

Cómo lideramos con confianza: Código de conducta comercial de Cisco

Mensaje de bienvenida de Chuck Robbins, presidente y director general

Equipo:

Uno de los principales diferenciadores de Cisco es la confianza que hemos construido con nuestras partes interesadas tanto internas como externas. Esta confianza es una parte integral de lo que somos en Cisco, y la ganamos y protegemos cada día, en cada interacción. Combinar la ética y la integridad en todo lo que hacemos es una responsabilidad compartida, y depende de cada uno de nosotros comprometernos a actuar siempre de la manera correcta.

Nuestro Código de conducta comercial (el Código) establece los principios que seguimos y los estándares deliberadamente altos que nos exigimos. Lo utilizamos para guiar nuestras acciones y decisiones diarias: en la forma en que desarrollamos productos y servicios, interactuamos con los clientes, colaboramos con nuestros partners y proveedores o apoyamos otras áreas de nuestro negocio. No obstante, nuestro Código es solo el punto de partida.

Aplicar nuestro Código y cumplir las políticas de Cisco ayudará a cada uno de nosotros a gestionar los riesgos inherentes a nuestras funciones y, en última instancia, a impulsar nuestro éxito colectivo. Gracias por su compromiso con los principios y las normas establecidos en nuestro Código, y por su atención constante para proteger y preservar la confianza que hemos construido juntos.



Chuck Robbins
Presidente y director general



Contenido

Conocemos nuestro Código y hablamos cuando es necesario

- 04 Opciones para informar
- 04 Prohibición de represalias

Protegemos los activos y la información de Cisco y de terceros

- 06 Protección de los activos físicos
- 06 Uso responsable y seguro de la tecnología
- 07 Gestión responsable de la información y los datos
- 08 Protección y respeto de los derechos de propiedad intelectual

Competimos de manera justa y en cumplimiento de la ley

- 10 Fomento de la competencia
- 11 Prevención del soborno y la corrupción
- 12 Cumplimiento de las normas para hacer negocios con el sector público
- 12 Observancia de los requisitos del comercio internacional

Nos manejamos con precisión, honestidad e integridad

- 14 Documentación y generación de informes precisos de la información
- 15 Obtención de las aprobaciones necesarias y cumplimiento de los controles internos
- 16 Cumplimiento de los requisitos de registro y retención de documentos

Separamos los intereses personales y comerciales

- 18 Gestión de conflictos de intereses
- 19 Prevención del uso de información privilegiada
- 20 Prudencia al hablar en público
- 20 Separación de la participación política personal

Promovemos entornos de trabajo seguros y respetuosos, dentro y fuera de Cisco

- 22 Respeto hacia los demás y expectativa de trato respetuoso
- 23 Fomento de entornos de trabajo seguros
- 23 Cumplimiento de nuestras obligaciones externas
- 24 Nuestras responsabilidades

Conocemos nuestro Código y hablamos cuando es necesario

Todas las personas en Cisco tienen la oportunidad de contribuir a la innovación y la excelencia. Lo hacemos siendo personas confiables, responsables y comprometidas con nuestras acciones.

Nuestro Código es una guía útil para actuar con confianza dentro de nuestro negocio y en nuestras relaciones con terceros. Se aplica a todos los empleados, directores y funcionarios de Cisco, así como a todas las filiales y empresas subsidiarias de Cisco. Lea y utilice nuestro Código cuando tenga dudas.

Ser confiables y responsables no significa tener siempre todas las respuestas, pero sí implica tomar medidas para encontrarlas. Cuando una decisión no esté clara, revise primero nuestro Código y la orientación vinculada en él. Si necesita ayuda o tiene preguntas, consulte con administración, con cualquier líder de Cisco o con los equipos de Personas y Comunidades, Finanzas o Legal. Haga preguntas siempre que tenga dudas; envíe un correo electrónico al [equipo de Ética y Cumplimiento](#) para recibir orientación. Todos debemos ejercer el buen juicio y actuar de forma responsable.

Todos tenemos la responsabilidad de alzar la voz cuando algo no parece correcto, incluso si no contamos con todos los detalles. Si ve o sospecha una infracción de nuestro Código o de una política de Cisco, hable al respecto. Puede informar de forma anónima, cuando la ley lo permita, a través de [Cisco EthicsLine](#). El informe se gestionará de forma rápida, eficiente y con el máximo esfuerzo para mantener la confidencialidad.

Opciones para informar

Hay varias opciones para informar inquietudes. Elija la opción que le resulte más cómoda.

- [Cisco EthicsLine](#) (disponible por formulario web o teléfono, 24 horas al día, 7 días a la semana, en 27 idiomas)
- Su gerente
- Su representante de Personas y Comunidades
- El equipo Legal o de Finanzas
- [El equipo de Ética y Cumplimiento](#)
- [Threat.Cisco.com](#) para incidentes de ciberseguridad o de datos conocidos o sospechados
- [Centros de seguridad corporativa](#) para cuestiones de seguridad física
- [Relaciones laborales globales](#) para asuntos personales y del entorno laboral

Prohibición de represalias

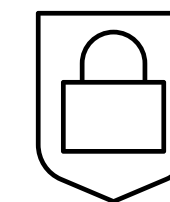
En Cisco valoramos la comunicación abierta y transparente, y nos comprometemos a gestionar las inquietudes con cuidado. Cisco apoya a quienes plantean preocupaciones de buena fe, incluso si finalmente resultan infundadas. Las represalias y las amenazas de represalias están estrictamente prohibidas. Tomar represalias contra alguien que hace una pregunta, plantea una preocupación genuina o participa en una investigación constituye, en sí mismo, una infracción de nuestro Código.



