas.

A continuación se determinan medidas preventivas concretas de aquellos riesgos con alta probabilidad de ocurrencia y/o cuyas consecuencias se consideran relevantes, definiendo las actuaciones fundamentales para evitarlos, sin perjuicio de otras que se consideren:

### 1. Delitos de corrupción en los negocios

- En general, no se puede solicitar, recibir ni aceptar ningún beneficio o ventaja no justificados, para favorecer indebidamente a otros.
- No se pueden ofrecer ni conceder beneficios o ventajas injustificadas para verse favorecido indebidamente frente a un tercero.



- No se pueden ofrecer ni aceptar ventajas ni regalos que no sean simbólicos, procurando no verse comprometido actualmente o en el futuro para cuando deban tomarse decisiones que afecten a implicados en estos actos.

## 2. Delitos informáticos.

- Obtención, revelación y utilización de datos reservados de carácter personal o familiar, mediante la utilización de medios informáticos puestos a disposición del personal.
- No podrán realizarse los siguientes actos: obtención y divulgación de datos personales o familiares por medios informáticos sin estar autorizado; reproducción no autorizada de programas informáticos protegidos; proporcionar claves de acceso a terceros no autorizados; utilizar claves de terceros sin estar autorizados; interceptación del correo electrónico de terceros; cesión de datos reservados; difusión de mensajes calumniosos o injuriosos a través de internet; utilizar programas informáticos para alterar, simular o falsear datos de la entidad, etc.

## 3. Descubrimiento y revelación de secretos

- Revelación de secretos de la entidad por medio de datos, escritos o electrónicos (no se podrán obtener ni difundir).
- No se podrá falsear la información sobre los productos o servicios que se ofrezcan.
- No alterar ni modificar la facturación.
- No emplear violencia, amenaza o engaño para alterar los precios; ni se difundirán noticias o rumores falsos de la entidad ni de otras empresas.

## 4. Insolvencias punibles y de frustración de la ejecución.

- No se puede buscar la insolvencia de propósito para perjudicar a los acreedores.
- No se puede dificultar la ejecución de embargos o apremios judiciales o administrativos.
- En el caso de insolvencia actual o inminente, se pondrá especial atención para no ocultar, dañar o destruir bienes propios, para no realizar actos de disposición no justificados económica y empresarialmente, vender por debajo de coste, incumplir el deber de llevar contabilidad, llevar doble contabilidad o cometer irregularidades relevantes, destruir o alterar libros contables, destruir, ocultar o alterar la documentación social que hay que conservar.
- Habrá que poner especial atención en la formulación de las cuentas anuales, no realizar actos que oculten la situación económica real, no favorecer a determinados acreedores sin justificación económica o empresarial.



## 5. Cohecho

- Nadie podrá ofrecer o entregar retribuciones a autoridades o funcionarios y empleados públicos para que éstos realicen un acto contrario a la legalidad o en consideración a su cargo, ni aun cuando sean aquéllos quienes lo soliciten.
- Denunciar este tipo de conductas en los procedimientos de contratación, de subvenciones o de subastas convocadas por la Administración o entes públicos.

## 6. Blanqueo de capitales.

- No se pueden realizar transacciones sobre bienes cuando se sepa o se sospeche que tienen origen ilícito. La prudencia ha de ser máxima, pues el origen ilícito no se puede ocultar ni encubrir, ni se puede ayudar a la persona que haya participado en la infracción.
- Atender especialmente a la regularidad de los medios de pago utilizados, a pagos extraordinarios no previstos en los contratos o acuerdos, mediante cheques al portador o en divisas no acordadas, o por personas distintas a las que han contratado.
- No se establecerán relaciones con personas o entidades que no proporcionen la información exigida por la ley o que no sea posible identificar al socio, propietario o beneficiario último.

## 7. Acoso Laboral, sexual o mobbing

- Poner especial atención a esta clase de comportamientos, dada la amplia plantilla y centros de trabajo del grupo.
- Vigilar actos tales como bromas, insultos y alusiones relativas al sexo, raza, edad, nacionalidad, religión, discapacidad, etc.
- Igualmente habrá que prevenir y vigilar aproximaciones sexuales indeseadas, solicitudes de favores y sugerencias sexuales, actos verbales o físicos inadecuados, etc.
- Son rechazables también las conductas verbales o físicas que incidan negativamente en el trabajo de otro o creen un entorno de trabajo hostil o intimidatorio.

## 5. CANAL DE DENUNCIAS

Cualquier acto o indicio ilícito dentro del ámbito de la empresa SEGURISA debe ser denunciado por el personal a través de los canales establecidos, asegurando la recepción por parte del Comité de Control Normativo o el Responsable de Control Normativo. Los procedimientos para la denuncia se encuentran en el documento SEGURISA\_PROTOCOLO DENUNCIAS.



El sistema permite que los empleados denuncien a otros empleados, superiores, directivos y administradores, mientras que los directivos y superiores pueden denunciar a cualquier empleado. Si los administradores deben denunciar, lo harán directamente al Responsable de Control Normativo.

Al recibir una denuncia relevante, se acusará recibo al denunciante y se le informará sobre el progreso. Se garantizará la confidencialidad del denunciante y se protegerá a quienes denuncien de buena fe.

Las denuncias serán analizadas por el Responsable de Control Normativo, que elaborará un informe sobre los hechos y propondrá medidas a adoptar. Este informe se presentará al Comité de Control Normativo en su próxima reunión o en una convocatoria urgente si es necesario. En casos de irregularidades menores, se informará al Comité sin necesidad de un análisis exhaustivo.

Además, el Responsable de Control Normativo podrá notificar a las autoridades judiciales si es pertinente. El Comité llevará un registro confidencial de las denuncias y sus acciones, evaluando y mejorando los controles establecidos en función de las denuncias recibidas.

## 6. FORMACIÓN

SEGURISA informará a todos los responsables de departamento y áreas de la organización sobre el contenido de la Política de Prevención de Riesgos Penales, utilizando para ello todos o algunos de los siguientes medios:

- Formación a distancia
- Organización de cursos o jornadas formativas
- Información mediante mailing o web de SEGURISA

Los responsables de área o departamento, serán los encargados de informar a todo el personal bajo su responsabilidad, así como al personal de nueva incorporación, recopilando, en la medida de lo posible, justificante de entrega del mismo.

## 7. OBLIGACIONES

Todo el personal del SEGURISA tiene la obligación de comunicar al Responsable de Cumplimiento Normativo todo acto, comportamiento, suceso o indicio ocurrido o realizado en el ámbito de





actuación susceptible de ser considerado como ilícito o irregular, utilizando para ello los canales de denuncia descritos en el apartado 5 del presente PPRP. SEGURISA garantiza la indemnidad de la persona que efectúe la oportuna comunicación, por lo que no se podrá tomar medida alguna de represalia contra el informante de buena fe.

## 8. RÉGIMEN DISCIPLINARIO

La infracción de las obligaciones de cualquier miembro del personal de SEGURISA reseñadas en el presente PPRP, dará lugar a la aplicación del régimen disciplinario contenido en el Estatuto de los Trabajadores o en el Convenio en vigor de aplicación.