KEEPER

Ficha técnica

Cumpla fácilmente con los requisitosdel anexo A.9 de la norma ISO 27001 con Keeper

La norma ISO 27001 es una norma internacional de seguridad de la información que proporciona un marco y directrices para establecer, implementar y administrar los sistemas de gestión de la seguridad de la información. La norma ISO 27001 se diseñó para ayudar a las organizaciones a proteger sus recursos críticos y cumplir con los requisitos reglamentarios necesarios para su industria.

Como parte del proceso para cumplir con la norma ISO 27001, las organizaciones deben restringir el acceso de los empleados únicamente a la información que sea relevante para su función para reducir las posibilidades de que los datos lleguen a usuarios no autorizados y se expongan a riesgos.

Al aprovechar las soluciones de seguridad cibernética líderes de Keeper Security, las organizaciones de todos los tamaños pueden asegurarse de cumplir de forma sencilla y económica con las disposiciones del anexo A.9 de la norma ISO 27001 y reforzar su postura de seguridad.

Requisito	Solución
A.9.1.1: Política de control de acceso	La política de control de acceso define las reglas y los procedimientos para garantizar la seguridad de los recursos de información y aplicar los privilegios mínimos. Keeper garantiza el cumplimiento con controles de acceso basados en roles (RBAC) establecidos por los administradores para garantizar que se otorguen los privilegios mínimos en toda la organización. El módulo de alertas e informes avanzados (ARAM) de Keeper les proporciona a las organizaciones informes claros sobre el acceso a los recursos privilegiados
A.9.2.1: Registro y cancelación de registro de los usuarios	Las organizaciones deben garantizar que exista un proceso formal que rija cómo se les otorga acceso a los usuarios a los archivos y los servicios de la empresa, y cómo se revoca ese acceso. El RBAC de Keeper define las políticas de acceso de los usuarios a nivel de rol y aplica el principio de privilegios mínimos. Keeper también dispone de acceso por tiempo limitado, lo que les permite a los usuarios compartir registros durante un período determinado y revocar el acceso automáticamente tras su vencimiento. Cuando se combina con la rotación de contraseñas de Keeper Secrets Manager, los usuarios y los administradores pueden asegurarse de que los destinatarios nunca tengan acceso permanente. Eliminar usuarios de la plataforma de Keeper es sencillo. Los administradores pueden eliminar usuarios de forma rápida y sencilla y transferir el contenido de su bóveda a un miembro del equipo adecuado, lo que garantiza la continuidad de las operaciones empresariales.
A.9.2.2: Concesión de acceso de los usuarios	Un sistema, preferiblemente automatizado, debe firmar y revocar los derechos de toda la organización. Keeper SSO Connect permite administrar los accesos de forma centralizada, lo que les permite a los equipos de TI monitorear y controlar el acceso de los usuarios a los recursos autorizados. Este enfoque simplifica la gestión de accesos, mejora la visibilidad y garantiza el cumplimiento de las políticas de seguridad.
A.9.2.3: Gestión de los derechos de acceso privilegiado	El acceso privilegiado otorga derechos a los administradores de sistemas y a quienes tienen acceso a información confidencial. Los usuarios privilegiados suelen ser administradores de TI y seguridad, profesionales de recursos humanos, directivos de alto nivel u otras personas que necesitan acceder a sistemas privilegiados. La norma ISO 27001 requiere que se realice una revisión periódica de las cuentas de administrador y un registro de todos los derechos privilegiados. Keeper ofrece gestión de contraseñas, secretos y conexiones privilegiadas de nivel empresarial en una plataforma unificada. La solución de Keeper les permite a las organizaciones lograr visibilidad, seguridad, control e informes completos de todos los usuarios con privilegios en todos los dispositivos.

Requisito	Solución
A.9.2.4: Gestión de la información secreta de autenticación de los usuarios	La información secreta de autenticación debe estar sumamente cifrada y se deben utilizar mecanismos adicionales para respaldar su seguridad. Estos sistemas deben gestionarse de forma eficiente y permanecer confidenciales. Keeper Secrets Manager (KSM) es una plataforma de conocimiento cero totalmente gestionada y basada en la nube que protege secretos como claves de API, contraseñas de bases de datos, claves de acceso, certificados y cualquier tipo de datos confidenciales. KSM almacena todos los secretos y las credenciales en Keeper Vault con cifrado a nivel de registro para ofrecer el cifrado más seguro del mercado. Los administradores pueden aplicar medidas de seguridad adicionales, como la autenticación multifactor (MFA) y la rotación de credenciales, para garantizar que los secretos siempre sean seguros.
A.9.4.1: Einschränkung des Datenzugriffs	Las políticas de control de acceso deben aplicarse a todos los sistemas de la empresa y deben establecerse medidas para reflejar los diferentes niveles de restricción de acceso en toda la organización. Keeper proporciona lo siguiente para asegurar su cumplimiento: • Controles de acceso basados en roles • Uso compartido granular para aplicar reglas como el almacenamiento de credenciales de solo lectura o en carpetas compartidas obligatorias, así como la capacidad de revocar la capacidad de compartir accesos y limitar a los usuarios a compartir o recibir credenciales de forma interna. • Controles de acceso privilegiados para información y datos confidenciales
A.9.4.2: Procedimientos de inicio de sesión seguros	Las organizaciones deben aplicar otros métodos además de las contraseñas para proteger los procedimientos de inicio de sesión. Los intentos exitosos y fallidos deben registrarse. Keeper ofrece varias opciones para los métodos de inicio de sesión adicionales a las contraseñas. Keeper admite una amplia variedad de soluciones de MFA, almacena y autocompleta claves de acceso, y ayuda a las organizaciones que aprovechan las soluciones de inicio de sesión único (SSO) a incluir el acceso a sus bóvedas a través de su proveedor de SSO, lo que garantiza un acceso seguro y sin problemas. El módulo ARAM de Keeper les permite a los equipos respaldar el cumplimiento y las auditorías con más de 200 tipos de eventos diferentes, entre ellos, los intentos de inicio de sesión exitosos y fallidos, e informes personalizados, notificaciones en tiempo real e integración en soluciones SIEM de terceros.
A.9.4.3: Solución de gestión de contraseñas	Las organizaciones deben implementar un sistema de gestión de contraseñas que ayude a generar y aplicar contraseñas seguras y a garantizar su cumplimiento en los procedimientos de recuperación. Keeper lidera el sector en materia de certificaciones de seguridad y cumplimiento, y cifra a nivel de registro, lo que proporciona la seguridad más sólida de la industria. Todos los usuarios de Keeper pueden crear contraseñas y frases de contraseña de forma sencilla para todos los registros, lo que garantiza que se aprovechen las contraseñas seguras. BreachWatch de Keeper proporciona monitoreo de la dark web para alertar a los usuarios y los administradores de las credenciales que han sido expuestas.
A.9.4.5: Control de acceso al código fuente de los programas	El código fuente se ve constantemente amenazado por los cibercriminales que intentan acceder a los sistemas de la empresa. Las organizaciones deben implementar un control de acceso estricto para proteger estos sistemas. Keeper Secrets Manager protege su entorno y previene la proliferación de secretos eliminando las credenciales codificadas del código fuente, los archivos de configuración y los sistemas de CI/CD. Los usuarios y los administradores deben almacenar de forma segura todas las credenciales en su Keeper Vault para eliminar la proliferación y proporcionar informes y alertas sencillos. Los usuarios de Keeper pueden gestionar un número ilimitado de secretos, aplicaciones y entornos.