ISA GLOBAL CYBERSECURITY ALLIANCE

Aplicación de normas ISO/IEC 27001, ISO/IEC 27002 y la serie ISO/IEC 62443 en entornos de tecnología operativa

Junio 2025



South American Spanish Edition

www.isagca.org

Índice

Introducción 3

Antecedentes 4

Alcance de ISO/IEC 27001:2022 e ISO/IEC 27002:2022 4

TI y TO 4

Ámbito de aplicación de la serie de normas ISA/IEC 62443 5

Las normas ISO/IEC 27001, ISO/IEC 27002 y la serie ISO/IEC 62443 abordan dos puntos complementarios de un enfoque general de ciberseguridad de la TO 5

Las normas ISO/IEC 27001 e ISO/IEC 27002 tratan sobre establecer un sistema de gestión de la seguridad de la información para la infraestructura de TI de una organización 6

La serie de normas ISA/IEC 62443 aborda las necesidades específicas que se requieren para la ciberseguridad en entornos de TO 6

Las normas ISO/IEC 27001, ISO/IEC 27002 e ISA/IEC 62443 deben combinarse para la protección de las instalaciones operativas 7

Ampliar y adaptar el SGSI basado en la norma ISO/IEC 27001 para la infraestructura de TO 7

Al aplicar ISA/IEC 27002, hay que considerar los controles de seguridad para la gestión de riesgos de los requisitos de la norma ISA/IEC 62443-2-1 para la infraestructura de TO 8

La serie de normas ISA/IEC 62443 aporta un valor único al promover un enfoque integral 9

Pasos Siguientes 11

Referencias 11

Derechos de autor ©2026 International Society of Automation. Todos los derechos reservados.

Aplicación de las normas ISO/IEC 27001, ISO/IEC 27002 y la serie ISO/IEC 62443 a entornos de tecnología operativa

Introducción

Muchas organizaciones (especialmente las de gran tamaño) han establecido políticas y procedimientos que regulan la seguridad informática en su entorno de oficina; muchos de ellos se basan en la norma ISO/IEC 27001:2022 [27001] e ISO/IEC 27002:2022 [27002].[1] Algunas han Algunas empresas han intentado gestionar su infraestructura de TO bajo un mismo sistema de gestión y han aprovechado los numerosos puntos en común entre la TI y la TO.
Aunque lo ideal sería seleccionar siempre controles e implementaciones comunes tanto para las TI como para la TO, las organizaciones se han enfrentado a diversos retos a la hora de hacerlo, como el bloqueo de las pantallas de los operadores de la TO, lo que genera condiciones inseguras; productos antivirus incompatibles con los equipos de la TO; prácticas de aplicación de parches que alteran los horarios de producción; o el tráfico de red procedente de copias de seguridad

rutinarias que bloquea los mensajes de control de seguridad.

La serie de normas ISA/IEC 62443 [62443][2] aborda explícitamente cuestiones como estas; esto ayuda a una organización a mantener la conformidad con las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022 [27001/2][3] a través de enfoques comunes siempre que sea posible, al tiempo que se destacan las diferencias entre los enfoques de TI y de OT cuando sea necesario.

Las series de normas ISO/IEC 27001 e ISO/IEC 27002 se revisaron en 2022. En este contexto, el presente documento ofrece orientación a las organizaciones que conocen la norma 27001/2 y están interesadas en proteger la infraestructura de TO de sus instalaciones operativas basándose en la serie de normas ISA/IEC 62443.

En él se describe la relación entre la serie de normas ISA/IEC 62443 y la norma ISO/IEC 27001/2, así como la forma en que ambas normas pueden utilizarse de manera eficaz dentro de una misma organización para proteger tanto la TI como la TO.

1 Cuando se haga referencia a la norma ISO/IEC 27001, utilizaremos la referencia [27001]. Cuando se haga referencia a la norma ISO/IEC 27002, utilizaremos la referencia [27002].

2 Cuando se haga referencia a todos los documentos de la serie de normas ISA/IEC 62443, se podrá utilizar la referencia [62443].

3 Cuando se haga referencia a ambos documentos [27001] y [27002], podemos utilizar la referencia [27001/2].

La norma ISA/IEC 62443 no incluye ningún requisito específico relativo a un SGSI, pero exige el establecimiento de un sistema de gestión de la seguridad como parte del programa de seguridad del propietario del activo. Si la organización ha establecido un SGSI, el programa de seguridad en el entorno de la tecnología operativa TO deberá coordinarse con él. En este documento partimos de la base de que la organización cuenta con un SGSI establecido conforme a la norma ISO/IEC 27001, así como con políticas y procedimientos relacionados con la seguridad de las tecnologías de la información basados en la norma ISO/IEC 27002.

Antecedentes

Alcance de ISO/IEC 27001:2022 e ISO/IEC 27002:2022

La norma ISO/IEC 27001 establece los requisitos para crear, implantar, mantener y mejorar continuamente un SGSI, así como una lista de controles de gestión de riesgos comúnmente aceptados. Además, la norma [27002] ofrece orientaciones adicionales para las organizaciones que implementan estos controles de tratamiento de riesgos (el término «control» se define en la norma ISO/IEC 27000—el glosario y la introducción a la serie 27000, como «medida que modifica el riesgo»). Los controles de gestión de riesgos están diseñados para que las organizaciones los utilicen como referencia a la hora de seleccionar los controles pertinentes para su ámbito de aplicación específico.

