

Junio 2025

Protección de la tecnología operativa: Comprender la serie de normas ISA/IEC 62443 desde la perspectiva de las ISO/IEC 27001 e ISO/IEC 27002

South American Spanish Edition

www.isagca.org

Secciones

Prólogo 2
1 Resumen ejecutivo 3
2 Aportaciones fundamentales de las normas ISA/IEC 62443 para la seguridad de las TO 4
2.1 Salud, seguridad y medio ambiente 6
2.2 Continuidad del proceso físico 8
2.3 La negación del servicio como «efecto no deseado» 9
2.4 Zonas de seguridad y diseño de redes 11
2.5 Controles rigurosos de la integridad del sistema 14
2.6 Niveles de seguridad 18
2.7 Propósito de la TO 20
2.8 Alcance 20
3 Estructura de la serie de normas ISA/IEC 62443 23
4 Aclaraciones sobre cuestiones de interés común 24
5 Prácticas comunes de las Tecnologías de la Información y las Tecnologías Operativas 27
6 Conclusión 34
7 Definiciones y abreviaturas 34
7.1 Definiciones 34
7.2 Abreviaturas 37
8 Referencias 38
8.1 Normas ISA/IEC 62443 38
8.2 Normas ISO/IEC 27001 e ISO/IEC 27002 38
8.3 Otras referencias 39

Índice de tablas

Tabla 1. Ejemplos de requisitos de la norma ISA/IEC 62443-2-1 que concretan las directrices de la norma ISO/IEC 27002 25
Tabla 2. Ejemplos de controles y orientaciones de la norma ISO/IEC 27002 que constituyen requisitos de la norma ISA/IEC 62443-2-1 28

Tabla de figuras

Figura 1. Temas clave – aportaciones de la serie de normas ISA/IEC 62443 a la seguridad de las TO seguridad 4
Figura 2. Categorías de requisitos de la norma ISA/IEC 62443-2-1 descritas en este documento 23
Figura 3. Funciones de los principales actores en la serie de normas ISA/IEC 62443 24
Figura 4. Recomendaciones de la norma ISO/IEC 27002 que constituyen requisitos de la serie de normas ISO/IEC 62443 24

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

Prólogo

Este informe lo elabora la Alianza Global de Ciberseguridad de la Sociedad Internacional de Automatización (ISAGCA). Para saber más sobre esta organización, visite www.isagca.org. El presente documento constituye una interpretación de las normas ISA/IEC 62443 con el fin de facilitar la comprensión y la aplicación de dicha serie de normas. No es un documento elaborado por el comité ISA99 encargado de desarrollar la norma y, por lo tanto, puede que no refleje las opiniones del comité.

www.ISAGCA.org

1 Resumen ejecutivo

El objetivo de este documento es responder a las siguientes preguntas: si ya dispone de un sistema de gestión de seguridad que abarque sus operaciones de TI basado en las normas ISO/IEC 27001 [27001] e ISO/IEC 27002 [27002], ¿cómo puede utilizar las normas ISA/IEC 62443 [62443][1] para que su sistema de gestión de seguridad abarque también sus operaciones de tecnología operativa (TO)? ¿Qué aspectos de esta expansión podrían ser únicos de la tecnología operativa y cuáles tendrían en común con las tecnologías de la información?

El requisito ORG 1.1 de la norma ISA/IEC 62443-2-1, 2.ª edición [62443-2-1], exige que, si ya se dispone de un sistema de gestión de seguridad de la información para las TI (un SGSI), ya sea basado en la norma ISO/IEC 27001 / ISO/IEC 27002 [27001/2][2] o en cualquier otro enfoque, es necesario coordinar las medidas que se adopten para la gestión de la seguridad de la tecnología operativa (TO) con dicho SGSI. En la práctica, esto significa que los controles que abordan los problemas comunes de las TI y de la TO, así como aquellos que cumplen los requisitos específicos de la TO, protegen de forma conjunta, eficiente y eficaz a toda la empresa. Aunque no pretende ser una correspondencia completa entre normas, este documento incluye correspondencias parciales entre [27001/2] y el contenido de [62443] con el fin de responder a estas preguntas, e incluye referencias específicas a aproximadamente la mitad de los requisitos de [62443-2-1].

El principio fundamental de [62443] es que la protección de los datos de la TO y de la TO en sí misma se aborda como un medio para mitigar los riesgos físicos asociados al control informático de un proceso físico, y no como un fin en sí mismo. Las ventajas específicas que ofrece el cumplimiento de la norma [62443] para la seguridad de los entornos de la TO se describen en los siguientes ámbitos: mitigación de riesgos para la salud, la seguridad y el medio ambiente; continuidad del proceso físico controlado; interrupción del control de un proceso físico como «efecto no deseado» de los controles de seguridad; zonificación basada en requisitos de seguridad; controles rigurosos de la integridad del sistema; y la relación entre el riesgo y la selección de los controles de seguridad.

Las normas [27001/2] y [62443] también comparten un ámbito significativo de interés común, como lo demuestran los requisitos de la norma [62443], que se consideran mejoras de los controles o recomendaciones de seguridad [27001/2], o que son prácticamente idénticos a ellos. Por lo tanto, [62443] no solo ofrece ventajas únicas para los entornos de terapia ocupacional, sino que también aporta información al proceso de establecimiento de prioridades que guía la aplicación de [27001/2] en dichos entornos.

[1] Cuando se haga referencia a todos los documentos de la serie de normas ISA/IEC 62443, utilizaremos la referencia [62443]
[2] Cuando se haga referencia a ambos documentos [27001] y [27002], utilizaremos la referencia [27001/2].

2 Aportaciones fundamentales de la serie de normas ISA/IEC 62443 para la seguridad de las TO

Dado que la tecnología operativa (TO) gestiona un proceso físico, su funcionamiento puede conllevar riesgos físicos. La gestión de riesgos en el ámbito de la TO se centra en mitigar los riesgos físicos asociados al proceso físico que se gestiona, así como los riesgos relacionados con la vida y el medio ambiente ajenos al sistema de TO. La protección de los datos de la TO y de la propia TO no es un fin en sí mismo, sino más bien un medio para mitigar estos riesgos físicos. Por lo tanto, la gestión de riesgos en el ámbito de la TO no se centra en los efectos adversos sobre las tecnologías de la información. De hecho, está necesariamente integrada en las actividades «no cibernéticas» de gestión de riesgos empresariales que se ocupan de los riesgos físicos. Estos riesgos son distintos de las consecuencias habituales de los ciberataques que afectan a los sistemas informáticos, como la violación de la privacidad de los clientes o la pérdida de operaciones empresariales.

Dado que la TO gestiona un proceso físico, las consecuencias de que la TO deje de estar disponible o pierda su integridad van más allá de la privacidad y de las pérdidas económicas o empresariales; abarcan lesiones, la pérdida de vidas humanas y la destrucción de bienes y del medio ambiente. Si bien la confidencialidad de los datos que utilizan los sistemas de tecnología operativa puede ser importante, las consecuencias de la pérdida de disponibilidad o integridad del sistema suelen ser mucho más graves. Además, el periodo de tiempo tolerable sin disponibilidad antes de ocasionar consecuencias significativas puede ser de varios órdenes de magnitud más corto en los sistemas de TO que en los sistemas de TI.

Estas características del entorno de riesgo de las TO determinan los requisitos de [62443]. Figura 1. Se muestran seis áreas clave en materia de requisitos en las que [62443] contribuye al buen funcionamiento de una instalación que ya cumple con la norma [27001/2]. Los requisitos de [62443] en estas áreas hacen referencia a conceptos propios de un entorno TO (como «operador de procesos» o «función de seguridad») o describen un ámbito en el que el nivel de riesgo asociado al que se refieren los requisitos es significativamente mayor en un entorno TO que en un entorno típico de TI empresarial. El texto que sigue a la Figura 1 describe brevemente cada una de estas áreas.

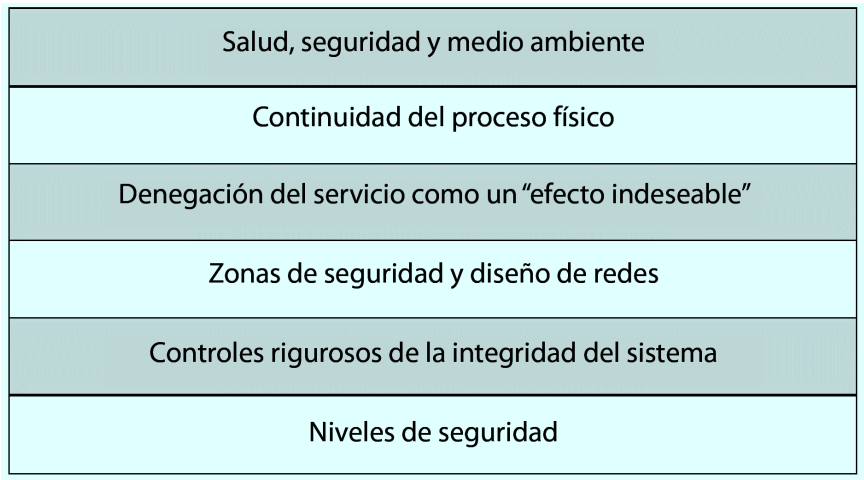

Figura 1. Temas clave – aportaciones de la serie de normas ISA/IEC 62443 a la seguridad de las TO

1. **Salud, seguridad y medio ambiente.** [62443] define los riesgos físicos como riesgos para la salud, la seguridad y el medio ambiente, y se refiere a ellos como «HSE, por sus siglas en inglés». Estos riesgos pueden materializarse si la funcionalidad de la TO no se diseña teniendo en cuenta dichos riesgos, no funciona según lo previsto o debido a que

no está operando en absoluto. En otras palabras, la falta de un diseño orientado a la seguridad, la pérdida de integridad de las TO o la pérdida de disponibilidad de las mismas generan riesgos en materia de HSE. Aunque la integridad y la disponibilidad tanto de los datos como de los sistemas se reconocen ampliamente como aspectos fundamentales de la ciberseguridad, la gravedad potencial de los riesgos físicos y los plazos ineludibles para su materialización hacen que en [62443] se establezcan requisitos más rigurosos en estos ámbitos de lo que podría ser necesario en un entorno no relacionado con la TO.

2. **Continuidad del proceso físico**. Un proceso físico no se detiene cuando el TO asociado deja de funcionar. Los requisitos de [62443] no solo tienen por objeto minimizar el tiempo durante el cual el sistema TO en su conjunto no está disponible, sino que también exigen un diseño específico que contemple qué ocurre con el proceso físico gestionado cuando las funciones normales del sistema TO dejan de estar disponibles.

3. **La negación del servicio como «efecto no deseado».** Los requisitos de [62443] tienen en cuenta no solo la respuesta de la TO ante una situación de servicio denegado provocada por un adversario, sino también cómo evitar situaciones comunes que podrían provocar involuntariamente una negación del servicio por la aplicación de un control de seguridad o, en otras palabras, causadas por «fuego amigo».

4. **Zonas de seguridad y diseño de redes.** El proceso de evaluación de riesgos y diseño del sistema descrito en [62443-3-2] requiere agrupar los activos en zonas de seguridad. Los riesgos se evalúan por zonas y se protegen los límites y las conexiones entre ellas (denominadas «conductos»). La segmentación de la red y los requisitos asociados ofrecen una posible aplicación del concepto de zona de seguridad. [62443] también exige explícitamente que se tengan en cuenta aspectos relacionados con el riesgo a la hora de diseñar las interconexiones y dependencias de la red.

