ISO/IEC 27001:2022

Mapeo de cumplimiento para la Plataforma de seguridad de datos Varonis

Índice

Índice 2
descripción general 3
Cómo Varonis asigna las normas y regulaciones ISO/IEC 27001 3
Conclusión 12
Programe una evaluación de riesgo de datos gratuita. 13

descripción general

La serie 27000 de la Organización Internacional de Normalización (ISO) es un marco reconocido internacionalmente para las prácticas recomendadas en la gestión de la seguridad de la información.

Desarrollado y publicado por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), el pilar principal de la serie ISO/IEC 27000 es ISO/IEC 27001, que describe las prácticas recomendadas, las metodologías y la implementación de la gestión de la seguridad de la información en una organización.

El enfoque distintivo de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de los datos de una organización. A menudo, las empresas comienzan descubriendo e identificando posibles problemas de seguridad a través de un ejercicio (por ejemplo, una evaluación de riesgos), y luego definen lo que debe hacerse para prevenir y remediar los problemas existentes. En definitiva, la filosofía central de ISO 27001 se basa en la gestión de riesgos: identificar los riesgos y luego tratarlos sistemáticamente.

Varonis ayuda a cumplir con las normas y regulaciones ISO 27001 como una solución totalmente integrada

"Tenemos la certificación ISO 27001 y una gran parte de eso es la clasificación de datos y el control de datos confidenciales. Ahí es donde Varonis ha sido útil".

Administrador de sistemas, proveedor de servicios

Leer el caso de estudio →

que se centra en proteger los datos empresariales dondequiera que residan: en la nube y en premisas.

Cómo Varonis asigna las normas y regulaciones ISO/IEC 27001

ISO 27001 es la norma internacional líder que se centra en la seguridad de la información y puede ayudar a las organizaciones a cumplir con los requisitos legales, lograr una ventaja competitiva, reducir los costos evitando que ocurran incidentes de seguridad y ayudarlas a definir sus procesos y procedimientos.

Proteger sus datos con Varonis lo ayudará a proteger a sus empleados de la responsabilidad personal, proteger los datos de los clientes y evitar multas costosas por incumplimiento. Este documento se centra en los requisitos que Varonis puede permitir que implemente su organización.

A continuación, le indicamos cómo Varonis puede ayudar a las organizaciones a lograr la seguridad de los datos según lo previsto por la ISO/IEC 27001:2022:

A.6: Organización de la seguridad de la información	Cómo ayuda Varonis
5 Controles organizacionales	**Varonis:**
5.2 Roles y responsabilidades de seguridad de la información. Control. Los roles y las responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización.	Reduce de manera significativa el riesgo de pérdida y uso indebido de datos al ayudar a las organizaciones a gestionar el acceso a los datos, capacitar a los propietarios de datos para otorgar y revocar el acceso directamente, y reparar y mantener automáticamente los permisos del sistema de archivos, lo que hace que las organizaciones sean menos vulnerables a las amenazas internas y externas, cumplan mejor los requisitos y sigan un modelo de privilegios mínimos de forma constante.
5.3 Segregación de obligaciones. Control. Se segregarán las obligaciones en conflicto y las áreas de responsabilidad contradictorias.	Ayuda a limitar los controles de acceso y los reportes según el alcance de cada usuario. Los propietarios de datos solo verán (y gestionarán el acceso) los recursos compartidos por los que son responsables en la interface de usuario. Un operador de seguridad podrá ver reportes y rastrear alertas activadas, pero no podrá administrar la red.
5.4 Responsabilidades de la gerencia. Control. La gerencia requerirá que todo el personal aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida y las políticas y los procedimientos específicos del tema de la organización.	Le permite aplicar un modelo de privilegios mínimos en sus repositorios de datos principales y establecer un flujo de trabajo para que los propietarios de datos otorguen acceso temporal a empleados y contratistas.
5.6 Contacto con grupos de interés especial. Control. La organización debe establecer y mantener contacto con grupos de interés especial u otros foros y asociaciones profesionales especializados en seguridad.	Cuenta con investigadores expertos en seguridad, ingenieros, soporte técnico, servicios profesionales y especialistas en seguridad disponibles en horario de oficina, a través de cursos en línea, webinars, eventos presenciales y comunidades de clientes.
5.7 Inteligencia de amenazas. Control. La información relativa a las amenazas a la seguridad de la información se recopilará y	Le brinda inteligencia procesable y análisis de seguridad sobre sus datos: analice patrones de comportamiento para ver cuándo un usuario está actuando de manera sospechosa y

