FACULTAD DE CIENCIAS CONTABLES, AUDITORÍA
SISTEMAS DE CONTROL DE GESTIÓN Y FINANZAS
UNIVERSIDAD AUTÓNOMA GABRIEL RENÉ MORENO

INVESTIGACIÓN FORMATIVA (EXPOSICIÓN)

ICCAF

II-2025

EXPO

CIENCIA FACULTATIVA XV

NOMBRE DEL TEMA: ISO 27000 1-2

NÚMERO DE GRUPO: _____ **TURNO DE PRESENTACIÓN:** MAÑANA

DOCENTE GUÍA: LIC. MARIO GERARDO PINTO VIRHUEZ

INTEGRANTES:

NELVY URQUIZU RENGIPO	221015086
WENDY NICOLE VACA RODRIGUEZ	220085862

NÚMERO INTERNO DE GRUPO:

APOYAN: UAGRM

INDICE

INTRODUCCION

La familia de normas ISO 27000 se entiende como un conjunto de reglas o una “guía de buenas prácticas” que ayuda a las organizaciones a proteger su información valiosa. Puede compararse con un manual diseñado para resguardar secretos y garantizar que los datos estén seguros frente a pérdidas, robos o modificaciones no autorizadas. Dentro de esta familia, destacan especialmente dos normas: la ISO/IEC 27001 y la ISO/IEC 27002. La ISO 27001 establece qué debe hacer una empresa para proteger su información. Es similar a cuando en el trabajo se dictan reglas básicas para mantener el orden, como cuidar tus pertenencias, no compartir contraseñas, apagar el ordenador al finalizar la jornada, entre otras. De esta manera, la norma exige que las organizaciones creen un sistema de seguridad que asegure que sus datos no se pierdan, no sean robados ni alterados sin autorización. Por otro lado, la ISO 27002 actúa como una guía práctica que explica cómo aplicar en la realidad las reglas de la ISO 27001. En este sentido, ayuda a las organizaciones a traducir los requisitos formales de la 27001 en acciones concretas, fortaleciendo la protección de la información y fomentando una cultura de seguridad. Su objetivo principal es ofrecer un conjunto de buenas prácticas, controles y directrices que permitan llevar a cabo una gestión adecuada de la seguridad de la información. En conjunto, ambas normas se complementan: mientras la ISO 27001 define el marco y los requisitos que deben cumplirse, la ISO 27002 proporciona la metodología práctica para implementarlos con eficacia dentro de las organizaciones.

JUSTIFICACIÓN

El objetivo de la serie de normas ISO 27000 es proporcionar un marco integral y las mejores prácticas para que las organizaciones establezcan, implementen, mantengan y mejoren continuamente a un sistema de gestión de la seguridad de la información (SGSI), protegiendo así la información de acceso no autorizados alteraciones o eliminaciones, y garantizando la confiabilidad integridad y disponibilidad de los datos

OBJETIVOS

OBJETIVO GENERAL

El objetivo general de la serie ISO27000 es proporcionar un marco completo y un conjunto de pautas para la gestión de seguridad de la información (SGSI), permitiendo a las organizaciones de todos los tipos y tamaños proteger sus activos de información asegurando su confidencialidad, seguridad y disponibilidad.

OBJETIVOS ESPECIFICOS

- Proporcionar un marco de referencia
- Proteger activos de información
- Gestionar los riegos
- Mejorar continuamente la seguridad
- Garantizar el cumplimiento legal
- Ser aplicable en cualquier organización

DESARROLLO DEL TEMA

ISO 27000

Las normas ISO 27001 e ISO 27002 Dentro de la serie ISO 27000) Son estándares internacionales para la seguridad de la información. La ISO 27001 define los requisito para un sistema de gestión de Seguridad de la información (SGSI) mientras que la iso 27002 es un código de practica que proporciona los controles y guias implementar la seguridad. Ambas se actualizaron en 2022 para modernizar los controles de seguridad ante las amenazas actuales, como la inteligencia de amenazas y seguridad en la nube.

El triángulo de la seguridad informática es un modelo fundamental que representa los tres pilares esenciales sobre los que se construye la protección de la información: confidencialidad, integridad y disponibilidad (CIA, por sus siglas en inglés: Confidentiality, Integrity, Availability). Su relevancia radica en que ofrece una base clara y universal para diseñar políticas, controles y sistemas de seguridad dentro de cualquier organización.

1. Confidencialidad

Garantiza que la información solo sea accesible para personas autorizadas.

Evita el acceso no autorizado, robo de datos o filtraciones de información sensible.

Es crucial en sectores como el financiero, la salud o la gestión gubernamental.

2. Integridad

Asegura que los datos no sean alterados, manipulados o dañados de manera no autorizada.

Permite que la información sea confiable y precisa.