5. **Controles rigurosos de la integridad del sistema.** [62443] requiere elaborar una descripción detallada del sistema. Mantener la «integridad del sistema» significa mantener y cumplir con esta descripción con el paso del tiempo. En los entornos de la TO es posible establecer una definición detallada del sistema y garantizar un cumplimiento estricto, ya que los sistemas TO se mantienen relativamente estables a lo largo del tiempo. Estos controles son necesarios, ya que pequeños cambios en el comportamiento del sistema pueden acarrear riesgos significativos en estos entornos. Es posible que estos mismos controles no sean viables ni necesarios en muchos entornos informáticos, que interactúan con un conjunto más amplio de usuarios y pueden ser más dinámicos, además de más tolerantes ante comportamientos inesperados del sistema.

6. **Niveles de seguridad.** Todas las organizaciones que cuentan con un programa de seguridad deben decidir : «¿Cuánta seguridad es suficiente?». El proceso de evaluación de riesgos [62443-3-2] consiste en asignar un nivel de seguridad objetivo a una zona de seguridad. Todos los requisitos técnicos del sistema y de los componentes, incluidos los relativos a los demás temas que se muestran en la Figura 1, se clasifican por nivel de seguridad en [62443-3-3] y [62443-4-2], respectivamente. Esto establece un vínculo entre el resultado de la evaluación de riesgos (nivel objetivo) y las especificaciones de adquisición (nivel de capacidad).

En última instancia, todos estos temas se remontan a una única característica: la TO interactúa con el mundo físico y, por lo tanto, su uso conlleva riesgos físicos. En los apartados 2.1 a 2.6 se describe con más detalle cómo los requisitos específicos de [62443] abordan cada una de estas áreas y cómo dichos requisitos se relacionan con los controles y las directrices existentes de [27001/2].

Muchos de estos temas se presentan como requisitos individuales en [62443], los cuales no tienen un equivalente directo en la lista de controles de [27001/2]. En algunos casos, tanto la norma ISA/IEC 62443 como la [27001/2] establecen el mismo requisito general, pero en la [62443] se recoge un aspecto clave de ese requisito, relacionado con las tecnologías operativas, que no se menciona explícitamente en la norma ISO/IEC 27001 ni en las orientaciones adicionales de la norma ISO/IEC 27002.

En el resto de la sección 2, el contenido, con el mismo formato que en el ejemplo que figura a continuación, proporciona un identificador alfanumérico, un título y el texto de un requisito extraído de [62443]. El texto extraído del requisito de [62443] aparece en cursiva y con fondo gris.

ISA/IEC 62443-2-1 **USER 1.3 Persistencia de la identidad del usuario**

El propietario de los activos deberá disponer de políticas y procedimientos para verificar que los identificadores de usuario, los autenticadores, las funciones y los derechos de acceso asociados específicos del IACS que se utilizan para respaldar las operaciones esenciales del IACS, incluidas las cuentas de los operadores, estén configurados de tal forma que no se desactiven automáticamente.

2.1 Salud, seguridad y medio ambiente

2.1.1 Relación con [27001/2]

Una característica distintiva de la tecnología operativa es que se encarga de un proceso en el mundo físico y genera la posibilidad de que se produzcan ciberataques que plantean riesgos «físicos» para la salud, la seguridad y el medio ambiente. Las consecuencias de salud y seguridad pueden afectar a los empleados y/o al público. Muchas organizaciones que utilizan la norma [27001/2] no cuentan con tecnología operativa ni se enfrentan a los riesgos asociados a ella.

En el caso de aquellas organizaciones que sí lo hagan, dichos riesgos se identificarían bajo los requisitos de gestión de riesgos establecidos en la cláusula 6.1.2 de la norma ISO/IEC 27001, ya que se trata de «riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información», en particular en lo que respecta a los parámetros que influyen en un proceso físico y a la información sobre el estado del proceso. Sin embargo, ninguna de las medidas de control de [27001/2] menciona explícitamente los riesgos físicos derivados de ciberataques.

2.1.2 Extractos de la serie de normas ISA/IEC 62443

Tratar el tema de los riesgos para la salud, la seguridad y el medio ambiente en el contexto de la ciberseguridad constituye una importante aportación de la norma [62443]. En particular, [62443-2-1] incluye requisitos específicos relacionados con seguridad y funciones de seguridad.[3]

Un concepto relacionado con la función de seguridad en la norma ISA/IEC 62443 es el de «función esencial». Una función de seguridad es un tipo de función esencial, según la siguiente definición de [62443-4-2]:

> **Función esencial**
> *Función o capacidad necesaria para mantener la salud, la seguridad y el medio ambiente (HSE), así como la disponibilidad del equipo bajo control.*

Los tres requisitos de [62443-2-1] que se citan a continuación se refieren explícitamente a funciones de seguridad o a funciones esenciales. Estos requisitos establecen, en resumen, que no se puede anular automáticamente el acceso del operador a las funciones de seguridad u otras funciones esenciales, que existe un control estricto sobre la configuración de los sistemas de seguridad y que los sistemas que no son de seguridad no interfieren con los sistemas de seguridad. A continuación se detallan dichos requisitos (resaltados sobre fondo gris), precedidos de una explicación de los fundamentos en los que se basan y de las posibles diferencias con respecto a entornos ajenos a la tecnología operativa.

El requisito [62443-2-1] USUARIO 1.3 refleja el hecho de que, en el entorno TO, los riesgos derivados de un operador incapaz de interactuar con un sistema de seguridad u otra función esencial superan las ventajas en términos de eficiencia y seguridad que supone la automatización de la revocación de los derechos de acceso. Por el contrario, en muchos entornos de tecnologías de la información, las contraseñas pueden eliminarse automáticamente si no se utilizan durante un determinado periodo de tiempo, o en caso de cambio de puesto de trabajo, como aplicación del control [27001/2] **5.18 Derechos de acceso.**

ISA/IEC 62443-2-1 **USER 1.3 Persistencia de la identidad del usuario**

El propietario de los activos deberá disponer de políticas y procedimientos para verificar que los identificadores de usuario, los autenticadores, las funciones y los derechos de acceso asociados específicos del IACS que se utilizan para respaldar las operaciones esenciales del IACS, incluidas las cuentas de los operadores, estén configurados de tal forma que no se desactiven automáticamente.

[3] Algunos ejemplos de funciones de seguridad son los controladores que pueden abrir una válvula de seguridad cuando un sensor indica una presión elevada; o un sistema de frenado diseñado para reducir la velocidad de un tren si se supera un umbral de velocidad.

DATOS 1.3 permite un control estricto de la configuración de los sistemas de seguridad, ya que estos datos son de vital importancia y rara vez es necesario modificarlos. En muchos entornos de tecnologías de la información, la reconfiguración de los sistemas puede ser algo habitual. Las recomendaciones generales de la norma ISO/IEC 27002 sí exigen planificar y evaluar el impacto potencial de los cambios, así como incluir consideraciones de emergencia, como los procedimientos de contingencia, en el apartado **8.32 Gestión de cambios**

ISA/IEC 62443-2-1 **DATOS 1.3 Modo de configuración del sistema de seguridad**

Si se autoriza el uso de sistemas de seguridad en el IACS, el propietario de los activos deberá contar con políticas y procedimientos relacionados con:
a) actualizar la configuración del sistema de seguridad únicamente cuando el modo de configuración esté activado, y
b) activar el modo de configuración únicamente cuando sea necesario realizar cambios en la configuración.

El objetivo de RED 1.3 es evitar que otros dispositivos o redes interfieran en el funcionamiento del sistema de seguridad, garantizando que este pueda desempeñar sus funciones de forma eficaz y dentro del plazo establecido. En muchos entornos informáticos, el tráfico procedente de otras redes a menudo puede provocar retrasos en el tráfico interno de una red, y las interrupciones breves pueden considerarse aceptables. Las directrices relativas al control general 27002 **8.22 Segregación de redes** establecen que la importancia crítica de una función puede ser un motivo para segregar determinadas redes.

ISA/IEC 62443-2-1 **RED 1.3 Segmentación de la red a partir de los sistemas de seguridad**

Si el IACS incluye una red de sistemas de seguridad, el propietario de la instalación deberá contar con políticas y procedimientos relacionados con la protección de dichos sistemas frente a interferencias procedentes de redes ajenas a los sistemas de seguridad y de los dispositivos de estas.

2.2 Continuidad del proceso físico

2.2.1 Relación con [27001/2]

El control [27001/2] **5.30 Preparación de las TIC para la continuidad del negocio** tiene por objeto garantizar la disponibilidad de toda la información de la organización y los activos relacionados en caso de interrupción, incluidos los ciberataques. En el caso de una organización que cuente con TO, un análisis del impacto empresarial ante un escenario de ciberataque incluiría no solo la interrupción de los procesos empresariales, sino también la interrupción de los procesos físicos controlados por la TO.

La guía 27002 sobre control **5.24 Planificación y preparación para la gestión de incidentes de seguridad de la información** recomienda definir y aplicar las «*prioridades de la organización para gestionar los incidentes de seguridad de la información, incluido el plazo de resolución en función de las posibles consecuencias y la gravedad*».

2.2.2 Extractos de la serie de normas ISA/IEC 62443

En relación con estas prácticas recogidas en [27001/2], la norma ISA/IEC 62443 exige la implantación de políticas y procedimientos para hacer frente a la interrupción del control normal del proceso físico por parte del IACS y señala la posible necesidad de una respuesta inmediata ante determinados ciberataques al IACS.

En concreto, el requisito [62443-2-1] DISPONIBILIDAD 1.3 que se cita a continuación aborda el diseño y la planificación para hacer frente a las consecuencias de una interrupción imprevista de los procesos físicos debida a un ciberataque. Establece que, si no es posible mantener el funcionamiento normal debido a un ciberataque, los equipos de TO puedan colocarse en un estado predeterminado. Esto permite a la organización planificar cómo actuar ante un ataque al sistema de control y evitar, en la medida de lo posible, daños en los equipos o las instalaciones. La pérdida de capacidad de producción puede minimizarse. Cualquier impacto inevitable sobre la salud, la seguridad o el medio ambiente que se produzca como consecuencia de la transición al estado predeterminado puede identificarse con antelación, y pueden planificarse medidas de mitigación.

ISA/IEC 62443-2-1 **DISPONIBILIDAD 1.3 Estado de fallo**

El propietario del activo deberá contar con políticas y procedimientos destinados a restablecer el IACS a un estado predeterminado en caso de que no sea posible mantener el funcionamiento normal como consecuencia de una brecha de seguridad detectada.

Dado que las consecuencias en el proceso físico derivadas de la indisponibilidad de la Solución de Automatización pueden producirse muy rápidamente, la norma [62443-2-1] hace hincapié explícitamente en la necesidad de tener en cuenta los eventos que requieren una detección y una respuesta inmediatas, tal y como se establece en el requisito EVENTO 1.1.