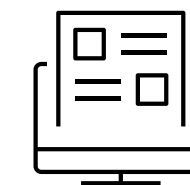
Las personas con funciones de liderazgo modelan la confianza y la responsabilidad todos los días. Como líder, es responsable de crear un entorno en el que las personas se sientan seguras para hablar, hacer preguntas y plantear inquietudes sin temor a represalias. Nunca presione a los empleados para lograr resultados de una manera que infrinja nuestro Código, las políticas de Cisco o la ley. Informe las inquietudes de inmediato utilizando la [Cisco EthicsLine](#) o la opción de informar que sienta más cómoda.

Protegemos los activos y la información de Cisco y de terceros

Los activos de Cisco son fundamentales para nuestro negocio y nuestro éxito a largo plazo. Debemos protegerlos y utilizarlos adecuadamente; esto incluye espacios físicos, dispositivos, software, propiedad intelectual y datos. Del mismo modo, al gestionar activos o información de terceros, debemos protegerlos y utilizarlos únicamente según lo autorizado y para su propósito previsto. Respetar los derechos de propiedad preserva la confianza de nuestros clientes, partners y proveedores.



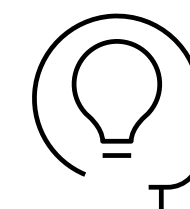
Protección de los
activos físicos



Gestión responsable
de la información y los
datos



Uso responsable
y seguro de la
tecnología



Protección y respeto
de los derechos de
propiedad intelectual

Protección de los activos físicos

Todos somos responsables de proteger los activos físicos de Cisco, desde los espacios de trabajo y las instalaciones hasta las computadoras, los dispositivos, los equipos y los suministros. Los activos de Cisco son para uso empresarial y deben tratarse con cuidado.

La confianza significa:

- ➞ Proteger los activos contra robos, daños, desperdicio y uso indebido. Esto incluye asegurar los dispositivos cuando no están en uso.
- ➞ No tomar prestados ni retirar activos de Cisco de las instalaciones sin la debida autorización.

Tenga en cuenta lo siguiente

Los activos de Cisco se deben utilizar con fines comerciales y de manera responsable, segura y conforme a las políticas de Cisco. El uso de los activos de Cisco no es privado. Para proteger la propiedad y los recursos de la empresa, Cisco puede supervisar los activos y dispositivos utilizados para realizar actividades comerciales.

Más información [Uso de la Política de activos de Cisco](#)
[Uso de la Política de instalaciones de Cisco](#)

Uso responsable y seguro de la tecnología

Las redes, las plataformas, el software y otras tecnologías son esenciales para nuestro trabajo, pero el uso indebido o los errores pueden dar lugar a ciberdelitos, accesos no autorizados a datos, pérdida de información confidencial, daños de la reputación, sanciones regulatorias o litigios. Los incidentes pueden producirse en un instante, por lo que es fundamental mantenerse alerta y cumplir todas las políticas de Cisco relacionadas con la seguridad, la privacidad y el uso de la inteligencia artificial.

La confianza significa:

- ➞ Crear contraseñas sólidas, proteger las credenciales de inicio de sesión y utilizar autenticación multifactor.
- ➞ Conectarse a una red Cisco o red privada virtual (VPN) al acceder a información confidencial y no intentar deshabilitar ni eludir los controles de red.
- ➞ Verificar los sitios web y estar alerta frente a la suplantación de identidad (phishing) y otros ataques de ingeniería social.
- ➞ Descargar únicamente software aprobado y mantener los dispositivos y aplicaciones actualizados.
- ➞ No acceder, distribuir, descargar ni cargar material ilegal o inapropiado.

Más información

[Política de uso aceptable](#)
[Norma de dispositivos confiables](#)
[Keep Cisco Safe](#)

Gestión responsable de la información y los datos

La información y los datos también son activos valiosos, y la forma en que los gestionamos es fundamental para mantener la confianza en Cisco. Gran parte de la información que manejamos en nuestro trabajo es propiedad de Cisco y debe protegerse. La información confidencial, ya sea de Cisco, de clientes, partners u otros terceros, requiere especial cuidado. Todos somos responsables de prevenir pérdidas o filtraciones de datos y de no acceder, usar ni compartir información de forma indebida.