Una implementación certificada requiere el cumplimiento de todos los controles del SGSI y de los controles de tratamiento de riesgos que se hayan seleccionado dentro del ámbito de aplicación.

TI y TO

«TI» es el término común que se utiliza para referirse a todo el abanico de tecnologías destinadas al tratamiento de la información, incluyendo el software, el hardware, las tecnologías de la comunicación y los servicios relacionados. En general, las TI no incluyen las tecnologías integradas que no generan datos para uso empresarial. La tecnología operativa o «TO» se define como «tecnología destinada a detectar, gestionar o provocar cambios mediante la supervisión o el control de una entidad física». Nota 1 de la entrada: Incluidos el personal y los procesos necesarios para gestionar los sistemas. Nota 2 de la entrada: Manejado por personal cualificado o no cualificado, o totalmente automatizado. Nota 3 de la entrada: «incluye las tecnologías digitales y cualquier otra tecnología» [IEC]. Cada vez es más frecuente el uso de productos y sistemas de TI en las infraestructuras de TO y, recientemente, la llegada del IoT (Internet de las cosas) y del IoT industrial ha difuminado aún más la distinción entre TI y TO. Sin embargo, la principal diferencia es que los entornos de TI, en general, deben cumplir con estrictos requisitos de integridad, disponibilidad

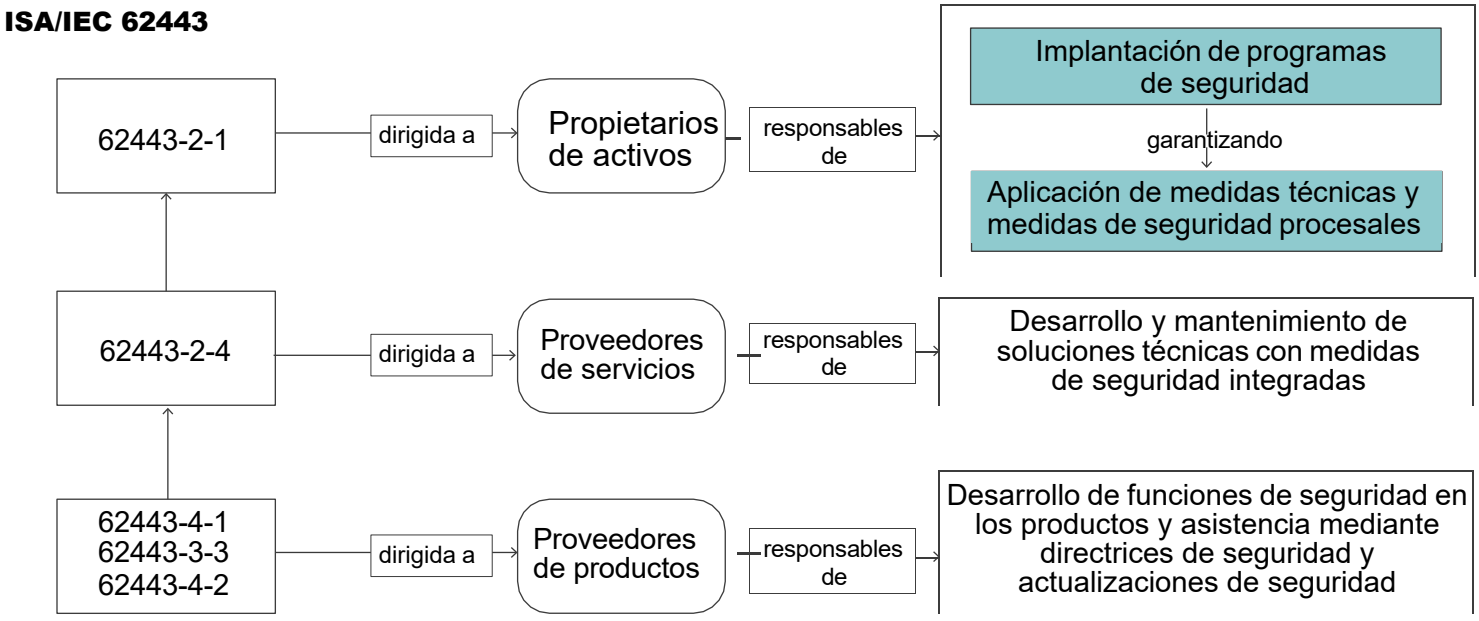

Figura 1. La serie de normas ISA/IEC 62443 se dirige a todas las entidades implicadas en la protección de las instalaciones operativas

y las restricciones de rendimiento, debido a que un funcionamiento fuera de dichos límites podría afectar a la salud, la seguridad o el medio ambiente.

Ámbito de aplicación de la serie de normas ISA/IEC 62443

El ámbito de aplicación de la serie de normas ISA/IEC 62443 es la seguridad de los «sistemas de automatización y control industrial (IACS)» utilizados en instalaciones de TO. Esto incluye los sistemas de control utilizados en plantas e instalaciones de fabricación y procesamiento, así como en operaciones geográficamente dispersas, como los servicios públicos (es decir, electricidad, gas y agua), los oleoductos y las instalaciones de producción y distribución de petróleo. La serie de normas ISA/IEC 62443 también ha ido ganando aceptación fuera de su ámbito de aplicación original, por ejemplo, en la automatización de edificios, en los sistemas médicos y en otros sectores y aplicaciones, como las redes de transporte, que utilizan activos automatizados o controlados o supervisados a distancia.