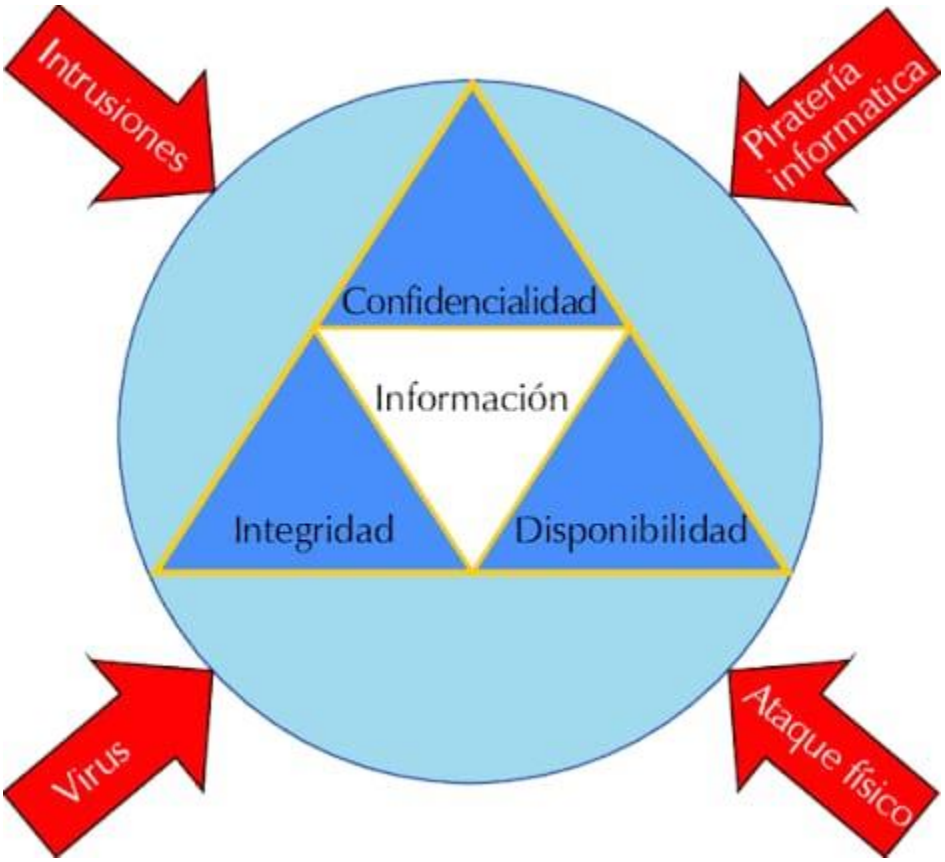
Es vital en procesos donde los errores o cambios en los datos pueden generar consecuencias graves, como en transacciones bancarias o registros médicos.

3. Disponibilidad

Garantiza que la información y los sistemas estén siempre accesibles cuando los usuarios autorizados los necesiten.

Evita interrupciones en los servicios debido a fallos técnicos, ataques cibernéticos o desastres.

Es esencial para la continuidad de negocio y la operatividad de servicios críticos.



ISO 27001 frente a ISO 27002

Las organizaciones que deseen explorar los sistemas de gestión de seguridad de la información pueden haber encontrado las normas ISO 27001 y 27002.

La norma ISO 27001 es la principal norma de la familia 27000. Las empresas pueden certificarse según la norma ISO 27001, pero no pueden hacerlo según la norma ISO 27002:2022, ya que se trata de una norma/código de prácticas de apoyo.

El Anexo A de la norma ISO 27001, por ejemplo, proporciona una lista de controles de seguridad, pero no indica cómo implementarlos, sino que hace referencia a la norma ISO 27002.

Por el contrario, la norma ISO 27002 proporciona orientación sobre la implementación de los controles utilizados en la norma ISO 27001. Lo bueno de la norma ISO 27002 es que los controles no son obligatorios; las empresas pueden decidir si quieren usarlos o no, dependiendo de si son aplicables en primer lugar.

QUE ES LA ISO 27000 Y PARA QUE SIRVE

Cumplimiento legal y regulatorio: la norma ISO 27000 ayuda alas organizaciones a cumplir con una variedad de requisitos legales y regulatorio relacionados con la seguridad de la información.

OBJETIVO

El principal objetivo de la norma ISO 27001 es establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) para proteger la confidencialidad, integridad y disponibilidad de la información de una organización, así como sus activos relacionados. Esto se logra identificando y gestionando riesgos de seguridad, cumpliendo con normativas, fomentando una cultura de seguridad y garantizando la mejora continua del sistema

CARACTERISTICAS

¿Qué es la seguridad de la información?

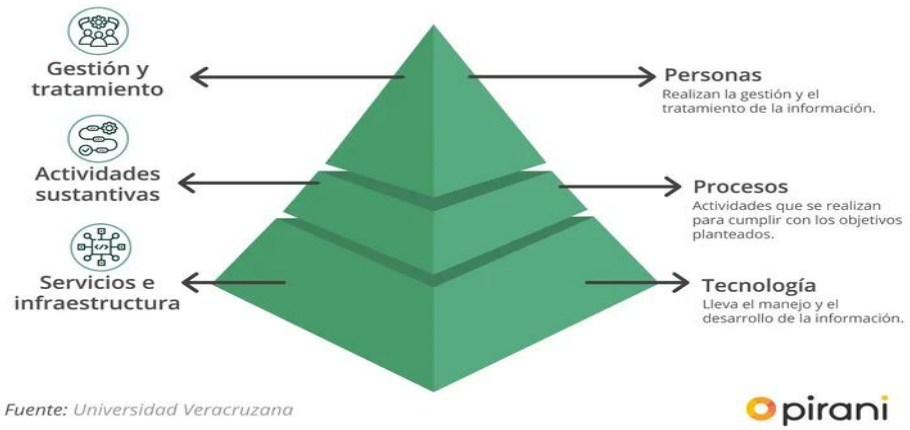
La seguridad de la información se define como un proceso integrado que permite proteger la identificación y gestión de la información y los riesgos a los que esta se puede ver enfrentada. Esta gestión se hace a través de estrategias y acciones de mitigación para asegurar y mantener de manera confidencial los datos de una empresa.

