–

Programa de Integridad del Grupo SEK - Security Ecosystem Knowledge

POLÍTICA ANTICORRUPCIÓN Y ANTISOBORNO

NEOSECURE By SEK Security Ecosystem Knowledge

¡Hola!

Formamos parte de un grupo que actúa, entre otras actividades, con el reto de atender a muchísimos clientes todos los días. En nuestros negocios, nos relacionamos con nuestros clientes, compañeros de trabajo, varios socios comerciales, la comunidad en que nos encontramos y la administración pública en todas las esferas.

La *Política anticorrupción y antisoborno* (en adelante, la "Política") que aquí les presentamos refuerza nuestro compromiso con esos principios y valores.

El Grupo SEK - Security Ecosystem Knowledge no admite ninguna práctica de corrupción o soborno, adoptando una política de "tolerancia cero" ante cualquier acción u omisión que pueda llevar a la vulneración de las disposiciones legales al respecto. Así, espera la cooperación de sus Colaboradores y de todos aquellos con quienes se relacione la observancia integral de la legislación y de esta *Política*.

¡Esperamos que lean esta *Política* y los incentivamos a que denuncien cualesquiera actos rechazados en este documento!

Presidente – Grupo SEK - Security Ecosystem Knowledge

CONTENIDO

1. OBJETIVO

1.1. La presente *Política anticorrupción y antisoborno* (en adelante, la "Política"), aprobada por el Consejo de Administración, tiene como objetivo establecer las directrices, las normas y los procedimientos del programa de prevención y lucha contra la corrupción para todas las empresas del grupo económico de que forma parte, de conformidad con la legislación vigente, el *Código de conducta y ética del Grupo SEK - Security Ecosystem Knowledge*, las políticas, los manuales, las instrucciones de trabajo y los procedimientos establecidos por cada empresa del susodicho grupo.

2. CONCEPTOS

2.1. Cuando se escriban con la primera letra mayúscula, se atribuyen los siguientes significados a las expresiones a continuación:

"Administración Pública": es cualquier organismo o entidad de la administración pública directa o indirecta, nacional o extranjera, que desempeñe actividades de gestión y/o ejecución de servicios públicos en las esferas federal, estatal o municipal.

"Administrador/es": en singular o plural, se trata de los directores independientes y los miembros del Consejo de Administración del Grupo SEK - Security Ecosystem Knowledge.

"Funcionario/s": son todas las personas que, (i) aunque transitoriamente o sin remuneración, ejerzan cargos, empleos o funciones públicas en cualquier organismo o entidad de la administración pública o en empresas contratadas o ajustadas para la ejecución de la actividad objeto de concesión por la administración pública; (ii) ejerzan cargos, empleos o funciones en empresas públicas o controladas por el gobierno, incluso sociedades de economía mixta, además de fundaciones públicas; (iii) integren partidos políticos o sean candidatas a cargos políticos; y (iv) ejerzan cargos, empleos o funciones públicas en organismos, entidades estatales o representaciones diplomáticas de países extranjeros, además de personas jurídicas controladas, directa o indirectamente, por el poder público de países extranjeros u organizaciones públicas internacionales. La definición de funcionario incluye a personas políticamente expuestas (PPE), quienes pueden definirse como personas que ocupan o hayan ocupado cargos, empleos o funciones públicas relevantes.

"Canal de la Transparencia": es el que se estipula en el numeral 12 de este documento, que trata de servir de instrumento para que empleados y terceros puedan comunicar sus inquietudes y denuncias relacionadas con esta *Política* y solicitar la aclaración de dudas.

"Colaboradores": significa el público interno de las empresas del Grupo SEK - Security Ecosystem Knowledge, es decir, en singular o plural, todo/s el/los empleado/s, Administrador/es, pasante/s, aprendiz / aprendices y miembro/s de comités de gobernanza corporativa, teniendo en cuenta todos los segmentos de negocios y sus divisiones y marcas de actuación.

"Corrupción": significa ofrecer, prometer, dar o recibir, directa o indirectamente, algo a alguien con el objetivo de influenciar la toma de decisiones a fin de obtener una Ventaja Indebida. La simple promesa, sin la efectiva entrega de "algo", también se considera un acto de corrupción. El bien ofrecido, recibido o prometido no se limita a valores en efectivo. También puede ser cualquier beneficio o favor, incluso el pago de gastos, la oferta de regalos, viajes, entretenimiento, entre otras conductas.