La figura 1 ofrece una visión general del alcance de algunos documentos fundamentales de [62443]. La norma ISA/IEC 62443-2-1 [62443-2-1] está dirigida a las organizaciones responsables de los sistemas de control industrial (IACS), entre las que se incluyen los propietarios y los operadores (denominados «propietarios de activos» en la serie), y establece los requisitos para el programa de seguridad de los propietarios de activos.

Además, la serie de normas ISA/IEC 62443 establece los requisitos de conformidad para todas las demás entidades que prestan apoyo a los propietarios de activos en la implementación de medidas de seguridad técnicas y procedimentales destinadas a proteger las instalaciones operativas frente a amenazas cibernéticas. La norma ISA/IEC 62443-2-4 [62443-2-4] establece los requisitos de seguridad para los proveedores de servicios de integración y mantenimiento que prestan apoyo a los propietarios de activos en el desarrollo y la explotación de soluciones técnicas específicas para la tecnología operativa (OT). ISA/IEC 62443-3-3 [62443-3-3] e ISA/IEC 62443-4-2 [62443-4-2] definen los requisitos relativos a las capacidades de seguridad de los sistemas y los componentes, respectivamente. La norma ISA/IEC 62443-4-1 [62443-4-1] incluye requisitos relativos al ciclo de vida para los proveedores de productos, con el fin de garantizar el desarrollo y el soporte de productos con capacidades de seguridad adecuadas. Además, la norma ISA/IEC 62443 incluye documentos de orientación sobre cuestiones específicas, como la gestión de parches y la partición de sistemas basada en el riesgo en zonas y conductos. Cabe señalar que los proveedores de productos y los prestadores de servicios pueden ser propietarios de instalaciones de producción, por lo que desempeñan el papel de propietarios de dichos activos.

ISO/IEC 27001, ISO/IEC 27002 y las normas ISA/IEC 62443 aborda dos aspectos complementarios de un enfoque global de ciberseguridad de las TO

Las normas ISO/IEC 27001/2 se han utilizado ampliamente durante muchos años como base para organizar la seguridad de la información de las organizaciones.
Los procesos y la estructura general de gestión de las organizaciones responsables del entorno de TO

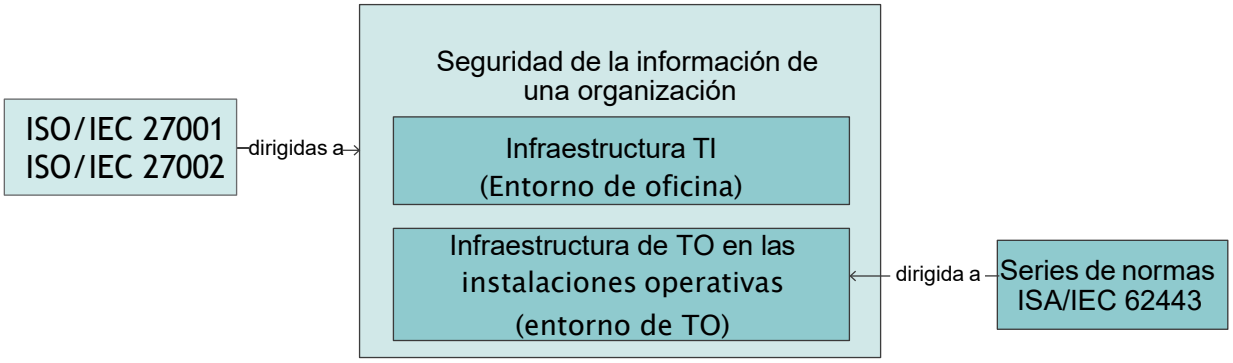

Figura 2. Ámbito de aplicación de las normas ISO/IEC 27001, ISO/IEC 27002 y la serie de normas ISA/IEC 62443