ISA/IEC 62443-2-1 **EVENTO 1.1 Detección de eventos**

El propietario del activo deberá contar con políticas y procedimientos relacionados con la notificación, el registro, el análisis y la respuesta (inmediata o diferida) a los incidentes relacionados con la seguridad de los sistemas de control industrial automatizados (IACS) que se detecten, con el fin de respaldar las actividades de gestión de la seguridad.

2.3 La denegación de servicio como «efecto no deseado»

2.3.1 Relación con [27001/2]

El apartado 6.1.1 de la norma ISO/IEC 27001 exige que la planificación del sistema de gestión de la seguridad de la información incluya el tratamiento de los riesgos con el fin de «prevenir o reducir los efectos indeseados» derivados de la implantación de dicho sistema. Por lo tanto, es necesario que una organización identifique y gestione el riesgo de que se produzcan efectos secundarios indeseables derivados de la aplicación de los controles de seguridad.

2.3.2 Extractos de la serie de normas ISA/IEC 62443

En concreto, algunas medidas de ciberseguridad habituales pueden, por sí mismas, afectar negativamente a la disponibilidad del sistema. En el análisis anterior sobre los riesgos físicos se ha señalado que, en el entorno de la tecnología operativa, la indisponibilidad del sistema puede acarrear graves consecuencias, ya que los usuarios no podrían llevar a cabo las acciones necesarias para gestionar el proceso físico. Graves consecuencias pueden producirse muy rápidamente a partir de la indisponibilidad de los sistemas operativos mientras que, en muchos entornos TI, los breves periodos de «tiempo de inactividad», aunque puedan ser indeseables, tienen consecuencias menos graves.

Por este motivo, los siguientes requisitos [62443-2-1] abordan situaciones concretas en las que los mecanismos de seguridad están diseñados para evitar que se produzcan situaciones de denegación de servicio.

En el requisito [62443-2-1] USER 1.8 que se cita a continuación, [62443-2-1] no exige el bloqueo automático de la pantalla si el hecho de no poder acceder a ella puede suponer un riesgo mayor para el IACS que el que supondría el acceso a una pantalla desatendida. La guía 27002 para el control **7.7 Escritorio y pantalla despejados**, en el punto c, recomienda que todos los ordenadores y sistemas se configuren con una función de tiempo de espera o de cierre de sesión automático.

ISA/IEC 62443-2-1 **USUARIO 1.18 Bloqueo de pantalla**

El propietario de los activos deberá contar con políticas y procedimientos relativos al bloqueo de las pantallas de los usuarios… salvo que la imposibilidad de acceder a la pantalla pueda suponer un riesgo mayor para el IACS…

De acuerdo con los requisitos [62443-2-1] RED 1.5 y RED 1.5, el IACS está diseñado para funcionar cuando está desconectado de redes externas, ya que la desconexión es una respuesta habitual ante un ataque (tal y como se describe en la guía [27002] para el control **8.20 Seguridad de las redes**, punto m).

ISA/IEC 62443-2-1 **RED 1.4 Autonomía de la red**

El propietario de los activos deberá contar con políticas y procedimientos relativos a la capacidad de hacer funcionar el IACS tal y como está diseñado cuando esté desconectado de las redes externas (por ejemplo, funcionamiento a prueba de fallos, apagado seguro, funcionamiento restringido y funcionamiento normal).

ISA/IEC 62443-2-1 **RED 1.5 Desconexión de redes externas**

El propietario del activo deberá contar con políticas y procedimientos relativos a la capacidad de desconectar el IACS de las redes externas para protegerse a sí mismo o a dichas redes frente a amenazas reales o presuntas.

[62443-2-1] El apartado COMPATIBILIDAD 2.3 que se cita a continuación aborda el problema de que se ha constatado que la protección contra el malware provoca problemas de rendimiento o disponibilidad en los componentes de la Solución de Automatización, lo que interfiere en el control de procesos u otras funciones del sistema. Por lo tanto, la norma [62443-2-1] exige que las organizaciones se aseguren de que tanto dicho software como los archivos de definiciones de malware se sometan a pruebas de compatibilidad con los dispositivos y sistemas de la Solución de Automatización. En el caso de muchos sistemas informáticos contemplados en [27001/2], el proveedor del software de protección contra malware suele realizar dichas pruebas en plataformas habituales. Por lo tanto, esto no suele considerarse un requisito de prueba para los propietarios de dichos activos informáticos. Sin embargo, es poco probable que los proveedores de software de protección contra malware dispongan de los medios necesarios para realizar pruebas de compatibilidad con los productos de la Solución de Automatización. La guía [27002] para el control **8.7 Protección contra el malware** señala, en el apartado «Información adicional», que «no siempre es posible instalar software de protección contra el malware en algunos sistemas (por ejemplo, en algunos sistemas de control industrial)».

ISA/IEC 62443-2-1 **COMPATIBILIDAD 2.3 Validación e instalación de software de protección contra malware**

El propietario del activo deberá disponer de políticas y procedimientos relativos a las pruebas de compatibilidad, la aprobación y la instalación de software de protección contra malware y de cualquier archivo de firmas de malware relacionado, en un plazo razonable tras su lanzamiento.

Los propios procesos de copia de seguridad también pueden tener efectos no deseados en el funcionamiento de los IACS, tal y como se refleja en el siguiente requisito.

ISA/IEC 62443-2-1 **DISPONIBILIDAD 2.2 No interferencia en las copias de seguridad**

El propietario del activo deberá contar con políticas y procedimientos que garanticen que los procesos de copia de seguridad no afecten negativamente al funcionamiento normal del IACS.

El requisito [62443-2-1] USUARIO 1.3 **Persistencia de la identidad del usuario** , citado anteriormente en la sección 2.1.2, es un ejemplo más de un requisito relativo a la autenticación de usuarios, cuyo objetivo es evitar una situación de denegación de servicio en el acceso a funciones esenciales debido a la supresión automática de los derechos de acceso de los usuarios.

2.4 Zonas de seguridad y diseño de redes

2.4.1 Relación con [27001/2]

El [27001/2] control **8.22 Segregación de redes** dice: «Los grupos de servicios de información, usuarios y sistemas de información deben estar separados en las redes de la organización». Entre otras recomendaciones se incluye lo siguiente: «…los dominios [de red] pueden seleccionarse en función de los niveles de confianza, importancia y sensibilidad (por ejemplo, dominio de acceso público, dominio de equipos de sobremesa, dominio de servidores, sistemas de bajo y alto riesgo), según las unidades organizativas…».

2.4.2 Extractos de la serie de normas ISA/IEC 62443

El principio más general de dividir los activos en zonas de seguridad ocupa un lugar central en [62443]. El concepto de «zonas» que aparece en [62443] no implica necesariamente el uso de una técnica concreta, como la segregación de redes.
La norma exige técnicas de partición que garanticen la protección entre zonas (particiones). Otras técnicas posibles son el uso de hardware virtualizado o mantener contenidas las aplicaciones.

En concreto, la norma [62443-2-1] exige la división en zonas tal y como se indica en los dos requisitos siguientes.

ISA/IEC 62443-2-1 **RED 1.1 Segmentación de zonas no pertenecientes al IACS**

El propietario de la instalación deberá contar con políticas y procedimientos que separen las zonas IACS de las no IACS y que limiten cualquier interconexión al mínimo necesario para el funcionamiento del IACS y dentro de unos límites de riesgo aceptables.

ISA/IEC 62443-2-1 **RED 1.2 Documentación de las zonas y de las interconexiones entre zonas de red**

El propietario de los activos deberá disponer de políticas y procedimientos para documentar y mantener una referencia de todas las zonas del IACS y de las interconexiones y/o conductos entre zonas de red, los riesgos de seguridad asociados a cada una de ellas y su clasificación como de confianza o no fiables.

El requisito de la norma [62443-3-3] REQUISITOS DEL SISTEMA 5.2 exige medidas de protección para los límites de las zonas (independientemente de cómo se implementen dichas zonas).

ISA/IEC 62443-3-3 **REQUISITOS DEL SISTEMA 5.2 Protección de los límites de las zonas**

El sistema de control deberá permitir supervisar y controlar las comunicaciones en los límites de las zonas, con el fin de garantizar la compartimentación definida en el modelo de zonas y conductos basado en el riesgo.

En [62443-3-2] se proporcionan más especificaciones sobre la zonificación, que exigen particionar activos del IACS de otros activos empresariales o comerciales, así como de los activos de seguridad de otros activos, tal y como se establece en los Requisitos de Zona y Conductos (RZC) RZC 3.1 a RZC 3.3 que se citan a continuación.

ISA/IEC 62443-3-2 **RZC 3.1 Establecer zonas y conductos**

La organización agrupará los IACS y los activos relacionados en zonas o canales según el nivel de riesgo. La agrupación se basará en los resultados de la evaluación inicial de riesgos de ciberseguridad o en otros criterios, como la importancia crítica de los activos, la función operativa, la ubicación física o lógica, el acceso requerido (por ejemplo, los principios de privilegio mínimo) o la organización responsable.

ISA/IEC 62443-3-2 **RZC 3.2 Separar los activos de la empresa de los del IACS**

Los activos del IACS se agruparán en zonas separadas, lógica o físicamente, de los activos de los sistemas de negocio o de la empresa.

ISA/IEC 62443-3-2 **RZC 3.3 Separar los activos relacionados con la seguridad**

Los elementos del IACS relacionados con la seguridad se agruparán en zonas separadas, lógica o físicamente, de las zonas no relacionadas con la seguridad que contengan elementos del IACS. No obstante, si no es posible separarlas, toda la zona se considerará una zona relacionada con la seguridad.

Además de estos requisitos de zonificación, [62443-2-1] también incluye requisitos específicos en materia de segmentación de redes.

[62443-2-1] Los requisitos sobre segmentación de redes establecen, en resumen, que las redes de seguridad deben estar protegidas contra interferencias (RED 1.3, citado anteriormente en la sección 2.1.2 en el apartado dedicado a la seguridad) y que el IACS debe poder desconectarse de todas las redes externas y ser capaz de funcionar según lo previsto en dicha situación (RED 1.4, RED 1.5, citados anteriormente en la sección 2.3, en el apartado dedicado a la denegación de servicio). Además, se identifican, documentan y gestionan los riesgos relacionados con la conexión entre los segmentos de la red interna del IACS (RED 1.6).

ISA/IEC 62443-2-1 **RED 1.3 Segmentación de la red a partir de los sistemas de seguridad**

Si el IACS incluye una red de sistemas de seguridad, el propietario de la instalación deberá contar con políticas y procedimientos relacionados con la protección de dichos sistemas frente a interferencias procedentes de redes ajenas a los sistemas de seguridad y de los dispositivos de estas.

ISA/IEC 62443-2-1 **RED 1.4 Autonomía de la red**

El propietario de los activos deberá contar con políticas y procedimientos relativos a la capacidad de hacer funcionar el IACS tal y como está diseñado cuando esté desconectado de las redes externas (por ejemplo, funcionamiento a prueba de fallos, apagado seguro, funcionamiento restringido y funcionamiento normal).

ISA/IEC 62443-2-1 **RED 1.5 Desconexión de redes externas**

El propietario del activo deberá contar con políticas y procedimientos relativos a la capacidad de desconectar el IACS de las redes externas para protegerse a sí mismo o a dichas redes frente a amenazas reales o presuntas.

