POLÍTICA DEL SISTEMA DE GESTIÓN DE RIESGOS PENALES y GESTIÓN DE RIESGOS DE SOBORNO (ANTI-CORRUPCIÓN)

Índice

1 Política de Gestión de Riesgos Penales y de Gestión de Riesgos de Soborno.

Audisec, Seguridad de la Información S.L., como parte de la responsabilidad de formular políticas y organizar sistemas de gestión internos, emite esta política del sistema de gestión de riesgos penales y de Gestión de Riesgos de Soborno.

Audisec, Seguridad de la Información S.L, asume una serie de obligaciones en relación con el cumplimiento penal y el compromiso en que dichas obligaciones sean asumidas, respetadas y aplicadas no solo por la empresa si no por todos sus empleados y demás partes interesadas.

La Alta Dirección expone la siguiente Política de Compliance Penal, como muestra de su compromiso para cumplir los requisitos de esta política, del Sistema de Gestión de Compliance Penal y de toda la legislación penal aplicable; así como el compromiso en la búsqueda permanente de la mejora continua de la empresa y del Sistema de Gestión de Compliance Penal.

1.1 Objeto

El objeto de la Política del Sistema de Gestión de Riesgos Penales y Gestión de Riesgos de Soborno, por un lado, permite establecer las bases de actuación para la identificación y gestión de los riesgos para prevenir la comisión de delitos que afectan a la organización, la cual deberá ser de obligado cumplimiento para todos los empleados y terceros que se considere oportuno que trabajan en Audisec, Seguridad de la Información S.L, y por otro lado, se establecen las normas básicas y un marco para prevenir y detectar sobornos y operaciones en las operaciones de Audisec, Seguridad de la Información S.L. De manera explícita, la presente política determina que los empleados de la Organización no permiten el pago, solicitud o aceptación directa de pagos inapropiados (por ejemplo, sobornos o propinas ilegales), cualquiera que sea su forma.

El propósito de esta Política es reiterar el compromiso de Audisec, Seguridad de la Información S.L., con el total cumplimiento por parte de la Empresa, directores, trabajadores, de toda ley local Anti-Soborno y Anti-Corrupción aplicable. Esta Política complementa al Código de Conducta y Ética en los Negocios y da una pauta para el cumplimiento de las políticas de la empresa aplicables a las operaciones de Audisec, Seguridad de la Información S.L, en todo el mundo.

La voluntad de Audisec, Seguridad de la Información S.L, es combatir y prevenir la comisión de cualquier acto ilícito en el seno de la misma, por lo que esta política supone un compromiso de vigilancia y sanción de los actos y conductas delictivas, mantenimiento del sistema de gestión y la creación de una cultura empresarial enfocada a la ética y a la honestidad.

1.2 Alcance

El alcance de la presente Política comprende a todas las actividades desarrolladas por Audisec, Seguridad de la Información S.L. No se exceptúa ningún proceso ya que la comisión de delitos se puede dar en todas las áreas de actividad.

Esta Política es aplicable para todos los trabajadores de Audisec, Seguridad de la Información S.L. El requisito de reporte de esta Política también es aplicable a los contratistas y proveedores de

Audisec, Seguridad de la Información S.L. El propósito de esta Política es complementar todas las leyes, reglas, y otras políticas corporativas aplicables. No es su propósito reemplazar a ninguna ley local.

1.3 Principios fundamentales para la Gestión de Prevención de Delitos Penales.

La Dirección de Audisec, Seguridad de la Información S.L, es consciente de la importancia de los riesgos penales, está comprometida a tratar los riesgos que pudieran afectar a la organización, mediante la identificación, gestión y control de las diferentes actividades de la organización, estableciendo para ello la presente Política como un mecanismo que permita servir como marco para la definición de objetivos además de para alcanzar los objetivos de la organización, aportar una seguridad y garantías a los diferentes grupos de interés y proteger la reputación de la organización.

. Los principios por los que se rige son:

a) Implantación de las actuaciones necesarias para prevenir la comisión de actos ilícitos mediante las medidas preventivas identificadas como consecuencia del análisis de riesgo realizado.

b) Favorecer la comunicación de las posibles irregularidades, a través del canal de comunicaciones, a través del cual, cualquier empleado o tercero interesado puede poner en conocimiento los actos que tenga conocimiento, garantizando la confidencialidad del informante así como que no sufrirá represalias por el hecho de haber informado.

c) Investigar cualquier comunicación que se presente, garantizando la confidencialidad del comunicador y los derechos de las personas investigadas.

d) Sancionar disciplinariamente, de acuerdo con lo establecido en la legislación aplicable en cada momento, a las conductas que estén destinadas a impedir o dificultar el descubrimiento de delitos y la no comunicación de un hecho delictivo.

e) En caso de incumplimiento de la presente política o de las obligaciones derivadas del sistema de gestión de compliance penal, podrá ser sancionado conforme a la normativa laboral.