Según la Universidad Libre de Colombia, se define como “todas las medidas preventivas y de reacción del individuo, la organización y las tecnologías para proteger la información; buscando mantener en esta la confidencialidad, la autenticidad y la integridad.

Es importante tener claro que **los términos seguridad de la información y seguridad Informática son diferentes.** Este último trata solamente de la seguridad en el medio informático, mientras que el primero es para cualquier tipo de información, sea esta digital o impresa.

La seguridad de la información abarca muchas cosas, pero todas estas giran en torno a la información, por ejemplo: la disponibilidad, la comunicación, la identificación de problemas, el análisis de riesgos, la integridad, la confidencialidad y la recuperación de los riesgos".

Para implementar la seguridad de la información en tu organización, es importante que tengas en cuenta **tres elementos claves: las personas, los procesos y la tecnología.**



Fuente: Universidad Veracruzana

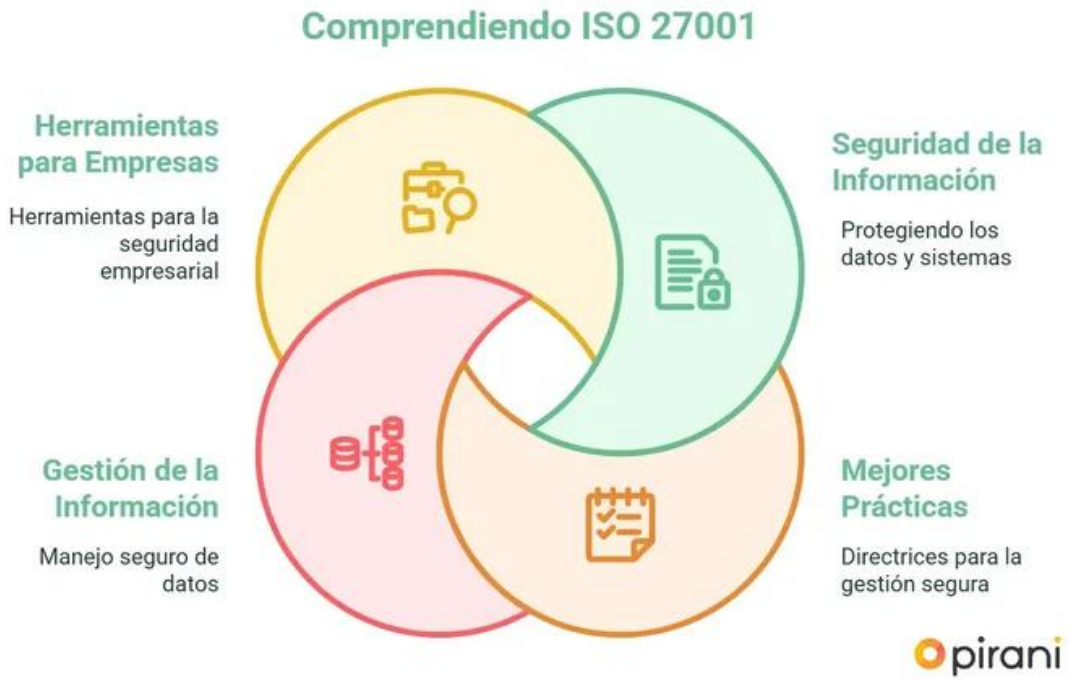
- **Personas:** realizan la gestión y el tratamiento de la información. Pueden ser empleados, directivos, autoridades competentes, clientes, proveedores, contratistas y prestadores de servicio.

- **Procesos**: son las actividades que se realizan para cumplir con los objetivos planteados, la mayoría de estas incluyen información o dependen de esta, por eso, son vulnerables.

- **Tecnología:** está relacionada con los servicios e infraestructura de la empresa, es la que lleva el manejo y el desarrollo de la información, además, brinda la oportunidad de almacenar, recuperar, difundir y darle mantenimiento a los datos de valor que se encuentran ahí

¿De qué trata la norma ISO 27001?

Es una **norma internacional creada por la Organización Internacional de Normalización (ISO)** para garantizar buenas prácticas de seguridad de la información. Además, la norma ISO 27001 brinda herramientas que permiten a las empresas gestionar su información de manera segura.



¿Qué permite la ISO 27001?

En términos generales, **la norma ISO 27001 permite que los datos suministrados sean confidenciales, íntegros, disponibles y legales para protegerlos de los riesgos que se puedan presentar**. Contar con este sistema dentro de la organización genera confianza entre los clientes, proveedores y empleados, además, es un referente mundial.

Así mismo, la implementación de esta norma permite evaluar y controlar los riesgos que se hayan identificado, creando un plan que ayude a prevenirlos y, en caso de presentarse, a mitigar su impacto.

Importancia de la ISO 27001

La información de las compañías, su activo más importante, puede sufrir **algún tipo de fraude, hackeo, sabotaje, vandalismo, espionaje o un mal uso por parte del recurso humano.**

Estos actos delictivos, generalmente, son realizados por ingenieros, *hackers*, empleados u organizaciones dedicadas al robo de datos, que lo único que buscan es interferir en la reputación de la empresa. Por esta razón, es tan importante contar con herramientas que te permitan evitar que este tipo de hechos sucedan.

