Obstáculos para la adopción del inicio de sesión único (SSO) para pequeñas y medianas empresas: identificación de desafíos y oportunidades

Publicación: mayo de 2024
Agencia de Ciberseguridad y Seguridad de la Infraestructura

Índice

1 Planteamiento del problema

En este estudio, se exploran los obstáculos y los desafíos para la adopción del inicio de sesión único (SSO, por sus siglas en inglés) por parte de las pequeñas y medianas empresas (SMB, por sus siglas en inglés). Además, se identifican posibles formas de superar estos desafíos, que, a su vez, mejoran el nivel de seguridad en dichas empresas.

El SSO es un sistema de control de acceso y autenticación de usuarios que permite acceder a múltiples aplicaciones, herramientas y sistemas con un solo conjunto de credenciales. Centralizando el proceso de autenticación, dicho método agiliza la gestión de identidades y simplifica la experiencia del usuario, ya que este solo necesita recordar un nombre de usuario y una contraseña para todas las cuentas. El SSO puede ayudar a reforzar las medidas de seguridad, ya que reduce la frecuencia con la que los usuarios tienen que ingresar sus credenciales de inicio de sesión. Además, puede reducir la duplicación de contraseñas en varias plataformas, lo que reduce la posibilidad de que se filtren.

Como parte de este estudio, la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA, por sus siglas en inglés) interactuó con varias partes interesadas involucradas con el SSO. Estos incluyen proveedores de SSO, proveedores de servicios gestionados con experiencia, organizaciones sin fines de lucro dedicadas a mejorar la ciberseguridad y SMB que tienen experiencia en la adopción de SSO y la migración entre las plataformas de SSO. Con base en estos debates, la CISA descubrió que, a pesar de los beneficios del SSO, la adopción de sus capacidades para la gestión de identidades sigue siendo baja, particularmente entre las SMB. Existen numerosos obstáculos para implementar con éxito una solución de SSO viable. Estos incluyen costos, obstáculos técnicos, así como falta de conocimientos y recursos.

Las pequeñas empresas suelen optar por contraseñas manuales y métodos prácticos para gestionar el acceso y las identidades, en lugar de la opción de SSO. Estos métodos tienden a ser más rentables en términos del costo de compra, que no incluye el costo oculto asociado con los gastos administrativos. A menudo, una razón principal de la diferencia en el costo de compra es que el SSO solo está disponible como un servicio prémium de nivel empresarial, que conlleva precios personalizados que son bastante más altos que los de los servicios esenciales. Un servicio prémium de nivel empresarial con SSO puede costar más por usuario que un servicio de nivel inferior sin dicho método. Además de un mayor costo por usuario, este modelo de precios prémium generalmente requiere una cantidad mínima de usuarios. Este costo incremental adicional, que puede aumentar de forma significativa el costo total por usuario en comparación con un servicio de nivel inferior sin SSO, puede ser un obstáculo financiero sustancial para muchas organizaciones. La diferencia de precio a menudo genera que las SMB seleccionen servicios más baratos y de nivel inferior que carecen de funciones de SSO.

Además, configurar las funciones avanzadas de SSO a menudo requiere conocimientos y experiencia técnicos especializados, así como tiempo. La combinación de costos adicionales, la necesidad de habilidades técnicas y el tiempo que se necesita lleva a muchas empresas a seguir dependiendo de métodos manuales, como hojas de cálculo, para manejar el acceso de los usuarios a diversas aplicaciones y sistemas. Con el fin de fomentar la adopción del SSO por parte de las SMB, los proveedores de dicho método deben abordar sus inquietudes y ofrecer asistencia técnica integral y soluciones adaptadas a las necesidades y prioridades de estas empresas.

Este estudio se organiza de la siguiente manera: en la Sección 2, se presentan los hallazgos clave relacionados con las ventajas del SSO, los desafíos que enfrentan las SMB en términos de la adopción de este método y la función que el Gobierno puede desempeñar para fomentar su adopción. En la Sección 3, se describe qué es el SSO y cómo funciona. En la Sección 4, se identifican los beneficios de la adopción de dicho método. En la Sección 5, se presenta una descripción general de la bibliografía sobre cómo las SMB adoptan la tecnología en general y se describe cómo puede aplicarse en el caso de la adopción del SSO. En la Sección 6, se presentan los resultados de la interacción de la CISA con las partes interesadas del SSO mediante la identificación de factores y aspectos clave que influyen en la adopción de este método, y se destaca cómo los proveedores y clientes tienen puntos de vista diferentes. En la Sección 7, se resumen los hallazgos del estudio sobre los beneficios de la adopción del SSO, los desafíos que experimentan las SMB en la implementación de dicho método, las necesidades de estas empresas y las prácticas típicas de los proveedores. En la Sección 8, se proporcionan recomendaciones sobre cómo ayudar a garantizar una implementación fluida y exitosa con el objetivo de fomentar la adopción del SSO por parte de las SMB. Finalmente, en el apéndice, se presenta una breve descripción del método de investigación utilizado en el estudio y el proceso asociado de interacción de las partes interesadas.

2 Hallazgos clave

A continuación, describimos las ventajas y los desafíos relacionados con la adopción del SSO, así como la función que puede desempeñar el Gobierno en el abordamiento de algunos de esos desafíos.

Ventajas de la adopción del SSO

Según Chang y Lee (2012), el SSO se diseñó centrándose principalmente en la seguridad y la experiencia del usuario, lo que lo distingue de otras soluciones de gestión de accesos, como los nombres de usuario y las contraseñas individuales. El SSO mejora la experiencia del usuario, lo que hace que sea más probable que los usuarios implementen de forma adecuada las medidas de seguridad. Los usuarios pueden habilitar y deshabilitar con facilidad la capacidad de ingresar a múltiples sistemas, plataformas, aplicaciones y recursos. Además, puede resolver con eficacia el problema del tiempo de inactividad relacionado con las contraseñas y los gastos de restablecimiento. Cuando se implementa y configura de forma correcta, la tecnología del SSO ofrece numerosas ventajas a las SMB en términos de mejora de la ciberseguridad. Cusack y Ghazizadeh (2016) y D'Costa-Alphonso y Lane (2010) coinciden en que el SSO reduce las divulgaciones, los errores humanos y los riesgos de ciberseguridad. El SSO también garantiza la finalización de una sesión del proveedor de identidad en cuanto el usuario cierra la sesión de todos los servicios autenticados por dicho proveedor (Ramamoorthi y Sarkar, 2020). Esto reduce el riesgo de que se produzcan ataques como el de falsificación de solicitud entre sitios (Armando et al., 2013).

