WHITE PAPER

# Estándar ISO / IEC 27001

Importancia | Evolución | Cambios de actualización

SGS

# La evolución de las amenazas cibernéticas

Con la Industria 4.0 y el Internet de las cosas (IoT), las amenazas cibernéticas se han vuelto más sofisticadas y ocurren casi a diario. Estos ataques no afectan solo a la empresa objetivo, sino también a sus socios comerciales, proveedores y clientes.

La pandemia mundial y la guerra entre Rusia y Ucrania también han puesto los ciberataques en el punto de mira. El conflicto ha demostrado que la guerra no se limita solo al campo de batalla, sino que también se libra en el ámbito digital, ya que actores amenazantes patrocinados por el Estado intentan difundir desinformación y desestabilizar infraestructuras críticas.

Las organizaciones, individuos y naciones deben mantener el ritmo de la evolución de las amenazas cibernéticas e implementar las últimas medidas de protección para evitar la pérdida de datos, demandas y daño reputacional, entre otros factores dañinos.

## Definiendo amenazas

### La seguridad de la información

La seguridad de la información, también conocida como InfoSec, se refiere a los procesos y herramientas utilizados para proteger la información confidencial de una empresa de modificaciones, interrupciones, destrucción e inspección no autorizada.

### Ciberseguridad

Ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Estos ciberataques suelen tener como objetivo acceder, cambiar o destruir información confidencial, extorsionar dinero a los usuarios o interrumpir los procesos normales de la empresa.

### La protección de privacidad

La protección de la privacidad consiste en evitar que la información personal caiga en manos equivocadas, como hackers. La definición varía de persona a persona.

# Las 10 principales amenazas

### 1. TECNOLOGÍA CON SEGURIDAD DÉBIL

La tecnología está evolucionando más rápido que nunca. Con mucha frecuencia, las nuevas tecnologías tienen acceso a internet, pero no tienen un plan de seguridad. Esto crea un riesgo grave, ya que cada conexión no segura significa una vulnerabilidad.

### 2. ATAQUES EN REDES SOCIALES

Los ciberdelincuentes constantemente encuentran nuevas formas de explotar a los usuarios de las redes sociales y su información privada. Una forma malintencionada es utilizar emojis y emoticonos para hacer que el usuario baje su guardia.

### 3. MALWARE MÓVIL

Los expertos en seguridad han observado riesgos en la seguridad de los dispositivos móviles desde que estos comenzaron a conectarse a internet.

Además, los usuarios de teléfonos móviles suelen ser indiferentes a las amenazas. Teniendo en cuenta nuestra dependencia incesante de los teléfonos móviles y lo poco que los ciberdelincuentes los han atacado, grandes amenazas son una posibilidad clara.

### 4. ENTRADA DE TERCEROS

Los ciberdelincuentes prefieren el camino de menor resistencia. El servidor de Microsoft Exchange fue víctima de un gran ciberataque en marzo de 2021. Esto interrumpió a nueve agencias gubernamentales y 60.000 empresas privadas.

### 5. DESCUIDAR LA CONFIGURACIÓN ADECUADA

Las herramientas de Big Data pueden ser personalizadas para adaptarse a las necesidades de una organización. Las empresas siguen descuidando la importancia de configurar adecuadamente las configuraciones de seguridad.

Fifth Third Bank fue víctima de uno de los mayores brechas de datos del 2020, debido a que un ex empleado retuvo el acceso.

### 6. SOFTWARRE DE SEGURIDAD

Actualizar el software de seguridad es una práctica básica de gestión de tecnología y obligatoria para proteger los datos. El software se desarrolla para defenderse contra amenazas conocidas. Esto significa que cualquier nuevo código malicioso que afecte a un software de seguridad desactualizado no será detectado.

### 7. INGENIERÍA SOCIAL

Los ciberdelincuentes saben que las técnicas de intrusión tienen una vida útil limitada. Han recurrido a la ingeniería social fiable y no técnica que se basa en la interacción social y la manipulación psicológica para acceder a datos confidenciales.

Esta forma de intrusión es impredecible y efectiva.