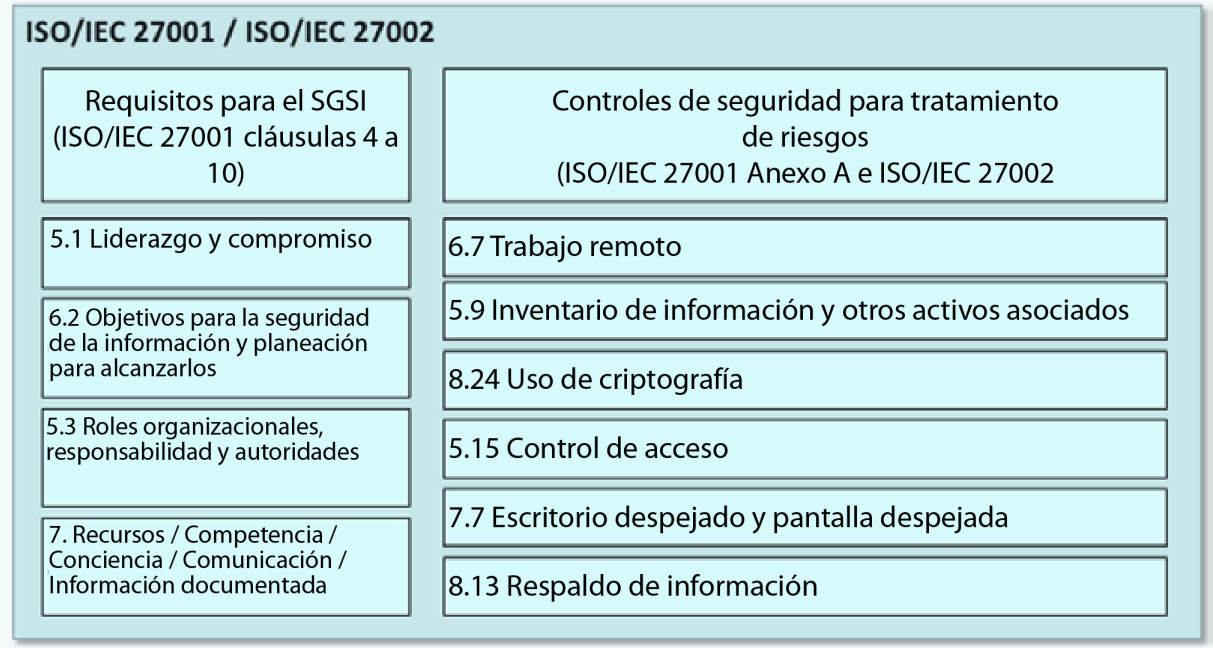

Figura 3. Ejemplos de requisitos para el SGSI y controles de seguridad para el tratamiento de riesgos

pueden integrarse en un SGSI basado en estas normas, tal y como se describirá a continuación. La norma ISA/IEC 62443 aborda las necesidades específicas de las infraestructuras de TO y complementa los SGSI ya establecidos.

La infraestructura de TO de las instalaciones operativas puede estar integrada en la infraestructura de TI de la organización o estar organizada de forma autónoma. En ambas situaciones, las normas ISO/IEC 27001, ISO/IEC 27002 y la serie ISA/IEC 62443 pueden utilizarse para abordar aspectos complementarios de un enfoque global de ciberseguridad para entornos de tecnología operativa.

ISO/IEC 27001 / ISO/IEC 27002 abordan la implantación de un sistema de gestión de la seguridad de la información para la infraestructura informática de una organización

La norma ISO/IEC 27001/2 establece requisitos genéricos destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. Los requisitos para establecer, implantar, mantener y mejorar continuamente un SGSI se describen en las cláusulas 4 a 10 de la norma ISO/IEC 27001.No es aceptable excluir ninguno de los requisitos especificados en estas cláusulas cuando una organización declare su conformidad con esta norma. Además, incluye controles de gestión de riesgos que abordan cuestiones de seguridad que deben tenerse en cuenta en una estrategia de seguridad integral. Según la norma, una organización puede seleccionar controles de la lista que figura en [27001/2] y diseñar controles adicionales para satisfacer sus necesidades específicas. La distinción entre los requisitos del SGSI y los controles de seguridad para el tratamiento de riesgos especificados en [27001/2] queda ilustrada mediante algunos ejemplos que se muestran en la figura 3.

La serie de normas ISA/IEC 62443 aborda las necesidades específicas relacionadas con la ciberseguridad en entornos de TO.

Los IACS en instalaciones en funcionamiento deben cumplir unos requisitos específicos de integridad, rendimiento y disponibilidad para garantizar la continuidad operativa. La pérdida de la continuidad operativa puede manifestarse, por ejemplo, en forma de una explosión, un apagón o el uso de una fórmula o dosis incorrecta de un medicamento que salva vidas. Muchas instalaciones operativas cuentan con sistemas de seguridad específicos para prevenir situaciones operativas que pudieran tener consecuencias para la salud, la seguridad y el medio ambiente.

Security Control ISO/IEC 27001/2	Consideraciones de TO	ISA/IEC 62443 reference
7.7 Escritorio despejado y pantalla despejada	El bloqueo de pantalla del operador de la TO puede crear condiciones inseguras.	*ISA/IEC 62443-2-1 USUARIO 1.18* puede requerir excluir el bloqueo de pantalla del operador de la TO
8.7 Controles contra malware	Los productos antivirus suelen ser incompatibles con los activos de TI operativa	*ISA/IEC 62443-2-1 COMPATIBILIDAD 2.3* puede requerir excluir el bloqueo de pantalla del operador de la TO
8.13 Respaldo de información	El tráfico de red procedente de las copias de seguridad rutinarias bloquea los mensajes de control de seguridad	*ISA/IEC 62443-3-3 RS 5.1 2.3* requiere la segmentación física de las redes de los sistemas de control críticos respecto a las redes de los sistemas de control no críticos
8.8 Gestión de vulnerabilidades técnicas	Prácticas de parcheo pueden interrumpir el calendario de producción	*ISA/IEC 62443-2-3 sección 5, punto f,* requiere probar y planear la aplicación de parches para asegurar continuidad operacional.

Figura 4. Consideraciones relacionadas con las TO respecto a la implementación de algunos controles de seguridad de las TI

Los requisitos de seguridad de la norma ISA/IEC 62443 están concebidos para evitar que se impida o se interrumpa el funcionamiento seguro. Además, las funciones específicas de seguridad requieren una protección especial y, por lo tanto, están sujetas a requisitos de seguridad específicos establecidos en la norma.

La norma ISA/IEC 62443 aborda estos retos típicos, a los que a menudo hay que enfrentarse al ampliar las implementaciones de controles de seguridad de TI existentes al ámbito de la TO, tal y como se muestra en la figura 4. La serie de normas ISA/IEC 62443 incluye requisitos que abordan todos los aspectos de seguridad que deben tenerse en cuenta en un programa de seguridad integral, del mismo modo que la norma ISO/IEC 27001/2 incluye una lista de controles para el tratamiento de riesgos que abordan aspectos de seguridad similares. Los requisitos de la norma ISA/IEC 62443 abordan necesidades específicas del entorno de TO y complementan la lista de controles de gestión de riesgos de la norma ISO/IEC 27001/2, añadiendo detalles fundamentales relevantes para dicho entorno.