analizará para producir inteligencia sobre amenazas.	compare su actividad con la de sus pares, sus horas de trabajo normales y su comportamiento típico. Con Varonis, las organizaciones pueden visualizar las amenazas de seguridad con un panel intuitivo, investigar incidentes de seguridad e incluso hacer un seguimiento de las alertas y asignarlas a los miembros del equipo para su cierre.
5.9 Inventario de información y otros activos asociados. Control. Se desarrollará y mantendrá un inventario de información y otros activos asociados, incluidos los propietarios.	Mapea y monitorea sus sistemas de almacenamiento de información y de correo electrónico y actualiza diariamente las ACL y las estructuras de archivos de los recursos supervisados para garantizar que se dispone de la información más actualizada sobre sus datos.
5.10 Uso aceptable de la información y otros activos asociados. Control. Se identificarán, documentarán e implementarán las reglas para el uso aceptable y los procedimientos para el manejo de la información y otros activos asociados.	Monitorea sus repositorios de datos para detectar patrones de uso desviados, lo que podría ser una infracción de una política de uso aceptable. Envía alertas a su equipo de seguridad o SIEM para comenzar la investigación y la respuesta a incidentes. Detecta comportamientos contrarios a la política comercial establecida para sus requisitos específicos.
5.12 Clasificación de la información. Control. La información se clasificará de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, integridad, disponibilidad y los requisitos pertinentes de las partes interesadas.	Detecta e identifica datos confidenciales y regulados, como PII, GDPR e HIPAA, junto con los datos que se consideren confidenciales en sus principales repositorios de datos y correos electrónicos. Los datos se pueden categorizar y clasificar automáticamente según el tipo y la confidencialidad. Identifica automáticamente los datos confidenciales nuevos y recientes que sus usuarios crean en ubicaciones no seguras. Proporciona la capacidad de etiquetar los metadatos para la integración con etiquetas de Microsoft Purview Information Protection (MPIP) para que pueda hacer un seguimiento

	de los datos confidenciales a medida que se mueven por la red. Establece políticas para migrar o poner en cuarentena los datos confidenciales de acuerdo con la política.
5.13 Etiquetado de la información. Control. Se desarrollará e implementará un conjunto adecuado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información adoptado por la organización.	Etiqueta automáticamente archivos confidenciales para MPIP. Puede configurar qué tipo de etiquetas coinciden con qué metadatos según las clasificaciones de Varonis.
5.15 Control de acceso. Control. Se establecerán e implementarán reglas para controlar el acceso físico y lógico a la información y otros activos asociados en función de los requisitos comerciales y de seguridad de la información.	Implementa un flujo de trabajo para su política de control de acceso: los usuarios solicitan acceso en la consola y los propietarios de datos aprueban o rechazan solicitudes en la consola o por correo electrónico. El flujo de trabajo elimina la carga de la gestión de acceso del personal de TI y la pone en manos de los propietarios de los datos, quienes pueden tomar mejores decisiones sobre las solicitudes de acceso de los usuarios.
5.16 Control de gestión de identidades. Se gestionará todo el ciclo de vida de las identidades.	Crea un inventario de todos los usuarios, grupos y dispositivos en la red vinculada a su historial de actividad apto para búsquedas. Resuelve todas las membresías de usuarios y grupos y los niveles de acceso, incluidas relaciones complejas y profundamente anidadas. Correlaciona usuarios y grupos con listas de control de acceso en repositorios de datos para ver fácilmente a qué puede acceder este usuario o grupo.
5.18 Derechos de acceso. Control. Los derechos de acceso a la información y otros activos asociados se aprovisionarán, revisarán, modificarán y eliminarán de acuerdo con la política y las reglas de control de acceso específicas de la organización.	Proporciona una API que funciona junto con otros sistemas para agregar o eliminar el acceso de los usuarios. Puede implementar este proceso para proporcionar a los usuarios un nivel base de permisos en función de su grupo, o revocar automáticamente todo el