"Grupo SEK - Security Ecosystem Knowledge": significa CBS HOLDING GLOBAL, LTD. y todas las demás empresas controladas por ésta y/o empresas asociadas que pertenezcan al o puedan integrar el mismo grupo económico de que forma parte.

"Ley Anticorrupción y Antisoborno": se trata de todas las leyes y reglamentos nacionales o extranjeros que buscan establecer reglas que disuadan las prácticas de corrupción, soborno, malos manejos administrativos, manipulación de licitaciones y contratos públicos, lavado de activos, donaciones políticas o electorales, incluso, entre otros, la *Ley de lucha contra la corrupción* (Ley 12846/13) de Brasil, reglamentada por el Decreto 8420/15 y sus respectivas modificatorias, Decreto Ley 2848/1940 (Código Penal Brasileiro); Ley 8429/1992 (*Ley de malos manejos administrativos* de Brasil); Ley 8666/1993 (*Ley de licitaciones* de Brasil); Ley 9504/1997 (*Ley electoral* de Brasil); Ley 9613/1998 (*Ley de prevención del lavado de dinero* de Brasil); *Ley sobre prácticas corruptas en el extranjero* (FCPA) de Estados Unidos; y la *Ley sobre el soborno* del Reino Unido (UKBA), incluso sus reglamentos y otras reglas relacionadas, además de sus futuras modificatorias.

"Persona/s relacionada/s": personas relacionadas con funcionarios por cualquier motivo, incluso, sin limitaciones, familiares o parientes de funcionarios, como cónyuges, compañero/a, hermanos, padres, hijos o hijastros, abuelos, nietos, yernos, nueras, tíos, sobrinos, cuñados y suegros.

"Política": es la presente *Política anticorrupción y antisoborno*.

"Terceros": significa todo el público externo del Grupo SEK - Security Ecosystem Knowledge, es decir, aquéllos sin relación de trabajo o vinculación legal y reglamentaria, como los proveedores de bienes y/o servicios, clientes, apoderados, consultores en general y demás terceros que mantengan o pretendan mantener relaciones con las empresas integrantes del Grupo SEK - Security Ecosystem Knowledge, de cualquier naturaleza y forma, y cualesquiera personas naturales y/o jurídicas subcontratadas y/o relacionadas con ellos.

"Ventaja indebida": es todo evento, con o sin valor económico, que no habría ocurrido sin la promesa o la oferta de "algo" o "algún bien". La celebración de un contrato o la dispensa de pago de una multa son ejemplos de ventaja indebida, así como el acceso a informaciones confidenciales y privilegiadas. El término ventaja indebida debe interpretarse en sentido amplio, por cualquier naturaleza y forma.

3. APLICABILIDAD

3.1. Esta *Política* corresponde a todas las empresas integrantes del Grupo SEK - Security Ecosystem Knowledge e, indistinta e indiscriminadamente, a todos los Colaboradores y Terceros con que se relacionen, de forma neutral e imparcial, en el marco del compromiso del Grupo SEK - Security Ecosystem Knowledge con la conducción de sus negocios con ética, integridad y de acuerdo con la legislación vigente en los países en que el Grupo SEK - Security Ecosystem Knowledge actúe o a que esté sometido.

4. VIGENCIA, MODIFICACIONES Y ACTUALIZACIONES

4.1. La presente *Política* quedará en vigor por tiempo indefinido, siendo que las actualizaciones y las modificaciones solamente se realizarán si son aprobadas por el Consejo de Administración.

Formatado: Espanhol (Espanha)

5. COMENTARIOS INICIALES Y SUPUESTOS

5.1. El compromiso con la ética y la integridad debe determinar y orientar todas las acciones de Colaboradores, Terceros y relaciones del Grupo SEK - Security Ecosystem Knowledge en la realización de sus negocios y actividades, siempre de conformidad con los más elevados estándares morales y legales, sin tolerancia a cualquier forma de Corrupción, soborno, pago de facilitación, favores indebidos o cualquier otra conducta inadecuada, con independencia de la cuantía en cuestión.

5.2. El Grupo SEK - Security Ecosystem Knowledge y todos aquéllos con que se relacione, interna o externamente, deben comprender y actuar de conformidad con las leyes de lucha contra la corrupción y soborno correspondientes en todas las relaciones con la Administración Pública y Funcionarios.