La confianza significa:

- ➔ Seguir las políticas de manejo y [clasificación de datos](#) de Cisco.
- ➔ Recopilar, acceder y compartir información exclusiva, confidencial y de terceros únicamente cuando esté autorizado y para un propósito comercial válido.
- ➔ Usar la inteligencia artificial de manera responsable: solo utilizando herramientas de IA aprobadas y solo con el nivel de clasificación de datos permitido para cada herramienta específica.
- ➔ Manejar los datos personales con sensibilidad, transparencia, equidad y responsabilidad; observar los requisitos especiales al manejar datos personales sensibles, como información de salud protegida u otros datos regulados.
- ➔ Prevenir la divulgación inapropiada de información confidencial y exclusiva, y evitar mostrarla o conversar sobre ella en lugares donde otros puedan ver o escuchar.
- ➔ Informar de inmediato toda sospecha de exposición de información confidencial en [Threat.Cisco.com](#).

Más información

[Política de protección de datos](#)

[Centro de excelencia en privacidad: políticas y normas](#)

[Norma sobre protección de datos](#)

[Clasificación y taxonomía de datos](#)

[Gestión de inteligencia artificial](#)

Tenga en cuenta lo siguiente

Casi toda la información de propiedad de Cisco o generada por Cisco es confidencial, incluido lo siguiente:

- Planes de negocio, proyecciones o desarrollos de la empresa
- Ganancias, resultados no anunciados y otros datos financieros
- Comunicaciones de la administración
- Información empresarial diaria en nuestros sistemas y redes
- Software, código y otras innovaciones y trabajos creativos, como manuales, activos de marca y material de sitios web

Se entiende por “Datos personales” (o información de identificación personal [PII]) todo tipo de información que pueda utilizarse razonablemente para identificar a un individuo o hacerlo de otra manera identificable y pueden incluir nombre, dirección, dirección de correo electrónico, número de teléfono o credenciales de inicio de sesión.

- **Datos personales confidenciales** hace referencia a un subconjunto de datos personales que están categorizados como sensibles por la ley, relacionados con individuos en comunidades vulnerables, que requieren notificación de violación, o que pueden causar daño significativo si se exponen (por ejemplo, discriminación, robo de identidad, daño físico o financiero).

Protección y respeto de los derechos de propiedad intelectual

La propiedad intelectual es la base de nuestros productos, nuestra marca y nuestro negocio. Estos activos son críticos para el liderazgo continuo de Cisco en la industria y nos diferencian frente a nuestros clientes. Nosotros protegemos estos activos y respetamos los derechos de propiedad intelectual de terceros. La confianza de nuestros clientes, partners e incluso competidores depende de preservar los derechos de propiedad intelectual dentro y fuera de Cisco.

La confianza significa:

- ➞ Usar las marcas comerciales, los trabajos con derechos de autor y otra propiedad intelectual de Cisco solo para fines comerciales aprobados.
- ➞ Informar el uso no ético o no autorizado de la propiedad intelectual, por ejemplo, nuestro logotipo o código fuente.
- ➞ Reconocer la propiedad intelectual de terceros; nunca acceder, distribuir, descargar ni cargarla sin permiso; y no trasladar los secretos comerciales de empleadores anteriores a Cisco.
- ➞ Recordar que las mejoras o creaciones que realice durante su trabajo, incluidas las innovaciones técnicas, pertenecen a Cisco.
- ➞ Divulgar de manera oportuna las actividades de desarrollo externas, incluidas las contribuciones a proyectos de código abierto, incluso si se realizan en su tiempo libre.

Más información

[Cisco Intellectual Property Online \(CIPOL\)](#)

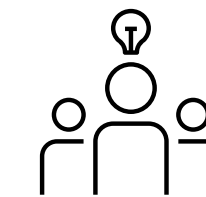


Tenga en cuenta lo siguiente

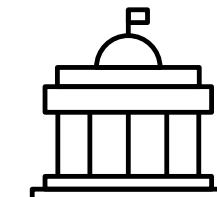
La propiedad intelectual es intangible e incluye patentes, derechos de autor, marcas comerciales y secretos comerciales. Comprende desde nuestro código fuente, procesos de fabricación, materiales de capacitación y conocimiento técnico interno.

Competimos de manera justa y cumpliendo la ley

Generamos confianza al competir de manera justa y al apoyarnos en la calidad y el valor de las ofertas de Cisco. Competimos con vigorosidad, pero de manera ética y legal. Recuerde, ganar no solo depende de lo que vendemos, sino de cómo lo vendemos.



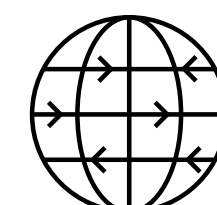
Fomento de la competencia



Cumplimiento de las normas para hacer negocios con el sector público



Prevención del soborno y la corrupción



Observancia de los requisitos del comercio internacional

Fomento de la competencia

Cisco fomenta la competencia en el mercado, lo cual beneficia a los clientes y promueve la innovación. Prohibimos prácticas comerciales que reduzcan la competencia, incluso de manera indirecta o no intencional. Esto se aplica a la manera en que interactuamos con los competidores, trabajamos con los partners de canal y nos relacionamos con los clientes.

