–

Programa de Integridad
del Grupo SEK - Security Ecosystem Knowledge

CÓDIGO DE CONDUCTA Y ÉTICA DE LOS COLABORADORES

NEOSECURE
By SEK Security Ecosystem Knowledge

MENSAJE DEL PRESIDENTE

¡Hola!

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

Como equipo tenemos un gran e importante reto para el desarrollo de los negocios del Grupo SEK - Security Ecosystem Knowledge y, para ello, deseamos mantener relaciones saludables, sostenibles y éticas.

Los valores éticos del Grupo SEK - Security Ecosystem Knowledge se fundan en el respeto mutuo, la seriedad y la honestidad con que actuamos en nuestros negocios y los profesionales con quienes nos relacionamos. Por ello, los invito a que lean ese *Código* y lo utilicen como una guía sobre la conducta que esperamos de cada uno de ustedes.

Creemos que, con la fidelidad de elevados principios éticos, aportaremos, además del desarrollo de los negocios del Grupo SEK - Security Ecosystem Knowledge, al crecimiento de cada profesional que actúa con nosotros para que construyamos juntos una trayectoria de éxito y sostenibilidad.

Presidente – Grupo SEK - Security Ecosystem Knowledge

ÍNDICE

CAPÍTULO I – OBJETIVO

El presente *Código de Conducta y Ética de los Colaboradores* (en adelante, el "Código") establece las expectativas mínimas del Grupo SEK - Security Ecosystem Knowledge, que incluye CBS HOLDING GLOBAL, LTD., sus filiales, asociadas, controladas, actuales y que vengan a integrar su grupo económico, con independencia del país en que actúen, con relación a la conducta de todos sus colaboradores (en adelante, el "Grupo SEK - Security Ecosystem Knowledge").

La ética, la transparencia y la integridad son valores esenciales para el Grupo SEK - Security Ecosystem Knowledge y fundamentales para su éxito y reputación.

Con esa finalidad, el Grupo SEK - Security Ecosystem Knowledge espera un fuerte compromiso de sus colaboradores con la conformidad legal y los principios de ética, transparencia e integridad.

A efectos de este Código, los colaboradores son el público interno del Grupo SEK - Security Ecosystem Knowledge, es decir, los socios, los directores, los miembros de comités, los directores independientes y los empleados (quienes mantengan relaciones de trabajo) de las empresas pertenecientes al SEK, incluso sus administradores, practicantes y aprendices, teniendo en cuenta todos sus segmentos de negocios, marcas y divisiones.

CAPÍTULO II – MISIÓN, VISIÓN Y VALORES

Nuestra misión, visión y valores se fundan en los principios de ética, transparencia, cordialidad e integridad en la actuación ante nuestros colaboradores, clientes y todo el público externo con que el Grupo SEK - Security Ecosystem Knowledge se relacione. El público externo comprende los terceros que se relacionen con el 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 terceros.

No aceptamos conductas impropias, discriminaciones y conductas que vulneren la legislación de los países en que actuamos. Todos los colaboradores deben actuar con honestidad, ética, cordialidad, respeto y dignidad, a tono con nuestros valores.

CAPÍTULO III – ALCANCE Y VIGENCIA DE ESTE CÓDIGO

Este *Código de conducta y ética* forma parte del Programa de Integridad del Grupo SEK - Security Ecosystem Knowledge y debe ser observado por todos los colaboradores. El presente *Código* permanecerá en vigor por tiempo indefinido.

Las normas establecidas en este *Código* son generales y corresponden indistintamente a todos los colaboradores del Grupo SEK - Security Ecosystem Knowledge, con independencia de la empresa, la división o la marca a que estén vinculados, y también atañen indistintamente a todos los niveles jerárquicos y al país de actuación del colaborador.

El presente *Código* es abarcador y debe leerse e interpretarse juntamente con otras políticas y procedimientos de integridad, pero seguramente no agota todas las situaciones. Por lo tanto, podrán surgir casos imprevistos que pueden generar dudas con relación a la manera adecuada de proceder. En ese caso, no proseguir y despejar las dudas a través del Canal de la Transparencia indicado en el capítulo XXII abajo.

CAPÍTULO IV – ENTORNO LABORAL

El entorno laboral debe reproducir nuestros valores y nuestras creencias. Todos los colaboradores deben ser tratados con respeto y dignidad y tener la oportunidad de crecer profesionalmente. No toleramos ninguna forma de racismo, discriminación o acoso. Trabajamos por un entorno seguro, higiénico y respetuoso.

El SEK está comprometida (i) con la creación y el mantenimiento de un entorno laboral respetuoso, que favorezca el trabajo en equipo y la dignidad de los colaboradores; (ii) con la oferta de un entorno laboral adecuado con miras a la seguridad, la higiene, la salud y el bienestar; y (iii) con el incentivo de la formación de los colaboradores.

1. Promoción de los derechos humanos, de la igualdad y del respeto por la diversidad y prohibición del prejuicio

El SEK respeta y apoya la protección de los derechos humanos y no consiente, no tolera cualquier abuso.

Las relaciones mantenidas por el Grupo SEK - Security Ecosystem Knowledge, la realización de sus negocios y los procesos de contratación y promoción profesionales deben garantizar la transparencia y criterios objetivos que promuevan un entorno ético, colaborativo y motivador, manteniendo una postura de abertura y respeto por la diversidad, sin tolerar cualquier tipo o forma de discriminación o prejuicio con relación a, entre otros, raza, género, creencia religiosa, orientación sexual, color, condición social y/o económica, nacionalidad, región deferente, equipo de fútbol, estado civil, etc.

En otras palabras, todos los colaboradores deben respetar las diversidades, la dignidad personal y la privacidad, impidiendo cualquier tipo de discriminación, racismo, prejuicio y acoso moral o sexual.