ISO/IEC 27001, ISO/IEC 27002 y la serie de normas ISA/IEC 62443 debería combinarse para la protección de las instalaciones operativas

El análisis anterior muestra cómo la norma ISA/IEC 62443 complementa a la norma ISO/IEC 27001/2 al incorporar aspectos específicos propios del entorno de la TO. Sin embargo, la norma ISA/IEC 62443 no incluye todos los elementos necesarios para la seguridad en la TO. En concreto, la norma ISA/IEC 62443 no incluye requisitos relativos a la gestión de la seguridad, sino que la delega en un SGSI ya establecido por el propietario del activo. La norma ISO/IEC 27001/2 también incluye algunos controles que son relevantes para la TO, pero que quedan fuera del ámbito de aplicación de la norma ISO/IEC 62443. Por lo tanto, se recomienda un método para aplicar ambas normas a la infraestructura de TO, y en este documento se describe uno de ellos.

El concepto reconoce que la norma [62443-2-1] aborda el programa de seguridad de los propietarios de activos para sus instalaciones operativas de TO; por consiguiente, esta parte de la serie de normas ISA/IEC 62443 debería servir de enlace con la norma ISO/IEC 27001/2. Los demás documentos de la norma ISA/IEC 62443 tienen por objeto servir de apoyo a los propietarios de activos y se basan en los requisitos de la norma [62443-2-1].

Ampliar y adaptar el SGSI basado en ISO/IEC 27001 a la infraestructura de TO.

Aunque la norma ISA/IEC 62443 no define los requisitos para establecer, implementar, mantener y mejorar continuamente un

SGSI, el primer requisito de la norma [62443-2-1] establece que los programas de seguridad del IACS deben coordinarse con cualquier SGSI ya establecido. Se recomienda que, para la infraestructura de TO, las organizaciones establezcan un SGSI basado en las cláusulas 4 a 10 de la norma ISO/IEC 27001. Debe garantizarse que la estructura y la aplicación sean propicias y flexibles para la inclusión del entorno TO dentro de su ámbito de aplicación sin que ello tenga repercusiones negativas en el SGSI establecido en la TI. Por ejemplo, esto exigirá claridad en cuanto a la asignación de responsabilidades de gestión de TI/TO, las responsabilidades relativas a las interfaces entre los sistemas de TI y TO, una planificación adecuada de los recursos para las competencias técnicas comunes y específicas de TI y TO, y un uso eficaz de los conceptos y la terminología de ambas normas.

Tenga en cuenta los controles de seguridad para el tratamiento de riesgos de la norma ISO/IEC 27002 al aplicar los requisitos de la norma ISA/IEC 62443-2-1 a la infraestructura de TO

Una forma práctica de organizar el conjunto combinado de controles de seguridad de la norma [27002] y los requisitos de la norma [62443-2-1] consiste en aprovechar la estructura de la norma [62443-2-1] en los Elementos del Programa de Seguridad (EPS), que son agrupaciones lógicas de requisitos que abarcan un tema específico. Todos los aspectos relacionados con la seguridad deben abordarse en un programa de seguridad integral. Algunos ejemplos de EPS son la gestión de la configuración, la seguridad de redes y comunicaciones, la seguridad de los componentes, control de acceso de los usuarios y protección de los datos. Algunos EPS se subdividen para abarcar diferentes aspectos de seguridad incluidos en la misma SPE. El enfoque propuesto recomienda incorporar a los requisitos de cada EPS y, respectivamente, de cada sub-SPE, los controles de seguridad para el tratamiento de riesgos correspondientes de [27002], tal y como se muestra en la figura 5.

Aunque la mayoría de los controles [27002] están relacionados con uno o varios temas tratados en las SPE, algunos son de carácter general, como «5.5 Contacto con las autoridades», «6.2 Condiciones de empleo» y «5.32 Derechos de propiedad intelectual». Estos son los «controles generales de seguridad» que aparecen en la figura 5. Deben tenerse en cuenta en el enfoque basado en el riesgo del propietario de los activos y adaptarse al entorno de TO del mismo modo que se adapta el SGSI. Cabe señalar que el hecho de tener en cuenta la combinación de los controles [27002] y los requisitos [62443-2-1] no implica que deban aplicarse todos ellos. Los requisitos aplicables deben seleccionarse tras un análisis de riesgos realizado por el propietario del activo, en función de sus necesidades específicas y condiciones de funcionamiento.

A la hora de implementar el programa de seguridad, el propietario del activo podrá tener en cuenta, siguiendo un enfoque basado en el riesgo, todos los aspectos pertinentes, basándose en la combinación de los requisitos sobre este tema establecidos en ambas normas.