Teniendo en cuenta los recientes incidentes cibernéticos relacionados con los servicios de SSO (por ejemplo, el incidente cibernético de Okta; Bradbury [2023], Bracken [2023], Newman [2023]), los expertos en ciencia forense digital y respuesta a incidentes recomiendan no bloquear las herramientas de ciberseguridad bajo dicho método. Si se dispone de suficientes conocimientos y recursos dedicados, puede justificarse un enfoque más diferenciado y estrechamente supervisado para las herramientas de ciberseguridad. Sin embargo, los analistas de ciberseguridad perciben que los beneficios proporcionados por las capacidades del SSO superan los riesgos potenciales, incluso en el contexto del incidente cibernético más reciente de Okta.

Aunque durante mucho tiempo se limitaron a una función de apoyo, las tecnologías de la información (IT, por sus siglas en inglés) en general, y la ciberseguridad en particular, se han convertido ahora en una parte esencial del comportamiento estratégico de cualquier empresa que busque una mayor competitividad. En algunos casos, la madurez de la ciberseguridad y la adopción de tecnologías de la información avanzadas son un elemento esencial de la estrategia corporativa de una empresa y pueden servir como factor potencial de diferenciación de productos o servicios.

Desafíos de la adopción del SSO que enfrentan las SMB

Las SMB representan más del 90 % de todas las empresas a nivel mundial y se prevé que crezcan un 6.1 % anual entre 2020 y 2025 (Quirt et al., 2022). Las SMB enfrentan el obstáculo de lidiar con numerosos inicios de sesión y contraseñas necesarios para las aplicaciones web. Estos desafíos pueden crear dificultades en la gestión de contraseñas para los usuarios finales (Komorowski et al., 2016). Si bien las nuevas tecnologías que pueden agilizar el acceso y la gestión de identidades pueden parecer atractivas para las SMB, su implementación podría representar un desafío.

Las SMB a menudo se muestran reacias a adoptar tecnología basándose en unos pocos artículos publicados que explican las ventajas que la tecnología puede aportar a una organización, pero no exploran como se debe las implicaciones en términos de costos (Fink, 1998). Para algunas SMB, la falta de información concluyente sobre el SSO proveniente de fuentes confiables reduce su voluntad de implementarlo. Aunque estén informadas, estas empresas a menudo necesitan aclaraciones sobre dónde adquirir una solución de SSO viable (Riches, 2007).

Debido a la estructura organizacional, la voluntad de actualizarse a otras formas de inicio de sesión seguras y eficientes, como el SSO, puede no ser una prioridad cuando las ganancias son cruciales para algunas SMB. La idea de adoptar este método puede resultar atractiva, pero las fuerzas externas del mercado pueden afectar de forma significativa las decisiones de adopción por parte de las SMB. La ciberseguridad es, por naturaleza, una función de apoyo al negocio y es dominada por prioridades empresariales, como atraer a nuevos clientes, conservar a los existentes, garantizar la financiación, cumplir la normativa y atraer talento. Las SMB suelen tener recursos y experiencia limitados cuando se trata de gestionar nuevas tecnologías. Por lo tanto, los costos de la implementación del SSO, junto con la falta de experiencia técnica necesaria para configurar e implementar la solución de forma adecuada, obstaculizan aún más la adopción de este método entre dichas empresas.

Participación del Gobierno

El Gobierno puede desempeñar una función importante a la hora de animar a las SMB a adoptar políticas y aplicar nuevas tecnologías. Los servicios de apoyo en forma de incentivos financieros o subvenciones pueden aumentar la adopción de determinadas medidas, pero las limitaciones en el uso de los fondos tienden a disuadir a las SMB de aceptar servicios de apoyo gubernamentales.

A través de su colaboración con entidades del sector público y privado, la CISA puede contribuir a iniciativas gubernamentales, como la promoción de resultados positivos en ciberseguridad (por ejemplo, una mayor tasa de adopción del SSO). Dicha agencia puede proporcionar publicaciones técnicas, apoyo y recursos de capacitación, y materiales educativos. Además, sus asociaciones sirven como canales eficaces y creíbles para difundir información precisa y procesable, y, al mismo tiempo, aumentar la conciencia, la divulgación y la participación. Además, los posibles esfuerzos conjuntos de colaboración entre el Gobierno y las partes interesadas del SSO ofrecen una oportunidad para que los proveedores clave de servicios de dicho método, las organizaciones que representan a la comunidad de SMB y los proveedores de servicios administrados se reúnan y exploren formas de mejorar las ofertas de servicios de SSO que son más accesibles y asequibles para las SMB.

3 Conceptos básicos del SSO

Los objetivos principales del servicio de SSO son administrar de manera eficiente y efectiva la identidad del usuario y de la organización, crear una ubicación centralizada para acceder a un sistema y establecer archivos de registro coherentes que documenten todos los casos de uso. Conectar todas las aplicaciones comerciales y operativas bajo una gestión de identidad centralizada puede mejorar la eficacia y generar rendimientos. No obstante, la estructura de precios actual y otros desafíos descritos con más detalle en las secciones 5 y 6 obstaculizan significativamente la adopción del SSO. Las organizaciones no pueden aprovechar las ventajas de dicho método y, en cambio, dependen de prácticas manuales de gestión de acceso e identidad (por ejemplo, seguimiento y gestión de contraseñas mediante hojas de cálculo). Un ejemplo de esto es cuando las personas dependen de hojas de cálculo o documentos colaborativos para realizar un seguimiento de sus contraseñas, o cuando los administradores optan por una hoja de cálculo para gestionar todas las contraseñas asociadas a los servicios informáticos. Estas hojas de cálculo compartidas también pueden contener datos sobre errores, viajes y gastos, seguimiento del tiempo y detalles del portal de atención al cliente. Depender de hojas de cálculo manuales para la gestión de identidades, credenciales y accesos conlleva notables dificultades y riesgos potenciales. Las prácticas manuales de gestión de identidades y accesos que se utilizan actualmente se ilustran en la Figura 1.