5.3. Las infracciones de las leyes de lucha contra la corrupción y soborno no se toleran. Además, pueden exponer el Grupo SEK - Security Ecosystem Knowledge y a sus accionistas, Administradores y Colaboradores a consecuencias graves en cuanto a su reputación e imagen, además de posibles sanciones administrativas, judiciales y penales.

5.4. Les compete al Grupo SEK - Security Ecosystem Knowledge y a todos sus Colaboradores y Terceros conocer, difundir y cumplir todas las condiciones de esta *Política*.

5.5. Las Leyes Antisoborno y Anticorrupción no sancionan solamente al individuo que comete el acto de Corrupción, sino también a los individuos que actuaron para incentivarlo, es decir, atañen a cualquier individuo que:

- Apruebe el pago de la coima o cualquier tipo de Ventaja Indebida;
- Presente o acepte facturas emitidas de forma fraudulenta;
- Retransmita instrucciones para el pago de la coima o cualquier tipo de Ventaja Indebida;
- Encubra el pago de la coima o la realización de la Ventaja Indebida; o
- Coopere con el acto de Corrupción.

5.6. En caso de cualquier duda sobre el contenido de esta *Política* y su aplicación, solicitar aclaraciones al Comité de Ética a través del Canal de la Transparencia (indicado en el numeral 12 abajo).

6. DIRECTRICES Y REGLAS

6.1. El Grupo SEK - Security Ecosystem Knowledge asume el compromiso de realizar sus actividades en estricto cumplimiento de las leyes aplicables, incluso las legislaciones anticorrupción y antisoborno y las demás normas que rijan las relaciones con la Administración Pública y los Funcionarios.

6.2. Pagos indebidos a funcionarios: queda terminantemente prohibido prometer, ofrecer o darles, directa o indirectamente, cualquier Ventaja Indebida a Funcionarios nacionales o extranjeros o a personas relacionadas.

6.2.1. La prohibición estipulada en esta *Política* corresponde tanto a las conductas cometidas directamente por cualquiera de las empresas del Grupo SEK - Security Ecosystem Knowledge o las cometidas por sus Colaboradores y/o Terceros.

6.2.2. La prohibición expresa consignada en esta *Política* también corresponde a pagos que tengan como objetivo acelerar o agilizar la práctica de actos rutinarios por parte de Funcionarios (por ejemplo, la emisión de licencias, permisos o autorizaciones; certificados; la realización de inspecciones o visitas) (conocidos como pagos o tasas de "agilización", "aceleración" o "urgencia"). Tales pagos quedan terminantemente prohibidos por esta *Política* y no podrán hacerse, bajo ninguna circunstancia, directamente o a través de cualesquiera Terceros y/o en cualquier monto o forma.

6.3. Pagos indebidos a particulares: queda terminantemente prohibido ofrecer o autorizar, directa o indirectamente, cualquier oferta, promesa de pago o pago a través de Ventaja Indebida a cualquier empleado, agente o representante de empresas privadas que mantenga (o pueda mantener) relaciones comerciales con las empresas del Grupo SEK - Security Ecosystem Knowledge, que pueda representar cualquier conflicto de intereses o con la finalidad de tratar de obtener intereses indebidos con tales empresas o, indirectamente, con la participación o la involucración de empresas públicas.

6.4. Pagos indebidos a Administradores, Colaboradores o Terceros: esta *Política* también corresponde a la oferta de Ventajas Indebidas a Colaboradores y Terceros. Queda terminantemente prohibido para Colaboradores y Terceros solicitar, ofrecer, prometer, recibir o aceptar cualquier Ventaja Indebida, de cualesquiera terceros, en beneficio propio o de persona relacionada, para influenciar la práctica de cualquier acto en el desempeño de sus actividades en y para las empresas del Grupo SEK - Security Ecosystem Knowledge.

6.5. Respuestas a solicitudes o exigencias de pagos indebidos: si se recibe una solicitud de pago extraordinario o entrega de Ventaja Indebida por parte de un Funcionario o persona relacionada, rechazarla inmediatamente, de forma explícita y definitiva, y notificar con la máxima urgencia al superior inmediato o al Comité de Ética (a través del Canal de la Transparencia, disponible conforme a lo indicado en el numeral 12 abajo).