ISA/IEC 62443-2-1 **RED 1.6: Control de acceso a la red interna**

El propietario del activo deberá contar con políticas y procedimientos para identificar, documentar y mitigar o gestionar de cualquier otra forma los riesgos de seguridad asociados a las comunicaciones entre los segmentos de la red interna del IACS, lo que incluye determinar un nivel de riesgo tolerable y responder a los riesgos que superen dicho nivel.

2.5 Controles rigurosos de la integridad del sistema.

2.5.1 Relación con [27001/2]

El control de la norma [27001/2] **5.9 Inventario de la información y otros activos relacionados** requiere llevar un inventario de activos. Las directrices de [27002] incluyen: «El nivel de detalle del inventario de información y otros activos asociados debe ser el adecuado para las necesidades de la organización». Además, el requisito **8.9 «Gestión de la configuración»** establece lo siguiente: «Las configuraciones, incluidas

las de seguridad del hardware, el software, los servicios y las redes deben establecerse, documentarse, implementarse, supervisarse y revisarse».

2.5.2 Extractos de la serie de normas ISA/IEC 62443

[62443-2-1] incluye requisitos detallados sobre la gestión del inventario y la configuración de los activos. Del mismo modo que la pérdida de *disponibilidad* del sistema puede tener graves consecuencias, la pérdida de *integridad* del sistema de TO también puede afectar a la salud, la seguridad y el medio ambiente. Los componentes de una Solución de Automatización en producción no pueden diferir de los que se han probado y aprobado definitivamente, debido al riesgo de que se produzcan consecuencias graves. Esta preocupación da lugar a los requisitos de [62443-2-1] relativos al mantenimiento de la documentación necesaria para identificar y describir los componentes actuales del sistema, así como sus conexiones de red.

La norma [62443-2-1] especifica en el apartado CM 1.1 que el inventario de activos incluye dispositivos, componentes de hardware, componentes de software y todos los protocolos y puertos de comunicación utilizados.

ISA/IEC 62443-2-1 **CM 1.1 Inventario de activos de referencia**

El propietario del activo deberá disponer de políticas y procedimientos para documentar, verificar y mantener, a lo largo de todo el ciclo de vida del IACS, el inventario de referencia de todos los dispositivos, componentes de hardware, componentes de software, protocolos de comunicación y puertos de comunicación abiertos utilizados en el IACS, incluyendo, entre otros:

- *a) responsabilidades organizacionales,*
- *b) fabricante,*
- *c) modelo,*
- *d) números de versión,*
- e) *números de serie,*
- *f) interfaces de red,*
- *g) direcciones de comunicación,*
- *h) niveles de revisión/parches,* e
- i) *historial.*

[62443-2-1] también especifica, en el apartado CM 1.1 y en los requisitos que se citan a continuación, los campos de datos concretos necesarios para la documentación del inventario de activos, lo que define un nivel mínimo de detalle adecuado para el entorno TO. Ejemplos de campos de datos especificados en los requisitos CM 1.1 y CM de [62443-2-1]
1.2 son: fabricante, número de modelo, número de serie, número de versión, nivel de revisión/parche, historial y conectividad física y lógica de todos los dispositivos y componentes de software de la Solución de Automatización. CM 1.3 exige la documentación y la verificación de los parámetros de configuración.

ISA/IEC 62443-2-1 **CM 1.2 Planos y documentación de infraestructuras**

El propietario del activo deberá disponer de políticas y procedimientos para verificar y mantener actualizada la referencia de planos y documentación que muestren la conectividad física y lógica de todos los dispositivos y componentes de software del IACS.

ISA/IEC 62443-2-1 **CM 1.3 Ajustes de configuración**

El propietario de los activos deberá disponer de políticas y procedimientos para documentar los parámetros de configuración de todos los dispositivos y aplicaciones de software del IACS, así como para verificar que su funcionamiento se ajusta a la configuración documentada.

[62443-2-1] CM 1.4 además exige que cualquier modificación de los datos de este inventario de activos sea autorizada, validada y aprobada.

ISA/IEC 62443-2-1 **CM 1.4 Control de cambios**

El propietario del activo deberá disponer de políticas y procedimientos para autorizar, validar y aprobar los cambios en la configuración de referencia actual y en los planos y la documentación de la infraestructura, incluidos los niveles de revisión y de parches.

[62443-2-1] también exige el seguimiento de las conexiones de acceso remoto en RED 3.2, tal y como se indica a continuación. En el entorno de los IACS, es habitual que los proveedores de equipos IACS soliciten acceso remoto para la resolución de problemas, las reparaciones o las actualizaciones de sus equipos. Es posible que estas situaciones no estén planificadas de antemano, que sean de corta duración y que requieran privilegios específicos y limitados en el IACS, los cuales pueden variar en cada caso. Una gestión cuidadosa es fundamental para la seguridad de la solución de automatización. Los activos generales de TI y sus conexiones pueden ser más dinámicos que los de los IACS, lo que hace que el seguimiento de los activos y las conexiones con el nivel de detalle exigido en [62443-2-1] resulte menos factible en un entorno de TI que en uno de TO, incluso con un alto grado de automatización.

ISA/IEC 62443-2-1 **RED 3.2 Conexiones de acceso remoto**

Si se autoriza el uso del acceso remoto en el IACS, el propietario de los activos deberá contar con políticas y procedimientos relativos a la autorización, la autenticación, el cifrado, la documentación, el registro y la supervisión de todas las conexiones interactivas de acceso remoto. La documentación de cada conexión deberá incluir, entre otros:

a) su finalidad,
b) la aplicación de acceso remoto que se va a utilizar,
c) las tecnologías de cifrado y autenticaciones utilizadas,
d) cómo se establecerá la conexión (por ejemplo, a través de Internet, mediante una red privada virtual (VPN) o a través de una DMZ), con las instrucciones necesarias,
e) las circunstancias que requieren la conexión,
f) el tiempo que debe permanecer abierta la conexión, incluidos los periodos de inactividad previstos,
g) la ubicación y la identidad del dispositivo de cliente remoto, la aplicación y el usuario, y
h) cualquier requisito normativo que deba cumplirse antes de establecer la conexión

Aunque el seguimiento de los activos no es el objetivo principal del siguiente requisito de [62443-2-1], dicho requisito implica un seguimiento minucioso de los activos:

La guía de 27002 sobre controles **8.8 Gestión de vulnerabilidades técnicas** establece, en el apartado «Adopción de medidas adecuadas para abordar las vulnerabilidades técnicas»: «... si no hay ninguna actualización disponible o si la actualización no se puede instalar, se deben considerar otros controles...» La norma [62443-2-1] COMPATIBILIDAD 3.5, citada a continuación, amplía los requisitos para este escenario, estableciendo que, en cualquier caso en el que no se instale un parche, es obligatorio abordar el riesgo asociado y documentar la resolución de dicho riesgo. Se trata, en esencia, de un requisito para realizar un seguimiento de determinados tipos de cambios en el sistema que no se han llevado a cabo, además del requisito de realizar un seguimiento de los cambios que sí se han llevado a cabo.

ISA/IEC 62443-2-1 **COMPATIBILIDAD 3.5 Medidas de mitigación de parches de seguridad**

El propietario del activo deberá contar con políticas y procedimientos relacionados con la evaluación del riesgo que supone no instalar los parches de seguridad pertinentes y, si dicho riesgo no es aceptable, deberá abordarlo y documentar la solución.

2.6 Niveles de seguridad

2.6.1 Relación con [27001/2]

Tal y como se establece de forma más explícita en los apartados 6.1.2 y 6.1.3, la norma 27001 exige que las decisiones relativas a los controles de seguridad se tomen «en función del riesgo». Del mismo modo, [62443] y muchas otras normas de ciberseguridad utilizan este enfoque. Un reto que plantea cualquier enfoque basado en el riesgo es: ¿cómo se traduce un nivel de riesgo en la elección de una aplicación concreta de un control? Muchos controles de seguridad pueden implementarse con distintos «niveles de solidez». Quizá el ejemplo más habitual sea el de la autenticación de un solo factor frente a la de múltiples factores. Normalmente, a los riesgos se les asigna una clasificación numérica o cualitativa por parte de una organización (por ejemplo, un número entre 1 y 5, o «alto», «medio» y «bajo»). Entonces, ¿qué nivel de riesgo justifica la autenticación multifactorial?

2.6.2 Extractos de la serie de normas ISA/IEC 62443

[62443] ayuda a traducir el riesgo en la selección de controles, utilizando el concepto de nivel de seguridad. Hay cuatro niveles. Estos niveles constituyen uno de los factores que se tienen en cuenta a la hora de determinar el riesgo, es decir, el tipo de adversario frente al cual debe protegerse una zona de seguridad. El nivel de seguridad más bajo requiere protección frente a errores involuntarios cometidos por personas con buenas intenciones. El nivel de seguridad más alto exige protección frente a un atacante altamente calificado e intencionado. El proceso de evaluación de riesgos [62443-3-2] consiste en asignar un nivel de seguridad objetivo a una zona de seguridad. En otras secciones de [62443] se enumeran las capacidades de los componentes y sistemas y se clasifican según su nivel de seguridad. Cada nivel incluye los requisitos de todos los niveles inferiores.

A modo de ejemplo, la norma [62443-3-3] REQUISITOS DEL SISTEMA 1.1, que se cita a continuación, exige que, para el nivel de seguridad más alto (4), se disponga de autenticación multifactorial para todos los usuarios humanos. En el nivel de seguridad 3, la autenticación multifactorial está disponible para todos los usuarios humanos que accedan al sistema a través de redes no fiables. En los niveles de seguridad 1 o 2, no se requiere la autenticación multifactorial. Esta clasificación por nivel de seguridad no es un algoritmo automatizado para seleccionar controles, sino que ofrece un punto de partida para tomar esas decisiones.

ISA/IEC 62443-3-3 **REQUISITOS DEL SISTEMA 1.1 – Identificación y autenticación de usuarios humanos. Requisito básico, Nivel de seguridad 1**

El sistema de control deberá permitir identificar y autenticar a todos los usuarios humanos. Esta funcionalidad garantizará dicha identificación y autenticación en todas las interfaces que permitan el acceso de usuarios humanos al sistema de control, con el fin de respaldar la segregación de funciones y el principio del privilegio mínimo, de conformidad con las políticas y procedimientos de seguridad aplicables.

REQUISITOS DEL SISTEMA 1.1 Mejora de los requisitos 1
Identificación y autenticación únicas, Nivel de seguridad 2

El sistema de control deberá permitir identificar y autenticar de forma unívoca a todos los usuarios humanos.

REQUISITOS DEL SISTEMA 1.1 Mejora de los requisitos 2
Autenticación multifactorial para redes no fiables, nivel de seguridad 3

El sistema de control deberá permitir el uso de la autenticación multifactorial para el acceso de usuarios humanos al sistema de control a través de una red no fiable.

REQUISITOS DEL SISTEMA 1.1 Mejora de los requisitos 3
Autenticación multifactorial para todas las redes, nivel de seguridad 4

El sistema de control deberá permitir el uso de la autenticación multifactorial para todos los accesos de usuarios humanos al sistema de control.

Del mismo modo, todos los requisitos relativos a los componentes y sistemas que figuran en [62443-4-2] y [62443-3-3] tienen asociado un nivel de capacidad de seguridad.