	acceso de un empleado que ya no pertenece a la empresa. Implementa un proceso de aprovisionamiento de acceso de usuarios, concediendo a los usuarios permisos básicos y proporcionando un flujo de trabajo para que los usuarios soliciten más acceso para hacer su trabajo.
5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información. Control. La organización planificará y preparará la gestión de incidentes de seguridad de la información definiendo, estableciendo y comunicando los procesos, los roles y las responsabilidades de gestión de incidentes de seguridad de la información.	Ayuda a detectar la actividad inusual de archivos y correos electrónicos y el comportamiento sospechoso de los usuarios, y activa alertas en todas las plataformas para proteger sus datos antes de que sea demasiado tarde. El equipo de respuesta a incidentes de Varonis es un grupo de analistas de seguridad y personas que responden a incidentes que pueden ayudarlo a mitigar un ataque en curso o proporcionar una investigación forense de un incidente de seguridad, todo de forma gratuita.
5.26 Respuesta a incidentes de seguridad de la información. Control. Los incidentes de seguridad de la información se responderán de acuerdo con los procedimientos documentados.	Ofrece activadores de respuesta automáticos, que pueden detener el ransomware en seco y mitigar el impacto de las cuentas comprometidas y las posibles brechas de datos.
5.27 Aprender de los incidentes de seguridad de la información. Control. Los conocimientos adquiridos en los incidentes de seguridad de la información se utilizarán para reforzar y mejorar los controles de seguridad de la información.	Proporciona los datos iniciales de alerta y auditoría para investigar incidentes de seguridad: visualice las amenazas de seguridad con un panel intuitivo, investigue incidentes de seguridad e incluso haga un seguimiento de las alertas y asígnelas a los miembros del equipo para su cierre. En caso de una brecha de datos, nuestro equipo de respuesta a incidentes puede ayudarlo a reaccionar rápidamente ante el ataque y proporcionará recomendaciones para mejorar la detección y respuesta al finalizar su sesión de trabajo.
5.28 Recopilación de datos. Control. La organización debe establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de datos relacionada con eventos de seguridad de la información.	

5.29 Seguridad de la información durante las interrupciones. Control. La organización debe planificar cómo mantener la seguridad de la información en un nivel apropiado durante la interrupción.	Ofrece activadores de respuesta automáticos, que pueden detener el ransomware en seco y mitigar el impacto de las cuentas comprometidas y las posibles brechas de datos.
5.32 Derechos de propiedad intelectual. Control. La organización implementará procedimientos adecuados para proteger los derechos de propiedad intelectual.	Ayuda a optimizar las prácticas de privacidad de datos y a bloquear los datos confidenciales para cumplir con los requisitos de actividad de datos y las leyes de brecha de datos. Con Varonis, las organizaciones pueden mover automáticamente los datos de acuerdo con la política comercial, poner en cuarentena los datos confidenciales o regulados que están sobreexpuestos y archivar o eliminar los datos obsoletos que ya no se utilizan.
5.33 Protección de registros. Control. Los registros estarán protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.	
5.34 Privacidad y protección de la información personal identificable (PII). Control. La organización debe identificar y cumplir con los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales.	Ayuda a las empresas a cumplir con los requisitos de cumplimiento: identificar y clasificar automáticamente los datos PII, establecer controles de acceso y políticas de protección de datos, y crear una estrategia unificada de seguridad de datos para proteger los datos de los clientes.
6 Controles de personas	**Varonis:**
6.3 Concientización, educación y capacitación sobre seguridad de la información. Control. El personal de la organización y las partes interesadas pertinentes recibirán concientización sobre la seguridad de la información, capacitación y actualizaciones periódicas de la política de seguridad de la información de la organización y políticas y procedimientos para temas específicos, según corresponda para su función laboral.	Proporciona un equipo de respuesta a incidentes (IR) gratuito, que puede ayudar a capacitar a su equipo para responder a las últimas evoluciones del panorama de amenazas. En caso de una brecha de datos, nuestro equipo de respuesta a incidentes puede ayudarlo a responder ante el ataque y proporcionará recomendaciones para mejorar la detección y respuesta al finalizar su sesión de trabajo. Nuestra evaluación de la resistencia cibernética puede medir la exposición de sus datos y poner a prueba su pila de seguridad frente a las últimas tácticas y maniobras de los