La confianza significa:

- ➞ Nunca coordinar acciones ni compartir información competitivamente sensible con competidores, incluidos precios, clientes o datos de mercado.
- ➞ Promover la competencia entre partners de canal tratándolos de manera justa y basada en criterios objetivos, especialmente respecto a descuentos y oportunidades de clientes.
- ➞ No establecer precios de reventa ni márgenes para partners de canal ni fijar precios con clientes que compren a través de ellos.

Más información [Política antimonopolio](#)
[Capacitación y cumplimiento antimonopolio](#)

Prevención del soborno y la corrupción

Desarrollamos nuestro negocio de manera transparente y honesta, y exigimos lo mismo de nuestros partners y proveedores. No toleramos el soborno ni la corrupción en ningún aspecto de nuestro negocio.

La confianza significa:

- ➔ Ganar negocios por mérito, y nunca ofrecer, dar o aceptar algo de valor para influir indebidamente en decisiones comerciales u obtener una ventaja injusta.
- ➔ Ofrecer o aceptar únicamente obsequios, viajes, entretenimiento u otras cosas de valor que tengan un propósito comercial legítimo, razonable y permitido por la ley y las políticas aplicables.
- ➔ Identificar empleados del gobierno o de entidades estatales (G/SOE) y obtener aprobaciones necesarias antes de ofrecerles cualquier cosa de valor.
- ➔ Obtener aprobaciones previas y documentar claramente la base objetiva para ofrecer descuentos no estándar, incentivos y otros beneficios discrecionales.
- ➔ No permitir nunca que un tercero haga en nombre de Cisco algo que Cisco no tiene permitido hacer por sí misma.
- ➔ Al interactuar con proveedores, partners u otros terceros, seguir los procesos de incorporación, monitorear sus actividades y abordar rápidamente cualquier inquietud que pueda surgir.

Más información

[Política global anticorrupción y antisoborno](#)

[Obsequios, viajes y entretenimiento \(GTE\)](#)

[Lineamientos sobre las cortesías en el sector público de EE. UU.](#)

[Herramienta de búsqueda de G/SOE](#)

[Código de conducta del proveedor](#)

[Código de conducta para partners](#)

Tenga en cuenta lo siguiente

“**Cualquier cosa de valor**” es más que obsequios, comidas, viajes, alojamiento o entretenimiento. Las donaciones caritativas, patrocinios, descuentos no estándar, incentivos de canal, condiciones comerciales favorables y favores o beneficios personales, como préstamos, educación, empleos (pagados o no) u oportunidades de inversión, son todos “cosas de valor”. Cualquier cosa de valor puede considerarse un soborno si se otorga con un propósito indebido.

Los funcionarios gubernamentales incluyen a cualquier persona que trabaje para una **entidad gubernamental o entidad de propiedad estatal (G/SOE)**, comúnmente denominada “sector público”.

- Hay una definición completa de G/SOE en la [Política de obsequios, viajes y entretenimiento](#).
- No siempre está claro si una entidad es una G/SOE. La segmentación de ventas no es un indicador confiable.
- La definición de Cisco puede diferir de la forma en que las entidades se definen por ley. Por lo tanto, tómese el tiempo necesario para revisar la definición y utilice las herramientas y recursos de Cisco para identificar posibles G/SOE antes de ofrecer cualquier cosa de valor.

Cumplimiento de las normas para hacer negocios con el sector público

Cisco vende directa e indirectamente a entidades gubernamentales (G/SOE) en todo el mundo. Estos clientes tienen reglas específicas del sector público y de adquisiciones que van más allá de nuestras obligaciones comerciales estándar. Como partner de confianza de clientes gubernamentales, debemos tomar medidas para identificar de forma proactiva y cumplir con todas las regulaciones y los procedimientos aplicables. Comuníquese con el Departamento Legal para obtener ayuda con preguntas relacionadas con los requisitos del sector público.

La confianza significa:

- ➔ Antes de participar en negocios con el sector público de EE. UU., debe leer y comprender nuestro [Código de Ética del Sector Público de EE. UU.](#), que incluye obligaciones adicionales.
- ➔ Cumplir con las reglas de adquisiciones del sector público, incluidas aquellas que rigen las oportunidades de fuente limitada y los procesos de licitación competitiva.
- ➔ No redactar ofertas o licitaciones para una G/SOE si Cisco tiene la intención de presentar una oferta para el contrato, y nunca buscar, aceptar, compartir ni utilizar información de licitación que no esté disponible para todos los licitantes.
- ➔ Manejarse con veracidad, integridad y precisión al facturar y al responder a ofertas, certificaciones u otras solicitudes de información de G/SOE.

Más información

[Departamento Legal del Sector Público de EE. UU.](#)

Observancia de los requisitos del comercio internacional

Cisco está sujeta a controles comerciales, incluidas leyes de importación, exportación, sanciones y antiboicot, en todo el mundo. Las regulaciones comerciales afectan el flujo de hardware, software, tecnología, información y servicios de Cisco entre países. Las infracciones pueden dar lugar a sanciones significativas y perjudicar nuestra capacidad para hacer negocios. Los controles comerciales evolucionan rápidamente y son complejos, por lo que es importante conocer los requisitos y solicitar asistencia cuando sea necesario.