En el análisis de la sección 2 se ha abordado la siguiente cuestión: ¿cuáles son las diferencias clave entre los requisitos de ciberseguridad de los sistemas de TO para los propietarios de activos que figuran en la norma ISA/IEC 62443 y los que figuran en [27001/2]? Las dos secciones siguientes se centran en los aspectos de seguridad más habituales que abordan estas normas.

2.7 Propósito de la TO

El libro blanco «Aplicación de las normas ISO/IEC 27001 / ISO/IEC 27002 y la serie de normas ISA/IEC 62443 a los entornos de tecnología operativa» [OTE, siglas en inglés] ofrece una visión general de cómo las normas [27001/2] y [62443] pueden utilizarse conjuntamente como normas complementarias por parte de las organizaciones responsables de la seguridad de los entornos de tecnología operativa (TO). Cada una de estas normas aporta elementos únicos a un programa de seguridad para entornos de tecnología operativa (TO). El presente artículo describe con mayor detalle el valor único que aporta [62443] a un entorno TO, dirigido a un público que ya haya implementado [27001/2] o esté familiarizado con él. El objetivo aquí es responder a las siguientes preguntas: si ya dispones de un sistema de gestión de la seguridad [27001/2] que abarca tus operaciones de TI, ¿cómo puedes utilizar la serie de normas ISA/IEC 62443 para ampliar dicho sistema de gestión de la seguridad de modo que también cubra tus operaciones de TO (tecnología operativa)? ¿Qué aspectos de esta expansión podrían ser únicos de la tecnología operativa y cuáles tendrían en común con las tecnologías de la información?

La Organización Internacional de Normalización (IEC, siglas en inglés) ha reconocido y estructurado el desarrollo de normas para las tecnologías de la información (TI) y las tecnologías operativas (TO) como dos iniciativas relacionadas, pero diferenciadas. Citando la «página web de la IEC»: *«La ciberseguridad suele asociarse con las tecnologías de la información y, a menudo, es gestionada por el departamento de TI, centrándose en proteger el flujo de datos en el mundo virtual. Sin embargo, las infraestructuras críticas y el entorno automatizado de las fábricas o refinerías tienen requisitos de seguridad que forman parte del mundo real. Dependen de las tecnologías operativas (TO) para garantizar la correcta ejecución de acciones automatizadas, como cerrar una válvula para evitar el desbordamiento de productos químicos o poner en marcha un generador para evitar un apagón… El Comité Técnico Conjunto ISO/IEC (JTC 1, sus siglas en inglés) elabora la familia de normas ISO/IEC 27000 para los sistemas de tecnologías de la información (TI). El Comité Técnico 65 (TC 65) de la IEC publica la norma IEC 62443 para la tecnología operativa presente en infraestructuras industriales y críticas, entre las que se incluyen, entre otras, las empresas de suministro eléctrico, los sistemas de gestión del agua, los sistemas sanitarios y los sistemas de transporte».*

El objetivo principal de este documento es ofrecer una visión técnica detallada de la relación entre estas dos normas, dirigida a los responsables de la toma de decisiones que estén considerando la adopción de la norma [62443], además de la [27001/2], para su entorno de tecnología operativa (OT). Para aquellas organizaciones que hayan decidido adoptar ambas normas, el documento identifica los principales aspectos específicos de la norma [62443] para el entorno TO, así como los fundamentos que los justifican. Además, el análisis de los temas comunes a ambas normas permite identificar aquellas áreas en las que una organización se beneficiará al tener en cuenta la coordinación deseada entre TI y TO, así como las diferencias necesarias entre las implementaciones de los controles de seguridad en TI y TO para cumplir los requisitos.

2.8 Alcance

2.8.1 Alcance del debate

[27001/2] se aplica a cualquier tipo de organización, así como a los sistemas informáticos que utiliza para llevar a cabo sus actividades. El presente análisis se centra en aquellos puntos de la norma [62443] que recogen los requisitos que deben cumplir las entidades responsables de un IACS (sistema de automatización y control industrial) en funcionamiento, una función análoga a la del público destinado de la norma [27001/2]. En [62443], estas organizaciones se denominan «propietarios de activos».

Nota: En [62443], se distingue entre el *propietario de un activo* y el *proveedor de un producto*, que es el responsable de desarrollar un producto IACS destinado a ser utilizado por otra entidad. A partir de ese momento, dicha entidad pasa a ser propietaria de los activos y utiliza el producto IACS del proveedor. Otra parte de la norma [62443], la ISA/IEC 62443-4-1 [62443-4-1], se aplica a los proveedores de productos y aborda el tema de cómo desarrollar un producto de sistema de control seguro.
Así pues, una organización que desarrolle productos para sistemas de control podría aplicar la norma [27001/2] a sus propios sistemas informáticos internos y la norma [62443-2-1] a sus propias instalaciones de fabricación. Sin embargo, ninguna de ellas aborda el proceso de desarrollo de un producto de sistema de control seguro, que es un tema independiente tratado en [62443-4-1].

Los puntos del documento [62443] que se aplican a los propietarios de activos y a las referencias son los siguientes:

- ISA/IEC 62443-2-1 [62443-2-1],
- ISA/IEC 62443-3-2 [62443-3-2] y
- ISA/IEC 62443-3-3 [62443-3-3].

A continuación, la sección 3 describe con más detalle el uso de los roles en la estructura general de [62443]. Este documento incluye correspondencias parciales entre [27001/2] y el contenido de [62443], con el fin de responder a las preguntas planteadas anteriormente, e incluye referencias específicas a aproximadamente la mitad de los requisitos de [62443-2-1]. El artículo destaca las diferencias específicas entre los entornos de TI y de TO para describir las ventajas de estos requisitos concretos de [62443].

El objetivo del presente artículo es que el alcance del contenido de las dos normas seleccionadas para su análisis refleje la naturaleza y el valor de las principales aportaciones singulares de [62443], así como el grado de similitud entre ambas normas.

2.8.2 Temas relacionados

Los siguientes temas relacionados quedan fuera del alcance de este artículo. No obstante, también resultarían de interés para aquellas organizaciones que estén considerando la aplicación tanto de la norma [27001/2] como de la [62443]. Se obtienen ventajas adicionales al aplicar los demás puntos de [62443] junto con [62443-2-1], [62443-3-2] y [62443-3-3]. Los demás puntos de la norma se aplican a entidades distintas del propietario del activo, que desempeñan funciones fundamentales a la hora de ayudar al propietario del activo a garantizar la seguridad de las TO. Entre estas funciones se incluyen los desarrolladores de hardware y software ([62443-4-1]), los integradores y los proveedores de servicios de mantenimiento ([62443-2-4]), tal y como se describe con más detalle en la sección 3.

La aplicación de la norma [27001/2] aporta un valor único cuando ya se ha aplicado la norma [62443], lo cual constituye el tema inverso al que se aborda aquí. El propio [62443] exige, en virtud del requisito [62443-2-1] denominado ORG 1.1 «Sistema de gestión de la seguridad de la información (SGSI)», que los procesos de gestión exigidos por un SGSI estén coordinados con un programa de seguridad del IACS o formen parte del mismo. Este requisito podría cumplirse mediante el uso de un SGSI conforme a la norma [27001/2]. En consecuencia, el artículo [OTE] mencionado anteriormente recomienda utilizar ambas normas en el entorno de OT y ofrece ejemplos de las aportaciones específicas de cada una de ellas. Algunos ejemplos de temas tratados en [27001/2] que no se enumeran explícitamente en [62443-2-1], pero que entran dentro del requisito ORG 1.1, son el liderazgo y el compromiso, la auditoría interna y los términos relativos a la ciberseguridad en los contratos de trabajo.

Un recurso útil que se centra en definir y detallar las diferencias entre los entornos de TI y de TO es la sección 2.3 de la norma NIST 800-82, Rev. 3 [NIST 800-82].

2.8.3 TO e IACS

La «tecnología operativa (TO)» es el hardware y el software que detectan o provocan un cambio mediante la supervisión y/o el control directo de equipos, activos, procesos y eventos industriales [Gartner-ITG].

El lector observará que [62443] no utiliza el término «TO», sino el de «Solución de Automatización», que a su vez se define como los elementos de hardware y software de un IACS. El ámbito de aplicación declarado para la norma [62443] es el IACS. No obstante, la norma ISA/IEC 62443 ha sido aceptada y aplicada en ámbitos no industriales relacionados con la gestión de procesos físicos, como los dispositivos médicos y la automatización en edificios. En este artículo se reconoce el ámbito de aplicación más amplio de [62443] y se utiliza el término más general «TO», salvo cuando se cita directamente [62443].

Continuando con la cita de la página web de la IEC presentada en la sección 2.7: «El Comité Técnico 65 (TC 65) de la IEC publica la norma IEC 62443, relativa a la tecnología operativa presente en infraestructuras industriales y críticas, entre las que se incluyen, entre otras, las empresas de suministro eléctrico, los sistemas de gestión del agua, la sanidad y los sistemas de transporte. Estas normas horizontales, también conocidas como normas básicas, son independientes de la tecnología. «Se pueden aplicar en numerosas áreas técnicas».

2.8.4 Resumen del análisis

La parte dedicada al análisis de este trabajo se encuentra en las secciones 2, 4 y 5, tal y como se muestra en la Figura 2. La sección 3 ofrece información general sobre la estructura de [62443] y, a continuación, se presenta un resumen de las conclusiones.

La sección 2 *Aportaciones fundamentales de la serie de normas ISA/IEC 62443 para la seguridad de las TO*, describe los ámbitos de seguridad fundamentales que benefician de manera específica a los programas de seguridad de las TO, los requisitos de la norma [62443] para dichos ámbitos y las características específicas de los entornos de TO que dan lugar a dichos requisitos.

La sección 4, Precisiones sobre cuestiones comunes, describe los requisitos de [62443] que podrían considerarse precisiones de las recomendaciones recogidas en [27002]. Estas recomendaciones constituyen orientaciones adicionales para la aplicación de los controles enumerados en el anexo de la norma [27001]. Estas directrices no son obligatorias a efectos del cumplimiento de la norma 27001, ya que tienen carácter de recomendaciones y no de requisitos (según las definiciones de la sección 4 del presente informe). Sin embargo, algunos casos concretos de estas 27 002 recomendaciones sí tienen carácter de requisitos en [62443].

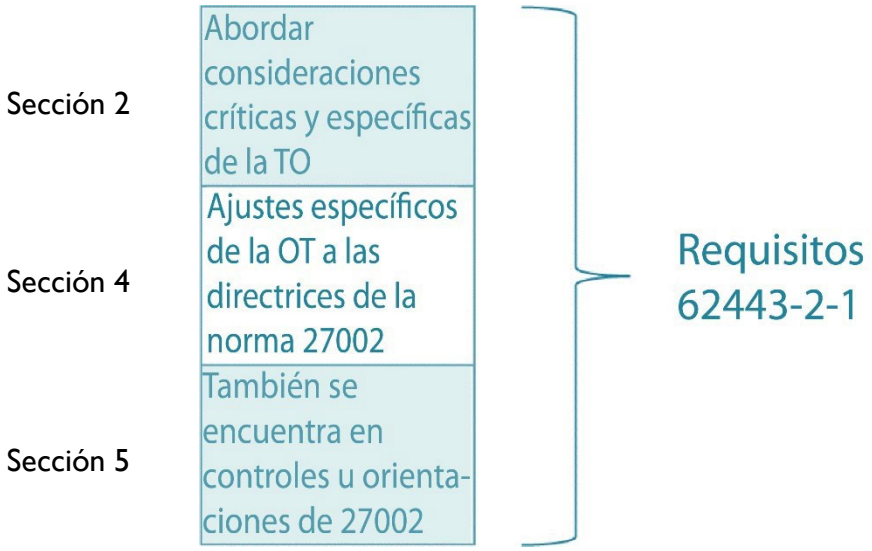

Figura 2. Categorías de requisitos de la norma ISA/IEC 62443-2-1 descritas en este documento

La sección 5, Prácticas comunes de *TI/TO*, identifica las áreas temáticas en las que ambas normas presentan un contenido prácticamente idéntico. En algunos casos, la norma [62443] exige el uso de un control identificado en [27001/2]. En otros casos, la norma [62443] exige el cumplimiento de una recomendación de las directrices de la norma ISO/IEC 27002.