2. Prohibición del trabajo esclavo y menores o de infracciones de los derechos de la mujer

El SEK no admite, de ninguna forma, el trabajo esclavo, infantil y en condiciones inadecuadas de salud y seguridad y la infracción de los derechos de la mujer.

3. No tolerancia al acoso y al abuso de poder

El SEK no admite acosos – de naturaleza sexual, económica o moral – o situaciones que configuren presiones, intimidaciones o amenazas en las relaciones entre colaboradores, con independencia de nivel jerárquico.

4. Prohibición del uso de alcohol, drogas y tenencia de arma

Quedan terminantemente prohibidas la tenencia de armas y la ingesta de drogas y bebidas alcohólicas en el horario de trabajo y/o el ingreso a las empresas del Grupo SEK - Security Ecosystem Knowledge en estado de ebriedad o bajo el efecto de estupefacientes.

No se permiten armas de ninguna especie en las instalaciones del Grupo SEK - Security Ecosystem Knowledge, salvo para la ejecución de un contrato formalmente celebrado con el Grupo SEK - Security Ecosystem Knowledge; además, los profesionales que las porten estarán expresa y legalmente autorizados.

También se prohíbe expresamente cualquier actividad que favorezca o pueda favorecer, directa o indirectamente, el consumo y el comercio de drogas, interna o externamente, siendo que la mera sospecha en ese sentido ya debe comunicarse inmediatamente al superior inmediato, al Departamento Jurídico y/o a través del Canal de la Transparencia indicado en el capítulo XXII abajo.

5. Salud y seguridad en el entorno laboral

El SEK promueve un entorno laboral seguro y adopta medidas para proteger a los colaboradores que actúen en sus instalaciones, previniendo riesgos inherentes al trabajo. De esta forma, espera la misma conducta de sus colaboradores.

CAPÍTULO V – USO DE RECURSOS DE TECNOLOGÍA DE LA INFORMACIÓN, DESCARGAS Y CLAVES DE ACCESO

El SEK espera que sus recursos de tecnología se utilicen estrictamente para la ejecución de las funciones y los servicios contratados, según los límites de acceso y las autorizaciones que se concedan a los colaboradores. Los colaboradores deben usar los recursos de tecnología de forma racional, respetuosa y consciente y observar las directrices establecidas por Seguridad de la Información y las normas y las políticas de privacidad y protección de datos personales, además de aquéllas recogidas en este Código.

1. Derechos de propiedad intelectual

Los recursos de tecnología de la información no deben usarse para fines particulares y no se autorizan la descarga, la copia, el almacenamiento, la creación, la transmisión o la distribución de contenidos ilegales, criminales o que puedan vulnerar derechos de autor, restricciones o infracciones de licencias u otros derechos de propiedad intelectual. El colaborador que reciba ese tipo de material de otro colaborador debe comunicárselo al Canal de la Transparencia conforme a lo estipulado en el capítulo XXII abajo.

2. Claves de acceso

Las claves de acceso son herramientas de protección de las informaciones y los datos del Grupo SEK - Security Ecosystem Knowledge y, por ello, su uso siempre debe ser personal e intransferible. Se considera una vulneración de las directrices de este Código o intercambio de claves de acceso a sistemas informáticos.

3. Privacidad y protección de datos personales

El SEK respeta las leyes y los reglamentos referentes a la privacidad y la protección de datos personales en los países en que actúa. Para ello, asume el compromiso de promover la privacidad y la protección de los datos personales de cualquier titular de datos, en estricto cumplimiento de lo que dispone la Política de privacidad y protección de datos personales del Grupo SEK - Security Ecosystem Knowledge, además de sus procedimientos.

El SEK reitera que sus colaboradores y terceros deberán actuar de forma transparente y cumplidora de las exigencias legales y normativas sobre privacidad y protección de datos personales y alienta comunicaciones sobre eventuales vulneraciones de las normas o prácticas indebidas de privacidad y protección de datos personales a través del Canal de la Transparencia conforme a lo estipulado en el capítulo XXII abajo.

CAPÍTULO VI – INTERNET, CORREO, REDES SOCIALES

El SEK espera que sus colaboradores respeten los principios éticos y la legislación vigente en los países en que actúa siempre que utilicen Internet, el correo electrónico y las redes sociales en general, observando asimismo todas las orientaciones estipuladas en este *Código*, incluso en cuanto a las reglas de secreto y confidencialidad.

El uso de redes sociales relacionado con los temas y las empresas del Grupo SEK - Security Ecosystem Knowledge está limitado al departamento de *Marketing*. Ningún otro profesional, colaborador o no, está autorizado a registrar opiniones o contestar comentarios publicados en las redes sociales con el nombre de las empresas del Grupo SEK - Security Ecosystem Knowledge, incluso todas sus marcas y divisiones.

Al utilizar correos electrónicos corporativos, los colaboradores deben velar por la imagen y la seguridad de los datos del Grupo SEK - Security Ecosystem Knowledge y los datos personales que constan en sus entornos. También se debe prestar la debida atención para impedir que informaciones confidenciales queden vulnerables al alcance de terceros, con acceso no autorizado.

Cuando utilice mensajes electrónicos autorizados, el colaborador debe emplear un lenguaje compatible con el entorno profesional. Queda prohibido el uso inadecuado o indebido del correo electrónico corporativo, que incluye el intercambio, el envío o la recepción de mensajes para fines particulares. Queda prohibido enviar mensajes electrónicos corporativos a direcciones electrónicas particulares.

La participación en redes sociales (Facebook, Twitter, Instagram, grupos de WhatsApp, etc.) y otros foros, *blogs* u otros medios, de forma escrita o virtual, y

la respectivas opiniones o manifestaciones allí divulgadas se llevarán a cabo de forma que quede claro el carácter estrictamente personal del remitente, sin que se vincule, se mencione o se utilice, de cualquier forma, la imagen o el nombre de las empresas del Grupo SEK - Security Ecosystem Knowledge, sus marcas, divisiones o cualesquiera referencias que las identifiquen o asocien.