Tener en tu empresa un Sistema de Gestión de Seguridad de la Información te permite cumplir con los requerimientos legales, pues muchos países lo exigen. **En la norma ISO 27001 encuentras la metodología que debes seguir para implementarlo y poder cumplir con lo exigido.**

Obtener la certificación en ISO 27001 genera un valor agregado para tu compañía con respecto a tus competidores, además, mayor confianza entre tus clientes y futuros clientes. Esta certificación también ayuda a disminuir la probabilidad de ocurrencia de incidentes que generen grandes pérdidas para tu empresa, así evitas consecuencias perjudiciales y ahorras dinero.

Estructura de la ISO 27001

Aplicabilidad de la ISO 27001

La ISO 27001 es aplicable a cualquier organización que desee proteger su información, ya sea en el sector privado, público o sin fines de lucro. Aunque puede implementarse en empresas de cualquier tamaño.

- Empresas tecnológicas
- Sector financiero
- Industria de la salud
- E-commerce y retail

Proceso de implementación de la ISO 27001

Implementar la ISO 27001 implica un proceso estructurado que abarca desde la planificación inicial hasta la auditoría final para la certificación. Los siete pasos clave son:

1. **Análisis inicial**: Evaluar el estado actual de la seguridad de la información y definir los objetivos del SGSI.

2. **Identificación de riesgos**: Realizar un análisis exhaustivo para identificar las amenazas y vulnerabilidades existentes.

3. **Definición del alcance**: Determinar qué áreas, procesos y activos estarán cubiertos por el SGSI.

4. **Desarrollo de controles y políticas**: Implementar los controles requeridos por la norma y documentar políticas claras.

5. **Capacitación**: Asegurar que los empleados estén alineados con las políticas y prácticas del SGSI.

6. **Auditoría interna**: Evaluar el cumplimiento del SGSI antes de la auditoría externa.

7. **Certificación**: Pasar la auditoría externa para obtener la certificación.

Este proceso no solo garantiza el cumplimiento normativo, sino que también fomenta una cultura de seguridad dentro de la organización.

¿Qué son los controles de la norma y por qué son importantes?

Los controles de la **ISO 27001** son las medidas específicas diseñadas para gestionar y mitigar los riesgos de seguridad de la información en una organización. Estas medidas no son "**opcionales**", sino que forman la base para implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) efectivo.

Cada control aborda un aspecto clave de la seguridad y está diseñado para prevenir, detectar y responder a amenazas de forma estructurada.

La norma organiza los controles en **4 temas principales** que se agrupan en **14 dominios**

Controles organizativos:

- Incluyen políticas, roles y responsabilidades de seguridad.
- Ejemplo: Crear una **política de seguridad de la información** que establezca reglas claras para todos los empleados.

Controles relacionados con las personas:

Garantizan que los empleados y terceros comprendan y cumplan con las políticas de seguridad.

Ejemplo: Realizar **capacitación en ciberseguridad** y establecer procesos de revisión de antecedentes laborales.

Controles físicos:

- Diseñados para proteger los activos físicos y el entorno de trabajo.

- Ejemplo: Implementar sistemas de acceso restringido y cámaras de vigilancia en áreas críticas.

Controles tecnológicos:

- Relacionados con el uso de tecnologías para proteger la información.
- Ejemplo: Uso de **cifrado de datos**, firewalls y monitoreo de redes.

Ejemplos clave de controles de la ISO 27001

Control de acceso

- Asegurar que solo el personal autorizado pueda acceder a la información confidencial. Esto incluye contraseñas robustas, autenticación multifactor (MFA) y gestión de identidades.

Gestión de activos

- Inventariar y clasificar los activos de información para identificar su criticidad y nivel de protección necesario.

Seguridad en las operaciones

- Establecer procedimientos para garantizar la disponibilidad de los sistemas críticos y minimizar interrupciones, como realizar **copias de seguridad** y monitorear actividades sospechosas.

Cambios recientes en los controles de la ISO 27001:2022

Con los principales cambios de la norma, los controles fueron reorganizados en 4 temas clave (en lugar de los anteriores 14 dominios) y se incorporaron nuevos controles que reflejan las **amenazas actuales en ciberseguridad**. Algunos de los controles nuevos son:

- **Monitoreo continuo**: Implementar herramientas avanzadas para monitorear las redes y detectar actividades anómalas.

- **Gestión de amenazas a la cadena de suministro**: Mitigar riesgos relacionados con proveedores o socios que manejan datos críticos.

- **Protección frente a ataques físicos y remotos**: Adaptar controles a entornos híbridos y remotos.

Flexibilidad en los controles

Un punto importante es que no todos los controles son obligatorios. Cada organización debe realizar un análisis de riesgos para determinar qué controles son necesarios según sus necesidades específicas. Esto garantiza que el SGSI esté alineado con las características del negocio, reduciendo costos innecesarios y optimizando recursos.

Implementar y monitorear estos controles de forma efectiva puede ser un desafío. Por eso, apoyarte en un software especializado, como el de **Pirani**, puede marcar una gran diferencia en la gestión de los riesgos y el cumplimiento de la norma

Ventajas de implantar la ISO 27001 con el software de Pirani

- Permite que los procesos de seguridad estén equilibrados y a la vez coordinados entre sí.