6.6. Relaciones con Funcionarios: las relaciones con Funcionarios deben fundarse en las directrices de esta *Política*, el respeto y la legalidad, con ética y transparencia. Los Colaboradores podrán mantener contacto con Funcionarios solamente cuando esto sea necesario en razón de sus atribuciones corporativas y en las instalaciones de los organismos públicos y/o las instalaciones de las empresas del Grupo SEK - Security Ecosystem Knowledge – en este último caso, siempre en presencia de dos o más Colaboradores. Esa regla también deberá ser observada por Terceros, según sea el caso.

6.6.1. Reuniones: la celebración de reuniones con Funcionarios:

- Debe antecederle una solicitud formal por escrito, presentada ante el organismo correspondiente, por medio electrónico o fax, cuando sea posible; La solicitud deberá contener la identificación del solicitante; la fecha y la hora en que pretende ser visto y, en su caso, las razones de la urgencia; el tema de que tratar; y la identificación de acompañantes, si es que existen, y su interés en el asunto;
- Deben celebrarse en organismos, reparticiones o edificios públicos adecuados, en horario comercial, o durante horarios debidamente estipulados en las normas de funcionamiento de los organismos;

- Deben contar, preferiblemente, con la presencia de dos representantes de las empresas del Grupo SEK - Security Ecosystem Knowledge;
- Deben registrarse en la agenda corporativa (Outlook);
- Los registros en calendarios digitales (por ejemplo, Outlook) obligatoriamente deben contar con una copia de seguridad para la protección de la información sobre la ocurrencia de la reunión;
- Tras la reunión, se deben registrar debidamente los nombres de todos los participantes, la fecha, el horario y el lugar de la reunión, además de un breve resumen de los temas discutidos y cualesquiera otras informaciones relevantes;
- En caso de seguimiento de Funcionarios en inspecciones y visitas *in loco*, los Colaboradores, Administradores y Terceros solamente deben facilitarles informaciones exclusivamente técnicas y operacionales, presentando sólo los documentos exigidos por la autoridad; y
- Los trámites para la obtención y la renovación de licencias, permisos y autorizaciones gubernamentales deben seguir un procedimiento claro y transparente y deberán realizarse por personas entrenadas, quedando expresamente prohibido el pago de cualquier tasa, en cualquier concepto, no estipulada en las leyes y los reglamentos correspondientes. Todas las indagaciones deben ser contestadas de forma oficial y con argumentos técnicos y jurídicos.

6.6.2. Mensajes electrónicos y llamadas telefónicas:

- Deben tener contenido claro y objetivo y siempre deben tener como destinatarios por lo menos dos (2) Colaboradores del Grupo SEK - Security Ecosystem Knowledge;
- Deben tener lenguaje técnico, respetuoso, cordial y adecuado; y
- Cuando se trate de asuntos estratégicos en llamadas telefónicas, se recomienda que el contenido de la conversa se registre posteriormente por escrito y se reenvíe a todos los que tomen parte en el asunto, incluso quienes no hayan participado en la llamada.

6.6.3. Buenas prácticas en la interacción con Funcionarios:

- Las relaciones con Funcionarios deben ser éticas, profesionales, cordiales y transparentes, con comunicación técnica, clara y directa, evitando interpretaciones ambiguas;
- Al encontrar a Funcionarios en ocasiones sociales, evitar el contacto y, si eso no es posible, mantener un nivel adecuado de profesionalismo y formalidad, no tratando, bajo ninguna circunstancia, de temas sensibles del Grupo SEK - Security Ecosystem Knowledge fuera de los entornos adecuados;
- Siempre evitar interacciones con Funcionarios que puedan parecer sospechosas o sugerir la práctica de irregularidades (encuentros en estacionamientos, habitaciones de hoteles, envío de mensajes codificados, entre otros); y
- En caso de interacciones informales con Funcionarios (seminarios, asociaciones, conferencias, cumpleaños, fiestas, cenas, entre otros), los Administradores, Colaboradores y Terceros deben abstenerse de tratar de temas específicos y de interés del Grupo SEK - Security Ecosystem Knowledge. Si el Funcionario toma la iniciativa de tratar del tema, deberá sugerir la celebración de una reunión específica, en un entorno profesional y durante horas de trabajo, para mantener el carácter profesional e institucional de la interacción.