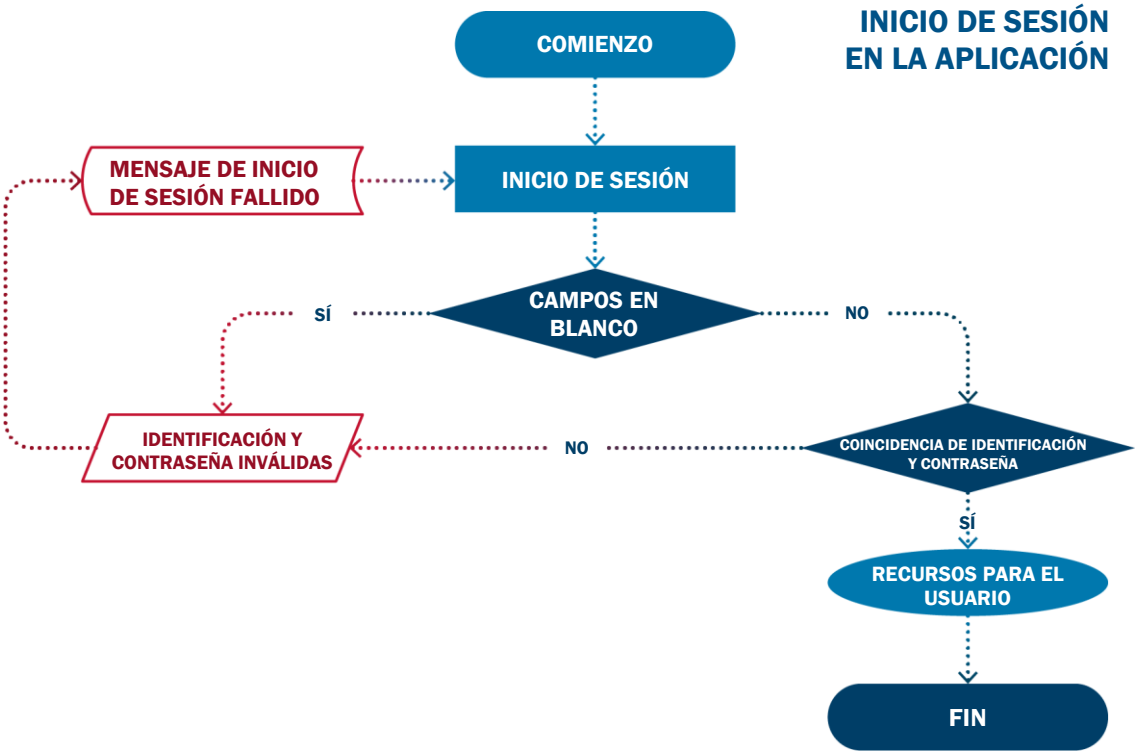

Figura 1: Autenticación de usuarios mediante contraseña

Durante un procedimiento de inicio de sesión estándar, los usuarios deben ingresar sus credenciales, como una identificación de usuario y una contraseña, en los campos designados de la aplicación. Una vez que la autenticación del usuario se completa con éxito, se le concede acceso a los recursos deseados. Sin embargo, si se proporcionan credenciales incorrectas, se muestra un mensaje de error que solicita al usuario que vuelva a ingresar las credenciales correctas. Este proceso se produce de forma independiente para cada una de las aplicaciones que requieren que una persona inicie sesión, con un conjunto separado de credenciales únicas por aplicación y con el administrador realizando un seguimiento manual de las listas de usuarios autorizados para cada aplicación.

Además, la gestión de cada etapa del ciclo de vida de las cuentas de usuario para cada una de las aplicaciones conlleva otro nivel de responsabilidad y carga administrativa. La Figura 2 ilustra el ciclo de vida de las cuentas de usuario, que se describe brevemente más abajo.

Figura 2: Ciclo de vida de las cuentas de usuario

La carga administrativa asociada con la gestión de cuentas de usuario comienza con el establecimiento de una nueva identidad de usuario. Además, abarca un conjunto específico de actividades hasta la desactivación de las cuentas del personal que abandona la organización. En organizaciones más grandes y maduras, una vez que un candidato acepta una oferta de trabajo y se confirma su identidad, el sistema de Recursos Humanos notifica al Departamento de IT para iniciar el proceso de incorporación. Esto implica crear una nueva cuenta de usuario adaptada específicamente al puesto del nuevo empleado dentro de la empresa, con los privilegios correspondientes asignados en consecuencia. Sin embargo, es posible que las SMB no dispongan de un sistema de Recursos Humanos (HR, por sus siglas en inglés) separado ni un Departamento de IT, donde se combina una gestión de acceso a medida con otras funciones. A medida que los empleados avanzan profesionalmente dentro de la organización, sus privilegios pueden ajustarse a los cambios que se produzcan en sus funciones. Las organizaciones deben realizar auditorías periódicas para evaluar diferentes funciones y privilegios asociados a fin de otorgar solo los permisos necesarios. Las cuentas inactivas plantean riesgos potenciales; por lo tanto, cuando un empleado deja la empresa, su cuenta se desactiva de inmediato para mitigar estos riesgos de manera efectiva.

Las empresas que enfrentan el desafío de iniciar sesión en aplicaciones separadas con diferentes credenciales y administrar de forma manual el ciclo de vida de las cuentas de usuario son las que más se beneficiarían del SSO. Esto resulta muy importante para las SMB y aún más fundamental para aquellas que se encuentran por debajo del umbral de la ciberpobreza. El umbral de la ciberpobreza es un punto de división que marca la diferencia entre las organizaciones que pueden y deben desempeñar funciones de ciberseguridad, y aquellas que no pueden y no deben hacerlo.