- Aunque es imposible reducir a cero el riesgo, permite crear metodologías que contribuyan a la mitigación de los mismos y a aumentar la seguridad en la información que se tiene.

- En caso de que se llegue a presentar un riesgo permite que este no cause pérdidas tan profundas y que se cuente con un plan de acción para actuar de manera eficaz.

- Permite cumplir con los requerimientos legales exigidos por los entes de control.

- Genera valor agregado dentro de la compañía, pues aún no son muchas las empresas que cuenten con la certificación ISO 27001.

- Gracias a la eficiencia que se emplea permite reducir costos.

- Genera confianza con todos los miembros de la entidad, ya sean clientes, proveedores o empleados.

- Da la posibilidad de que se puedan activar alertas en caso de que se llegue a presentar alguna actividad sospechosa.

- Permite hacerles seguimiento a los controles de seguridad.

- Es una herramienta que da la posibilidad de planificar y hacerle seguimiento a los procesos.

- Contribuye a la imagen corporativa (reputación).

- Permite contar con una metodología clara y eficaz.

- Reduce el riesgo de pérdida o robo de la información.

Novedades de la norma ISO 27001

La **ISO 27001** fue actualizada en **2022** con una serie de modificaciones importantes para mantener su relevancia frente a las amenazas y desafíos actuales en la seguridad de la información. Estas actualizaciones buscan mejorar la aplicabilidad y efectividad del estándar, con especial enfoque en la ciberseguridad y la gestión de riesgos modernos.

A continuación, exploramos las principales novedades introducidas en esta revisión:

- Reestructuración de los controles
- Introducción de nuevos controles
- Enfoque en la ciberseguridad
- Mayor flexibilidad para entornos híbridos.

INTRODUCCION A LA NORMA ISO 27002

La norma ISO 27002 es un estándar internacional que proporciona directrices para la implementación de controles de seguridad de la información. A diferencia de la norma ISO 27001, que se centra en los requisitos para establecer un Sistema de Gestión de la Seguridad de

la Información (SGSI), la norma ISO 27002 actúa como un complemento a la norma ISO 27001. Un estándar que ofrece un conjunto detallado de directrices y mejores prácticas para implementar los controles de seguridad identificados en el Anexo A de la ISO 27001. Es una norma clave como recurso detallado para las organizaciones que buscan una guía sobre las mejores prácticas en seguridad de la información.

Aplicabilidad de la norma ISO 27002

La norma ISO 27002 es aplicable a todas las organizaciones, independientemente de su tamaño, tipo o industria. Su propósito es ayudar a las organizaciones a seleccionar e implementar controles de seguridad adecuados, de acuerdo con los riesgos que enfrentan.

Esta versión, actualizada en febrero de 2022, ha sido adaptada para responder a los desafíos modernos en la protección de la información y ha reducido el número de controles.

La estructura de la norma divide sus controles en cuatro categorías principales:

Controles Organizacionales:

Estos controles tienen como objetivo principal proporcionar un esquema operativo para la seguridad de la información. Se enfocan en:

- Definición de estructuras de gobernabilidad y roles.
- Establecimiento de políticas claras.
- Fomento de una cultura de seguridad de la información.
- Asegurar el cumplimiento regulatorio.
- Gestión proactiva de riesgos.
- Adaptabilidad ante el cambio.

1. Adopción de prácticas reconocidas internacionalmente para la seguridad de la información:

2. Reducción de los riesgos asociados con amenazas a la seguridad de la información:

3. Demostración a las partes interesadas y terceros de un compromiso claro con la seguridad de la información:

4. Mejora de la cultura organizativa en relación con la seguridad de la

Concienciación y capacitación: Al adoptar la norma en la organización, se fomenta la formación y concienciación constante sobre seguridad entre los empleados, lo que a su vez refuerza la cultura de seguridad.

Responsabilidad y propiedad: La norma promueve la asignación clara de responsabilidades en materia de seguridad, garantizando que todos los integrantes de la organización comprendan su papel en la protección de la información.

Por qué es importante la norma ISO 27002?

Si su organización recopila, utiliza o procesa datos, siempre habrá riesgos y amenazas a la seguridad de la información que debe tener en cuenta.

Para protegerse contra estos riesgos, debe contar con un Sistema de Gestión de Seguridad de la Información (SGSI) para garantizar la confidencialidad, disponibilidad e integridad de toda la información y los activos de información.

El principal desafío que enfrentan las empresas que se inician en el ámbito de la gestión de la seguridad de la información es su amplio alcance. La implementación y el mantenimiento de un SGSI abarcan un espectro tan amplio que la mayoría de los gerentes no saben por dónde empezar.

Si esto le suena familiar o si simplemente busca estar al tanto de la seguridad de su información, entonces un excelente punto de partida es implementar los controles sugeridos en la norma ISO/IEC 27002**.**

¿Cuales son los beneficios?

Al implementar los controles de seguridad de la información que se encuentran en la norma ISO 27002, las organizaciones pueden tener la seguridad de que sus activos de información están protegidos por las mejores prácticas aprobadas y reconocidas internacionalmente.

Las organizaciones de todos los tamaños y niveles de madurez de seguridad pueden obtener los siguientes beneficios al adherirse al código de prácticas ISO 27002:

Proporciona un marco de trabajo para la resolución de problemas de seguridad de la información, ciberseguridad, seguridad física y privacidad de la información.