### 8. FALTA DE ENCRIPTACIÓN

Proteger los datos sensibles en tránsito y en reposo es una medida que pocas industrias han adoptado, a pesar de su efectividad. La industria de la salud maneja datos extremadamente sensibles y comprende la gravedad de perderlos, por lo que muchos interesados ponen un gran énfasis en la encriptación.

### 9. DATOS CORPORATIVOS EN DISPOSITIVOS PERSONALES

Ya sea que una organización distribuya teléfonos corporativos o no, los datos confidenciales aún se están accediendo en dispositivos personales.

Las herramientas de gestión móvil limitan la funcionalidad, pero asegurar los vacíos de seguridad no es una prioridad para muchas organizaciones.

### 10. TECNOLOGÍA DE SEGURIDAD INADECUADA

Invertir en software de monitoreo de seguridad de red se ha convertido en una tendencia creciente después de las dolorosas rupturas de las brechas de datos de 2014.

El software está diseñado para alertar cuando se producen intentos de intrusión, pero estas alertas solo son valiosas si alguien las aborda. Las empresas dependen demasiado de la tecnología para protegerse completamente contra los ataques cuando debería ser una herramienta gestionada.

# El estándar destacado de protección: ISO/IEC 27001

## Un linaje legendario

ISO/IEC 27001 se puede remontar al British Standard 7799, escrito por el Departamento de Comercio e Industria del Reino Unido (DTI) y publicado en 1995.

### PARTE 1

La primera parte de BS 7799, que contiene las mejores prácticas de gestión de seguridad de la información, fue revisada en 1998. Después de mucho debate entre organismos de normalización de todo el mundo, fue adoptada por ISO y IEC y se convirtió en ISO/IEC 17799 - Tecnología de la información - Código de prácticas para la gestión de la seguridad de la información en el 2000, esta norma fue revisada y en 2005 se incluyó un pequeño cambio de nombre. Finalmente, ISO e IEC incorporaron esta parte a la familia de normas ISO/IEC 27000 como ISO/IEC 27002:2007.

### PARTE 2

La segunda parte, titulada "Sistemas de gestión de seguridad de la información - Especificaciones con orientación para su uso", fue publicada por primera vez justo antes del cambio de milenio. Este elemento se enfocó en cómo implementar un sistema de gestión de seguridad de la información (SGSI), haciendo referencia a la estructura y los controles necesarios. Posteriormente, esto se convirtió en la norma ISO/IEC 27001:2005. En resumen, la norma ISO/IEC 27001 ha evolucionado significativamente desde su primera versión. La actualización de 2022 ha fortalecido su relevancia y aplicabilidad en el entorno actual, proporcionando un marco sólido y actualizado para la implementación de sistemas de gestión de seguridad de la información eficaces y confiables.

### PARTE 3

La tercera parte fue publicada en 2005, cubriendo el análisis y la gestión de riesgos. Se alineó con la norma ISO/IEC 27001:2005.

### UNIFICANDO LAS PARTES 1-3

Tras revisiones, unificación y mucho tiempo, la ISO y la IEC crearon ISO/IEC 27001:2013 - la norma de seguridad de la información de las mejores prácticas reconocida internacionalmente, para ayudar a las organizaciones a mantener seguros sus activos de propiedad intelectual y de información.

# La importancia de la certificación ISO/IEC 27001

Adoptada por decenas de miles de organizaciones, la certificación ISO/IEC 27001 demuestra el **compromiso** de una organización con la **seguridad de la información** y brinda **garantía** a los **clientes y otros socios** de que se toma en serio la protección de la información bajo su control.

La norma es agnóstica en cuanto a la tecnología, por lo que no importa qué entorno tecnológico tenga.

Está escrita de tal manera que cualquier organización, desde pequeñas empresas hasta grandes empresas multinacionales de miles de millones de dólares, puede utilizarla. ISO/IEC 27001 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI para la seguridad y protección de la información.

También incluye **requisitos** para evaluar y tratar los **riesgos de seguridad** de la información, adaptados a sus necesidades.