El SSO proporciona una herramienta unificada e integrada para la gestión de usuarios. El ciclo de vida de las cuentas de usuario se puede gestionar desde una ubicación centralizada, lo que reduce los gastos generales de gestión y evita las cuentas obsoletas. La Figura 3 muestra el proceso de SSO para acceder a múltiples aplicaciones.

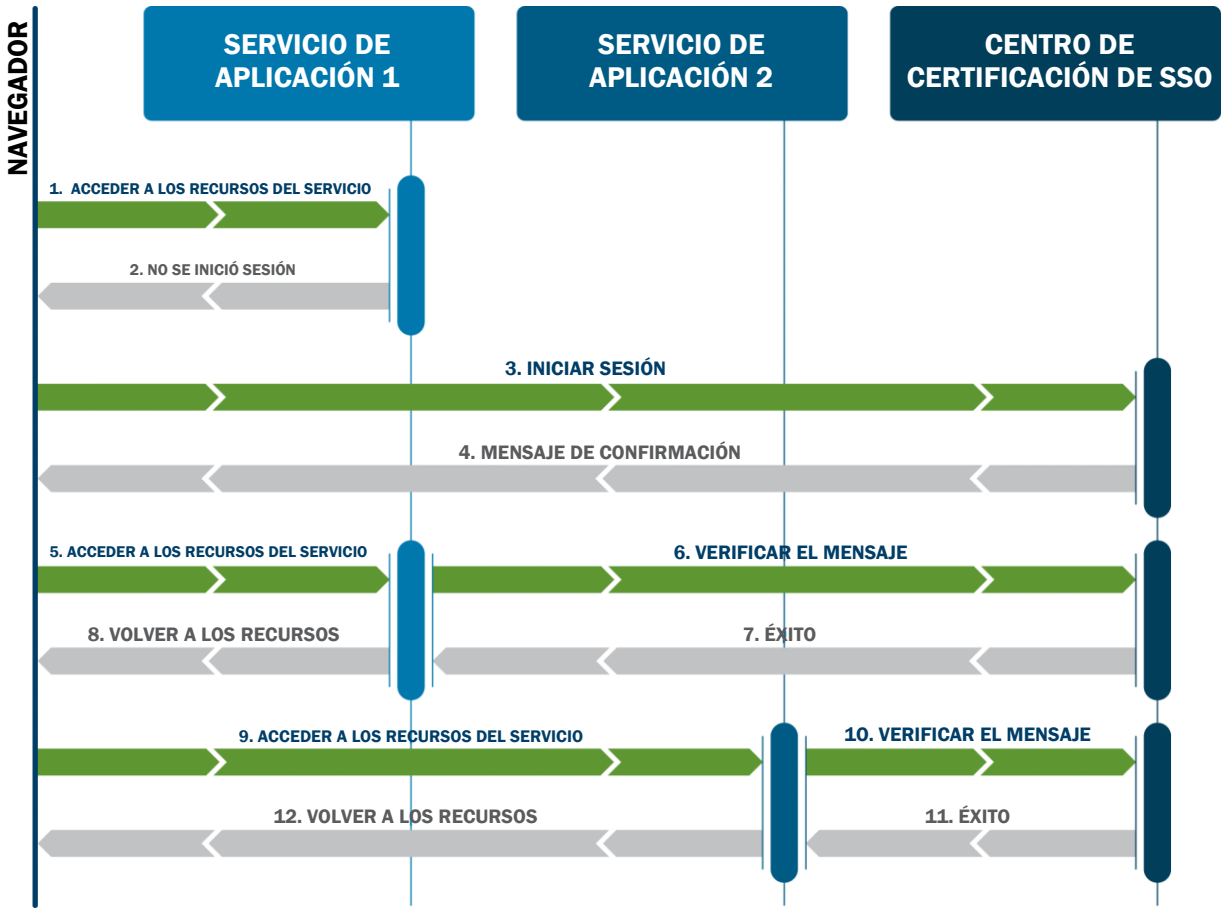

Figura 3. Proceso de SSO para múltiples aplicaciones

El proceso de SSO consta de varios pasos. Inicialmente, cuando un usuario solicita acceso a un servicio de aplicación específico, el servicio le notificará que no ha iniciado sesión y que debe proporcionar sus credenciales de inicio de sesión. Luego, el usuario proporciona las credenciales de inicio de sesión necesarias al Centro de Credenciales de SSO. Este centro emite un mensaje al usuario, en el que confirma su legitimidad. Luego, el usuario repetirá la solicitud inicial para acceder al servicio de la aplicación. El servicio de la aplicación verifica las credenciales del usuario consultando con el Centro de Credenciales de SSO. Dicho centro responde y confirma que el usuario se ha autenticado correctamente. Una vez que el servicio de la aplicación recibe esta confirmación, puede proporcionar los recursos deseados al usuario. Este proceso puede repetirse para servicios de aplicaciones adicionales. La ventaja clave es que el usuario solo necesita proporcionar sus credenciales al Centro de Credenciales de SSO una vez para acceder a múltiples servicios de aplicaciones.

4 Beneficios del SSO

La gestión unificada del acceso con un único conjunto de credenciales tiene múltiples beneficios operativos y resultados positivos en materia de ciberseguridad. La adopción del SSO puede traducirse en una mayor seguridad y privacidad, así como en un inicio de sesión y una experiencia del usuario simplificados y mejorados. Además, dicho método puede ayudar a facilitar el comercio electrónico y la adopción de tecnologías de la información, con prácticas de ciberseguridad más sólidas que podrían servir como factor de diferenciación de productos o servicios. A continuación, se describen brevemente estos beneficios.

Seguridad y privacidad

El SSO puede mejorar la seguridad de la autenticación (Chang y Lee, 2012; Joshi et al., 2018). Los mecanismos de dicho método mejoran la seguridad general de las redes informáticas distribuidas consolidando la autenticación del usuario y reduciendo la necesidad de múltiples contraseñas. Mediante la reducción del riesgo de acceso no autorizado y filtraciones de datos, el SSO proporciona un entorno más seguro para usuarios y empresas. La implementación de este método también puede proteger la privacidad del usuario reduciendo la cantidad de información personal compartida entre proveedores de servicios. Esta protección de la privacidad puede aumentar la confianza del usuario y fomentar la adopción de soluciones de SSO (Urueña et al., 2014).

