RESOURCE CENTER

Cómo la gestión de contraseñas ayuda a las empresas a obtener la certificación ISO 27001

Get the full interactive view at
https://bitwarden.com/es-la/resources/how-password-management-helps-companies-achieve-iso-27001-certification/

bitwarden

¿Qué es la norma ISO 27001?

Actualización: Desde marzo de 27001, Bitwarden cuenta con la certificación ISO 27001 de conformidad con los conjuntos de controles ISO 27001 relativos a la seguridad de los datos.

La norma internacional ISO 27001 sienta las bases para crear, mantener y desarrollar sistemas de gestión de la seguridad de la información (SGSI), incluida la gestión de datos. Las empresas que deseen obtener la conformidad o certificación ISO 27001 deberían considerar la posibilidad de añadir la gestión de contraseñas ISO 27001 a su conjunto de herramientas.

El grupo mundial de la Organización Internacional de Normalización (ISO) elabora y publica normas técnicas, industriales y comerciales de ámbito mundial. Actualizada por última vez en octubre de 2022, la norma ISO 27001 para SGSI proporciona un marco para la seguridad de los datos que consta de 93 conjuntos de controles. Para obtener la certificación ISO 27001, las empresas deben demostrar el cumplimiento de todas ellas.

> Para certificarse como empresa ISO 27001, debe cumplir 93 conjuntos de control.

El proceso de certificación ISO 27001 consiste en una auditoría realizada por organismos de certificación independientes que revisan las políticas y procedimientos de seguridad de los datos de la empresa, y cómo se aplican. El proceso puede ser largo, pero superar una auditoría de certificación ISO 27001 demuestra que su empresa ha realizado una evaluación de riesgos de seguridad para identificar posibles amenazas y ha introducido controles de seguridad para protegerse contra las violaciones de datos.

Índice

Ventajas de la certificación y el cumplimiento de la norma ISO 27001

La certificación ISO 27001 proporciona a las organizaciones una ventaja competitiva a la hora de atraer y retener clientes, ya que la certificación demuestra la existencia de sólidos controles de seguridad de la información. La certificación también puede atraer y retener a proveedores y otras partes interesadas preocupadas por cómo se gestiona y protege su información.

Incluso la preparación para el proceso de auditoría puede reforzar las políticas ISO 27001 existentes y mejorar los sistemas internos, las estructuras y los procesos empresariales cotidianos. El proceso de gestión de riesgos también puede ayudar a las organizaciones a cumplir mejor con las leyes de protección de datos, como CCPA y GDPR, y evitar multas por incumplimiento o pérdida de reputación debido a una violación de datos evitable.

Obtenga más información sobre cómo su empresa puede reforzar sus prácticas de ciberseguridad para superar las auditorías de seguridad.

Los conjuntos de control ISO 27001

Los 93 conjuntos de control figuran en el anexo A y se dividen en 4 grandes temas. Para obtener la certificación ISO 27001, las empresas deben demostrar el cumplimiento de estos controles. Las categorías son:

- Controles organizativos (37 controles)
- Controles de personas (8 controles)
- Controles físicos (14 controles)
- Controles tecnológicos (34 controles)

La versión anterior de ISO incluía 114 controles divididos en 14 categorías. Esa versión también incluía un lenguaje que regulaba los sistemas seguros de inicio de sesión y gestión de contraseñas.

El control de inicio de sesión seguro especificaba que "el acceso a los sistemas y aplicaciones debe controlarse mediante un procedimiento de inicio de sesión seguro cuando así lo exija la política de control de acceso". Con un gestor de contraseñas, los usuarios se benefician de añadir otra capa de seguridad a los inicios de sesión y de disponer de un lugar que les ayude a gestionar e integrar la autenticación de dos factores para todos los sitios web que la admitan.

El control del sistema de gestión de contraseñas establecía que "los sistemas de gestión de contraseñas serán cooperativos para garantizar la calidad de las contraseñas." ISO recomienda utilizar un gestor de contraseñas que permita a los usuarios crear contraseñas seguras y únicas y que ofrezca funciones de uso compartido seguro para la colaboración.

> **Los gestores de contraseñas establecen la seguridad de las contraseñas, aplican la 2FA y utilizan registros de eventos para supervisar la actividad de los usuarios, todas ellas funciones que las empresas deben conseguir para cumplir los requisitos de control de acceso ISO, protección de la IIP y protección de puntos finales.**

La última versión de la norma ISO 27001 aborda la gestión de contraseñas en el anexo A 5.17. Hay muchos requisitos adicionales del Anexo A que pueden cumplirse o apoyarse adoptando un gestor de contraseñas. Aunque no son exhaustivos, algunos ejemplos son:

- **Anexo A 5.3, Separación de funciones**: Se separarán las funciones y las áreas de responsabilidad conflictivas.
- **Anexo A 5.14, Transferencia de información**: Se establecerán normas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.
- **Anexo A 5.15, Control de acceso**: Se establecerán y aplicarán normas para controlar el acceso físico y lógico a la información y a otros activos asociados, basadas en los requisitos de seguridad de la empresa y de la información.