Como se trata de una norma de sistemas de gestión, **se alinea con otras normas** reconocidas a nivel mundial, como:

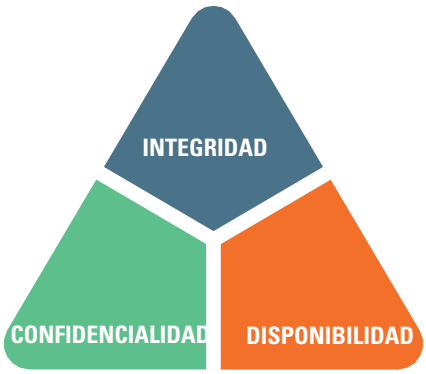
- **ISO/IEC 27701** (gestion de privacidad)
- **ISO/IEC 20000-1** (gestión de servicios TI)
- **ISO 22301** (continuidad del negocio)
- **ISO 9001** (calidad)
- **ISO 14001** (medio ambiente)
- **ISO 45001** (La salud y seguridad laboral)

Esta alineación le permite implementar los requisitos de varias de estas normas dentro de tu organización con un esfuerzo mínimo, al mismo tiempo que se beneficia de los **efectos sinérgicos**.

# Basado en la triada de la CIA

Implementar un SGSI demuestra tu dedicación a proteger la confidencialidad, integridad y disponibilidad (CIA) de la información bajo tu control.

La norma se alinea con la Triada de la CIA, que proporciona características de seguridad vitales. Te ayuda a evitar problemas de cumplimiento, respalda la continuidad del negocio y previene el daño reputacional.




Esto significa que **ISO/IEC 27001 abarca:**

- Políticas de seguridad de la información
- Seguridad de las comunicaciones
- Organización de la seguridad de la información
- Relaciones con proveedores
- Adquisición, desarrollo y mantenimiento del sistema Gestión de activos
- Seguridad de recursos humanos Control de acceso
- Gestión de incidentes de seguridad de la información Criptografía
- Cumplimiento
- Aspectos de seguridad de la
- información en la gestión de la continuidad del negocio
- Seguridad física y ambiental
- Seguridad en las operaciones

# ¿Cuáles son los principales beneficios?

ISO/IEC 27001 **puede llevar a:**

- Mayor credibilidad
- Menor riesgo de fraude, pérdida y divulgación de información
- Demostración de integridad en su sistema
- Transformación de la cultura empresarial y una mayor conciencia sobre la importancia de mantener la información segura
- Nuevas oportunidades de negocio con clientes conscientes de la seguridad Una noción más fuerte de la confidencialidad en todo el lugar de trabajo
- Mejor preparación para lo inevitable: el próximo evento o incidente de seguridad


# Evolución para enfrentar las amenazas

## El momento de actualizarse

El ISO/IEC 27001 fue actualizado por última vez en 2013 y el mundo cibernético y las amenazas que enfrenta han evolucionado dramáticamente, volviéndose cada vez más complejas con tecnologías más innovadoras, operaciones en la nube y negocios en línea. El estándar debe seguir el mismo rumbo y ser moldeable para acomodar actualizaciones.

El 15 de febrero de 2022 fue un día crucial. Se publicó el **ISO/IEC 27002:2022** - Information Security, Cybersecurity and Privacy Protection - Information Security Controls. Debido a esto, el Anexo A del ISO/IEC 27001 necesitaba actualizarse para alinearse con los controles del ISO/IEC 27002:2022.

## Los principales cambios en ISO/IEC 27001:2022

Lo siguiente es del Borrador Final de Norma Internacional (FDIS, por sus siglas en inglés) y no se esperan cambios significativos adicionales en ISO/IEC 27001:2022. Para obtener más detalles, puedes leer nuestro documento de orientación Comparando ISO/IEC FDIS 27001 con ISO/IEC

27001:2013. ¿Cuáles son los cambios?

### EL TÍTULO

El **nombre ha sido cambiado** para reflejar el verdadero alcance del estándar. Ahora es ISO/IEC 27001:2022 - Sistemas de Gestión de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad - Requisitos. Esto también se alinea con el nuevo título de ISO/IEC 27002:2022.