6.7. Regalos y entretenimiento: tanto la oferta como la recepción de regalos, hospitalidad y entretenimiento deben observar las siguientes reglas, límites y procedimientos:

- NO podrán realizarse OFERTAS, RECEPCIÓN, CONCESIÓN o PROMESA de cualquier Ventaja Indebida, incluso regalos, hospitalidad, entretenimiento o cualesquiera otras ventajas que incluyan a Funcionarios, con independencia del valor o del tipo de ventaja / beneficio. Cuando NO incluyan a Funcionarios, deberán observarse las reglas establecidas en el *Código de conducta y ética* del Grupo SEK - Security Ecosystem Knowledge;
- NO es permitido recibir y mantener REGALOS, OBSEQUIOS, HOSPITALIDAD o ENTRETENIMIENTO fuera de lo que permitan la ley y los criterios establecidos en esta *Política*. Si Colaboradores o Terceros, en nombre de cualquier empresa del Grupo SEK - Security Ecosystem Knowledge, reciben obsequios en desacuerdo con esta *Política*, deberán tomar medidas para devolver los obsequios al remitente, con una carta estándar de agradecimiento, de conformidad con el *Código de conducta y ética* del Grupo SEK - Security Ecosystem Knowledge;
- La realización de y la participación en eventos específicos que incluyan la Administración Pública y a Funcionarios deberán alinearse a los preceptos legales y éticos y los intereses del Grupo SEK - Security Ecosystem Knowledge y solamente serán posibles con la autorización previa del Comité de Ética; y
- En caso de dudas sobre la adecuación o la autorización de obsequios o entretenimiento, consultar al Comité de Ética (a través del Canal de la Transparencia indicado en el numeral 12 abajo).

6.8. Relaciones con organismos reguladores: las relaciones con los profesionales de organismos reguladores, entre otros, deben fundarse en los más elevados estándares morales y éticos, de conformidad con las estipulaciones en legislación vigente, el *Código de conducta y ética* del Grupo SEK - Security Ecosystem Knowledge y esta *Política*.

6.9. Participación en el proceso político: el Grupo SEK - Security Ecosystem Knowledge no participa en el proceso político, pero respeta el derecho individual de cada uno de sus Colaboradores y Terceros de participar en el proceso político en el país en que residan. Sin embargo, cuando esto ocurra, la susodicha participación deberá plantearse individualmente y queda terminantemente prohibido usar el nombre, los logotipos, las marcas y cualesquiera signos distintivos del Grupo SEK - Security Ecosystem Knowledge o dar la impresión de que se actúa en su nombre. Ninguna campaña política, de cualquier tipo, está permitida en las instalaciones de las empresas del Grupo SEK - Security Ecosystem Knowledge, como la distribución de volantes, el envío de correos corporativos, registros en los *chats* de trabajo, entre otros.

6.10. Patrocinios: quedan prohibidos cualesquiera patrocinios de cualquier persona física o jurídica, sea o no sea Funcionario, con el objetivo de influenciar, directa o indirectamente, una decisión de negocios. El patrocinio, cuando autorizado por los niveles de autoridad competentes, debe observar un proceso formal de contratación, es decir, para que se realice, debe ser comunicado previamente al Departamento Jurídico del Grupo SEK - Security Ecosystem Knowledge, con informaciones detalladas, y ser autorizado previamente por el Comité de Ética. El patrocinio deberá fundarse en instrumentos contractuales formalizados entre la empresa del Grupo SEK - Security Ecosystem Knowledge y los Terceros que los recibirán y registrados contablemente de forma adecuada y transparente.

6.11. Donaciones políticas y contribuciones caritativas: la legislación puede permitir, en determinadas situaciones, las donaciones y las contribuciones políticas por personas físicas dentro de los límites y procedimientos legales, siendo que tal hecho, cuando legalmente permitido, es respetado por el Grupo SEK - Security Ecosystem Knowledge con tal de que se realice de forma estrictamente personal y sin cualquier vinculación a las empresas del Grupo. Queda terminantemente prohibido hacer donaciones políticas a candidatos a cargos políticos o a partidos políticos a través de las empresas del Grupo SEK - Security Ecosystem Knowledge o en su nombre.

6.11.1. Se pueden hacer contribuciones caritativas solamente mediante el cumplimiento integral de la legislación vigente y del *Código de conducta y ética* del Grupo SEK - Security Ecosystem Knowledge, de conformidad con las directrices de esta *Política* y con tal de que sean aprobadas previamente por el Comité de Ética. Si son legalmente permitidas y debidamente aprobadas, las eventuales contribuciones caritativas solamente podrán ser hechas por empresas del Grupo SEK - Security Ecosystem Knowledge (y no directamente y en nombre de cualquier Colaborador). Dichas contribuciones caritativas deben ser registradas y contabilizadas adecuada y transparentemente, según los límites y las formalidades de la legislación aplicable. A estos efectos, los Colaboradores también deben garantizar que las contribuciones caritativas eventualmente realizadas por el Grupo SEK - Security Ecosystem Knowledge, cuando se autoricen, siempre sean utilizadas por las instituciones beneficiarias exclusivamente a efectos caritativos y que no sean aplicadas de forma equivocada, política o en desacuerdo con esta *Política* o cualesquiera otros preceptos éticos y leyes correspondientes.