El SSO también puede subsanar deficiencias en el proceso de cierre de sesión, ya que permite desconectar a los usuarios de todos los servicios conectados. Proporcionando un proceso de cierre de sesión seguro y eficiente, este método puede mejorar la confianza y la satisfacción del usuario en lo que respecta a los sistemas de SSO.

Inicio de sesión y experiencia del usuario simplificados y mejorados

La mejora de la experiencia del usuario es una ventaja importante del SSO, ya que simplifica el proceso de inicio de sesión permitiendo a los usuarios acceder a múltiples servicios con un único conjunto de credenciales (Ramamoorthi y Sarkar, 2020; Komorowski et al., 2016). Además de reducir los costos de asistencia asociados con la gestión de contraseñas, agilizar la experiencia del usuario puede aumentar la productividad y la satisfacción del usuario. La adopción de este método puede facilitar a los usuarios el consumo de contenidos multimedia en distintas plataformas (es decir, contenido de medios cruzados). Esto puede traducirse en una mayor participación de los usuarios y una experiencia de consumo de medios más coherente.

Facilitación del comercio electrónico y adopción de tecnologías de la información

Además de los beneficios directos de la mejora de la ciberseguridad, la adopción del SSO puede tener beneficios auxiliares. Los sistemas de SSO podrían fomentar las transacciones electrónicas entre las SMB mediante la simplificación del proceso de inicio de sesión y la mejora de la seguridad de las empresas en línea. Una mejor experiencia del usuario y una mayor seguridad, así como una mejora de los procesos internos que aumente la eficacia operativa y reduzca la carga del personal, pueden traducirse en un uso más óptimo del tiempo y de los recursos, lo que, a su vez, puede generar mayores ingresos y oportunidades de crecimiento para las SMB de comercio electrónico (Esmaeilpour et al., 2016; Govindaraju y Chandra, 2011).

Además, el SSO ayuda a reducir los obstáculos para la adopción de tecnologías de la información por parte de las SMB optimizando la autenticación de usuarios y el acceso a diversas aplicaciones y servicios (por ejemplo, servicios en la nube). Las funciones de este método pueden aumentar la eficacia organizacional y mejorar su competitividad en el mercado global (Santini et al., 2023; Vu et al., 2022; Blili y Raymond, 1993; Nguyen, 2009; Fink, 1998; Ghobakhloo et al., 2012).

5 Obstáculos y catalizadores de la adopción de tecnología por parte de las SMB

La CISA realizó una revisión bibliográfica para identificar los obstáculos y los catalizadores generales que afectan la adopción de tecnología y la difusión de la innovación entre las SMB. En esta sección, se presenta solo una breve descripción general de la bibliografía disponible (incluida la relativa a la comercialización de los proveedores) que intenta explicar tales obstáculos y catalizadores. El objetivo de resumir las investigaciones más recientes sobre este tema es ampliar los hallazgos específicos del SSO presentados en la Sección 6, que se obtuvieron como parte de los debates de los grupos focales. La revisión bibliográfica mejora estos hallazgos con una comprensión contextual más profunda de un conjunto mucho más amplio de factores y consideraciones que pueden impulsar una decisión de adopción favorable y explicar los motivos. Estos hallazgos son de aplicación directa y ampliamente generalizables a las decisiones de adopción de cualquier tecnología o práctica de ciberseguridad. A continuación, analizamos cómo se relacionan con la adopción del SSO en particular.

Cómo las SMB compran tecnología

Según Riches (2007), y como lo confirman los debates recientes sobre el SSO de la CISA con las SMB, dichas empresas dudan en adoptar cuanto antes las nuevas tecnologías, ya que su principal objetivo es maximizar las ganancias. Sin embargo, a menudo se enfrentan a dificultades para determinar en qué tecnologías invertir,

evaluar los beneficios de estas inversiones y encontrar proveedores fiables que ofrezcan precios razonables. Riches descubrió que las SMB podrían mejorar sus decisiones de compra realizando una investigación de mercado exhaustiva y participando en múltiples debates con desarrolladores de software o proveedores de productos. Esto puede ayudar a dichas empresas a identificar soluciones que se ajusten a su hoja de ruta informática actual y tengan en cuenta sus necesidades de escalabilidad.

Cuando las SMB colaboran estrechamente con los proveedores, puede resultarles más fácil adoptar, implementar y operar soluciones de SSO, lo que puede generar una mejor experiencia del usuario y mensajes favorables para los posibles adoptantes. Además, el nivel de formación y asistencia que ofrecen los proveedores tras la adopción de su solución de dicho método puede crear un fuerte deseo entre estas empresas de buscar servicios adicionales ofrecidos por el proveedor. La disponibilidad de diferentes niveles y opciones de precios, adaptados a diversos modelos de negocio, también influye significativamente en las decisiones de compra de este tipo de empresas.

Hay indicios de que los incentivos gubernamentales también han ayudado a las SMB a adoptar algunas tecnologías de la información. Dreyer y Nygaard (2020) incluyeron ejemplos de diversas formas de apoyo gubernamental (por ejemplo, subvenciones, préstamos, plataformas gratuitas en línea y servicios de consultoría y asesoramiento) que se brindaron durante la pandemia de COVID-19. Entre los ejemplos de ayudas financieras directas, se incluyen las subvenciones del Gobierno irlandés de hasta €2,500 a las SMB que reúnan los requisitos para desarrollar plataformas de comercio electrónico o comercio en línea, o los subsidios del Gobierno japonés para la sostenibilidad, la fabricación y la introducción de las tecnologías de la información a través del Proyecto de Promoción de la Revolución de la Productividad en las Pequeñas y Medianas Empresas (Small and Medium-Sized Enterprise Productivity Revolution Promotion Project). Con incentivos como estos, más SMB pudieron permitirse tecnologías prescritas para ellas, aunque a veces sin tener en cuenta el impacto de la tecnología. Por ejemplo, estos incentivos no abordarían los obstáculos no financieros a los que se enfrentan dichas empresas (por ejemplo, la falta de conocimientos técnicos necesarios para implementar una tecnología). Si se diseñan adecuadamente, los incentivos pueden mejorar la probabilidad de obtener los resultados deseados, al mismo tiempo que evitan consecuencias imprevistas y desfavorables. Para obtener más detalles sobre la eficacia, la eficiencia y la equidad relativas que se asocian a los diversos incentivos destinados a promover las inversiones en ciberseguridad, consulte un estudio exhaustivo de los incentivos que realizó un grupo de trabajo integrado del Departamento de Seguridad Nacional de Estados Unidos (U.S. Department of Homeland Security) (2013).