### NUMERACIÓN DE CLÁUSULAS

El nuevo estándar ISO/IEC 27001:2022 ha introducido **nuevas subcláusulas** para armonizar aún más la estructura del documento con otros estándares de sistemas de gestión, como ISO 9001 e ISO 22301.

Se **han intercambiado dos subcláusulas**: 10.1 y 10.2. La 10.1 es Mejora Continua, mientras que la 10.2 es No Conformidad y Acción Correctiva. **No hay cambios en sus requisitos.**

### NUEVO TEXTO

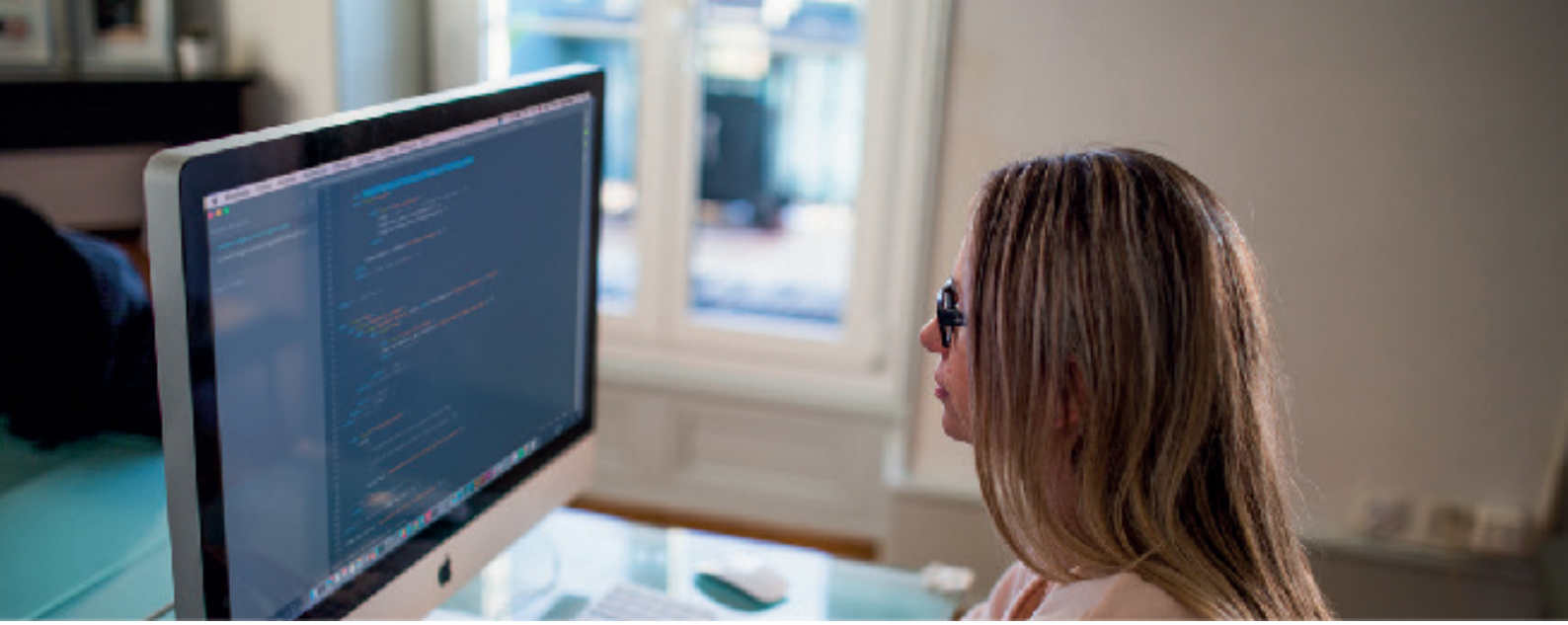
Aunque se ha agregado **nuevo texto** y se ha reorganizado algunas partes, estos cambios solo aclaran los requisitos y no agregan nuevos a la norma.

### ANEXO A

El título del Anexo A ahora es Referencia de Controles de Seguridad de la Información y los controles se han revisado para alinearse con ISO/IEC 27002:2022. En la edición de 2013, solo las descripciones de los controles se derivan de ISO/IEC 27002.