6.12. Controles contables: les compete a todos los Colaboradores garantizar el mantenimiento de registros contables, de modo exacto, correcto y completo, de todos los gastos, transacciones y pagos de las empresas del Grupo SEK - Security Ecosystem Knowledge. Queda terminantemente prohibido hacer registros falsos o imprecisos que oculten la naturaleza o el importe correcto de cualquier transacción. No se podrán crear o mantener fondos o cuentas no oficiales o sin registro para cualquier finalidad, con independencia de la justificación. No se podrán agregar asientos falsos, engañosos o imprecisos a los libros y registros contables del Grupo SEK - Security Ecosystem Knowledge.

6.13. Contratación de terceros: el Grupo SEK - Security Ecosystem Knowledge se preocupa por hacer negocios solamente con Terceros que sean renombrados e idóneos y compartan sus principios éticos, incluso en lo que respecta a la intolerancia a cualquier forma de corrupción y soborno. En ciertas circunstancias, las acciones de Terceros pueden generar responsabilidades directas para las empresas del Grupo SEK - Security Ecosystem Knowledge. Por ese motivo, es esencial realizar un análisis de riesgos adecuado y seguir procedimientos y precauciones al contratar y/o nombrar a Terceros para la prestación de servicios y/o actuar en nombre de cualquiera de las empresas del Grupo SEK - Security Ecosystem Knowledge, en su interés o en el de sus Colaboradores.

6.13.1. Antes de la contratación: antes de hacer negocios con el Grupo SEK - Security Ecosystem Knowledge, todos los Terceros deberán pasar por un análisis que verificará especialmente, sin limitaciones, sus relaciones con Funcionarios, la Administración Pública y personas relacionadas; su reputación; y sus calificaciones para la ejecución del trabajo para el cual serían contratados.

- Este análisis debe ser llevado a cabo por el encargado de la contratación, que deberá convocar a los demás departamentos para que lo ayuden en el tema,

especialmente el Departamento Jurídico y el de Compras. Además, el responsable interno de la contratación debe mantener el análisis en un archivo para que esté disponible siempre que lo soliciten la Administración, el Comité de Ética o el Departamento Jurídico;

- El proceso de análisis estará compuesto por una revisión que debe ser hecha de manera independiente por el Colaborador encargado de la contratación, siendo que los Terceros deberán cooperar y facilitar todas las informaciones que les soliciten, so pena de no contratación. Todo el proceso de contratación debe ser realizado con base en el mérito y no mediante el uso indebido de influencia sobre cualquier persona, con independencia de que sea o no sea Funcionario;

- Los contratos celebrados por el Grupo SEK - Security Ecosystem Knowledge con Terceros deberán contener una descripción clara del respectivo objeto contratado, los montos de conformidad con los precios de mercado, la vigencia, las obligaciones de las partes contratantes y, entre otros temas que se consideren necesarios, deberán incluir obligatoriamente las cláusulas de cumplimiento de esta *Política* y, en su caso, deberán observar el procedimiento de *due diligence* de Terceros de acuerdo con las reglas del Grupo SEK - Security Ecosystem Knowledge.

6.13.2. Después de la contratación: tras la contratación de Terceros, le compete al gestor responsable de la contratación hacer el seguimiento de sus actividades, siempre atento a eventuales señales de alerta o de incumplimiento de las *Leyes Antisoborno y Anticorrupción*, y denunciar cualquier indicio preocupante, de conformidad con el numeral 12 de esta *Política*. Si el Colaborador no es el gestor responsable de la contratación, pero sepa o tenga motivos legítimos para creer que un pago prohibido por las *Leyes Antisoborno y Anticorrupción* o por esta *Política* ha sido, es o pueda ser hecho o prometido a Terceros o Funcionarios en nombre de las empresas del Grupo SEK - Security Ecosystem Knowledge, directa o indirectamente, debe comunicar tal hecho inmediatamente a los canales de comunicación mencionados en el numeral 12 abajo.