Todos los mensajes, datos e informaciones redactados, enviados o recibidos por los sistemas electrónicos y los recursos de tecnología de la información del Grupo SEK - Security Ecosystem Knowledge le pertenecen, de modo que éste puede utilizarlos, enterarse de ellos y transmitirlos a terceros como le convenga.

En el marco de la legislación vigente en los países en que el Grupo SEK - Security Ecosystem Knowledge actúa, éste se reserva el derecho de almacenar, auditar, interceptar, acceder, monitorear y revelar comunicaciones, incluso mensajes almacenados, recibidos o enviados por cualquier colaborador a través de los sistemas electrónicos de la empresa, sean o no sean servidores propios, sin obligatoriedad de notificación previa a quienquiera que sea. Están prohibidas cualesquiera acciones adoptadas por el colaborador para impedir el acceso de las empresas del Grupo SEK - Security Ecosystem Knowledge a las susodichas informaciones.

El uso de Internet por parte del colaborador se limitará al acceso a sitios web que estén relacionados con la realización de las funciones que ejerza en cualquiera de nuestras empresas y conforme a lo autorizado por el departamento de Tecnología de la Información. Queda prohibido el uso en actividades de carácter personal.

El SEK se reserva el derecho de monitorear todos los accesos a Internet y mensajes electrónicos, pudiendo evaluar, a su sola discreción, el uso excesivo, aplicando las medidas disciplinarias adecuadas.

CAPÍTULO VII – USO DE BIENES DE PROPIEDAD DE LAS EMPRESAS DEL GRUPO

El SEK espera que sus activos, físicos o financieros, se utilicen exclusivamente para las finalidades que establezca y exclusivamente en el ámbito de la ejecución de las actividades contratadas con sus colaboradores.

No se permite la utilización de cualquier activo de cualquiera de las empresas del Grupo SEK - Security Ecosystem Knowledge que no sea en su beneficio exclusivo y según los límites y de la forma que la autorice.

Los colaboradores son responsables del uso adecuado de los activos y su protección, evitando el desperdicio, la pérdida, los daños, el uso indebido, el hurto o el abuso.

Se espera la misma conducta con relación a áreas de uso común, siendo que los colaboradores deben utilizarlas de modo que siempre contribuyan positivamente al bienestar de todos.

CAPÍTULO VIII – COMPROMISO CON EL MEDIO AMBIENTE Y EL USO RACIONAL DE RECURSOS NATURALES

El SEK espera de sus colaboradores el uso racional de recursos naturales, como el agua y la energía, aplicando adecuados estándares de consumo en sus actividades, evitando el desperdicio y diseminando una cultura de responsabilidad ambiental.

El SEK realiza sus negocios y actividades con responsabilidad social y ambiental, protegiendo y respetando el medio ambiente y buscando la eliminación de impactos ambientales negativos que puedan dimanar de sus actividades. Por ese motivo, también espera que sus colaboradores prioricen ese tema en la gestión y la ejecución de sus actividades, priorizando el uso adecuado de recursos naturales, la prevención de la contaminación y de impactos ambientales y la destinación adecuada de residuos.

CAPÍTULO IX – RELACIÓN CON TERCEROS DE LA INICIATIVA PRIVADA

El SEK, incluso sus colaboradores, asume el compromiso de actuar de forma legal, transparente, ética y responsable en las relaciones con la iniciativa privada.

Las expectativas acordadas entre el Grupo SEK - Security Ecosystem Knowledge y terceros deben ser atendidas por ambas partes, de conformidad con los instrumentos jurídicos propios, la legislación aplicable en los países en que actúa, este *Código* y los procedimientos y las políticas eventualmente existentes. El SEK no observará cualquier dispositivo que vulnere las disposiciones mencionadas y que no esté alineado a los supuestos éticos en que cree.

Es obligatorio que terceros cumplan el *Código de conducta de terceros* del Grupo SEK - Security Ecosystem Knowledge y todas las políticas integrantes de su Programa de Integridad. El SEK cuenta con los colaboradores para la información adecuada a terceros en el marco de su Programa de Integridad.

El SEK se reserva el derecho de, sin que ninguna carga recarga sobre ello, terminar cualquier relación jurídica mantenida con terceros o colaboradores siempre que compruebe el incumplimiento de las obligaciones relacionadas con su Programa de Integridad, como sus políticas, códigos de conducta, valores éticos, entre otros.

1. Proveedores y socios

Tanto la selección como la contratación de proveedores y prestadores de servicios se fundan en criterios técnicos objetivos y prestablecidos, como la idoneidad, la capacidad técnica y de suministro, la calidad, los plazos y los precios vigentes, no permitiendo cualquier favorecimiento o discriminación.

El SEK está comprometida con la contratación de empresas que velen por la conducta ética en los negocios, evalúa a sus proveedores antes de la contratación – de conformidad con las leyes específicas del país en que se encuentren sus empresas – a fin de recopilar informaciones acerca de su idoneidad y evita negocios con proveedores de reputación dudosa.

Las relaciones del Grupo SEK - Security Ecosystem Knowledge con sus proveedores y socios se fundan en la ética, la transparencia y la imparcialidad y están libres de cualquier favorecimiento indebido. Así, no se permite que los colaboradores reciban cualquier tipo de gratificación, pago o comisión de proveedores, prestadores de servicios y socios. El colaborador que se entere de tal situación debe comunicarla inmediatamente al superior inmediato o a través del Canal de la Transparencia indicado en el capítulo XXII abajo.

2. Comisiones, "coimas" y rebajas para la iniciativa privada

Los colaboradores o sus familiares están terminantemente prohibidos de ofrecer, solicitar o prometer, directa o indirectamente, a cualesquiera terceros o aun de recibir de ellos cualesquiera "ventajas indebidas", como sobornos, comisiones, favores, rebajas en compras o contrataciones en general o cualquier otro tipo de favorecimiento en nombre propio, de terceros o de cualquiera de las empresas del Grupo SEK - Security Ecosystem Knowledge.