f) Cumplir con el código ético y de conducta establecido en la empresa.

g) Conciencia a todos los empleados, para que no exista ningún tipo de tolerancia en la comisión de delitos.

h) Proporcionar los medios materiales y humanos al Comité / Oficial de Cumplimiento para que puedan llevar a cabo las labores encomendadas

1.4 Principios fundamentales para la Gestión de Riesgos Anti-Soborno.

La corrupción se define como la práctica que consiste en hacer abuso de poder, de funciones o de medios para sacar un provecho económico o de otra índole. El soborno es la oferta, promesa, o pago de efectivo, regalos, o incluso entretención excesiva, o el incentivo de cualquier tipo que se ofrezca o se entregue a una persona en una posición de confianza para influenciar los puntos de vista o conducta de esa persona, o para obtener una ventaja inadecuada. La corrupción pueden tomar varias formas, incluyendo la entrega o aceptación de:

- Pagos en efectivo;
- Trabajos o relaciones de “consultoría” falsos
- Sobornos
- Contribuciones políticas
- Contribuciones de caridad
- Beneficios sociales; o
- Regalos, viajes, hospitalidad, y reembolso de gastos

La política de Audisec, Seguridad de la Información S.L, con respecto al soborno y la corrupción es absolutamente clara: nadie puede ofrecer, dar ni recibir sobornos ni pagos indebidos con relación a su trabajo para Audisec, Seguridad de la Información S.L, de nadie ni a nadie en ningún momento y por ningún motivo, y nadie debe solicitar a nadie más que participe en un soborno o realice un pago indebido en representación de Audisec, Seguridad de la Información S.L, Ningún ejecutivo, director, empleado ni Socio comercial puede:

- Influir sobre la voluntad u objetividad de personas ajenas a la compañía para obtener algún beneficio o ventaja mediante el uso de prácticas no éticas y/o contrarias a la Ley aplicable.
- realizar ni ofrecer, de forma directa o indirecta, ningún pago -en metálico o de cualquier otro tipo y bajo cualquier forma contractual-, o cualquier otro beneficio o ventaja a cualquier persona física o jurídica:(i) al servicio de cualquier autoridad, entidad, pública o privada, partido político o candidatos para cargos públicos, con la intención de obtener o mantener, ilícitamente, negocios u otras ventajas; (ii) con la intención de que éstas abusen de su influencia, real o aparente, para obtener de cualquier autoridad, entidad, pública o privada, cualquier negocio u otra ventaja; o (iii) cuando se tenga conocimiento de que todo o parte del dinero o de la especie será ofrecida o entregada, directa o indirectamente, a cualquier autoridad, entidad, pública o privada, partido político o candidatos para cargos públicos, con cualquiera de los propósitos mencionados.
- No financiar ni mostrar apoyo o soporte de cualquier otra clase, directa o indirectamente, a ningún partido político, sus representantes o candidatos.
- No utilizar las donaciones para encubrir pagos indebidos.
- No solicitar ni percibir de manera indebida, directa o indirectamente comisiones, pagos o beneficios, de terceros con ocasión de o con causa en las operaciones de inversión, desinversión, financiación o gasto que lleve a cabo la compañía.
- Promover e incentivar entre sus socios, proveedores, contratistas y empresas colaboradoras el conocimiento de esta política y la adopción de pautas de comportamiento consistentes con la misma.
- Prestar especial atención a aquellos supuestos en que existan indicios de falta de integridad de las personas o entidades con las que se realizan negocios, con el fin de prevenir y evitar la realización de blanqueo de capitales provenientes de actividades delictivas o ilícitas.
- Reflejar fielmente y de forma adecuada todas las actuaciones, operaciones, y transacciones de la compañía en los registros y sistemas de la misma.

- Actuar bajo el principio de transparencia de la información, reportando todas las actuaciones, operaciones y transacciones de la Compañía de manera veraz, clara y contrastable.
- Realizar "pagos de facilitación": Los pagos realizados a Funcionarios Públicos para estimular o acelerar el cumplimiento de un deber u obligación existente (llamados por lo general "Pagos de facilitación") están prohibidos por Audisec, Seguridad de la Información S.L,

1.5 Sistema de Gestión de Riesgos Penales y Anti-Soborno.

La Política se ejecuta mediante el Sistema de Gestión, apoyado en la función de Comité / Oficial de Cumplimiento y soportado por los procedimientos, metodologías y herramientas de soporte internas, que permite:

a) Identificar los riesgos y amenazas que pueden afectar a la organización, gestionando su posible ocurrencia dentro de la organización.

b) Establecer una estructura de políticas y directrices, para la aprobación y despliegue de planes de tratamiento enfocados a mitigar los riesgos de la compañía.

c) Medir y controlar los riesgos siguiendo procedimientos y estándares de la organización.

d) Analizar los riesgos asociados a los servicios y procesos, como elemento esencial en la toma de decisiones y estrategias de negocio.

e) Mantener un sistema de control del cumplimiento de políticas y procedimientos implantados en la organización.

f) Evaluar la eficiencia y aplicación del Sistema de Gestión de Riesgos y las mejores prácticas y recomendaciones en materia de riesgos para su eventual incorporación al Sistema de Gestión.

g) Evaluar la eficacia de los controles implantados mediante un cuadro de indicadores, revisiones, e informes de control.

h) Auditar el Sistema para comprobar la adecuación de los procesos y los de los controles definidos para mitigar los riesgos identificados.