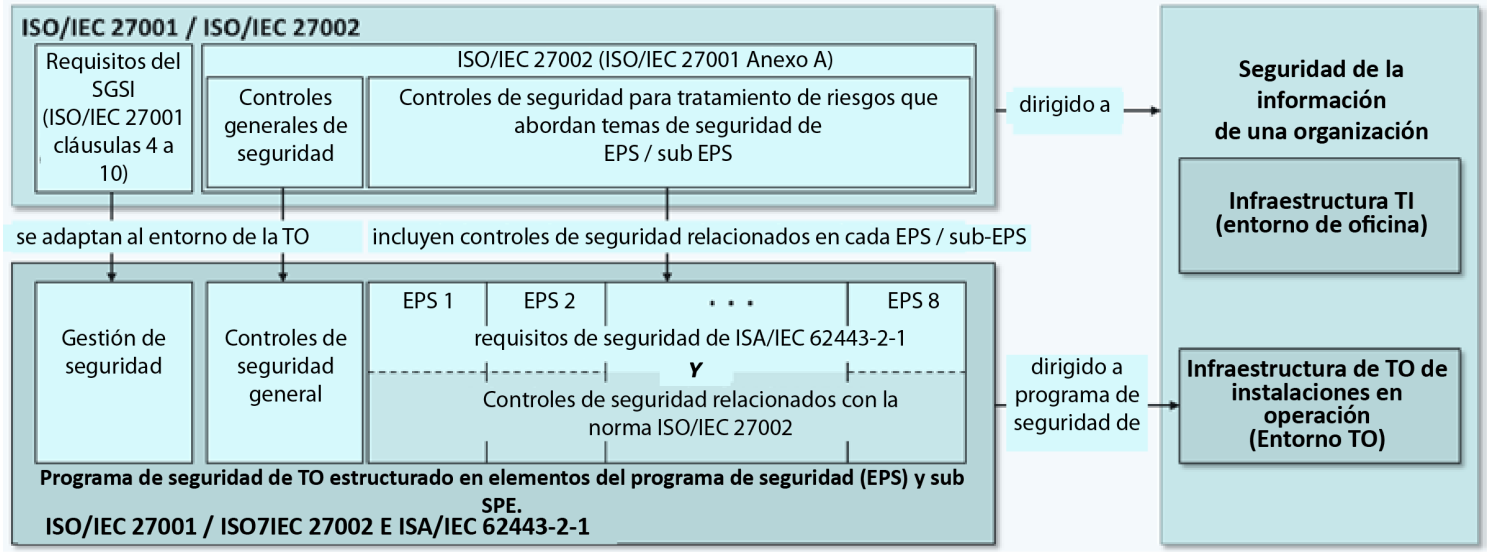

Figura 5. Combinación de los controles de las normas ISO/IEC 27001 e ISO/IEC 27002 y los requisitos de los programas de seguridad de TO de la norma ISA/IEC 62443-2-1

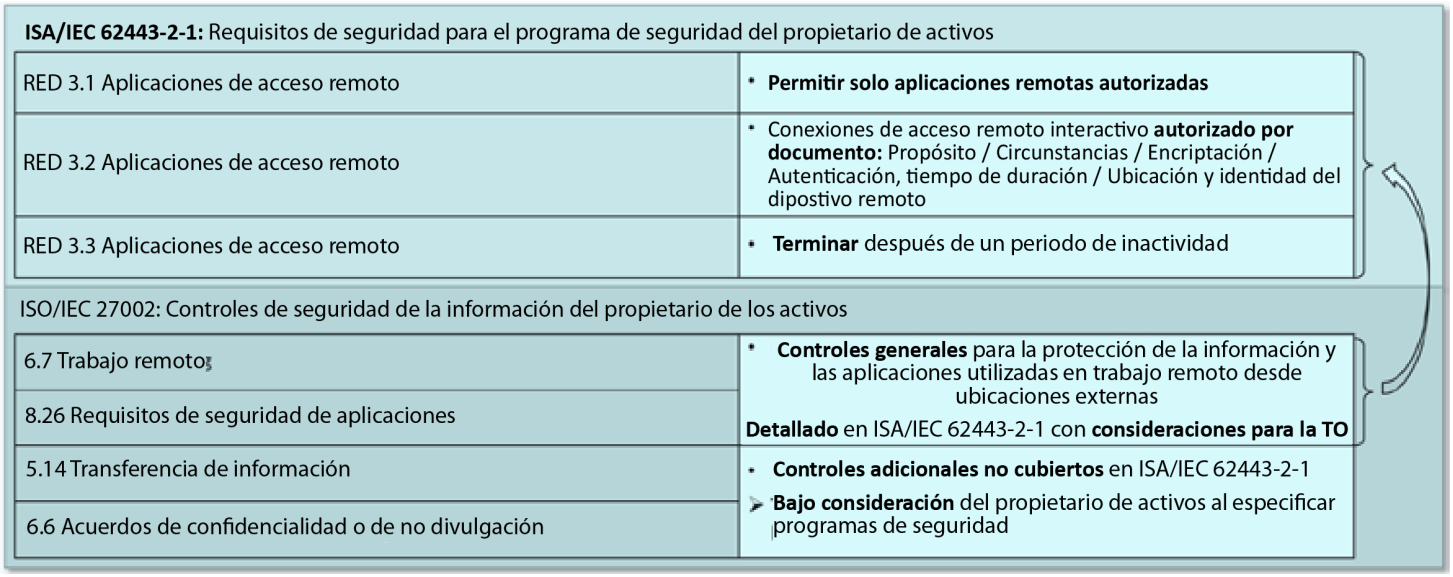

Figura 6. *RED 3 – Acceso remoto seguro:* Combinación de los requisitos [62443-2-1] y los controles [27002]

Las ventajas de incorporar en cada EPS y sub-EPS los controles de seguridad correspondientes de [27001/2] pueden ilustrarse con el ejemplo de la sub-EPS «RED 3 - Acceso remoto seguro», que forma parte de «EPS 3 – Seguridad de redes y comunicaciones» (Figura 6).