El SEK cree en la conducción ética y responsable de sus negocios y piensa que la corrupción en el medio corporativo provoca perjuicios inmensurables para la sociedad. La corrupción deconstruye los pilares básicos de la actuación de las empresas en un mercado libre, comprometiendo los criterios de elección por mejor precio, calidad y necesidad del servicio. Por eso, exige el compromiso ético y transparente de sus colaboradores en la conducción de sus negocios.

Quedan terminante prohibidos las comisiones, los sobornos, las rebajas, los descuentos y cualesquiera ventajas indebidas para o recibidos de la iniciativa pública, de conformidad con la Política anticorrupción y antisoborno del Grupo SEK - Security Ecosystem Knowledge.

A los efectos de este Código, el término "ventaja indebida" debe interpretarse de forma amplia e incluye cualquier beneficio (tangible o intangible) que posea valor o que pueda generar ganancias o ventajas para el receptor, incluso, entre otros, dinero, activos líquidos equivalentes, como tarjetas de regalo, viajes, comidas de precios excesivos, entradas, entretenimiento, hospitalidad, hospedaje, patrocinios, servicios – que no hayan sido solicitados, contratados y/o sometidos al proceso regular de acreditación y registro de proveedores establecido por las empresas del Grupo SEK - Security Ecosystem Knowledge–, además de préstamos, donaciones, descuentos indisponibles para el público, informaciones privilegiadas, becas de estudio o ayuda que estén fuera de las políticas y las reglas vigentes y establecidas por el Grupo SEK - Security Ecosystem Knowledge.

En caso de duda, no proceder y solicitar aclaraciones a través del Canal de la Transparencia indicado en el capítulo XXII abajo.

3. Obsequios, regalos y ventajas indebidas recibidos a consecuencia de relaciones con empresas privadas

El SEK espera que los obsequios, regalos y gratificaciones recibidos de terceros siempre se eviten y, cuando se reciban, que se atiendan las condiciones estipuladas en este *Código*.

Para evitar el riesgo o la incidencia o aun la apariencia de relaciones impropias, los colaboradores no deben ofrecer, solicitar, obtener o aceptar regalos en

general, así definidos como ventajas de cualquier naturaleza, como obsequios[1], entretenimiento[2], patrocinios, donaciones, entre otros (en adelante, los "Regalos"), en las relaciones con terceros de cualesquiera de las empresas del Grupo SEK - Security Ecosystem Knowledge.

Se podrán aceptar obsequios institucionales solamente cuando ofrecidos espontáneamente por cortesía de terceros, sin cualquier conflicto de intereses, y, además, con tal de que el monto correspondiente sea inferior a cincuenta dólares estadounidenses (USD 50,00). La autorización aquí estipulada no corresponde a relaciones con empresas públicas, como el gobierno, funcionarios u organismos públicos, de conformidad con el capítulo XI abajo, ya que se prohíbe terminantemente.

En el supuesto de que el colaborador reciba obsequios o regalos en desacuerdo con las reglas establecidas en este *Código*, deberá devolverlos al remitente con una carta explicativa, cuyo modelo se encuentra en el Anexo II, que lo informará sobre el necesario cumplimiento del Programa de Integridad y del *Código de conducta y ética* del Grupo SEK - Security Ecosystem Knowledge.

En caso de duda, no proceder y solicitar aclaraciones a través del Canal de la Transparencia indicado en el capítulo XXII abajo.

4. Entretenimiento

Quedan prohibidas la oferta o la recepción de ventajas relacionadas con el entretenimiento.

No podrán ser promovidos o alentados por terceros que mantengan o pretendan entablar relaciones con el Grupo SEK - Security Ecosystem Knowledge ni tampoco podrán ser recibidos o solicitados por los colaboradores cualesquiera tipos de patrocinio para entretenimiento, como fiestas de fin de año, conciertos, cursos y viajes, salvo cuando sean enviados previamente al Comité de Ética y éste los autorice expresamente. Al Comité de Ética le compete evaluar si tales eventos se refieren a casos infrecuentes o esporádicos, que no conlleven importes considerados excesivos, no representen cualquier conflicto de intereses y no influencien equivocadamente el juicio de los colaboradores.

El entretenimiento relacionado con entidades gubernamentales, funcionarios y organismos públicos debe observar las disposiciones recogidas en los capítulos XI y XII abajo.

5. Donaciones y patrocinios relacionados con empresas privadas

[1]A título de ejemplo, se consideran obsequios: lapiceros, camisetas / polos / remeras / poleras, llaveros, calendarios, entre otros, que contengan el logosímbolo de la empresa que ofreció el regalo y que no posean valor de mercado por encima del / de los límite/s establecido/s en este *Código de conducta y ética*.

[2] Son ejemplos de entretenimiento: entradas para el cine, eventos, conciertos, almuerzos, cenas, viajes, alojamiento, etc.

Las donaciones y los patrocinios que entidades privadas hagan "al" SEK o que sean realizados "por el" SEK a entidades privadas, a efectos de investigación, asistencia sanitaria, educación, filantropía, eventos, viajes o cualquier otra finalidad, deben ser actos desprendidos, sin la generación de cualquier tipo de ventaja o contrapartida material, no deben representar cualquier conflicto de intereses y deben registrarse contablemente.

Los patrocinios y las donaciones, cuando se satisfagan los supuestos arriba y cuando hayan sido debidamente autorizados por el Comité de Ética, siempre deben recibirse o pagarse de conformidad con las directrices documentadas en un contrato formalmente celebrado entre las partes. En cuanto a patrocinios, queda prohibido cualquier beneficio para el patrocinador que no se exprese debidamente en un contrato.