Por lo tanto, en relación con los temas tratados en las secciones 4 y 5, [62443] ofrece información sobre cómo priorizar los controles y las recomendaciones de [27001/2] para un programa de seguridad de las TO.

3 Estructura de la serie de normas ISA/IEC 62443

Según la definición de la sección 7.1, un IACS incluye una solución técnica —la «Solución de Automatización»— así como al personal y las políticas que intervienen en el funcionamiento de dicha solución técnica.
Una aportación singular de [62443] radica en su estructura, diseñada desde la perspectiva de los usuarios de la norma. La norma consta de varios apartados, cada uno de los cuales se dirige a un actor diferente y aborda fases distintas del ciclo de vida de un IACS. Es bien sabido que incluso la Solución de Automatización diseñada con mayor seguridad puede volverse insegura durante su funcionamiento debido a prácticas inadecuadas de integración, operación y mantenimiento. La norma [62443] establece de forma explícita las funciones y responsabilidades de los principales actores en materia de ciberseguridad:

- proveedores de productos, abordando el proceso de desarrollo, las capacidades de seguridad de los componentes y las capacidades de seguridad del sistema ([62443-4-1], [62443-4-2], [62443-3-3])
- proveedores de servicios, incluidos los integradores y los proveedores de servicios de mantenimiento, que se ocupan del diseño y el mantenimiento de los sistemas ([62443-2-4], [62443-3-2], [62443-3-3])
- propietarios de activos, abordando el funcionamiento seguro ([62443-2-1]).

Gracias a esta estructura de la norma, los actores que desempeñan un papel en la seguridad del IACS pueden identificar fácilmente los requisitos de los que son responsables. Los requisitos establecidos en los distintos puntos del

estándar se complementan entre sí y son eficaces en todo el espectro de agentes y fases del ciclo de vida que pueden afectar a la seguridad de los IACS. Por ejemplo, un propietario de activos de OT que aplique requisitos de adquisición basados en [62443-3-3] tiene la garantía de que el sistema que adquiera contará con las capacidades técnicas suficientes para llevar a cabo un funcionamiento seguro, de conformidad con [62443-2-1]. Del mismo modo, un integrador de sistemas que diseñe un sistema de conformidad con la norma [62443-3-3] tiene la garantía de que dicho cumplimiento es factible si selecciona para dicho sistema componentes que cumplan con la norma [62443-4-2].

La figura 3 muestra las funciones de los principales actores en materia de seguridad del IACS y los apartados más relevantes de [62443] en relación con ellos. Consulte la sección 8 para ver la lista completa de referencias de estos puntos de [62443].

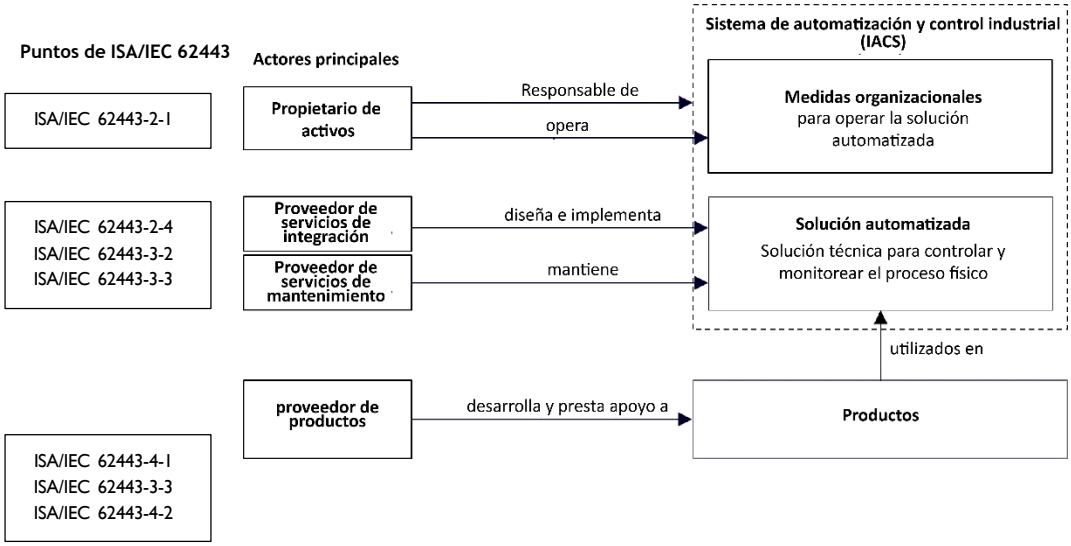

Figura 3. Funciones de los principales actores en la serie de normas ISA/IEC 62443

4 Aclaraciones sobre cuestiones de interés común

En el caso de algunos controles, las directrices [27002] recomiendan que una organización «considere» la aplicación del control en determinadas situaciones. En el caso de algunas de estas medidas de control, [62443-2-1] incluye un requisito que especifica las condiciones en las que debe aplicarse la medida de control para el TO. Estos requisitos podrían considerarse una ampliación de las directrices de la norma ISO/IEC 27002, que tienen en cuenta los riesgos que suelen ser inherentes a estas condiciones en el entorno de tecnología operativa (TO).

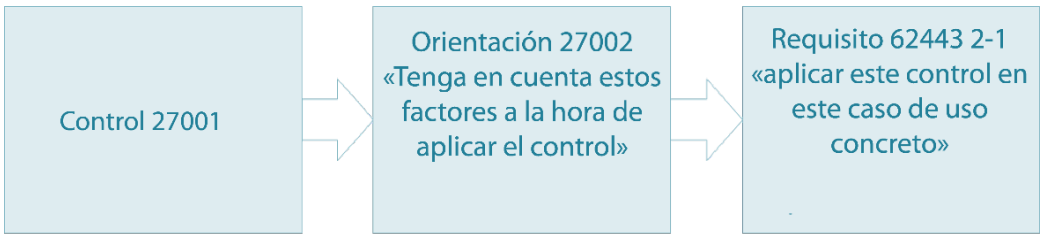

Figura 4. Recomendaciones de la norma ISO/IEC 27002 que constituyen requisitos de la serie de normas ISO/IEC 62443

En Tabla 1 se muestra ejemplos de requisitos de la norma [62443-2-1] que especifican casos concretos de aplicación de las orientaciones recogidas en la norma [27002]. A modo de ejemplo extraído de la tabla, en las directrices relativas al control **5.14 Transmisión de información**, [27002] recomienda tener en cuenta las restricciones aplicables a los medios de comunicación electrónicos. En [62443-2-1], el requisito RED 1.8 establece específicamente que las políticas y los procedimientos deben abordar las cargas útiles permitidas en los mensajes de usuario a usuario en las redes IACS.

Tabla 1. Ejemplos de requisitos de la norma ISA/IEC 62443-2-1 que concretan las directrices de la norma ISO/IEC 27002

ISO/IEC 27001 ID de control	**ISO/IEC 27002 referencia orientativa**	**ISO/IEC 27002 orientación - resumen**	**ISA/IEC 62443-2-1 ID y nombre del requisito**	**ISA/IEC 62443-2-1 requisito - resumen**
5.14 Transmisión de información	Transferencias electrónicas Puntos a), d), f)	Se debe tener en cuenta la protección contra el malware y las restricciones en los medios de comunicación electrónicos.	RED 1.8: Mensajería de usuarios	En el caso de los mensajes entre usuarios en las redes IACS, las políticas y los procedimientos establecen restricciones para los mensajes que contengan cargas potencialmente maliciosas, como archivos adjuntos, enlaces de red y scripts.
6.1 Selección	Penúltimo párrafo	Los procedimientos deben definir cómo, cuándo y por qué se debe llevar a cabo un control continuo del personal tras su incorporación inicial a la organización.	ORG 1.2 Verificación de antecedentes	Las políticas y procedimientos establecen la selección del personal antes de concederle acceso al IACS.
6.7 Trabajo remoto	Punto k) (primera lista)	Analiza la vulnerabilidad de la autenticación de un solo factor para el acceso remoto.	USUARIO 1.9 Autenticación multifactorial (MFA)	Las políticas y procedimientos abordan la autenticación multifactorial para los dispositivos IACS que admiten el inicio de sesión por parte de usuarios para el acceso remoto o cuando el dispositivo se encuentra en una zona de acceso público.
6.7 Trabajo remoto	Punto d) (segunda lista)	Entre las directrices y medidas relativas al trabajo remoto, hay que considerar los temporizadores de inactividad.	RED 3.3 Finalización del acceso remoto	Las políticas y los procedimientos establecen interrumpir las conexiones de acceso remoto interactivo tras un periodo de inactividad predefinido.

ISO/IEC 27001 ID de control	ISO/IEC 27002 referencia orientativa	ISO/IEC 27002 orientación - resumen	ISA/IEC 62443-2-1 ID y nombre del requisito	ISA/IEC 62443-2-1 requisito - resumen
8.26 Requisitos de seguridad de las aplicaciones	Punto k)	Valora si la aplicación tiene requisitos relativos a controles automatizados (por ejemplo, límites de autorización o autorizaciones dobles).	USUARIO 2.3 Autorizaciones múltiples	Las políticas y procedimientos establecen que las acciones que puedan tener graves repercusiones en el proceso industrial deben ser aprobadas por dos o más usuarios, salvo que el hecho de no llevar a cabo dicha acción pueda acarrear repercusiones aún mayores para el proceso industrial.

5 Prácticas comunes de TI/TO

Varios requisitos del documento [62443-2-1] exigen, en la práctica, bien la aplicación de los controles del documento [27001/2], bien el cumplimiento de las recomendaciones que figuran en las orientaciones de la norma ISO/IEC 27002 relativas a dichos controles.
Por lo tanto, la aplicación de dicho control de la [27001/2] implicaría el cumplimiento del requisito [62443-2-1] correspondiente. Estos requisitos del [62443] constituyen un ámbito importante de interés común tanto para los entornos de TI como para los de TO. Abarcan temas como la clasificación de la información en función de las medidas de seguridad necesarias, la verificación de la autenticidad e integridad del software que se va a instalar, el control de acceso basado en los principios del privilegio mínimo, la gestión de vulnerabilidades, la gestión de eventos de seguridad, la gestión de incidentes y la eliminación segura de los equipos. Las prácticas relacionadas con estos temas se describen de forma muy similar en ambas normas.