Los clientes y socios comerciales tendrán más confianza y una visión positiva de una organización que implementa los estándares recomendados y los controles de seguridad de la información.

Dado que las políticas y los procedimientos proporcionados se alinean con los requisitos de seguridad reconocidos internacionalmente, la cooperación con socios internacionales es más sencilla.

El cumplimiento de la norma ayuda a desarrollar las mejores prácticas de una organización, lo que aumentará la productividad general.

Proporciona una implementación, gestión, mantenimiento y evaluación definidos de sistemas de gestión de seguridad de la información.

Una organización que cumpla con la norma ISO tendrá una ventaja en las negociaciones contractuales y en la participación en oportunidades comerciales globales.

Al cumplir con los controles de seguridad de la información ISO 27002, uno puede beneficiarse de primas de seguro más bajas por parte de los proveedores.

La guía de implementación para el cumplimiento de la norma ISO 27001 se encuentra ampliamente referenciada dentro de la familia de normas ISO 27000, incluida la ISO 27701. Los controles de seguridad de la información ISO 27002 se pueden comparar con normas similares, por ejemplo, NIST, SOC2, CIS, TISAX® y muchas más**.**

Alcance de la norma ISO 27002:2013

La norma ISO 27002:2013 es/era un código de prácticas para un sistema de gestión de seguridad de la información (SGSI) y profundiza en un nivel de detalle mucho mayor que los Controles del Anexo A de la norma ISO 27001, que contiene técnicas de seguridad, objetivos de control, requisitos de seguridad, control de acceso, controles de tratamiento de riesgos de seguridad de la información, controles de información personal y propietaria, así como controles de seguridad de la información genéricos.

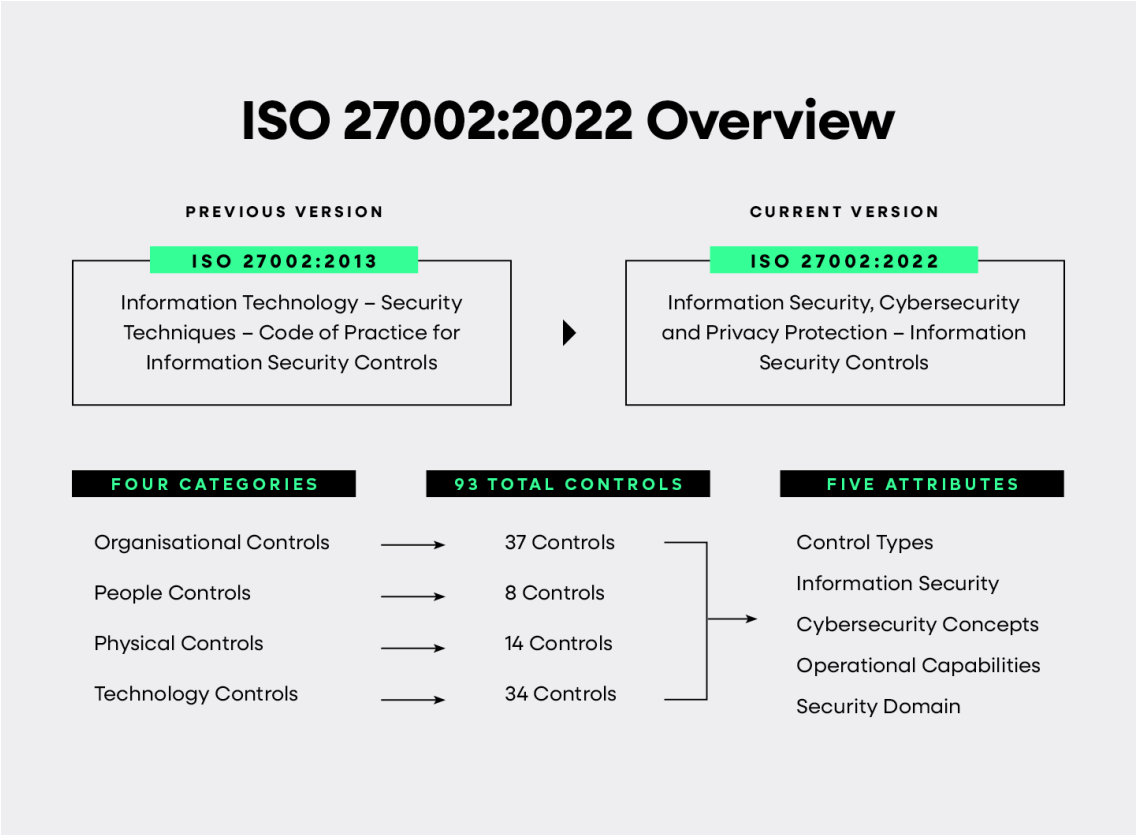
El objetivo principal de la norma ISO 27002:2013 fue proporcionar técnicas integrales de seguridad de la información y controles de gestión de activos para cualquier organización que necesitara un nuevo programa de gestión de seguridad de la información o quisiera mejorar sus políticas y prácticas de seguridad de la información existentes.

¿Qué ha cambiado en la norma ISO 27002:2022?

El primer cambio significativo en el estándar es dejar de lado el concepto de “Código de prácticas” y posicionarlo como un conjunto de controles de seguridad de la información que pueden funcionar de forma independiente.