Factores que influyen en las decisiones de adopción

La necesidad de aumentar la productividad al tiempo que se facilita el acceso al entorno de trabajo impulsa la decisión de adoptar el SSO. Santini et al. (2023) realizaron un metanálisis de 59 estudios sobre la adopción de tecnologías de la información entre las SMB y descubrieron que los recursos y las fuerzas del mercado eran los principales factores predictivos de la adopción de tecnologías de la información. Los recursos incluyen "infraestructura humana y tecnológica que respalda la implementación de la tecnología (por ejemplo, competencia tecnológica e infraestructura informática y tecnológica)" (Santini et al., 2023, p. 637), mientras que las fuerzas del mercado incluyen cambios en el crecimiento tecnológico, cambios en las preferencias del cliente y la cantidad de capital que tiene una empresa.

La reticencia a adoptar una nueva tecnología se debe no solo a la preocupación de tener que incorporar la nueva plataforma, sino también a la necesidad de tener más conocimientos sobre cómo implementarla correctamente. Muchas SMB no cuentan con experiencia interna en ciberseguridad. Algunas de estas empresas subcontratan asistencia únicamente de forma puntual. Si se dispone de experiencia interna, muchos directores de seguridad de la información de las SMB desempeñan múltiples funciones y, a veces, solo dedican una fracción de su tiempo a la ciberseguridad y a la implementación de nuevas tecnologías que harían que el entorno de trabajo sea seguro. En resumen, la asequibilidad, la concienciación, la escalabilidad, la formación, la compatibilidad y la facilidad de integración determinan las decisiones de compra.

Un obstáculo que impide que las SMB adopten soluciones de SSO proviene de la falta de conocimiento técnico. Para aprovechar al máximo las ventajas de la implementación de dicho método, es importante que estas empresas comprendan mejor la información necesaria para su adopción. Además, incluso si los proveedores destacados proporcionan la información necesaria, las SMB deben aprender los conocimientos técnicos y las

modalidades operativas básicas. Muchas de estas empresas evitan este problema, ya que requiere recursos adicionales y conlleva un importante costo de oportunidad.

Modelos de adopción de tecnología y difusión de la innovación

Diversas teorías y modelos explican las razones que subyacen a la toma de decisiones en torno a la adopción de tecnologías de la información. En el campo del marketing cuantitativo, se pueden aplicar varias teorías de adopción clásicas para comprender cómo las SMB adoptan el SSO o las nuevas tecnologías. En los siguientes párrafos se ofrece una breve descripción de estos modelos.

La primera teoría general que puede aplicarse a la adopción del SSO es la teoría de la difusión de la innovación. Esta teoría afirma que la difusión de la innovación es el proceso por el cual una innovación se comunica a través de determinados canales a lo largo del tiempo entre los miembros de un sistema social (Rogers, 2010). La investigación contextual con una perspectiva de la teoría de la difusión de la innovación fue más común en el campo de los sistemas de información para evaluar el valor de los sistemas de planificación de recursos empresariales (Ruivo et al., 2012) y para investigar el proceso de innovación tecnológica (Mamun, 2018).

El segundo conjunto de teorías de adopción clásicas que pueden aplicarse al SSO incluye el modelo de aceptación de la tecnología (Davis et al., 1989) y la teoría unificada de aceptación y uso de la tecnología (Venkatesh et al., 2003). Ambas teorías tienen limitaciones a la hora de analizar si una empresa adoptaría el SSO, ya que se centran más en si un usuario individual de una empresa utilizaría una nueva tecnología y no en si la propia empresa adoptaría una tecnología que se utilizaría en toda la empresa (Davis et al., 1989; Venkatesh et al., 2003).

Además, los factores que conducen a la adopción de tecnología a nivel empresarial son más impulsados por las empresas de forma individual. El modelo de aceptación de la tecnología investiga la aceptación de la tecnología desde la perspectiva del usuario (Yousafzai et al., 2007). Desde esta perspectiva, los usuarios tienden a adoptar nuevas tecnologías por dos razones principales: utilidad percibida y facilidad de uso percibida (Davis et al., 1989). Por el contrario, la teoría unificada de aceptación y uso de la tecnología afirma que la adopción de tecnología se ve influenciada por las expectativas de esfuerzo y rendimiento, las influencias sociales y las condiciones facilitadoras (Venkatesh et al., 2003). La mayor parte de la investigación sobre el modelo de aceptación de tecnología se aplicó a las intenciones de participar en el comercio electrónico de las SMB (Hoque et al., 2015; Herzallah y Mukhtar, 2015, 2016). Salimon et al. (2023) utilizaron el modelo de aceptación de la tecnología y la teoría unificada de aceptación y uso de la tecnología para investigar la adopción de tecnología por parte de las SMB de Malasia, de la que forma parte el SSO.

En otros estudios se han identificado otros factores además de los señalados en las teorías anteriores. Algunos estudios señalan las presiones institucionales como un antecedente esencial de la adopción de las tecnologías de la información a nivel empresarial, ya que las empresas adoptan nuevas tecnologías para proteger mejor su entorno informático (Chwelos et al., 2001; Sila, 2013). Otra perspectiva teórica propone que el entorno institucional, las estructuras organizativas y las prácticas afectan a la adopción de las tecnologías de la información (Goodstein, 1994). Teo et al. (2003) asociaron la adopción de las tecnologías de la información con la obtención de legitimidad social; la respuesta a presiones formales o informales, como la regulación gubernamental, y la satisfacción de las necesidades medioambientales de proveedores, clientes y empresas. Este estudio se basa en paneles de debate y en una revisión bibliográfica limitada.