La confianza significa:

- ➔ No realizar negocios en o con regiones embargadas: Cuba, Irán, Corea del Norte o las regiones de Crimea, Donetsk y Luhansk de Ucrania.
- ➔ Iniciar [revisiones de productos de exportación](#) para todas las nuevas ofertas.
- ➔ Junto con las solicitudes de pedidos y envíos, proporcionar datos completos y precisos, por ejemplo, clasificaciones de productos, país de origen, autorizaciones gubernamentales y valoración.
- ➔ Coordinar con los responsables de Requisitos legales y de cumplimiento para el comercio global antes de responder a solicitudes de antiboicot o contratar ciudadanos de regiones embargadas.

Más información

[Sede de Requisitos legales y de cumplimiento para el comercio global \(TLC\)](#)
[Política de exportación global](#)
[Política de cumplimiento de envíos internos globales](#)
[Política de uso aceptable](#)

Nos manejamos con precisión, honestidad e integridad

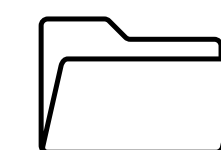
Generar confianza significa comprometerse con la precisión, la honestidad y la transparencia en todo lo que hacemos. Somos responsables de registrar la información y transmitirla de manera precisa, así como de conservar los registros comerciales de manera correcta. Seguimos todos los controles internos, los procesos y las políticas para preservar la integridad financiera y la eficiencia operativa de nuestra empresa. Al mantener estos estándares, protegemos a Cisco y conservamos nuestra reputación como una empresa ética.



Documentación
y generación de
informes precisos de
la información



Obtención de las
aprobaciones
necesarias y
cumplimiento de los
controles internos



Cumplimiento de
los requisitos de
registro y retención de
documentos

Documentación y generación de informes precisos de la información

Cisco depende de que los empleados proporcionen información precisa, completa y honesta. Ya sea que esté presentando informes de gastos, registrando horas trabajadas o proporcionando datos de ventas, es fundamental hacerlo correctamente. Llevar los libros y registros de manera precisa es esencial para la estrategia de Cisco y para cumplir con nuestras obligaciones de elaboración de informes.

La confianza significa:

- ➔ Proporcionar información precisa, completa y objetiva en todas las comunicaciones, y evitar tergiversaciones o inducir a otros a que cometan errores.
- ➔ Cooperar plenamente con las solicitudes de información de la empresa en investigaciones, auditorías y otras revisiones.

- ➔ Registrar todos los ingresos y gastos de manera oportuna, incluso al pagar a proveedores, presentar gastos y registrar acuerdos.

- ➔ No tergiversar transacciones ni crear fondos no registrados o apartados de los registros financieros oficiales.

Empleados con responsabilidades de elaboración de informes financieros

El director ejecutivo (CEO), el director de finanzas (CFO) y todos los empleados del departamento de Finanzas de Cisco también están sujetos al [Código de Ética para Funcionarios de Finanzas](#), que incluye obligaciones adicionales para garantizar la presentación justa y oportuna de los resultados financieros y la situación financiera de Cisco.

Tenga en cuenta lo siguiente

- **Los fondos no registrados o apartados de los registros financieros oficiales** son fondos colocados en una cuenta que no pertenece a Cisco, cuyo uso es dirigido por empleados de Cisco sin la debida transparencia, autorización o documentación. Constituyen una violación de la política, incluso si finalmente se utilizan para fines comerciales legítimos. Ejemplos incluyen utilizar presupuesto no gastado para pagar por adelantado a un proveedor por trabajo en trimestres futuros, u otorgar a un partner descuentos adicionales para compensar viajes de clientes o un acuerdo pasado.
- Las decisiones de la empresa y la confianza de los inversionistas dependen de que cada uno de nosotros proporcione información precisa. Si no sabe con certeza qué información proporcionar, qué procesos seguir o de quién necesita aprobación, solicite ayuda. Si ocurren errores o se omite información relevante, comuníquese y corrija. Recuerde que una omisión en sí misma puede constituir una tergiversación o inducir a otros a cometer errores.

Más información

[Política global de gastos](#)

[Código de Ética para Funcionarios de Finanzas](#)

Obtención de las aprobaciones necesarias y cumplimiento de los controles internos



Asegurar las aprobaciones y seguir los procesos internos ayuda a Cisco a obtener el mejor valor, registrar gastos e ingresos con precisión y evitar compromisos no autorizados. Esto genera confianza con nuestras partes interesadas internas y externas, garantiza que los fondos de Cisco se utilicen de manera responsable y respalda nuestras obligaciones como empresa pública.

La confianza significa:

➞ Obtener las aprobaciones requeridas y seguir los procesos internos antes de comprar bienes y servicios, incurrir en gastos u ofrecer condiciones no estándar.

➞ Garantizar que los acuerdos escritos reflejen claramente las condiciones reales del acuerdo y nunca asumir compromisos paralelos.

➞ Notificar de inmediato a Finanzas sobre cualquier pedido registrado antes de que un cliente final haya emitido una orden de compra válida a Cisco o a nuestro partner de canal (lo que se conoce como “registro blando”).