### OTROS CAMBIOS

Se han realizado algunas **actualizaciones** en varias cláusulas. Nuestro documento de orientación describe con precisión las diferencias entre los documentos FDIS y 2013, y proporciona nuestros comentarios para ayudarte.



# Fuertes lazos familiares

## Los principales cambios en ISO/IEC 27002:2022

Como se mencionó, muchas de las actualizaciones de ISO/IEC 27001 se deben a la evolución de ISO/IEC 27002. A continuación, se presenta un **resumen de los cambios** en este último. Para obtener más detalles, puedes leer nuestro documento técnico "Cambios clave en ISO/IEC 27002:2022"

### NÚMERO DE CONTROLES

ISO/IEC 27002:2022 tiene **93 controles** en comparación con los 114 de la versión de 2013.

### CATEGORIAS DE CONTROL

Los controles se han agrupado en **cuatro categorías** - Organizativas, Personas, Físicas y Tecnológicas- en lugar de los 14 temas y 36 categorías de la edición de 2013.

El diseño de las cuatro categorías enfatiza que la protección de la información y los datos es más que simplemente por medios tecnológicos. Para lograr los resultados de seguridad de la información, los **controles tecnológicos son solo los remedios** para prevenir o mitigar los riesgos de seguridad de la información.

Más importante aún, la **alta dirección** de las organizaciones debe establecer el marco y la dirección de la gestión de la seguridad de la información, así como identificar y comunicar la importancia e impacto de la información en el negocio.

Además, este nuevo diseño de control puede facilitar a la gerencia la **asignación de responsabilidades** dentro de la organización para mejorar la seguridad de la información.

### NUEVOS CONTROLES

Hay **11 nuevos controles** para abordar la evolución de las tecnologías y las prácticas industriales:

1. Inteligencia de amenazas
2. Seguridad de la información para el uso de servicios en la nube
3. Preparación de las TIC para la continuidad del negocio
4. Monitoreo de la seguridad física
5. Gestión de la configuración
6. Eliminación de información
7. Enmascaramiento de datos
8. Prevención de fuga de datos
9. Monitoreo de actividades
10. Filtrado web
11. Codificación segura

## CONTROLES FUSIONADOS

**Veinticuatro controles** en la edición de 2022 son el resultado de la fusión de algunos de la versión de 2013. La fusión significa una reducción en el número de controles, por lo que se trata de una norma más esbelta.

## ATRIBUTOS

ISO/IEC 27002:2022 **introduce atributos para cada control.** Cada control está asociado con cinco atributos con sus correspondientes valores de atributos.

1. **Tipos de control** - preventivo, detectivo, correctivo.
2. **Propiedades de seguridad de la información** - confidencialidad, integridad, disponibilidad.
3. **Conceptos de ciberseguridad:** identificar, proteger, detectar, responder, recuperar.
4. **Capacidades operativas:** gobernanza, gestión de activos, protección de la información, seguridad de recursos humanos, seguridad física, seguridad de sistemas y redes, seguridad de aplicaciones, configuración segura, gestión de identidad y acceso, gestión de amenazas y vulnerabilidades, continuidad, seguridad de las relaciones con proveedores, legal y cumplimiento, gestión de eventos de seguridad de la información, aseguramiento de la seguridad de la información. .
5. **Dominios de seguridad:** gobernanza y ecosistema, protección, defensa, resiliencia

## EL PROPÓSITO REEMPLAZA AL OBJETIVO

La versión de 2022 utiliza "Propósito" en lugar de "Objetivo".

Cada control tiene un propósito definido para ilustrar por qué debe implementarse el control.

## OTROS CAMBIOS

El título ahora incluye Seguridad de la Información, Ciberseguridad y Protección de la Privacidad - Controles de Seguridad de la Información para reflejar la amplitud de la norma. Se eliminó el término "Código de Práctica" para indicar que el documento es una referencia a controles de seguridad de la información genéricos. ISO/IEC 27000 ya no es la referencia normativa de ISO/IEC 27002:2022.

En su lugar, se aplican los términos y definiciones en la Cláusula 3 de la edición 2022.