6.14. Contratos con la Administración Pública – licitaciones, subastas inversas, concesiones, etc.: la contratación con la Administración Pública sigue estándares y procedimientos estipulados en legislación específica que son muy distintos de los correspondientes a los contratos firmados con la iniciativa privada. Por ese motivo, los Colaboradores y Terceros deben estar atentos a las disposiciones en la legislación específica sobre ese tipo de contratación, incluso siempre el Departamento Jurídico en el proceso de análisis de participación de la contratación y análisis previo de la documentación pertinente para su celebración.

6.14.1. Todos los participantes en el proceso de contratación con la Administración Pública deben actuar de conformidad con los más altos estándares éticos y dentro de la ley cuando interactúen con Funcionarios y competidores, de acuerdo con la legislación aplicable, esta *Política* y procedimientos internos establecidos para ese tipo de contratación.

6.14.2. Queda terminantemente prohibido practicar, directa o indirectamente, cualquier acto que pueda entenderse como fraude, lesión o frustración de procesos selectivos realizados por la Administración y Funcionarios.

6.14.3. En caso de duda sobre cómo relacionarse con la Administración Pública, Funcionarios, organismos gubernamentales o competidores en el marco de licitaciones

o contratos públicos, consultar al Comité de Ética (por el Canal de la Transparencia indicado en el numeral 12 abajo).

7. OPERACIONES DE FUSIONES, ADQUISICIONES E INCORPORACIONES

7.1. Siempre que el Grupo SEK - Security Ecosystem Knowledge trate de buscar nuevos negocios a través de la adquisición, la fusión o la incorporación de cualquier empresa o activo, se debe llevar a cabo un proceso de *due diligence* juicioso y se deben incluir en el contrato de compraventa las cláusulas anticorrupción adecuadas y se deben considerar otras opciones disponibles para evitar el riesgo de sucesión de cualquier pasivo anterior a la conclusión de la operación.

7.2. Se debe realizar, en el proceso de *due diligence*, un procedimiento a efectos de verificación del cumplimiento de las disposiciones de las *Leyes Antisoborno y Anticorrupción* antes de la realización del negocio. Si se identifican cualesquiera infracciones o sospechas de infracción de las *Leyes Antisoborno y Anticorrupción*, el Departamento Jurídico y el Departamento de Cumplimiento del Grupo SEK - Security Ecosystem Knowledge deberán ser notificados formalmente para que tomen las medidas adecuadas respecto del cumplimiento del Programa de Integridad y de esta *Política*.

8. COMPROMISO DE DENUNCIA

8.1. Les compete a todos los Colaboradores y Terceros comunicar cualquier infracción, conducta incompatible o sospecha de infracción de los principios de ética, honestidad, compromiso, responsabilidad y fiabilidad, del *Código de conducta y ética* del Grupo SEK - Security Ecosystem Knowledge, de las leyes y los reglamentos en vigor, de esta *Política* y de todas las demás políticas, manuales y procedimientos internos.

8.2. Las vulneraciones o las sospechas deben comunicarse al Canal de la Transparencia (véase el numeral 12 abajo) y podrán hacerse de forma identificada o anónima.

8.3. No se tolerarán retaliaciones o represalias en cualquier forma o medida en contra de cualesquiera Colaboradores o Terceros que presenten una denuncia de buena fe.

8.4. Cuando se comuniquen las vulneraciones, deberán interrumpirse prontamente las irregularidades o las infracciones detectadas. Le compete al Comité de Ética del Grupo SEK - Security Ecosystem Knowledge contribuir al manejo y a la remediación de los daños generados.

9. RESPONSABILIDADES

9.1. Les compete a todos los Colaboradores la diseminación de la presente *Política*. Además, deben garantizar el cumplimiento del *Código de conducta y ética* del Grupo SEK - Security Ecosystem Knowledge, lo que hace que cualesquiera Terceros también se comprometan con los susodichos documentos.

9.2. El Grupo SEK - Security Ecosystem Knowledge promoverá periódicamente entrenamientos relacionados con su Programa de Integridad, que podrán ser presenciales o en la modalidad a distancia, siendo que los Colaboradores y Terceros deberán participar en ellos a fin de garantizar el cumplimiento de sus responsabilidades definidas en el numeral 9.1 de esta Cláusula.