La tabla 2 ofrece ejemplos que reflejan estas prácticas comunes de TI/TO tal y como aparecen en [27001/2] y [62443-2-1].

Es importante destacar que, aunque la formulación de una recomendación o un requisito pueda ser la misma en ambas normas, las medidas que se adoptan para cumplir dicha recomendación o requisito no suelen ser las mismas en los entornos de TI y de TO. Los autores de las normas decidieron dejar el siguiente nivel de detalle a criterio de la organización que aplique la norma. Por ejemplo, tanto [27001/2] como [62443] tratan sobre la autenticación de usuarios humanos, pero ninguna de ellas exige el uso de la autenticación multifactorial. Aunque se pueda utilizar el mismo tipo de equipo tanto en un contexto de TI como en uno de TO, la decisión de utilizar o no la autenticación multifactorial para acceder a dicho equipo puede variar, debido a las diferencias en el entorno de riesgo relacionado con dicho equipo. Como segundo ejemplo, la formación en concienciación sobre ciberseguridad es una medida de control en [27001/2] y un requisito en [62443-2-1] para todas las personas que interactúan con el sistema TO. Sin embargo, puede haber diferencias en la formación en materia de concientización dirigida al personal que interactúa con el sistema de gestión de operaciones, al igual que puede haber diferencias en dicha formación para quienes interactúan con los sistemas de información de recursos humanos y con los sistemas contables. Además de la formación en sensibilización general,
[62443-2-1] establece un requisito adicional de formación relacionada con las responsabilidades asignadas en materia de ciberseguridad de TO.

Para cumplir con la norma ISO/IEC 27001, tal y como exige la subcláusula 6.1.3 de dicha norma, una organización no está obligada a aplicar todos los controles de [27001/2], pero sí debe evaluar la aplicabilidad de dichos controles de [27001/2] a su organización. En ese proceso de toma de decisiones, lo habitual habría sido que consultaran la guía correspondiente en [27002] para conocer los aspectos que deben tenerse en cuenta a la hora de aplicar el control. La organización también habría documentado sus decisiones sobre la aplicabilidad de estos controles en una declaración de aplicabilidad, que incluye «… *los controles necesarios; … la justificación de su inclusión; … si se han aplicado o no los controles necesarios; y… la justificación para excluir cualquiera de los controles».*

El hecho de que los requisitos que figuran en la tabla siguiente aparezcan en [62443-2-1] constituye una sólida justificación para incluir el control asociado [27001/2] en la declaración de aplicabilidad de una organización que cuente con una infraestructura de TO dentro del ámbito de aplicación de su sistema de gestión de la seguridad de la información, gestionado conforme a la norma ISO/IEC 27001.

Tabla 2. Ejemplos de controles y orientaciones de la norma ISO/IEC 27002 que constituyen requisitos de la norma ISA/IEC 62443-2-1

ISO/IEC 27001 ID y nombre del control	ISO/IEC 27002 Extracto de control u orientación	ISA/IEC 62443-2-1 ID y nombre del requisito	ISA/IEC 62443-2-1 Texto de requisitos - extracto
6.3 Sensibilización, educación y formación en materia de seguridad de la información	El personal de la organización y las partes interesadas pertinentes deben recibir la sensibilización, la formación y la capacitación adecuadas en materia de seguridad de la información. … (Control)	ORG 1.4 Capacitación en concientización sobre seguridad	El propietario del activo deberá contar con políticas y procedimientos que exijan que todo el personal (incluidos empleados, contratistas, subcontratistas, consultores, proveedores de productos y prestadores de servicios) que interactúe con el IACS reciba formación oficial en materia de ciberseguridad, que se actualice periódicamente.
8.9 Gestión de la configuración	Las configuraciones — incluidas las de seguridad— del hardware, el software, los servicios y las redes deben establecerse, documentarse, implementarse, supervisarse y revisarse. (Control)	CM 1.3 Ajustes de configuración	El propietario de los activos deberá disponer de políticas y procedimientos para documentar los parámetros de configuración de todos los dispositivos y aplicaciones de software del IACS, así como para verificar que su funcionamiento se ajusta a la configuración documentada.
8.7 Protección contra el malware	…analizar cualquier dato recibido a través de redes o de cualquier tipo de soporte de almacenamiento electrónico en busca de malware antes de su uso… (Directriz, punto f)1))	COMPATIBILIDAD 2.1 Libre de malware	El propietario de los activos deberá contar con políticas y procedimientos para verificar que todos los componentes y soportes portátiles (en caso de que se autorice el uso de soportes portátiles en el IACS) estén libres de malware conocido antes de su uso en el IACS.

ISO/IEC 27001 ID y nombre del control	ISO/IEC 27002 Extracto de control u orientación	ISA/IEC 62443-2-1 ID y nombre del requisito	ISA/IEC 62443-2-1 Texto de requisitos - extracto
5.15 Control de acceso	A las entidades solo se les concede acceso a la información y a otros activos relacionados, incluidos las redes y los servicios de red, que estén autorizados a utilizar. (Segunda lista de orientaciones, relativa a la aplicación de las normas de control de acceso, punto c))	USUARIO 1.5: Privilegio mínimo	El propietario del activo deberá contar con políticas y procedimientos para verificar que a los usuarios del IACS solo se les concedan los derechos de acceso que necesiten para llevar a cabo las tareas que se les hayan asignado.
5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC	Implantar procesos que garanticen que los componentes de los proveedores sean originales y no hayan sufrido modificaciones respecto a sus especificaciones… (Orientación, punto j))	COMPATIBILIDAD 3.1 Autenticidad e integridad de los parches de seguridad	El propietario del activo deberá contar con políticas y procedimientos relacionados con la verificación de la autenticidad e integridad de todos los parches antes de su instalación.
5.25 Evaluación y toma de decisiones sobre incidentes de seguridad de la información	La organización debe evaluar los sucesos relacionados con la seguridad de la información y decidir si deben clasificarse como incidentes de seguridad de la información. (Control)	EVENTO 1.7 Análisis de eventos	El propietario del activo deberá contar con políticas y procedimientos relativos al análisis de los sucesos relacionados con la seguridad del IACS, con el fin de identificar y caracterizar oportunamente los ataques, las vulneraciones de seguridad y los incidentes de seguridad.
8.25 Ciclo de vida del desarrollo seguro	Deben establecerse y aplicarse normas para el desarrollo seguro de software y sistemas… El desarrollo seguro es un requisito imprescindible para crear un servicio, una arquitectura, un software y un sistema seguros. (Control y orientación)	ORG 2.3 Desarrollo y soporte seguros	El propietario del activo deberá contar con políticas y procedimientos que regulen el uso de un proceso de ciclo de vida de desarrollo seguro para el desarrollo y el mantenimiento de los sistemas y componentes utilizados en el IACS.

ISO/IEC 27001 ID y nombre del control	ISO/IEC 27002 Extracto de control u orientación	ISA/IEC 62443-2-1 ID y nombre del requisito	ISA/IEC 62443-2-1 Texto de requisitos - extracto
8.8 Gestión de las vulnerabilidades técnicas	Se debe recabar información sobre las vulnerabilidades técnicas de los sistemas de información en uso, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas. (Control)	EVENTO 1.9 Gestión de vulnerabilidades	El propietario del activo deberá contar con políticas y procedimientos relacionados con la identificación, el tratamiento y la resolución, de forma oportuna, de las vulnerabilidades existentes y las recién identificadas en los sistemas de control industrial (IACS).
8.8 Gestión de las vulnerabilidades técnicas	…un inventario preciso de los activos… el inventario debe incluir el proveedor del software, el nombre del software, los números de versión y el estado actual de su implantación... (Primer párrafo de las orientaciones)	COMPATIBILIDAD 3.3 Estado de los parches de seguridad	El propietario del activo deberá contar con políticas y procedimientos relativos a la documentación y el mantenimiento del estado de los parches de seguridad de todos los componentes.
8.8 Gestión de las vulnerabilidades técnicas	Probar y evaluar las actualizaciones antes de instalarlas para garantizar que sean eficaces y no provoquen efectos secundarios inaceptables. (Orientaciones en el apartado «Adopción de medidas adecuadas para hacer frente a las vulnerabilidades técnicas», punto d))	COMPATIBILIDAD 3.2: Validación e instalación de parches de seguridad	El propietario del activo deberá contar con políticas y procedimientos relativos a las pruebas de compatibilidad, la aprobación y la instalación de parches de seguridad aplicables a los componentes, que deberán llevarse a cabo de forma oportuna tras su publicación.
5.12 Clasificación de la información	La información debe clasificarse de acuerdo con las necesidades de seguridad de la información de la organización, basándose en la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas. (Control)	DATOS 1.1 Datos clasificación	El propietario de los activos deberá contar con políticas y procedimientos relacionados con la identificación y clasificación de todos los datos del IACS que requieran protección, de acuerdo con sus requisitos de protección.

ISO/IEC 27001 ID y nombre del control	ISO/IEC 27002 Extracto de control u orientación	ISA/IEC 62443-2-1 ID y nombre del requisito	ISA/IEC 62443-2-1 Texto de requisitos - extracto
5.16 Gestión de identidades	Se debe gestionar el ciclo de vida completo de las identidades. (Control) Las identidades se desactivan o eliminan oportunamente si ya no son necesarias… (Punto d) de las directrices)	USUARIO 1.2 Usuario eliminación de la identidad	El propietario del activo deberá contar con políticas y procedimientos para eliminar o desactivar los identificadores, autenticadores, roles y derechos de acceso específicos del IACS correspondientes a usuarios humanos, procesos de software y dispositivos que no necesiten acceso o que ya no lo necesiten.
5.18 Derechos de acceso	Los derechos de acceso a la información y a otros activos relacionados deben concederse, revisarse, modificarse y retirarse de conformidad con la política específica de la organización en la materia y con las normas relativas al control de acceso. (Control) Modificar los derechos de acceso de los usuarios que han cambiado de función o de puesto de trabajo… Eliminar o ajustar los derechos de acceso físico y lógico, lo cual puede realizarse mediante la retirada, la revocación o la sustitución de llaves, información de autenticación, tarjetas de identificación o suscripciones (Puntos i) y j) de la orientación))	USUARIO 1.2 Usuario eliminación de la identidad	El propietario del activo deberá contar con políticas y procedimientos para eliminar o desactivar los identificadores, autenticadores, roles y derechos de acceso específicos del IACS correspondientes a usuarios humanos, procesos de software y dispositivos que no necesiten acceso o que ya no lo necesiten.