Los activos de TO de las instalaciones en operación suelen ser gestionados por proveedores de servicios externos desde ubicaciones situadas fuera de la propia instalación operativa. El acceso remoto a la infraestructura de tecnología operativa debe controlarse de forma estricta para evitar crear superficies de ataque innecesarias. Por consiguiente, la norma [62443-2-1] RED 3 exige a los propietarios de activos:

- garantizar que solo se permitan las aplicaciones remotas autorizadas,
- garantizar que se documenten las conexiones remotas interactivas autorizadas, incluyendo la finalidad, las circunstancias, las tecnologías de cifrado y autenticación, la duración, así como la ubicación y la identidad del dispositivo cliente remoto, y
- garantizar que el acceso remoto se interrumpa tras un periodo de inactividad.

Los requisitos anteriores son específicos de TO y detallan las medidas de control recomendadas [27002] relativas al trabajo remoto desde ubicaciones externas. La figura 6 muestra una lista de ejemplos de controles relacionados con este tema. La norma [27002] exige la protección de la información a la que se accede, se procesa o se almacena en lugares de trabajo remotos, así como la seguridad de los servicios de aplicaciones en redes públicas y protección de las transacciones de los servicios de aplicaciones. [62443-2-1] añade consideraciones relativas a la TO basadas en casos de uso que implican el acceso remoto, mediante la definición de los requisitos específicos de la TO en el apartado RED 3.1 a RED 3.3, tal y como se muestra en la figura 6. Por otra parte, [27002] aborda aspectos que no están contemplados en [62443-2-1], pero que pueden tenerse en cuenta en los programas de seguridad en entornos TO, por ejemplo:

- políticas y procedimientos de transferencia de información,
- acuerdos sobre la transferencia de información, y
- acuerdos de confidencialidad o de no divulgación.

Un plan de protección integral destinado a garantizar el acceso remoto a la infraestructura de tecnología operativa (OT) de las instalaciones en funcionamiento debería tener en cuenta todos los aspectos que abordan ambas normas.

La serie de normas ISA/IEC 62443 aporta un valor único al promover un enfoque integral

Los propietarios de activos confían en el diseño de soluciones técnicas adecuadas que incorporen medidas de seguridad, así como en las capacidades de seguridad de los productos utilizados en dichas soluciones. Como se muestra en la figura 1,ISA/IEC 62443 aporta un importante valor añadido dirigiéndose a todas las demás entidades que apoyan

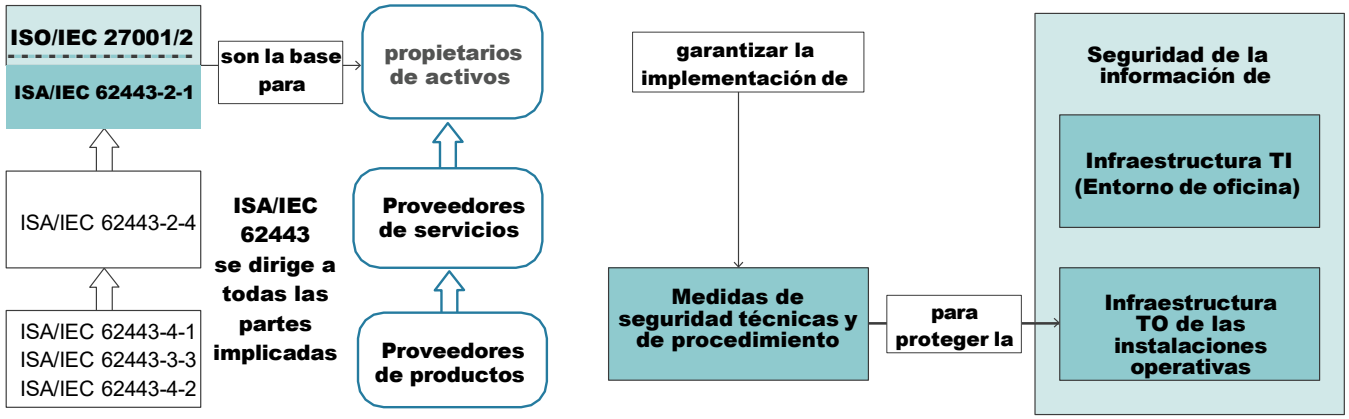

Figura 7. Junto con las normas ISO/IEC 27001 e ISO/IEC 27002, la serie de normas ISA/IEC 62443 sienta las bases para la protección de las instalaciones operativas.

los propietarios de activos a la hora de aplicar un enfoque de defensa en profundidad para la protección de sus instalaciones operativas frente a las amenazas cibernéticas. La figura 7 ilustra la relación entre las normas ISO/IEC 27001/2 e ISA/IEC 62443, así como las entidades organizativas asociadas, con el fin de crear un programa integral de ciberseguridad para la protección de las instalaciones operativas frente a las ciberamenazas.