➞ No eludir un proceso obligatorio ni alentar a otros a hacerlo; los plazos o la presión de un colega, gerente o cliente no son una excusa.

Más información

[Política de reservas globales](#)

[Política de negocios no estándar](#)

[Global Procurement Services](#)

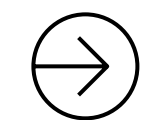
🔑 Tenga en cuenta lo siguiente

- Los descuentos pueden ser esenciales para igualar el precio de un competidor o ajustarse al presupuesto de un cliente, pero el uso indebido de descuentos puede erosionar las ganancias, financiar la corrupción, comprometer la precisión de los registros de Cisco y facilitar la desviación de productos. Apruebe o solicite descuentos únicamente con un caso comercial claro y documéntelos y regístrelos de manera adecuada.
- Un **compromiso paralelo** o “**nota complementaria**” es cualquier compromiso o declaración no autorizada, verbal o escrita, hacia un cliente, partner u otro tercero, realizada fuera de los procesos de aprobación y contratación de Cisco. Compartir precios de un acuerdo antes de su aprobación, aceptar devoluciones fuera de un contrato o prometer incentivos o concesiones futuras son ejemplos de compromisos paralelos y están prohibidos.

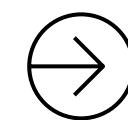
Cumplimiento de los requisitos de registro y retención de documentos

Crear, conservar y desechar los registros comerciales es parte de nuestro trabajo diario. Llevar a cabo una buena gestión de los registros nos ayuda a operar nuestro negocio de manera fluida y eficiente, a proteger adecuadamente los registros y a cumplir con nuestras obligaciones frente a otros.

La confianza significa:



Crear, identificar y clasificar adecuadamente los registros comerciales, que pueden incluir correos electrónicos, mensajes instantáneos, documentos, herramientas de colaboración o archivos electrónicos.



Conservar, administrar y desechar los registros de acuerdo con las políticas de retención de registros de Cisco y las directrices del Departamento Legal.

Más información

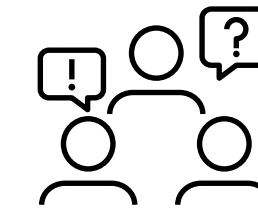
[Política de destrucción y retención de datos de la empresa](#)

[Política de uso adecuado y retención de los correos electrónicos](#)

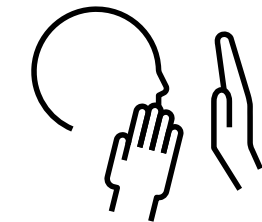
[Política de mensajería instantánea](#)

Separaremos los intereses personales de los comerciales

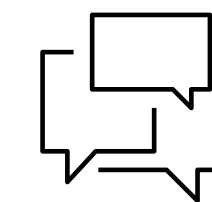
Hacer nuestro trabajo significa hacer lo correcto para Cisco. Aunque nuestras vidas personales y profesionales suelen estar separadas, a veces se superponen. Cuando esto ocurre, somos responsables de proteger los intereses de Cisco y de mantener la confianza de nuestros colegas, clientes y partners.



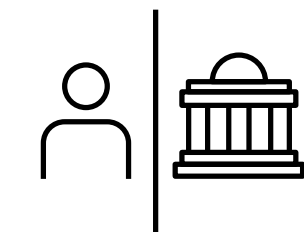
Gestión de conflictos de intereses



Prevención del uso de información privilegiada



Prudencia al hablar en público

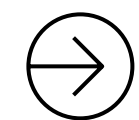


Separación de la participación política personal

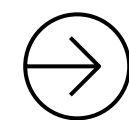
Gestión de conflictos de intereses

Un conflicto de interés ocurre cuando nuestras actividades o relaciones personales interfieren, o parecen interferir, con los mejores intereses de Cisco. Los conflictos pueden afectar la objetividad y la credibilidad, y obstaculizar hacer lo correcto para la empresa. Debemos tomar medidas proactivas para divulgar, documentar y buscar ayuda para resolver los conflictos que surjan. Incluso la apariencia de un conflicto puede dañar la confianza en Cisco y en los empleados.

La confianza significa:



Evitar actividades o relaciones que puedan influir o parecer influir en el negocio de Cisco o en sus responsabilidades laborales, o retirarse de ellas.



Utilizar los procesos de Cisco para divulgar de manera oportuna posibles conflictos, incluso si no sabe con seguridad que exista un conflicto o cree que su toma de decisiones no se verá afectada, y obtener la aprobación cuando sea necesario.

Más información [Conflictos de intereses, juntas externas y política de inversiones](#)
[Recursos para conflictos de intereses](#)
[Herramienta de divulgación de conflictos de intereses](#)



Tenga en cuenta lo siguiente

Los conflictos de interés pueden surgir en muchas situaciones, tales como:

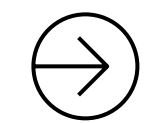
- Trabajo fuera de la empresa, ya sea remunerado o no, incluso como contratista, consultor o asesor.
- Participación en juntas directivas.
- Inversiones o participaciones de propiedad suyas o de un familiar.
- Desarrollo de invenciones o propiedad intelectual externas.
- Relaciones personales con otras personas en Cisco o dentro de nuestra industria.