ISO/IEC 27001 ID y nombre del control	ISO/IEC 27002 Extracto de control u orientación	ISA/IEC 62443-2-1 ID y nombre del requisito	ISA/IEC 62443-2-1 Texto de requisitos - extracto
7.14 Eliminación segura o reutilización de los equipos	Se debe comprobar que, en los equipos que contengan soportes de almacenamiento, se hayan eliminado o sobrescrito de forma segura todos los datos confidenciales y el software con licencia antes de su eliminación o reutilización. (Control)	DATOS 1.4 Datos política de conservación	El propietario del activo deberá contar con políticas y procedimientos relativos a la conservación de datos durante todo el ciclo de vida del IACS, incluida la eliminación de datos.
8.15 Registro	Deben generarse, almacenarse, protegerse y analizarse los registros que recogen actividades, excepciones, fallos y otros sucesos relevantes. (Control)	EVENTO 1.4 Registro de datos	El propietario del activo deberá contar con políticas y procedimientos relativos al registro de los incidentes relacionados con la seguridad del IACS en uno o varios registros de incidentes o de auditoría protegidos, así como a su conservación durante un período de tiempo adecuado.
5.24 Planificación y preparación para la gestión de incidentes de seguridad de la información	La organización debe planificar y prepararse para gestionar los incidentes de seguridad de la información mediante la definición, el establecimiento y la comunicación de los procesos, funciones y responsabilidades relacionados con la gestión de dichos incidentes. (Control)	EVENTO 1.8 Gestión y respuesta ante incidentes	El propietario del activo deberá disponer de políticas y procedimientos para implantar y mantener actualizado un proceso destinado a evaluar y responder a los incidentes relacionados con la seguridad de los sistemas de control industrial automatizados (IACS).

ISO/IEC 27001 ID y nombre del control	ISO/IEC 27002 Extracto de control u orientación	ISA/IEC 62443-2-1 ID y nombre del requisito	ISA/IEC 62443-2-1 Texto de requisitos - extracto
8.5 Autenticación segura	Deben implementarse tecnologías y procedimientos de autenticación seguros basados en las restricciones de acceso a la información y en la política específica sobre control de acceso. (Control)	USUARIO 1.8 Autenticación de usuarios humanos	El propietario del activo deberá contar con políticas y procedimientos relacionados con la identificación y autenticación de todos los usuarios humanos en todas las interfaces del IACS que puedan ser utilizadas por dichos usuarios para acceder al IACS. Esto incluye, entre otras cosas: a) interfaces interactivas de inicio de sesión para usuarios humanos en dispositivos, b) interfaces de aplicación, como servicios web, transferencias de archivos y servidores OPC, y c) interfaces de escritorio remoto que permiten a los usuarios acceder a dispositivos IACS a través de la red. NOTA: Algunos sistemas operativos gestionan la transmisión de la identidad del usuario autenticado de forma transparente para la aplicación y ponen dicha identidad a disposición de esta.
8.5 Autenticación segura	Deben implementarse tecnologías y procedimientos de autenticación seguros basados en las restricciones de acceso a la información y en la política específica sobre control de acceso. (Control)	USUARIO 1.6: Autenticación del servicio de software	El propietario del activo deberá contar con políticas y procedimientos relacionados con la identificación y autenticación de los servicios de software antes de su ejecución.

6 Conclusión

En varios ámbitos clave, [62443] aborda cuestiones de ciberseguridad que no suelen darse en un entorno informático. En estos ámbitos, una organización puede esperar que los controles y enfoques aplicables a su entorno TO sean distintos de los que resultan eficaces para su entorno de TI. En caso de que se pierda la disponibilidad o la integridad de la función de control físico que depende del sistema TO, podrían producirse graves consecuencias para la salud, la seguridad y el medio ambiente. Estos riesgos dan lugar a los requisitos de [62443] para evitar la indisponibilidad del sistema provocada por «fuego amigo», permitir la recuperación a un estado conocido en caso de pérdida de control, impedir interferencias externas en las funciones de seguridad o control, y realizar un seguimiento riguroso de la configuración de la solución de automatización y de todas las conexiones.

Un segundo subconjunto de requisitos de [62443], como los ejemplos de la sección 4, puede considerarse como casos concretos de recomendaciones más generales que figuran en las directrices de [27002]. Por lo tanto, [62443] exige, en la práctica, el cumplimiento de las recomendaciones de [27002] en escenarios específicos de TO.

Además, existe un amplio ámbito de interés común en materia de ciberseguridad entre las TI y TO, que se refleja en la similitud de la formulación de muchas recomendaciones y controles de la norma [27001/2] con los requisitos de la norma [62443]. Por lo tanto, [62443] ha «seleccionado» algunos de los controles de [27001/2] por considerarlos de especial interés para la TO. Por lo tanto, una organización que aplique ambas normas en un entorno de TO daría prioridad a la inclusión de estos controles a la hora de elaborar su Declaración de Aplicabilidad, necesaria para cumplir con la norma [27001/2]. Al mismo tiempo, la organización cumpliría así con los requisitos establecidos en [62443]. Sin embargo, es posible que las medidas adoptadas por una organización para cumplir con la misma recomendación o requisito [27001/2] en sus entornos de TO y de TI no sean las mismas, debido a las diferencias en cuanto a los riesgos y las características operativas de dichos entornos.

7 Definiciones y abreviaturas

7.1 Definiciones

propietario de activos

cargo organizativo que, en última instancia, es responsable de uno o varios IACS

Nota 1 de la entrada: Se utiliza en lugar del término genérico «usuario final» para establecer una diferenciación.

Nota 2 de la entrada: En el contexto del presente documento, el término «propietario de los activos» incluye también al operador del IACS. [FUENTE: ISA/IEC 62443-2-1]

Solución de Automatización

el sistema de control y cualquier componente de hardware y software complementario que se haya instalado y configurado para funcionar en un IACS

Nota 1 de la entrada: En este documento, «Solución de Automatización» se utiliza como nombre propio.

Nota 2 de la entrada: La diferencia entre el sistema de control y la solución de automatización radica en que el sistema de control se integra en el diseño de la solución de automatización (por ejemplo, un número concreto de

estaciones de trabajo, controladores y dispositivos en una configuración específica), que después se pone en práctica. La configuración resultante se denomina «Solución de Automatización».

Nota 3 de la entrada: La solución de automatización puede estar compuesta por componentes de varios proveedores, incluido el proveedor del sistema de control.
[FUENTE ISA/IEC 62443-2-1]

control

medida que modifica el riesgo

NOTA 1: Los controles incluyen cualquier proceso, política, dispositivo, práctica u otra medida que modifique el riesgo.

NOTA 2: Es posible que los controles no siempre ejerzan el efecto modificador previsto o supuesto.
[FUENTE: ISO/IEC 27000]

sistema de control

componentes de hardware y software de un IACS

NOTA 1: Los sistemas de control incluyen aquellos que realizan funciones de supervisión.

NOTA 2: El término «control» se refiere aquí al control de un proceso físico. Esto difiere del término «control» utilizado en la norma ISO/IEC 27001/2, tal y como se define en la entrada anterior.
[FUENTE: ISA/IEC 62443-4-2, se ha añadido la NOTA 2]

función esencial

función o capacidad necesaria para garantizar la salud, la seguridad, la protección del medio ambiente y la disponibilidad de los equipos sometidos a control

NOTA Las funciones esenciales incluyen, entre otras, la función instrumentada de seguridad (SIF), la función de control y la capacidad del operador para visualizar y manejar el equipo que se está controlando. La pérdida de funciones esenciales se denomina habitualmente «pérdida de protección», «pérdida de control» y «pérdida de visión», respectivamente. En algunos sectores, funciones adicionales, como el historial, pueden considerarse esenciales. [FUENTE: ISA/IEC 62443-4-2]

sistema de automatización y control industrial

conjunto de personal, equipos, programas informáticos y políticas que intervienen en el funcionamiento del proceso industrial y que pueden afectar o influir en su funcionamiento seguro y fiable
[FUENTE: ISA/IEC 62443-3-3]

tecnología operativa (TO)

hardware y software que detecta o provoca un cambio físico, mediante la supervisión y/o el control directo de equipos, activos, procesos y sucesos industriales
[FUENTE: Gartner IT Glossary]

recomendación

Expresión que, en el contexto de un documento, sugiere una posible opción o línea de actuación que se considera especialmente adecuada, sin mencionar ni excluir necesariamente otras.
[FUENTE ISO/IEC Directives Part 2 : 2021]

requisito

expresión, en el contenido de un documento, que establece criterios objetivamente verificables que deben cumplirse y de los que no se permite ninguna desviación si se pretende alegar la conformidad con el documento
[FUENTE ISO/IEC Directives Part 2 : 2021]

nivel de seguridad

grado de confianza en que el IACS no presenta vulnerabilidades y funciona según lo previsto
[FUENTE: ISA/IEC 62443-3-3]

zona de seguridad

agrupación de activos lógicos o físicos en función del riesgo u otros criterios, como la importancia crítica de los activos, la función operativa, la ubicación física o lógica, el acceso requerido (por ejemplo, los principios de privilegio mínimo) o la organización responsable
[FUENTE ISA/IEC 62443-3-2]

7.2 Abreviaturas

En este documento se utilizan las siguientes abreviaturas.

ANSI	American National Standards Institute (Instituto Nacional Estadounidense de Normalización)
DMZ	demilitarized zone (zona desmilitarizada)
ED	edición
FDIS	Final Draft International Standard (Borrador final de la norma internacional)
HR	Human Resources (Recursos Humanos)
HSE	Salud, seguridad y medio ambiente
IACS	industrial automation and control system(s) (sistemas de automatización y control industrial)
IEC	International Electrotechnical Commission (Comisión Electrotécnica Internacional)
ISA	International Society of Automation (Sociedad Internacional de Automatización)
ISAGCA	ISA Global Cybersecurity Alliance (Alianza Global de Ciberseguridad de la ISA)
ISO	International Organization for Standardization (Organización Internacional de Normalización)
IT (TI)	Information Technology (Tecnología de la información)
JTC	Joint Technical Committee (Comité Técnico Conjunto)
NIST	National Institute of Standards and Technology (US) (Instituto Nacional de Estándares y Tecnología (EE. UU.))
NIST SP	NIST Special Publication (Publicación especial del NIST)
OPC	Open Platform Communications (Comunicaciones de plataforma abierta)
OT (TO)	Operational Technology (Tecnología operativa)
SR	system requirement (requisitos del sistema)
SUC	system under consideration (Sistema bajo consideración)
TC	Technical Committee (Comité técnico)
ZCR	zone and conduit requirement (Requisitos de zonas y conductos (RZC))

8 Referencias

8.1 Normas ISA/IEC 62443

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 de los sistemas de automatización y control industrial. Punto 2-4: Requisitos del programa de seguridad para los proveedores de servicios de IACS

[62443-3-2] IEC 62443-3-2: 2020 - Seguridad de los sistemas de automatización y control industrial - Punto 3-2: Evaluación de riesgos de seguridad para el diseño de sistemas
ANSI/ISA 62443-3-2: 2020 Seguridad de los sistemas de automatización y control industrial, Punto 3-2: Evaluación de riesgos de seguridad para el diseño de sistemas

[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 para 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 de los 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 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)

8.2 Normas ISO/IEC 27001 e ISO/IEC 27002

[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

8.3 Otras referencias

[OTE] Aplicación de las normas ISO/IEC 27001 e ISO/IEC 27002 y de la serie de normas ISA/IEC 62443 para entornos de tecnología operativa, Alianza Global de Ciberseguridad de la ISA, www.isa.org/otstandards

[Gartner-ITG] Gartner: Glosario de TI, recuperado 2025-02-08 http://www.gartner.com/it-glossary

[NIST 800-82] NIST SP 800-82, revisión 3: Guía sobre la seguridad de la tecnología operativa (OT)

Protección de la tecnología operativa: Comprender la serie de normas ISA/IEC 62443 desde la perspectiva de las ISO/IEC 27001 e ISO/IEC 27002

South American Spanish Edition

www.isagca.org

ISA GLOBAL CYBERSECURITY ALLIANCE