Se recomienda a los usuarios de la edición 2022 que se refieran a sus términos y definiciones para facilitar su comprensión de los controles y la guía en el documento.

# Conclusión

## ¿Cómo lo hacemos en SGS?

El estándar ISO/IEC 27001 proporciona un sólido marco de gobernanza y permite que cualquier organización maneje regulaciones locales, regionales y globales de seguridad de la información y ciberseguridad.

Es el estándar al que se acude cuando las amenazas cibernéticas evolucionan. Muchas razones,como las amenazas intensificadas, los avances tecnológicos y una conectividad superior, como el 5G, pueden convertir a su empresa en un blanco para los ciberdelincuentes.

Estos cambios, de hecho, engendran cambios. Una **fortaleza clave** de ISO/IEC 27001 es su capacidad para mantener el ritmo en un mundo cibernético en constante cambio. Aunque las **actualizaciones de 2022** hacen que la documentación y las directrices sean más pesadas y añaden más responsabilidades, hay explicaciones claras y detalladas de cada control.

Como era de esperar, el **cambio más significativo** son las revisiones del Anexo A para alinearse con los controles de seguridad de ISO/IEC 27002:2022.

Los **cambios en las Cláusulas 4-10** son cambios editoriales menores para armonizar aún más la estructura con otros estándares de sistemas de gestión.

Si tu organización ya cumple con ISO/IEC 27001, no se necesitan cambios en la tecnología, solo actualizaciones en la documentación. Es posible que deba revisar las políticas internas de acuerdo con las nuevas subcláusulas y requisitos modificados. También se debe revisar el resultado de la evaluación de riesgos y el(los) plan(es) de tratamiento de riesgos, y actualizar la Declaración de Aplicabilidad (SoA).

El **período de transición** será de tres años a partir de la publicación oficial de ISO/IEC 27001:2022, por lo que tendrá tiempo suficiente para cumplir. Tu certificado ISO/IEC 27001 sigue siendo válido hasta que finalice este período.

Podemos asegurarnos de que hayas adaptado la documentación dentro del período de transición. Por lo tanto, no es necesario programar nuevas auditorías porque esto se llevará a cabo durante tus auditorías de vigilancia regulares.

Además, se requerirá tiempo adicional para evaluar la transición exitosa según el documento MD 26:2022 del Foro Internacional de Acreditación (IAF).

Sin embargo, cuando renueves tu certificación durante el período de transición, podrías trabajar en los nuevos controles para evitar dejarlo hasta última hora.

### MÁS INFORMACIÓN

**SGS España**
Email: es.ofertasBA@sgs.com

## ¿Cómo podemos ayudarte?

### 1. FORMACIÓN:

- Programa Auditor Jefe de Seguridad de la Información (ISO 27001:2022 y ENS)
- Cursos de formación en el Esquema de Gestión de Seguridad de la Información ISO/IEC ISO 27001 en su nueva versión: Auditor Interno, Cambios y novedades de la nueva versión....

### 2. CERTIFICACIÓN:

En la norma ISO 27001:2005 mejorando la credibilidad de tu organización y demostrando la integridad de datos y sistemas, así como el compromiso con la seguridad de la información.

Ya seas un cliente actual o nuevo en ISO/IEC 27001, podemos ayudarte, **SOLICITA PRESUPUESTO SIN COMPROMISO**.

# Referencias


Forbes – https://www.forbes.com/ sites/bernardmarr/2022/03/18/ the-biggest-cyber-security-risks-in-2022/?sh=7994336c7d7b.

Georgetown University (US) – https://scsonline.georgetown.edu/ programs/masters-technology-management/resources/top-threats- to-information-technology.

Privacy Affairs – https://www.privacyaffairs.com/cybersecurity- attacks-in-2021/.

Identity Force – https://www.identityforce.com/blog/2020-data-breaches.

ISMS.online – https://www.isms. online/iso-27001/.