Sutanonpaiboon y Pearson (2006) descubrieron que la adopción de las tecnologías de la información por parte de las SMB se relacionaba con los recursos financieros y tecnológicos. También señalan que varios tipos de dichas empresas pueden enfrentarse a presiones externas a la hora de integrar dispositivos tecnológicos en su organización. Govindaraju y Chandra (2011) descubrieron que los recursos humanos y las fuentes de información eran los obstáculos más críticos para la adopción de las tecnologías de la información en las SMB de Indonesia. Ghobakhloo et al. (2012) investigaron la función del administrador en la adopción del comercio electrónico en las pequeñas empresas. En este caso, los autores utilizaron la teoría de la difusión de la innovación como base para un modelo teórico. Descubrieron que la utilidad, la facilidad de uso, la compatibilidad con las necesidades específicas de una SMB, los riesgos y la complejidad son factores determinantes de la adopción de las tecnologías de la información por parte de dichas empresas. Esmaeilpour et al. (2016) aplicaron el modelo de aceptación de la tecnología para investigar las actitudes e intenciones de

uso de las tecnologías de la información en las SMB. Descubrieron un efecto positivo de la utilidad y la facilidad de uso sobre la actitud y la intención de comportamiento.

6 La perspectiva de los proveedores y clientes

A pesar de los beneficios operativos y los resultados positivos en materia de ciberseguridad de la gestión de acceso unificado con un único conjunto de credenciales proporcionadas por el SSO descritos en la Sección 4, su adopción sigue siendo lenta, sobre todo entre las SMB. Para comprender mejor los obstáculos más influyentes y los catalizadores de la adopción más allá de lo que pudimos aprender de la revisión bibliográfica, la CISA interactuó con proveedores, proveedores de servicios administrados con experiencia, organizaciones sin fines de lucro dedicadas a mejorar la ciberseguridad, y SMB que tenían experiencia en la adopción de este método y la migración entre sus plataformas. Para proporcionar una perspectiva equilibrada de la dinámica del mercado, en esta sección se analiza el mercado desde la perspectiva de los proveedores y de los clientes del SSO.

La CISA llevó a cabo varios grupos focales y mantuvo debates técnicos con varios tipos de partes interesadas involucradas en el mercado del SSO. Entre los participantes se encontraban proveedores del SSO, auditores de redes informáticas experimentados y SMB, que tienen un gran interés en fomentar la adopción de dicho método y han experimentado de primera mano tanto los obstáculos como los catalizadores. En el apéndice, se presenta una breve descripción del método de investigación utilizado en el estudio y el proceso asociado de participación de las partes interesadas.

A continuación, se presenta un resumen de los factores y las consideraciones clave que influyen en el índice de adopción del SSO basado en las interacciones de la CISA. En general, existen discrepancias significativas entre la percepción de los proveedores y la experiencia y expectativas del cliente en numerosas cuestiones. Algunas de las discrepancias citadas con más frecuencia entre las opiniones de proveedores y clientes incluyen temas como los beneficios de la adopción del SSO y su nivel de prioridad en relación con otras consideraciones comerciales, los costos y las limitaciones de recursos, los desafíos técnicos y el conocimiento de la tecnología, y las dificultades asociadas con la selección de proveedores y la actualización de los sistemas heredados para incorporar la tecnología de dicho método.

Beneficios y prioridades de la adopción

En cuanto a los beneficios de la adopción del SSO, las percepciones entre proveedores y clientes difieren mucho. Los proveedores del SSO reconocen una necesidad urgente de que las organizaciones adopten dicho método debido al aumento de los robos de identidad y a la mejora de los niveles de información sobre amenazas para las SMB (es decir, información que ayuda a las organizaciones a protegerse mejor contra los ciberataques). No obstante, los clientes tienden a ver la adopción del SSO con menos urgencia. Si bien los clientes reconocen la urgencia de abordar con rapidez los problemas relacionados con la seguridad, tienden a priorizar las preocupaciones de seguridad que podrían abordarse con dicho método solo cuando se produce un incidente, ya que un suceso de este tipo puede obligar a los clientes a reconocer la importancia y los beneficios de adoptar el SSO como medida preventiva. Aumentar los conocimientos de los clientes sobre los riesgos potenciales y las ventajas asociadas a la adopción del SSO (en particular, haciendo hincapié en la necesidad de medidas de seguridad proactivas incluso antes de que surja cualquier incidente) podría animar a las SMB a adoptar dicho método antes de lo que lo harían en otras circunstancias.

Las prioridades de adopción del SSO también suelen variar entre proveedores y clientes. Mientras que los proveedores pueden considerar la adopción de dicho método como esencial y una prioridad, los clientes pueden no verlo como tal dada su evaluación de los posibles riesgos de interrupción del servicio y los costos asociados (por ejemplo, el costo de oportunidad del tiempo y la pérdida de productividad debido a las interrupciones de la actividad). A la vista de su evaluación, es posible que no den prioridad a la inversión en este método frente a otros objetivos empresariales, como captar nuevos clientes, conservar los existentes y cumplir la normativa.