La norma revisada proporciona una estructura más sencilla que puede aplicarse en toda la organización. La versión revisada de la ISO 27002 ahora también puede utilizarse para gestionar un perfil de riesgo más amplio. Esto incluye la seguridad de la información y los aspectos más

técnicos de la seguridad física, la gestión de activos, la ciberseguridad y los elementos de seguridad de los recursos humanos que conlleva la protección de la privacidad.



ISO 27002:2022 Alcance ampliado

El primer cambio inmediato es el nombre del estándar.

Anteriormente, la norma ISO 27002:2013 se titulaba “Tecnología de la información – Técnicas de seguridad – Código de prácticas para controles de seguridad de la información”.

En la revisión de 2022, la norma ahora se denomina “Seguridad de la información, ciberseguridad y protección de la privacidad – Controles de seguridad de la información”.

¿Por qué ha cambiado?

Teniendo en cuenta el panorama de cumplimiento moderno, las regulaciones, por ejemplo, GDPR, POPIA y APPS y las cambiantes dificultades de continuidad comercial y riesgo

cibernético que enfrentan las organizaciones, la necesidad de que la norma ISO 27002 amplíe el alcance de sus controles de seguridad de la información era algo que ya se había anticipado.

El objetivo de la última revisión (2022) fue mejorar la intención de la norma al proporcionar un conjunto de referencia para los objetivos de control de seguridad de la información y ampliar su alcance para su uso en la seguridad de la información, la privacidad y la gestión de riesgos de ciberseguridad según el contexto.

En qué se diferencia la norma ISO 27002:2022 de la ISO 27002:2013

En términos generales, el número de controles de seguridad en la nueva versión de la norma ISO 27002:2022 ha disminuido de 114 controles en 14 cláusulas en la edición de 2013 a 93 controles en la edición de 2022. Estos controles de seguridad ahora se clasifican en cuatro "temas" de control.

Controles explicados

Un "control" se define como una medida que modifica o mantiene el riesgo. Una política de seguridad de la información, por ejemplo, solo puede mantener el riesgo, mientras que su cumplimiento puede modificarlo. Además, algunos controles describen la misma medida genérica en diferentes contextos de riesgo.

Cambios específicos en detalle

Los conjuntos de control ahora están organizados en cuatro (4) categorías o temas de seguridad en lugar de catorce (14) dominios de control. (anteriormente A5. a A.18)

Temas y atributos de la norma ISO 27002

Los atributos permiten categorizar los controles. Permiten alinear rápidamente la selección de controles con el lenguaje y los estándares comunes de la industria.

Estos atributos identifican puntos clave:

- Tipo de control
- Propiedades de InfoSec

- Conceptos de ciberseguridad
- Capacidades operativas
- Dominios de seguridad

El uso de atributos respalda el trabajo que muchas empresas ya realizan en su evaluación de riesgos y declaración de aplicabilidad (SOA). Por ejemplo, se pueden distinguir conceptos de ciberseguridad similares a los controles del NIST y el CIS, y se pueden reconocer las capacidades operativas relacionadas con otras normas.

Cada control ahora tiene una tabla con un conjunto de atributos sugeridos y el Anexo A de ISO 27002:2022 proporciona un conjunto de asociaciones recomendadas.

Propiedades de seguridad de la información:

La seguridad de la información implica la protección de diversos aspectos de la información, que pueden representarse mediante el modelo CIA. Estos aspectos incluyen la confidencialidad, la integridad y la disponibilidad de la información. Comprender esto permite la formulación e implementación de controles de seguridad de la información eficaces. Estos se definen ahora como atributos por control.

El modelo de la CIA explicado

Confidencialidad

La confidencialidad de la información implica la adopción de medidas para protegerla del acceso no autorizado. Una forma de lograrlo es establecer diferentes niveles de acceso a la información según quién la necesite y su grado de confidencialidad. Algunas medidas para gestionar la confidencialidad incluyen el cifrado de archivos y volúmenes, las listas de control de acceso y los permisos de archivo.

Las cuatro categorías incluyen:

- Organizativo
- Gente
- Físico

- Tecnológico

93 controles en la nueva versión de 27002

11 controles son nuevos

Se fusionaron un total de 24 controles de dos, tres o más controles de seguridad de la versión 2013; y se revisaron y modificaron los 58 controles de la norma ISO 27002:2013 para alinearlos con el entorno actual de seguridad cibernética y seguridad de la información.

Anexo A, que incluye orientación para la aplicación de atributos.

Anexo B, que corresponde a la norma ISO/IEC 27001 2013. Se trata básicamente de dos tablas que cruzan números/identificadores de control para facilitar la consulta y detallan qué es nuevo y qué se ha fusionado.

MARCO TEORICO

1. Introducción a la Gestión de la Seguridad de la Información

La seguridad de la información se ha convertido en un pilar esencial dentro de las organizaciones modernas debido al incremento de amenazas cibernéticas, la dependencia tecnológica y la necesidad de cumplir con normativas legales. En este contexto, la familia de normas ISO/IEC 27000 proporciona lineamientos internacionales para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

2. Norma ISO/IEC 27001

2.1 Definición

La ISO/IEC 27001 es una norma internacional publicada por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC). Establece los requisitos para implementar, mantener y mejorar un SGSI en cualquier tipo de organización.

2.2 Objetivo principal

Garantizar la confidencialidad, integridad y disponibilidad (CIA) de la información.