Cualquier colaborador que sea contactado por entidades o personas interesadas en ofrecer o solicitar donaciones o patrocinios debe reenviar la solicitud al Comité de Ética a través del Canal de la Transparencia indicado en el capítulo XXII abajo mediante el formulario recogido en el Anexo III.

Las donaciones y los patrocinios a entidades gubernamentales, funcionarios y organismos públicos deben observar las disposiciones recogidas en los capítulos XI y XII abajo.

CAPÍTULO X – RELACIONES CON EL GOBIERNO, FUNCIONARIOS Y ORGANISMOS PÚBLICOS

El SEK asume el compromiso de actuar de forma legal, transparente, ética y responsable en las relaciones con funcionarios públicos y la administración pública. El SEK espera que las relaciones entre colaboradores y funcionarios se funden en la ética y la transparencia, con base en las directrices legales y bajo los principios y las reglas descritos en este *Código* y en la *Política anticorrupción y antisoborno* del Grupo SEK - Security Ecosystem Knowledge.

"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.

"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.

El SEK no admite ninguna práctica de corrupción o soborno u oferta de ventaja indebida por parte de sus colaboradores, adoptando una política de "tolerancia cero" ante cualquier acción u omisión que pueda llevar a la vulneración de las disposiciones de las leyes específicas del país en que se encuentren sus empresas.

"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 ventajas indebidas. 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.

"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.

El SEK espera la cooperación de sus colaboradores, según la forma y los límites de la legislación correspondiente, con investigaciones o inspecciones realizadas por organismos, entidades o funcionarios públicos. El SEK no admite actos que puedan dificultar tales actividades y ellos deben ser inmediatamente comunicados al Departamento Jurídico y al de Cumplimiento.

Cualquier colaborador con relación de parentesco con funcionarios que posean poder decisorio en el ámbito de negocios y operaciones del Grupo SEK - Security Ecosystem Knowledge debe informar tal relación al Departamento Jurídico y al de Cumplimiento o a través del Canal de la Transparencia.

El SEK incentiva la denuncia de actos de corrupción y todos los que este *Código* repudie a través del Canal de la Transparencia, indicado en el capítulo XXII abajo. En caso de duda, no proceder y hacer una consulta por el Canal de la Transparencia.

CAPÍTULO XI – CONTRIBUCIONES POLÍTICAS

El SEK mantiene neutralidad política absoluta y no hace contribuciones, de cualquier forma, a partidos u organizaciones políticas o a candidatos a cargos electivos. En ese sentido, es prohibido hacer donaciones políticas a candidatos a cargos políticos o a partidos políticos por personas jurídicas, incluso con la finalidad de obtener ventajas o beneficios propios o para el Grupo SEK - Security Ecosystem Knowledge.

El SEK respeta el derecho de sus colaboradores de participar en el proceso político del país en que residen o internacionalmente, pero tal participación debe ocurrir de forma individual. Así, queda prohibido usar el nombre, los logotipos, las marcas y cualesquiera signos distintivos del Grupo SEK - Security Ecosystem Knowledge o dar la impresión de que actúa en su nombre.

Queda prohibida la propaganda política de cualquier especie en las instalaciones, los vehículos o los bienes de cualquiera de las empresas del Grupo SEK - Security Ecosystem Knowledge.

CAPÍTULO XII – LUCHA CONTRA EL LAVADO DE DINERO

El lavado de dinero es el intento de ocultar el origen ilícito de recursos financieros a través de la utilización de esos fondos en actividades legales para tratar de hacer que su origen parezca lícito.

Las empresas del Grupo SEK - Security Ecosystem Knowledge están obligadas a identificar, clasificar y cualificar a sus clientes y mantener el registro de todas las operaciones realizadas con ellos, adoptando políticas, procedimientos y controles internos compatibles con su tamaño y volumen de operaciones.

La práctica de lavado de dinero está prohibida.

El SEK espera que los colaboradores que posean pruebas o que sospechen de la ocurrencia de prácticas ilícitas las comuniquen inmediatamente al Departamento Jurídico, al de Cumplimiento o a través del Canal de la Transparencia indicado en el capítulo XXII.

CAPÍTULO XIII – COMPETENCIA

El SEK defiende la libertad de mercado y la libre iniciativa realizada con justicia, ética y observancia de las leyes en vigor en ellos países en que actúa. Los competidores deben ser tratados con respeto profesional y la competencia debe ser leal y saludable.

El SEK es contraria a cualquier tipo de acto ilegal y perjudicial para la libre competencia, como la celebración de acuerdos entre competidores de un mismo mercado, de forma explícita o implícita, con relación a precios, cuotas de producción y distribución o división territorial, con la finalidad de aumentar precios y beneficios conjuntamente. Por lo tanto, no son aceptables cualesquiera acciones que limiten o tengan la posibilidad de limitar la libre competencia.

Los colaboradores no deben propagar chismes o rumores que puedan mancillar la reputación de la competencia. Tampoco deben discutir con la competencia informaciones confidenciales y asuntos de carácter interno o reservado de las empresas del Grupo SEK - Security Ecosystem Knowledge.

Los colaboradores jamás deben obtener informaciones privilegiadas, planes o acciones de la competencia por medios ilegales y no deben transmitir ese tipo de informaciones de las empresas del Grupo SEK - Security Ecosystem Knowledge a la competencia.

Los colaboradores no deben divulgar informaciones confidenciales a la competencia, aun después de que ya no sean empleados o mantengan relaciones de trabajo o vinculación legal y reglamentaria con el Grupo SEK - Security Ecosystem Knowledge.

CAPÍTULO XIV – CONFLICTO DE INTERESES

El SEK rechaza cualquier contratación y/o establecimiento de obligación contaminada por un conflicto de intereses.

Se consideran conflictos de intereses todas las situaciones en que un colaborador o su cónyuge, hijo o familiar cercano posea intereses profesionales o personales que dificulten el cumplimiento, con imparcialidad, de sus obligaciones con el Grupo SEK - Security Ecosystem Knowledge, aunque ningún acto antiético o impropio resulte de ello. El colaborador también debe tratar de no poner el Grupo SEK - Security Ecosystem Knowledge en una situación de conflicto de intereses que pueda perjudicar sus negocios y su reputación.