Debemos ser especialmente conscientes de los conflictos cuando las actividades o relaciones involucren a partners, proveedores, competidores, entidades del sector público u otros actores del ecosistema de Cisco.

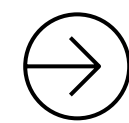
Prevención del uso de información privilegiada

Mientras trabaja en Cisco, puede conocer información relevante “interna” sobre Cisco u otra empresa que cotiza en bolsa y que no está disponible para el público, denominada información relevante no pública. Usar o divulgar esta información para beneficio personal es poco ético y contrario a la ley. Las infracciones pueden tener consecuencias graves para las personas y las empresas.

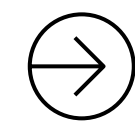
La confianza significa:



Reconocer cuándo posee información relevante no pública y protegerla contra divulgaciones inapropiadas.



No operar basándose en información privilegiada ni compartirla con otros que puedan operar con ella.



Nunca operar con derivados de Cisco ni cubrir valores de Cisco.

Más información [Política de información privilegiada](#)



Tenga en cuenta lo siguiente

La información relevante no pública no se limita a información financiera no divulgada; puede relacionarse con casi cualquier aspecto del negocio y de las operaciones de una empresa, por ejemplo:

- Propuestas de fusiones, adquisiciones o desinversiones
- Cambios significativos en la administración o el personal
- Nuevos productos o servicios
- Cambios en relaciones comerciales clave

Si tiene preguntas, comuníquese con insidertradingattorney@cisco.com.

Prudencia al hablar en público



Las declaraciones externas tienen un impacto poderoso en la marca y la reputación de Cisco. Cisco debe expresarse con una sola voz, compartiendo información clara, precisa y adecuada, coordinada en el momento correcto.

La confianza significa:

- ➔ Hablar en nombre de Cisco únicamente cuando tenga autorización para hacerlo y dejar claro cuándo sus declaraciones son personales.
- ➔ Obtener aprobación antes de hablar con medios o analistas, comprometerse con una recomendación, aceptar entrevistas o participar en un evento como orador, aceptar un premio de un proveedor o publicar un blog o artículo sobre Cisco o nuestro negocio.
- ➔ Expresarse con respeto y de manera profesional en línea, incluso en medios sociales.
- ➔ Cumplir con las restricciones sobre el intercambio de información de la empresa y propiedad intelectual al hablar en público o hacer publicaciones en redes.

Más información [Política de medios digitales y sociales](#)
[Política de respaldos](#)

[Política de oportunidades como orador](#)
[Política de portavoz en medios](#)

Separación de la participación política personal



Cisco respeta nuestros derechos como individuos a participar activamente en el proceso político utilizando nuestro propio tiempo y recursos. Sin embargo, toda participación política personal debe mantenerse separada de Cisco.

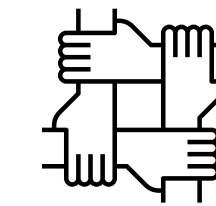
La confianza significa:

- ➔ No utilizar activos de Cisco, incluidos fondos de la empresa, instalaciones, equipos, canales de comunicación o marcas, para apoyar candidatos, causas, partidos u organizaciones políticas.
- ➔ Dejar claro que sus opiniones políticas personales son propias y no representan las opiniones de Cisco.
- ➔ Nunca participar en actividades de grupos de presión u otras actividades políticas en nombre de Cisco, a menos que esté autorizado por Asuntos Gubernamentales.

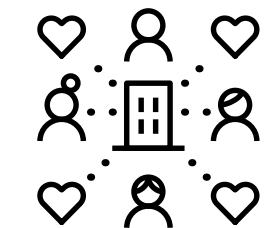
Más información
[Asuntos gubernamentales de Cisco](#)

Promovemos entornos de trabajo seguros y respetuosos, dentro y fuera de Cisco

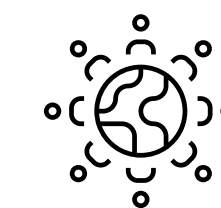
El respeto guía la forma en que trabajamos juntos y con otros. Cuando tratamos a las personas con equidad y dignidad, contribuimos a un lugar de trabajo seguro y honramos nuestras obligaciones ambientales, generamos confianza dentro de Cisco y con nuestros partners y comunidades.



Respeto hacia los demás y expectativa de trato respetuoso



Promover entornos de trabajo seguros

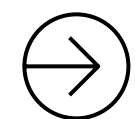


Cumplir con nuestras obligaciones externas

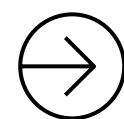
Respeto hacia los demás y expectativa de trato respetuoso

Todas las personas merecen sentirse valoradas e incluidas en el trabajo. En Cisco, construimos un sentido de pertenencia a través de acciones cotidianas: escuchar de manera abierta, reconocer las fortalezas de los demás y alzar la voz cuando algo no está bien. No toleramos la discriminación, el acoso, el hostigamiento, ni las represalias de ningún tipo, incluidas las acciones basadas en características protegidas por la ley. En su lugar, contribuimos a una cultura de confianza, respeto y equidad, donde todas las personas tienen la oportunidad de tener éxito.