	adversarios, reforzando su postura de seguridad y ayudando a capacitar a su equipo de seguridad.
6.4 Proceso disciplinario. Control. Se formalizará y comunicará un proceso disciplinario para tomar medidas contra el personal y otras partes interesadas relevantes que hayan cometido una infracción de la política de seguridad de la información.	Audita sus repositorios de datos primarios y crea alertas basadas en la actividad del usuario para evitar la exfiltración de datos, el robo o las brechas de datos.
6.5 Responsabilidades después del despido o el cambio de empleo. Control. Las responsabilidades y los deberes de seguridad de la información que sigan siendo válidos después del despido o el cambio de empleo se definirán, aplicarán y comunicarán al personal pertinente y otras partes interesadas.	Agiliza la gestión de los derechos de acceso para los usuarios que cambian de trabajo o abandonan la empresa. Varonis incluye una API para revocar o agregar acceso de usuario como parte del proceso de despido o cambio de empleados. Por ejemplo, si cambia un usuario del grupo de finanzas al grupo de RR. HH., la API eliminará al usuario del grupo de finanzas y lo agregará al grupo de RR. HH., mientras actualiza automáticamente sus ACL según sea necesario. De manera similar, si otorga un derecho de acceso a un contratista, puede usar Varonis para revocar automáticamente el acceso en la fecha de finalización del contrato.
6.7 Trabajo remoto. Control. Se implementarán medidas de seguridad cuando el personal trabaje de forma remota para proteger la información a la que se acceda, procese o almacene fuera de las instalaciones de la organización.	Monitorea el acceso remoto de sus datos y detecta inicios de sesión anormales o acceso desde ubicaciones extranjeras a su empresa. Con Varonis, podrá distinguir entre un inicio de sesión remoto de un usuario conocido y un pirata informático que intenta infiltrarse en su red utilizando credenciales robadas.
8 Controles tecnológicos	**Varonis:**
8.2 Derechos de acceso privilegiados. Control. Se restringirá y gestionará la asignación y el uso de derechos de acceso privilegiados.	Monitorea y analiza la actividad de las cuentas de usuario privilegiadas. Por ejemplo, si una cuenta de administrador actualiza un GPO o cambia un grupo, recibirá una alerta y verificará la autenticidad de la acción. Si un usuario se eleva a derechos administrativos, recibirá una alerta para verificar esa acción. La

	mayoría de las veces, la escalada de privilegios es parte de un ataque de infiltración.
8.3 Restricción de acceso a la información. Control. El acceso a la información y otros activos asociados se restringirá de acuerdo con la política específica del tema adoptada sobre el control de acceso.	Monitorea y detecta comportamientos anómalos que puedan suponer una infracción de sus políticas de acceso. Con Varonis, las organizaciones pueden gestionar los controles de acceso, monitorear y analizar la actividad del usuario y restringir el acceso a los datos de acuerdo con la política.
8.4 Acceso al código fuente. Control. El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software se gestionará adecuadamente.	Lo ayuda a controlar y limitar el acceso a los datos mediante la implementación de un modelo de privilegios mínimos y la auditoría de la actividad del usuario en esos datos. Varonis monitorea las cuentas de usuario y la actividad para detectar actividad anormal y comportamiento inusual: una cuenta de usuario que accede a datos fuera de su comportamiento típico es probablemente parte de un ataque de infiltración.
8.7 Protección contra software malicioso. Control. La protección contra el software malicioso se implementará y respaldará mediante la conciencia adecuada del usuario.	Protege a las organizaciones del software malicioso con detección rápida, controles de acceso optimizados y recuperación basada en datos. Varonis analiza los datos, la actividad de la cuenta y el comportamiento del usuario para alertar sobre actividades sospechosas y detener el ransomware.
8.9 Gestión de la configuración. Control. Se establecerán, documentarán, implementarán, monitorearán y revisarán las configuraciones de seguridad de hardware, software, servicios y redes.	Descubre errores de configuración críticos en todas sus plataformas de SaaS e IaaS que ponen a su organización en riesgo. Remedie automáticamente estos errores de configuración con solo pulsar un botón para mejorar su postura de seguridad de SaaS y eliminar las vías de ataque a los datos críticos.
8.10 Supresión de información. Control. La información almacenada en sistemas de información, dispositivos o en cualquier otro	Encuentra, mueve, archiva, pone en cuarentena o elimina datos de forma