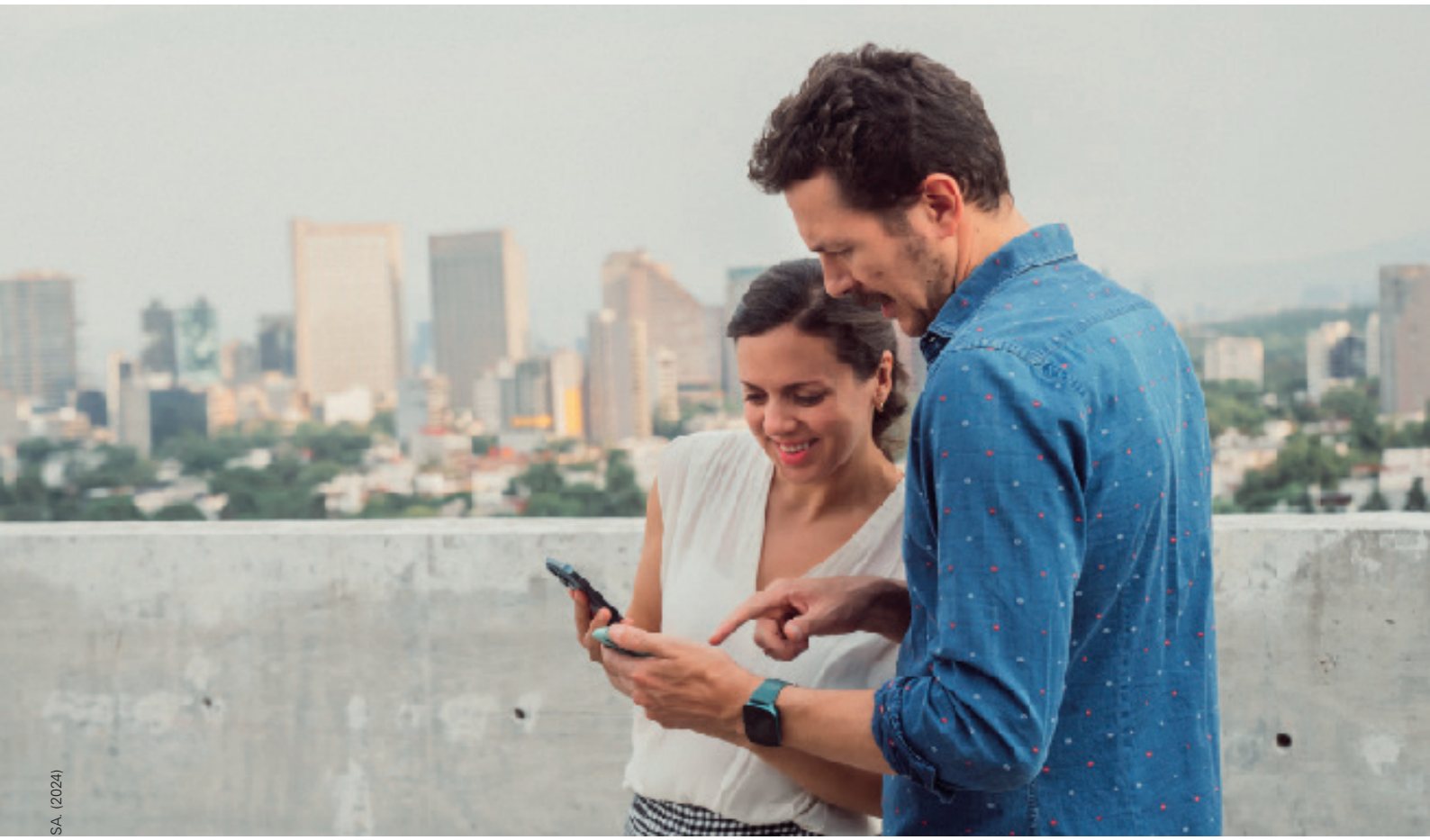
CISCO – https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html.

https://www.cisco.com/c/ en_uk/products/security/what-is- cybersecurity.html.

SGS – www.sgs.com.

ISO – https://www.iso.org/home. html.

IAF – https://iaf.nu/iaf_system/uploads/documents/IAF_MD_26_Transition_requirements_for_ISOIEC_27001-2022_09082022.pdf.





SGS

When you need to be sure