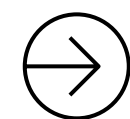
La confianza significa:



Tratar a todas las personas con dignidad y tomar decisiones laborales basadas en las calificaciones y el desempeño, no en prejuicios.



Evitar bromas, lenguaje o contacto físico que puedan resultar no deseados u ofensivos, incluso de manera involuntaria.



Apoyar adaptaciones razonables para personas con discapacidades, ayudando a que todos puedan dar lo mejor de sí en el trabajo.

Más información

[Política de igualdad de oportunidades de empleo \(EEO\)](#)

[Política de acoso en el lugar de trabajo](#)

[Política de adaptaciones razonables](#)



Tenga en cuenta lo siguiente

- Las **características protegidas** son rasgos y atributos protegidos por la ley. Estos incluyen, entre otros: edad, ascendencia, color, casta, ciudadanía, género, expresión de género, identidad de género, información genética, estado civil, condición médica, origen nacional, discapacidad física o mental, embarazo, raza, religión, sexo, orientación sexual y condición de militar o veterano.
- Nuestro Código se aplica ya sea que usted esté en la oficina, trabajando de forma virtual, en las instalaciones de un cliente o en cualquier evento relacionado con el trabajo. Independientemente del entorno, el respeto se construye en los pequeños momentos, y no siempre es evidente cuándo un comentario o una acción cruzan la línea. Deténgase y pregúntese: ¿Cómo podrían mis palabras o acciones afectar a otra persona? Si observa un comportamiento irrespetuoso, señálelo incluso cuando resulte incómodo.

Promover entornos de trabajo seguros

En Cisco, todas las personas tenemos derecho a un lugar de trabajo seguro, protegido y de apoyo. Nos protegemos a nosotros mismos y a los demás siendo conscientes de nuestro entorno, siguiendo los protocolos de seguridad y creando espacios donde todas las personas puedan concentrarse y prosperar.

La confianza significa:

- ➞ Seguir las instrucciones, políticas y prácticas de seguridad y protección.
- ➞ Reconocer los riesgos en el lugar de trabajo e informar de inmediato lesiones, accidentes, actos inseguros y condiciones inseguras. No se tolerarán amenazas ni actos de violencia.
- ➞ Cumplir con las reglas de acceso mediante tarjetas de identificación en las instalaciones y eventos de Cisco.

Más información

[Política de control de acceso global](#)
[Política de drogas y alcohol en el lugar de trabajo](#)
[Centro de seguridad corporativa](#)
[Página de seguridad, salud y medioambiente](#)

Cumplir con nuestras obligaciones externas

Guiados por estándares reconocidos a nivel mundial y cumpliendo con las leyes aplicables, nos esforzamos por promover los derechos humanos y prácticas responsables en todo nuestro negocio.

La confianza significa:

- ➞ Cumplir con nuestra política de derechos humanos, que incluye reportar de inmediato inquietudes sobre trabajo forzoso o trata de personas en nuestra cadena de suministro o con terceros con los que Cisco hace negocios.
- ➞ Cumplir con nuestras políticas internas orientadas a reducir el impacto ambiental y a realizar representaciones precisas sobre los productos de Cisco.

Más información

[Política global de derechos humanos](#)
[Política medioambiental corporativa](#)

Nuestras responsabilidades

Cada decisión correcta y ética que usted toma construye la cultura que hace que Cisco funcione. Cuando lidera con confianza al seguir nuestro Código, elegir la integridad por encima de la conveniencia, alzar la voz en lugar de guardar silencio y asumir responsabilidad en lugar de mirar hacia otro lado, inspira a otros a hacer lo mismo. La confianza que hemos construido juntos se gana a través de innumerables decisiones diarias tomadas por personas que eligen hacer lo correcto, incluso cuando es difícil y cuando nadie está mirando.

Es responsable de cumplir con nuestro Código, las políticas de Cisco y las leyes aplicables. El incumplimiento de nuestro Código puede dar lugar a medidas disciplinarias, incluida la terminación de la relación laboral. Si observa algo que no parece correcto, debe alzar la voz.

Todos los empleados de Cisco deben completar la capacitación asignada sobre nuestro Código y las políticas relacionadas. Completar esta capacitación es esencial para cumplir con sus responsabilidades y mantener los estándares de Cisco. Cuando cada uno de nosotros lidera con confianza y responsabilidad, creamos la base para el impacto que lograremos juntos.

Última revisión: febrero de 2026

© 2007-2026 Cisco Systems, Inc. Reservados todos los derechos. Cisco, el logotipo de Cisco, Cisco Systems y el logotipo de Cisco Systems son marcas comerciales registradas o marcas comerciales de Cisco Systems, Inc. o sus filiales en Estados Unidos y otros países. Todas las demás marcas comerciales mencionadas en este documento o sitio web son propiedad de sus respectivos dueños. El uso de la palabra partner no implica una relación de asociación entre Cisco y otra empresa.