10. VULNERACIONES Y PENALIDADES

10.1. Las vulneraciones de esta *Política* también se considerarán infracciones del *Código de conducta y ética* del Grupo SEK - Security Ecosystem Knowledge y sus infractores también quedarán sujetos a las penalidades legales, según sea el caso, y de conformidad con la *Política de gestión de consecuencias* del Grupo SEK - Security Ecosystem Knowledge.

10.2. Los Terceros responderán civil y penalmente de las infracciones de esta *Política*. Además, se aplicarán las penalidades contractuales previstas, incluso los daños y perjuicios pertinentes, en el marco de las condiciones contractuales y la *Política de gestión de consecuencias* del Grupo SEK - Security Ecosystem Knowledge.

10.3. La omisión ante el conocimiento de posibles vulneraciones por Colaboradores y Terceros se considerará una conducta antiética y pasible de aplicación de sanciones disciplinarias. Asimismo, la denuncia de situaciones irreales con el objetivo de perjudicar a otras personas o empresas por intereses personales o ilícitos también se considerará antiética y sujeto de sanciones, en el marco de esta *Política*.

11. CONFLICTOS, EXCEPCIONES Y ACLARACIONES

11.1. Cualquier excepción a las estipulaciones de esta *Política* deberá pedirse mediante el envío de una solicitud al Comité de Ética (por el Canal de la Transparencia indicado en el numeral 12 abajo) del Grupo SEK - Security Ecosystem Knowledge, con la descripción de lo que se solicita, las justificaciones y los criterios utilizados en el pedido, valiéndose, para ello, del formulario estándar que se adjunta al Anexo I de la presente *Política*.

11.2. No se podrá hacer ninguna excepción antes de que sea debidamente aprobada por el Comité de Ética. Tampoco podrán hacerse excepciones en desacuerdo con la legislación vigente y las directrices y los supuestos del Programa de Integridad.

12. CANAL DE LA TRANSPARENCIA

12.1. El Grupo SEK - Security Ecosystem Knowledge alienta a todos sus Colaboradores y Terceros a que hagan denuncias cuando detecten o sospechen de cualquier vulneración.

12.2. Todas las personas que se relacionen con el Grupo SEK - Security Ecosystem Knowledge deben comunicar las vulneraciones o posibles infracciones de las directrices de esta *Política* y las demás reglas establecidas por su Programa de Integridad a través del Canal de la Transparencia, disponible en: https://www.canaldatransparencia.com.br/seksecurityecosystemknowledge/

12.3. Los relatos pueden ser realizados por el denunciante de forma anónima, si éste prefiere no identificarse. Todas las situaciones informadas serán evaluadas y los debidos trámites serán llevados a cabo por el Comité de Ética del Grupo SEK - Security Ecosystem Knowledge según la más estricta confidencialidad, con justicia, profundidad, tempestividad, respeto y razonabilidad.

Todas las denuncias pueden hacerse anónimamente.
Se garantiza la confidencialidad para todas las personas y situaciones comunicadas.

***

Anexo I

FORMULARIO PARA LA SOLICITUD DE EXCEPCIÓN A LA DISPOSICIÓN ESPECÍFICA RELACIONADA CON LA POLÍTICA ANTICORRUPCIÓN Y ANTISOBORNO

Al Comité de Ética del Grupo SEK - Security Ecosystem Knowledge,

Solicitante: [introducir]

Por el presente, les solicito una excepción a la siguiente disposición específica relacionada con la *Política Anticorrupción y Antisoborno* del Grupo SEK - Security Ecosystem Knowledge:

- [introducir]

Tal solicitud de excepción específica se refiere a:

- Fecha: [introducir]
- Participantes del Grupo SEK - Security Ecosystem Knowledge: [introducir]
- Participantes de la otra parte: [introducir]
- Lugar: [introducir]
- Importe: [introducir]
- Departamento: [introducir]
- Relación con la otra parte: [introducir]
- Finalidad: [introducir]

La solicitud de excepción se justifica por [introducir justificación referente al pedido de excepción específica].

Por este acto, DECLARO que todas las informaciones arriba facilitadas son correctas, completas y verdaderas y reconozco que la prestación de informaciones incorrectas o su omisión puede conllevar sanciones legales y contractuales.

Además, DECLARO que solamente tras la autorización formal del Comité de Ética podré continuar la eventual implementación de la excepción, si es que la aprueban.

Quedo en espera de su deliberación para dar continuidad al tema.

[lugar], [•] de [•] de [•].

_____
Nombre completo
Firma