Las siguientes son algunas posibles situaciones de conflictos de intereses que deben manejarse:

1. Participación de colaboradores en negocios / ganancias externas

El SEK reconoce y respeta el derecho individual de cada colaborador de participar en negocios externos, con tal de que no supongan un conflicto de intereses.

El SEK reconoce el derecho que los colaboradores tienen de realizar trabajos externos, con tal de que tales actividades sean lícitas, no entren en conflicto con sus responsabilidades y su horario de trabajo, no comprometan el buen desempeño de sus funciones y no pongan en riesgo los negocios del Grupo SEK - Security Ecosystem Knowledge.

Las oportunidades de ganancias personales extras fuera del Grupo SEK - Security Ecosystem Knowledge no deben conllevar absolutamente ninguna relación con el nombre de sus empresas y marcas, productos o negocios. Tampoco deben estar asociadas al uso de influencias, relaciones, informaciones consideradas confidenciales u otros recursos de cualquiera de las empresas del Grupo SEK - Security Ecosystem Knowledge.

2. Precauciones en la participación de colaboradores en el ejercicio de sus funciones

Los colaboradores no pueden utilizar informaciones privilegiadas o confidenciales del Grupo SEK - Security Ecosystem Knowledge que se obtengan en función de su posición o cargo para beneficio personal o ganancia indirecta.

Los colaboradores deben evitar cualquier negocio o acción personal que entre en conflicto o tenga la apariencia de conflicto con los negocios y los intereses del Grupo SEK - Security Ecosystem Knowledge y no facilitar, a título de amistad o parentesco, la aceptación de terceros sin tener en cuenta los criterios de acreditación de acuerdo con la legislación vigente en los países en que actúa, este *Código* y/o las políticas del Grupo SEK - Security Ecosystem Knowledge, que puedan venir a comprometer el profesionalismo, la imparcialidad, la transparencia y la seriedad con los cuales se deben realizar los negocios.

3. Relaciones de parentesco

El SEK establece reglas de relaciones de parentesco que tienen en cuenta su derecho legal de evitar conflictos de intereses.

No se permite el trabajo de familiares consanguíneos o afines en línea recta o colaterales hasta el segundo grado (padre, madre, hijo, cónyuge, primos, hermanos, compañeros, etc.) en un solo departamento o en áreas afines o interrelacionadas.

Se consideran departamentos afines o interrelacionados, por ejemplo, Contabilidad y Cuentas por Pagar, Compras y Cuentas por Pagar, entre otros.

Los casos ya existentes en el momento de la divulgación de este *Código* constituirán una excepción a esta norma, con tal de que sean comunicados al Comité de Ética a través del Canal de la Transparencia informado en el capítulo XXII abajo. Se pueden evaluar nuevos casos para la autorización específica del Comité de Ética, con tal de que sean debidamente justificados y se compruebe la necesidad.

4. Participación de colaboradores en empresas de terceros

No es aceptable que los colaboradores mantengan relaciones de trabajo o de sociedad, formales o informales, con los proveedores o los competidores del Grupo SEK - Security Ecosystem Knowledge.

No se admite la participación de cualquier colaborador o de sus familiares consanguíneos, en línea recta, hasta el primer grado, a título de sociedad o en el desempeño de funciones de gestión, en terceros relacionados con el Grupo SEK - Security Ecosystem Knowledge durante la vigencia del contrato de trabajo o de vinculación legal y reglamentaria.

Se incluye en esa prohibición la participación como socio oculto en sociedades en comandita (sociedades de hecho), consorcios, sociedades comerciales o cualquier otro tipo de asociación.

Se excluyen de tal prohibición las participaciones de colaboradores que existan antes de la fecha de inicio de la relación de trabajo con el Grupo SEK - Security Ecosystem Knowledge y que hayan sido declaradas por escrito con ocasión de la contratación.

Se hará una excepción cuando tal participación ocurra en empresas de capital abierto, con acciones en bolsas de valores, cuando no rebase el uno por ciento (1%) del capital social de terceros o con la aprobación expresa del Comité de Ética del Grupo SEK - Security Ecosystem Knowledge.

5. Inversiones en negocios de la competencia

No se permiten inversiones, por parte de los colaboradores, en negocios que compitan con las actividades del Grupo SEK - Security Ecosystem Knowledge durante la vigencia del contrato de trabajo y/o de la vinculación legal y reglamentaria de los administradores, con tal de que se respeten las leyes específicas del país en que se encuentren sus empresas.

En todo caso, el colaborador está obligado a mantener el secreto, incluso después del término del contrato de trabajo y/o de la vinculación legal y reglamentaria, acerca de todas las informaciones confidenciales relativas a secretos comerciales

e informaciones confidenciales a que tenga acceso en virtud de su actuación en el Grupo SEK - Security Ecosystem Knowledge.

CAPÍTULO XV – INFORMACIONES SENSIBLES Y CONFIDENCIALES

Ningún colaborador está autorizado a utilizar las informaciones confidenciales del Grupo SEK - Security Ecosystem Knowledge, salvo en caso de autorización previa del Grupo SEK - Security Ecosystem Knowledge o determinación por orden judicial.