Asegurar la gestión de riesgos de seguridad de la información.

Proporcionar confianza a las partes interesadas (clientes, socios, reguladores).

2.3 Estructura

La ISO/IEC 27001 sigue la estructura de alto nivel (HLS) de los estándares de gestión ISO y se centra en:

1. Contexto de la organización.

2. Liderazgo.

3. Planificación.

4. Apoyo.

5. Operación.

6. Evaluación del desempeño.

7. Mejora continua.

2.4 Importancia

Certificación reconocida a nivel mundial.

Permite cumplir con requisitos legales y regulatorios

Mejora la resiliencia frente a incidentes de seguridad.

3. Norma ISO/IEC 27002

3.1 Definición

La ISO/IEC 27002 es una norma complementaria a la ISO/IEC 27001. Contiene un código de buenas prácticas y proporciona directrices detalladas para implementar los controles de seguridad establecidos en el Anexo A de la ISO/IEC 27001.

3.2 Objetivo principal

Orientar a las organizaciones en la selección, implementación y gestión de controles de seguridad de la información.

Servir como marco de referencia para la creación de políticas de seguridad.

3.3 Áreas de control

La norma se organiza en dominios, como:

Políticas de seguridad.

Organización de la seguridad de la información.

Seguridad de recursos humanos.

Gestión de activos.

Control de accesos.

Criptografía.

Seguridad física y ambiental.

Operaciones de seguridad.

Seguridad en las comunicaciones.

Adquisición, desarrollo y mantenimiento de sistemas.

Relación con proveedores.

Gestión de incidentes.

Continuidad del negocio.

Cumplimiento normativo.

3.4 Diferencia respecto a la ISO/IEC 27001

La ISO/IEC 27001 establece qué requisitos debe cumplir un SGSI.

La ISO/IEC 27002 explica cómo aplicar los controles de seguridad.

4. Relación entre la ISO/IEC 27001 y la ISO/IEC 27002

La ISO/IEC 27001 es la norma certificable, mientras que la ISO/IEC 27002 es una guía de implementación.

Ambas se complementan para ofrecer un sistema integral de gestión de la seguridad.

Juntas, permiten a las organizaciones proteger la información crítica y mitigar riesgos.

CONCLUSIÓN

En conclusión, las normas ISO 27000, 27001 y 27002 son importantes para establecer y mantener la seguridad de la información en una organización, ya que proporcionan un marco que permite gestionar riesgos, proteger datos y garantizar la confidencialidad, integridad y disponibilidad de la información. Su correcta aplicación fortalece la confianza, mejora la gestión interna y demuestra el compromiso de la empresa con la protección de los activos digitales frente a las amenazas actuales.

RECOMENDACIÓN

Se recomienda que las organizaciones adopten e implementen de manera continua las normas ISO 27000, 27001 y 27002, asegurando la seguridad de información, capacitando al personal y la actualización constante de los controles de seguridad. Esto permitirá mantener la información protegida, reducir riesgos tecnológicos y De esta forma, no solo se protege la información interna, sino también la de los clientes, fortaleciendo su confianza y garantizando la transparencia y seguridad en el manejo de sus datos frente a los riesgos tecnológicos actuales.

ANEXOS


ISO
27002
ISO


EVERYTHING YOU NEED TO KNOW ABOUT
ISO 27001
EVERYTHING YOU NEED TO KNOW ABOUT

BIBLIOGRAFIA

WEBGRAFIA

IT Governance. (s. f.). ISO/IEC 27001:2022 – Information Security Management (ISO27001). IT Governance UK. Recuperado de https://www.itgovernance.co.uk/iso27001

IT Governance. (s. f.). ISO 27001:2022 and ISO 27002:2022 — updates. IT Governance. Recuperado de https://www.itgovernance.co.uk/iso27001-and-iso27002-2022-updates

IT Governance. (2024, 13 de marzo). ISO 27001:2022 Annex A controls — explained. IT Governance Blog. Recuperado de https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained

Pirani. (s. f.). ISO 27001: de qué se trata y cómo implementarla. Pirani Risk (Academia). Recuperado de https://www.piranirisk.com/es/academia/especiales/iso-27001-que-es-y-como-implementarla

GlobalSUITE Solutions. (s. f.). Changes to the ISO 27002:2022 Standard Update. GlobalSUITE Solutions. Recuperado de https://www.globalsuitesolutions.com/the-main-changes-in-the-iso-270022022-standard-update/

GlobalSUITE Solutions. (s. f.). New version ISO 27001:2022. GlobalSUITE Solutions. Recuperado de https://www.globalsuitesolutions.com/new-version-iso-270012022/

6clicks. (s. f.). Align or get certified to ISO 27001. 6clicks. Recuperado de https://www.6clicks.com/solutions/iso-27001

6clicks. (s. f.). ISO 27001 Guide: A Comprehensive Guide / The complete guide to ISO 27001. 6clicks Resources. Recuperado de https://www.6clicks.com/guides/the-complete-guide-to-iso-27001

ISMS.online. (s. f.). ISO 27001 Requirement 6.2 — Establishing measurable information security objectives. ISMS.online. Recuperado de https://www.isms.online/iso-27001/requirements-2013/6-2-establishing-measurable-information-security-objectives-2013/

International Organization for Standardization. (2022). ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO. Recuperado de https://www.iso.org/standard/27001