1.6 Auditorías.

Las Auditorías de Audisec, Seguridad de la Información S.L, unidades operativas, y contratistas, se realizarán en forma periódica para asegurar el cumplimiento de los requisitos de esta Política y de los procedimientos y pautas aplicables. Las Auditorías podrán ser realizadas internamente por Audisec, Seguridad de la Información S.L, o externamente a través de terceros contratados. En la documentación de Auditoría se incluirán los planes de acción para la mejora del desempeño.

1.7 Registros

Todo el Personal y los Socios comerciales empleados por Audisec, Seguridad de la Información S.L, deben documentar y registrar de manera precisa todos los gastos realizados en representación de Audisec, Seguridad de la Información S.L y están prohibidos de ocultar o tergiversar los gastos de

la sociedad o realizar pagos en representación de Audisec, Seguridad de la Información S.L, sin las aprobaciones necesarias y la documentación de respaldo que verifique la validez de la operación.

1.8 Disciplina

Todo trabajador que no cumpla con los términos de esta Política estará sujeto a acción disciplinaria. Todo trabajador que tenga conocimiento directo sobre potenciales incumplimientos de esta Política pero que no comunique dichos incumplimientos potenciales a la gerencia de la Empresa o a la Unidad de Compliance, estará sujeto a acción disciplinaria. Todo trabajador que induzca a error u obstaculice a los investigadores que se encuentren realizando averiguaciones sobre potenciales incumplimientos de esta Política estará sujeto a acción disciplinaria. En todos los casos, la acción disciplinaria podrá incluir el término de la relación laboral. Todo agente tercero que no cumpla con los términos de esta Política, que tenga conocimiento de potenciales incumplimientos de esta Política y que no cumpla con informar a la gerencia de Audisec, Seguridad de la Información S.L respecto a dichos potenciales incumplimientos, o que induzca a error u obstaculice a los investigadores que se encuentren realizando averiguaciones sobre potenciales incumplimientos de esta Política, podrá ver su contrato reevaluado o terminado.

1.9 Mejora Continua

Audisec, Seguridad de la Información, S.L tiene un alto compromiso con la mejora continua del Sistema de Gestión de Riesgos penales y Antisoborno.

1.10 Comité de cumplimiento penal

El Comité de cumplimiento penal no tiene conflicto de intereses y demuestra en el día a día la integridad y compromiso con el compliance penal. Además el Comité de cumplimiento penal tiene:

- Capacidad y autoridad para el desarrollo de sus funciones.
- Las competencias necesarias para desarrollar sus funciones

El Comité de cumplimiento penal es independiente del resto de órganos de la entidad, garantizando la imparcialidad en toda la toma de decisiones.

1.11 Obligaciones de comunicar e información adicional.

Todo el Personal y Socios comerciales de Audisec, Seguridad de la Información S.L empleados por Audisec, Seguridad de la Información S.L o afiliados a Audisec, Seguridad de la Información S.L tienen la responsabilidad de comunicar inmediatamente cualquier sospecha o conocimiento de que se haya cometido una infracción de esta Política, otras políticas de Audisec, Seguridad de la Información S.L y cualquiera de las leyes aplicables.

Puede decidir realizar la comunicación ante su supervisor o a través de los canales de información enumerados a continuación.

Audisec, Seguridad de la Información S.L se asegurará de que tanto los canales de comunicación como la información de contacto precisa para estos mecanismos de comunicación se encuentren disponibles. Las comunicaciones pueden ser anónimas o nominativas.

Audisec, Seguridad de la Información S.L no tomará represalias ni tolerará las represalias contra empleados que comuniquen de buena fe una posible infracción de esta Política, incluso si una investigación determinara que no ha ocurrido ninguna infracción.

1. Control de versiones

ELABORACIÓN	REVISIÓN	APROBACIÓN
Responsable SG		Antonio Quevedo.
Fecha: 29/10/2019	Fecha:	Fecha: 29/10/2019
Versión 2.0		Firma:

52383986Z ANTONIO QUEVEDO (R: B13422902)

Firmado digitalmente por 52383986Z ANTONIO QUEVEDO (R: B13422902)
Fecha: 2019.10.31 11:56:41 +01'00'

aud[i]sec

seguridad de
la información