- **Anexo A 5.16, Gestión de identidades**: Se gestionará el ciclo de vida completo de las identidades.
- **Anexo A 5.17, Información de autenticación**: La asignación y gestión de la información de autenticación se controlará mediante un proceso de gestión, que incluirá el asesoramiento al personal sobre las mejores prácticas de gestión de la información de autenticación.
  - Un manual detallado sobre este criterio establece recomendaciones de contraseñas con consejos sobre su gestión, incluida la posibilidad de crear contraseñas seguras. Además, el objetivo recomienda a las organizaciones evitar credenciales débiles, ampliamente utilizadas o comprometidas.

> Teniendo en cuenta estos criterios, lo ideal sería que las organizaciones implantaran un sistema de gestión de contraseñas que les permitiera informar sobre las contraseñas expuestas, reutilizadas, débiles o potencialmente comprometidas, y disponer de información procesable al respecto.

- **Anexo A 5.34, Privacidad y protección de la información personal identificable (IPI)**: La organización debe identificar y cumplir los requisitos relativos a la preservación de la privacidad y la protección de la IIP de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales.
- **Anexo A 8.1, Dispositivos de punto final de usuario**: Se protegerá la información almacenada, procesada o accesible a través de dispositivos de punto final de usuario.
- **Anexo A 8.4, Acceso al código fuente**: Se gestionará adecuadamente el acceso de lectura y escritura al código fuente, a las herramientas de desarrollo y a las bibliotecas de software.
- **Anexo A 8.5, Autenticación segura**: Se aplicarán tecnologías y procedimientos de autenticación segura basados en las restricciones de acceso a la información y en la política específica del tema sobre control de acceso.
  - Este objetivo se centra en el uso de la autenticación multifactor para iniciar sesión de forma segura en los sistemas. Con un gestor de contraseñas, los usuarios se benefician de añadir otra capa de seguridad a los inicios de sesión, y también de tener un lugar para ayudar a gestionar e integrar la autenticación de dos factores (2FA) para todos los sitios web que la admiten. El objetivo también subraya que las contraseñas deben ser confidenciales en todo momento, lo que supone un argumento de peso a favor de una caja fuerte de contraseñas totalmente cifrada.

> Los sistemas de gestión de contraseñas permiten a las organizaciones identificar cualquier elemento de sus bóvedas con 2FA inactivo.

- **Anexo A 8.11, Enmascaramiento de datos**: El enmascaramiento de datos se utilizará de acuerdo con la política temática específica de la organización sobre control de acceso y otras políticas temáticas relacionadas, así como con los requisitos empresariales, teniendo en cuenta la legislación aplicable.
- **Anexo A 8.12, Fuga de datos**: Se aplicarán medidas de prevención de fuga de datos a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.

¿Lo sabías?

Bitwarden ofrece Informes de Salud de Bóvedas que pueden ayudar a fomentar fuertes prácticas de ciberseguridad y permitir a los empleados identificar cuentas con protección débil.

ISO recommends using a that enables users to create strong and unique passwords and offers secure sharing capabilities for collaboration.

Consiga la certificación ISO 27001 con la ayuda de un gestor de contraseñas

Un sistema de gestión de contraseñas es compatible con los numerosos requisitos del anexo A enumerados anteriormente, y con muchos de los requisitos incluidos en los conjuntos de control generales.

Los usuarios pueden mantener en secreto la información de autenticación, aplicar las mejores prácticas de contraseñas, como generar contraseñas fuertes y únicas, y compartir contraseñas de forma segura con un gestor de contraseñas que proteja la información sensible con cifrado de extremo a extremo. Al limitar quién puede ver determinada información sensible o crítica, los gestores de contraseñas también ayudan a segregar funciones y limitar las amenazas internas.

Las organizaciones que utilizan gestores de contraseñas establecen requisitos de seguridad de las contraseñas, imponen la autenticación de dos factores (2FA) y utilizan registros de eventos para supervisar la actividad de los usuarios, todas ellas capacidades que las empresas deben lograr para cumplir los requisitos de control de acceso ISO, protección de la información de identificación personal y protección de puntos finales. La mayoría de los gestores de contraseñas de renombre también facilitan la integración de SSO, equipando a los administradores con las herramientas que necesitan para gestionar el acceso y el proceso de autenticación. Esta capacidad ayuda a cumplir el requisito ISO de autenticación segura.

Al evaluar los gestores de contraseñas para respaldar la certificación ISO 27001, las organizaciones deben evaluar si el software sigue los estándares de seguridad y cumplimiento de grado empresarial, como el cumplimiento de SOC2 tipo 2, el cumplimiento de GDPR, el Marco de Privacidad de Datos y HIPAA. Las empresas deben seleccionar una solución que ofrezca cifrado de conocimiento cero de extremo a extremo.

Comience a utilizar Bitwarden

¿Está interesado en utilizar el gestor de contraseñas Bitwarden ISO 27001 para ayudar a cumplir las normas ISO 27001 para los sistemas de gestión de la seguridad de la información? Inicie hoy mismo una prueba gratuita para empresas con Bitwarden.

Casos prácticos:

Inventory Hive, una plataforma de software de inspección de propiedades y visitas virtuales líder en el Reino Unido, obtuvo la certificación ISO 27001 con Bitwarden.

Tanto Bitwarden Secrets Manager como Bitwarden Password Manager permiten a Titanom Technologies demostrar su resistencia a la ciberseguridad y ser considerada para la certificación ISO 27001.

"I want to set guidelines on the password generator about how strong the password must be. That's very important right now for us to achieve the ISO 27001 certification."

Jannis Morgenstern, head of IT at Titanom Technologies