La norma ISO/IEC 27001/2 incluye cuatro controles (del 5.19 al 5.22) que se refieren específicamente a los proveedores, así como varias referencias a los proveedores en las orientaciones relativas a otros controles. La norma ISA/IEC 62443 facilita la aplicación de estos controles al establecer partes específicas de la norma que deben cumplir los proveedores de TO que desempeñen funciones concretas. Esto proporciona al propietario del activo una base para imponer requisitos de ciberseguridad a los proveedores de TO y, potencialmente, exigir una certificación por parte de terceros conforme a las partes pertinentes de la norma ISA/IEC 62443 para sus proveedores de servicios de TO o para la adquisición de productos. Por ejemplo, la norma [62443-4-1] establece requisitos para los proveedores de productos con el fin de reducir y gestionar las vulnerabilidades, tales como la elaboración de modelos de amenazas, la aplicación de principios de diseño seguro, la eliminación de vulnerabilidades de código mediante el cumplimiento de las directrices de programación, la detección y eliminación de vulnerabilidades a través de pruebas como las de fuzzing, las pruebas de penetración y el análisis binario, la facilitación de directrices de seguridad a los usuarios y la corrección de las vulnerabilidades detectadas en la práctica mediante un proceso de actualizaciones de seguridad. Además, la norma ISA/IEC 62443 incluye requisitos relativos a las capacidades técnicas de seguridad de los productos utilizados en las infraestructuras de TO y define los niveles de seguridad (SLs) para diferenciar el nivel de exigencia de los requisitos de seguridad en función de los riesgos de ciberseguridad aceptables para los propietarios de los activos.

ISO/IEC 27001/2 e ISA/IEC 62443 se complementan entre sí a la hora de aplicar una estrategia integral, basada en el riesgo y de defensa en profundidad para la protección de las instalaciones operativas, incluyendo la contribución de todas las entidades:

- Los requisitos y controles combinados de las normas ISO/IEC 27001/2 e ISA/IEC 62443-2-1 constituyen la base para que los propietarios de activos establezcan programas de seguridad y garanticen el diseño y la aplicación de medidas de seguridad técnicas y procedimentales.
- Los requisitos de la norma ISA/IEC 62443-2-4 constituyen la base para que los proveedores de servicios presten apoyo a los propietarios de activos mediante el diseño y el mantenimiento de soluciones técnicas que ofrezcan las capacidades de seguridad necesarias.
- Los requisitos de la norma ISA/IEC 62443-4-1 constituyen la base para que los proveedores de productos presten apoyo a los propietarios de activos y a los proveedores de servicios mediante la aplicación de procesos de desarrollo seguros y la oferta de directrices y asistencia para integrar y mantener la seguridad de los productos utilizados en las infraestructuras de TO.
- Los requisitos de las normas ISA/IEC 62443-3-3 e ISA/IEC 62443-4-2 constituyen la base para proporcionar las capacidades de seguridad necesarias de los productos para que los propietarios de activos y los proveedores de servicios puedan implementar esquemas de protección.

Pasos siguientes

La asignación de los controles pertinentes [27002] a cada EPS o sub-EPS de [62443-2-1] debería constituir la base para aplicar el enfoque descrito. Con este fin, se podría elaborar un mapa de referencia que sirviera como recurso de uso común. Las organizaciones podrían utilizar dicha correspondencia de referencia para el desarrollo de sus programas de seguridad de la TO y adaptarla a sus necesidades específicas según sea necesario.

Referencias

[27001] ISO/IEC 27001, tercera edición, octubre de 2022 — Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos

[27002] ISO/IEC 27002, tercera edición, febrero de 2022 — Seguridad de la información, ciberseguridad y protección de la privacidad — controles de seguridad de la información

[IEC] International Electrotechnical Commission
https://www.iec.ch/

Nota: Las normas IEC 62443 y ANSI/ISA 62443 comparten el mismo contenido técnico. Las referencias que figuran a continuación se refieren tanto a la norma IEC como al documento ANSI/ISA.

[62443-2-1] IEC 62443-2-1: 2024 - Seguridad de los sistemas de automatización y control industrial – Punto 2-1: Requisitos del programa de seguridad para los propietarios de activos de IACS

ANSI/ISA-62443-2-1-2024 - Seguridad de los sistemas de automatización y control industrial – Punto 2-1: Requisitos del programa de seguridad para los propietarios de activos de IACS

[62443-2-4] IEC 62443-2-4: 2023 - Seguridad de los sistemas de automatización y control industrial. Punto 2-4: Requisitos del programa de seguridad para los proveedores de servicios de IACS

ANSI/ISA-62443-2-4-2023 - Seguridad para sistemas de automatización y control industrial - Punto 2-4: Requisitos del programa de seguridad para los proveedores de servicios de IACS

[62443-3-3] IEC 62443-3-3: 2013 - Redes de comunicación industrial - Seguridad de redes y sistemas – Punto 3-3: Requisitos de seguridad del sistema y niveles de seguridad

ANSI/ISA 62443 3 3 (99.03.03)-2013 - Redes de comunicación industriales - Seguridad de redes y sistemas – Punto 3-3: Requisitos de seguridad del sistema y niveles de seguridad

[62443-4-1] IEC 62443-4-1:2018 - Seguridad de los sistemas de automatización y control industrial. Punto 4-1: Requisitos para un ciclo de vida de desarrollo de productos seguro

ANSI/ISA-62443-4-1-2018 - Seguridad para sistemas de automatización y control industrial - Punto 4-1: Requisitos para un ciclo de vida de desarrollo de productos seguro

[62443-4-2] IEC-62443-4-2:2018 - Seguridad de los sistemas de automatización y control industrial. Punto 4-1: Requisitos técnicos de seguridad para los componentes de los sistemas de control industrial (IACS)

ANSI/ISA-62443-4-2-2018 - Seguridad para sistemas de automatización y control industrial - Punto 4-1: Requisitos técnicos de seguridad para los componentes de los sistemas de control industrial (IACS)

South American Spanish Edition



ISA GLOBAL CYBERSECURITY ALLIANCE