En función del cargo que ocupa, el colaborador podrá tener acceso a informaciones sobre los negocios del Grupo SEK - Security Ecosystem Knowledge o cualquiera de sus empresas. De todos modos, si, en función del cargo o no, con tal de que el acceso haya ocurrido estrictamente dentro de las reglas de este *Código* y demás normas internas del Grupo SEK - Security Ecosystem Knowledge, todas y cada una de las informaciones, de naturaleza técnica, operacional, jurídica, comercial, industrial, entre otras, incluso, sin limitaciones, la investigación, la especificación, la metodología, la formulación los insumos, los compuestos, las estrategias de negocios, los datos personales, los datos financieros, los datos sobre sueldos, los datos sobre clientes y proveedores, las informaciones sobre sistemas de apoyo, la calidad, etc., representan activos del Grupo SEK - Security Ecosystem Knowledge y pertenecen a él y a sus empresas exclusivamente, siendo que los colaboradores deben considerarlas "informaciones confidenciales". Eso también corresponde a las informaciones de terceros, protegidas por los contratos de confidencialidad celebrados con las empresas del Grupo SEK - Security Ecosystem Knowledge, y todas las que les sean transmitidas como confidenciales.

Se deben considerar las informaciones confidenciales con independencia del medio por que se reciban, por escrito, electrónica, digital o verbalmente o por cualquier otro proceso de registro o almacenamiento de datos.

Cualquier información confidencial debe mantenerse en secreto absoluto, a menos que tales informaciones pasen al dominio público, de forma inequívoca, por el propio SEK.

Los colaboradores deben velar por la confidencialidad y la protección de las informaciones confidenciales y no podrán divulgarlas a cualesquiera terceros, bajo cualquier concepto o pretexto, ni reproducirlas, retenerlas, cederlas, explotarlas o disponer de tales informaciones, de conformidad con las sanciones estipuladas en la legislación aplicable en los países en que actúa.

Las eventuales excepciones solamente se admiten mediante autorización previa y expresa formalizada por escrito por el Grupo SEK - Security Ecosystem Knowledge, a través de sus representantes legales, con poderes para ello.

En caso de duda, consultar al Comité de Ético a través del Canal de la Transparencia indicado en el capítulo XXII abajo.

CAPÍTULO XVI – REGISTROS CONTABLES

El SEK respeta las leyes y los reglamentos correspondientes a los registros contables en los países en que actúa, no admitiendo excepciones a su cumplimiento.

Todas las transacciones y operaciones del Grupo SEK - Security Ecosystem Knowledge deben ser respaldadas por documentos adecuados y registrados correcta y oportunamente, todos los impuestos deben haber sido debidamente pagados y registrados de conformidad con la legislación aplicable en los países en que actúa, con exactitud, estrictamente de acuerdo con la naturaleza de la operación.

Los registros de las actividades financieras y la contabilidad deben realizarse de forma exacta, completa y verdadera, y los controles relacionados deberán garantizar la rápida preparación y fiabilidad de informes y estados financieros. En el Grupo SEK - Security Ecosystem Knowledge, los colaboradores deben cooperar, sin restricciones, con auditorías internas y externas.

No se aprobará ni se realizará cualquier pago con la intención o la ciencia de que, total o parcialmente, se utilice para cualquier finalidad que no se describa en el documento comprobatorio de pago.

CAPÍTULO XVII- COMUNICACIÓN Y DECLARACIONES A LA PRENSA

El SEK mantiene un diálogo abierto y sistemático y se compromete a transmitir las informaciones necesarias con transparencia y veracidad.

Los colaboradores no están autorizados a hacer declaraciones a la prensa, que pueden ser realizadas exclusivamente por representantes autorizados y con la participación del gabinete de prensa a discreción de este último.

Las informaciones sobre los servicios prestados deben ser verdaderas, completas, actualizadas y, siempre que corresponda y sea necesario, respaldadas por pruebas científicas para promover una interlocución ética y fiable con sus partes interesadas.

CAPÍTULO XVIII – PROTECCIÓN DE LA PROPIEDAD INTELECTUAL

El *software*, las marcas, los signos distintivos, los conocimientos producidos internamente y los demás bienes de propiedad intelectual constituyen el patrimonio institucional del Grupo SEK - Security Ecosystem Knowledge y siempre deben ser protegidos por todos los colaboradores. Los sistemas, los programas o las aplicaciones desarrollados, creados o modificados con equipos y recursos del Grupo SEK - Security Ecosystem Knowledge por sus colaboradores durante la vigencia del contrato de trabajo pertenecen al SEK.

La propiedad intelectual respecta al derecho de protección de las ideas y las creaciones desarrolladas internamente o en sociedad e incluye la marca, la patente, los derechos de autor, el registro de *software*, etc.

Se debe proteger la propiedad intelectual de las empresas del Grupo SEK - Security Ecosystem Knowledge con relación al mal uso, a desviaciones o a la utilización indebida. El mismo cuidado y respeto deben observarse con relación a la propiedad intelectual de terceros.

CAPÍTULO XIX – GESTIÓN DE ÉTICA Y EL COMITÉ DE ÉTICA

Le compete a cada uno de los colaboradores del Grupo SEK - Security Ecosystem Knowledge velar por la gestión adecuada de la ética y la integridad en los negocios del Grupo SEK - Security Ecosystem Knowledge y por la observancia integral de este *Código* y de su Programa de Integridad.

El Comité de Ética es responsable de apoyar y promover acciones que traten de garantizar el cumplimiento de este *Código*, incluso demás políticas y procedimientos que hayan sido instituidos en el ámbito del Programa de Integridad del Grupo SEK - Security Ecosystem Knowledge.

El Comité de Ética es un organismo colegiado y funciona en carácter permanente. Depende del Consejo de Administración y tiene garantizada una estructura propia e independiente. Está compuesto por, como mínimo, tres (3) miembros titulares elegidos por el susodicho organismo.

Entre otras atribuciones estipuladas en su reglamento interior, el Comité de Ética debe:

- Evaluar permanentemente la actualidad y la pertinencia de este *Código*;
- Aprobar el cronograma de entrenamiento;
- Evaluar los casos de vulneración del *Código*; y
- Contestar y aclarar las dudas de colaboradores y terceros;
- Recomendar soluciones eficaces y oportunas para los conflictos éticos.