medio de almacenamiento se eliminará cuando ya no sea necesaria.	automática según el tipo de contenido, la antigüedad, la actividad de acceso y más.
8.12 Prevención de fuga de datos. Control. Las medidas de prevención de fugas de datos se aplicarán a sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información confidencial.	Audita sus repositorios de datos primarios y crea alertas basadas en la actividad del usuario para evitar la exfiltración de datos, el robo o las brechas de datos. Varonis analiza los dispositivos de perímetro, incluidos DNS y VPN, para detectar ataques como software malicioso, intrusiones de amenazas avanzadas persistentes y exfiltración, y los pone en contexto con la actividad y las alertas en sus repositorios de datos centrales.
8.13 Respaldo de información. Control. Las copias de seguridad de la información, el software y las imágenes del sistema se realizarán y comprobarán periódicamente de acuerdo con una política de copias de seguridad acordada.	Audita los cambios en estas carpetas y activa una advertencia si alguien hace un cambio no autorizado en las imágenes o los directorios de copia de seguridad.
8.15 Registro. Control. Se producirán, almacenarán, protegerán y analizarán registros que registren actividades, excepciones, fallos y otros eventos relevantes.	Monitorea, analiza y registra la actividad de los archivos, los eventos y el comportamiento del usuario en los repositorios de datos principales. Proporciona un registro detallado del contenido del servidor de archivos y cómo se usan, lo que incluye: nombres de archivos, carpetas, privilegios de acceso a archivos y carpetas (es decir, permisos NTFS de un usuario o grupo), uso de datos por nombre de usuario del nombre del grupo (es decir, crear, abrir, eliminar, renombrar), una lista de los posibles propietarios de los datos en la empresa, y más. La trazabilidad de auditoría puede compilarse automáticamente en reportes periódicos definidos por el usuario para que los responsables de cumplimiento y los auditores garanticen un uso y una custodia conformes. Los usuarios y administradores no podrán

	manipular y acceder a las bases de datos de Varonis que almacenan eventos de seguridad e información de registro.
8.16 Actividades de monitoreo. Control. Se monitorearán las redes, los sistemas y las aplicaciones en busca de comportamientos anómalos y se tomarán las medidas adecuadas para evaluar posibles incidentes de seguridad de la información.	Monitorea todos los inicios de sesión de cuentas privilegiadas y de administrador y audita los cambios en los archivos de configuración, los grupos de seguridad, los usuarios y los GPO, y puede alertar sobre estos cambios para comprobar que son legítimos o si un usuario se eleva a un grupo de seguridad con privilegios fuera de la directiva.
8.20 Seguridad de las redes. Control. Las redes y los dispositivos de red deben estar protegidos, administrados y controlados para proteger la información en los sistemas y aplicaciones.	Analiza los dispositivos de perímetro, incluidos DNS y VPN, para detectar ataques como software malicioso, intrusiones de amenazas avanzadas persistentes y exfiltración, y los pone en contexto con la actividad y las alertas en sus repositorios de datos centrales.

Conclusión

Lograr el cumplimiento total de ISO/IEC 27001 puede parecer una tarea abrumadora, pero en un mundo donde los clientes, socios y empleados están cada vez más preocupados por sus datos confidenciales, el cumplimiento ISO/IEC 27001 puede ser un activo sustancial. La certificación de la norma demuestra un fuerte compromiso con la seguridad de los datos y Varonis está a su disposición para ayudarlo en su recorrido por ISO/IEC 27001.

Programe una evaluación de riesgo de datos gratuita.

Varonis puede ayudarlo a gestionar su riesgo de seguridad y a cumplir con el ISO/IEC 27001 al identificar dónde almacena datos confidenciales, reducir el radio de ataque potencial de esos datos y monitorearlos en busca de amenazas potenciales. Para ver dónde tiene datos confidenciales en su entorno, regístrese para una evaluación de riesgo sobre los datos gratuita.

Nuestra evaluación gratuita a cargo de analistas expertos en análisis forense y respuesta a incidentes lo ayudará a encontrar y clasificar datos regulados en repositorios de datos en premisas y en la nube, medir la exposición de datos y alertar sobre el acceso sospechoso a información regulada.

Contáctenos

Acerca de Varonis

Varonis es pionera en seguridad y análisis de datos, y libra una batalla diferente de la que enfrentan las empresas de ciberseguridad convencionales. Varonis se centra en proteger los datos empresariales locales y en la nube: archivos y correos electrónicos importantes; información confidencial de clientes, pacientes y empleados; registros financieros; planes estratégicos y de productos; y otra propiedad intelectual.

La Plataforma de seguridad de datos Varonis detecta amenazas internas y ataques cibernéticos al analizar la información, la actividad de la cuenta y el comportamiento del usuario; evita y limita que se produzcan incidentes restringiendo el acceso a datos importantes y obsoletos; y mantiene la seguridad de forma eficiente mediante la automatización. Con énfasis en la seguridad de los datos, Varonis puede aplicarse a una variedad de casos de uso que incluyen control, cumplimiento, clasificación y análisis de amenazas. Varonis comenzó a operar en 2005 y cuenta con miles de clientes en todo el mundo, entre los que se incluyen líderes de la industria de muchos sectores, como tecnología, consumo, venta minorista, servicios financieros, atención médica, fabricación, energía, medios de comunicación y educación.