CAPÍTULO XX – DISPOSICIONES LOCALES ESPECÍFICAS

Los términos y las condiciones de este *Código* corresponden a todas las empresas y todos los colaboradores del Grupo SEK - Security Ecosystem Knowledge, con independencia del país en que se ubiquen.

Este *Código* tiene como supuesto el establecimiento de condiciones generales que todos los colaboradores y empresas del Grupo SEK - Security Ecosystem Knowledge deben seguir y observar, pero sin dispensar la obligación de observancia y cumplimiento de las leyes y las normas locales específicas de cada país, incluso, sin limitaciones, las recogidas en las normas de referencia mencionadas, a título de ejemplo, en el Anexo IV de este *Código*.

Si las leyes específicas del país en que las empresas del Grupo SEK - Security Ecosystem Knowledge se encuentran lo exigen, el presente *Código* podrá adjuntarse al reglamento interior de trabajo de sus empresas.

Cuando existan conflictos aparentes entre los estándares definidos en las leyes, los códigos, las reglas y los reglamentos locales o en caso de duda por parte de los colaboradores, el Canal de la Transparencia indicado en el capítulo XXII deberá ser habilitado para aclaraciones y orientaciones.

CAPÍTULO XXI – DENUNCIA DE VULNERACIONES Y EL CANAL DE LA TRANSPARENCIA

El SEK incentiva la comunicación sobre vulneraciones del presente *Código* y demás políticas del Programa de Integridad y no tolera ninguna retaliación o

represalia contra el denunciante. También incentiva la aclaración de dudas y el amplio uso del Canal de la Transparencia como herramienta por parte de sus colaboradores.

Los colaboradores tienen el deber de comunicar las vulneraciones o posibles infracciones de las directrices de este *Código* y demás políticas y reglas establecidas por el Programa de Integridad del Grupo SEK - Security Ecosystem Knowledge. Se puede realizar la comunicación al departamento de Cumplimiento o a través del Canal de la Transparencia, disponible en: https://www.canaldatransparencia.com.br/seksecurityecosystemknowledge/

El Canal de la Transparencia es administrado por una empresa externa e independiente para brindar anonimato al denunciante, si es que 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.

No se toleran represalias contra los denunciantes.

CAPÍTULO XXII – RESPONSABILIDADES

Es de responsabilidad de todos los colaboradores difundir el presente *Código* y hacer que cualesquiera terceros también asuman un compromiso con los susodichos documentos.

El SEK 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 arriba.

***

El presente *Código de conducta y ética* ha sido aprobado por el Consejo de Administración de CBS Holding Global, Ltd. en una reunión celebrada el 28/4/2022.

Anexo I

DECLARACIÓN DE CONOCIMIENTO Y ADHESIÓN AL CÓDIGO DE CONDUCTA Y ÉTICA
del Grupo SEK - Security Ecosystem Knowledge – colaboradores

El colaborador infrascrito DECLARA que ha recibido una copia del CÓDIGO DE CONDUCTA Y ÉTICA DEL SEK, comprometiéndose a leerlo integralmente, solicitar aclaraciones en caso de cualquier duda y obligándose a cumplir el susodicho *Código* plenamente en el ejercicio de sus actividades dimanantes del contrato de trabajo firmado.

Por fin, DECLARA que todas las informaciones que haya facilitado son correctas, completas y verdaderas y reconoce que la prestación de informaciones incorrectas o su omisión pueden conllevar sanciones disciplinarias.

[lugar], [•] de [•] de [•].

_____
Nombre completo
Firma

Anexo II

MODELO DE CARTA EXPLICATIVA
[CONFORME A LO MENCIONADO EN EL CAPÍTULO X (3)]

A la atención de
.....

REF.: Programa de Integridad – Devolución de obsequios o regalos

Estimados señores,

Tenemos el inmenso honor de recibir el obsequio / regalo descrito abajo, que amablemente nos enviaron, sin embargo, solamente en razón de determinaciones establecidas en nuestro Programa de Integridad, estamos impedidos de aceptarlo.

- [describir obsequio / regalo].

De esta forma, con esta carta, le devolvemos el susodicho obsequio / regalo y le agradecemos la atención y la amabilidad que nos han brindado.

Con nuestros mejores deseos,

Atentamente,

_____
[firma y nombre]

Anexo III

FORMULARIO DE AUTORIZACIÓN DE DONACIÓN Y PATROCINIO
[CONFORME A LO MENCIONADO EN EL CAPÍTULO X (5)]

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

Por el presente les informo que hemos recibido una solicitud referente a [pedido / recepción] de [donación / patrocinio] como sigue:

Empresa:
Tipo de donación / patrocinio: [bienes o dinero o ventajas]
Cuantía en cuestión:
Descripción de los bienes, derechos u otras ventajas (congresos, almuerzos, etc.):
Motivo de la donación / del patrocinio:
Describir el eventual conflicto de intereses:

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 pueden conllevar sanciones legales y contractuales. Otrosí, DECLARO que no hay ninguna situación de conflicto de intereses que denunciar, además de la que he descrito arriba.

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

[lugar], [•] de [•] de [•].

_____
Nombre completo
Firma

Anexo IV
Normas de referencia

El SEK respeta las leyes y las normas de los países en que actúa, incluso, entre otras, a título de ejemplo:

a) **Argentina:** Ley 27401/17 – Establece régimen de responsabilidad penal para las personas jurídicas por delitos cometidos contra la administración pública y cohecho transnacional;
b) **Brasil:** Ley 12846/13 – *Ley anticorrupción*;
c) **Chile:** Ley 20393/09 – Establece la responsabilidad penal de las personas jurídicas en los delitos de lavado de activos, financiamiento del terrorismo y delitos de cohecho que indica;
d) **Colombia:** SAGRILAFT; Ley 1778 del 2016 – *Ley Antisoborno*;
e) **Perú:** *Ley del código de ética en la función pública* (Ley 27815) y su reglamento aprobado por el Decreto Supremo nro. 033-2005-PCM.