Implicaciones financieras y limitación de recursos

La percepción de costos varía significativamente entre proveedores y clientes con respecto a la implementación del SSO. Los proveedores de dicho método y aplicaciones creen que el precio se justifica por sí solo. Los vendedores pueden agrupar servicios para reducir los gastos generales y atraer a clientes con presupuestos

variables, por lo que dejan de centrarse en el costo y se centran en el valor. Existen opciones de precios escalonados que se adaptan a diferentes presupuestos y tamaños de empresa. Sin embargo, algunos clientes sienten que están sujetos a lo que comúnmente se conoce como "impuesto de SSO", porque perciben que dicho método es excesivamente costoso debido al mayor costo del servicio de nivel prémium que incluye este método en comparación con el servicio de nivel inferior que no lo incluye, junto con el requisito de suscribirse a un número mínimo de plazas que puede superar el número real de usuarios. Los clientes también creen que pagan por paquetes redundantes o que se les cobran opciones adicionales que no desean ni necesitan y que no aportan valor por el dinero pagado. La Agencia de Seguridad Nacional (National Security Agency) y la CISA (2023) explican este aspecto en su guía conjunta sobre gestión de identidad y acceso de la siguiente manera:

> En numerosas aplicaciones [de terceros], las funciones del SSO se combinan con otras funciones "empresariales" de gama alta de tal forma que resultan inaccesibles para las pequeñas y medianas organizaciones. Esta práctica empresarial priva a estas organizaciones de los beneficios de seguridad de la [autenticación multifactor] y otras capacidades críticas que derivan de la adopción de dicho método y se basa en la suposición errónea de que se trata de una funcionalidad "empresarial". En el mercado actual, el SSO es una funcionalidad fundamental para organizaciones de todos los tamaños y debe incluirse en cualquier plan de precios dirigido a clientes empresariales, independientemente de su tamaño. (pág. 9)

Las limitaciones de recursos también pueden producir una experiencia de adopción del SSO desfavorable. Los clientes con frecuencia necesitan personal más dedicado para implementar una solución de dicho método. Los que no pueden cubrir sus necesidades de personal deben recurrir a personal con exceso de trabajo y escasa formación, lo que puede provocar dificultades durante la implementación. No obstante, los proveedores suelen asignar recursos dedicados a un proyecto de adopción del SSO y es posible que no sean conscientes de las dificultades que experimenta el cliente y perciban que la implementación avanza según lo previsto.

Los proveedores tienen interés en fomentar la adopción del SSO; sin embargo, a veces presentan un argumento comercial a favor de dicho método que no siempre refleja con exactitud las limitaciones y los objetivos de las SMB. Existe un incentivo inherente para convencer a dichas empresas de que adopten tecnologías a un nivel de servicio que no necesariamente las beneficiará. Estas prácticas de ventas adicionales implican incorporar o agrupar niveles de paquetes o servicios innecesarios junto con algunos que pueden ser útiles para las empresas que los compran. Algunos proveedores vincularán a algunas SMB al nivel de servicio que hayan elegido, aunque esté infrautilizado. Dicha información y experiencias de adopción negativas impactan las decisiones de adopción de otras empresas.

Conocimientos y conciencia técnicos

Los proveedores confían en que ofrecen suficientes materiales de capacitación y guías prácticas para ayudar a los clientes a implementar de forma eficaz la tecnología de SSO. Creen que las organizaciones deberían poder superar cualquier obstáculo técnico asociado con su implementación; no obstante, los clientes tienen diferentes percepciones y experiencias de usuario. Ven este método como una solución compleja con numerosas partes móviles que pueden impedir su implementación exitosa, por lo que se convierte en un posible obstáculo para su adopción. Antes de que los clientes se planteen adoptarlo, hay que resolver estos problemas de implementación.

Además, los clientes tienen distintos grados de satisfacción con la exactitud e integridad del material de apoyo y las instrucciones proporcionados. Incluso algunos de los usuarios con más experiencia y conocimientos técnicos han informado de la necesidad de enviar numerosos tickets de asistencia y entablar múltiples interacciones con el personal de atención al cliente de su proveedor para subsanar las deficiencias o resolver las inexactitudes y omisiones. Para las SMB con recursos limitados, el costo de oportunidad de ese tiempo hace que la implementación adecuada del SSO resulte muy costosa y provoque una experiencia de usuario negativa desde el principio.

En cuanto a la conciencia tecnológica, los proveedores a menudo ven el SSO como una práctica de seguridad estándar mínima que todas las organizaciones deben seguir, independientemente de su tamaño o industria. Destacan sus beneficios más allá de la seguridad (por ejemplo, la posible reducción de los costos del seguro cibernético para las SMB). No obstante, los clientes tienen perspectivas diferentes. Algunos lo ven como un valor agregado que mejora su postura de seguridad, mientras que otros lo ven como un gasto innecesario que

no aporta mejoras operativas significativas ni rendimientos acordes. Este último punto de vista puede reflejar una falta de conocimiento de todos los beneficios que el SSO puede brindar y resalta la necesidad de transmitir mensajes claros sobre sus ventajas.

Rivalidad entre proveedores y desafíos de los sistemas heredados

El mercado de soluciones de SSO es altamente competitivo. Como tal, los proveedores ofrecen distintos servicios y tecnologías que permiten flexibilidad. Intentan agilizar el proceso de selección mediante la publicación de datos de marketing y detalles técnicos. Sin embargo, los clientes pueden sentirse abrumados durante este proceso. A menudo, confían en opiniones de clientes poco fiables o en recomendaciones de soluciones que no se ajustan a sus necesidades. Es posible que tomen decisiones basadas en información sesgada y no verificada, y no totalmente en un sólido análisis de las ventajas y desventajas del proveedor que tenga en cuenta sus necesidades y peculiaridades empresariales.

La compatibilidad del SSO y su interoperabilidad con sistemas heredados también es un desafío. Los clientes pueden tener plataformas existentes que necesitan ayuda para adaptarse a las nuevas ofertas tecnológicas de dicho método. Para su adopción, estos clientes primero deben invertir en actualizar los sistemas heredados. Los clientes también suelen confiar en aplicaciones independientes más antiguas creadas con tecnología obsoleta y consideran que la implementación del SSO es disruptiva y de alto riesgo, dadas las importantes actualizaciones necesarias en las tecnologías existentes.

Dichos clientes pueden necesitar pruebas precisas y concluyentes de los beneficios de este método, así como descripciones de su rendimiento operativo real y de la experiencia de los usuarios proporcionadas por anteriores adoptantes a través de un canal de difusión de información fiable y acreditada. Dicha información puede ayudarlos a evaluar si los beneficios a largo plazo de la adopción compensan las molestias temporales que pueda causar la implementación del SSO. Además, la adopción también puede depender de la capacidad de las SMB para conseguir financiación. La dependencia de sistemas heredados muy obsoletos suele ser consecuencia de circunstancias financieras limitadas durante un período prolongado. Por lo tanto, incluso con un análisis de costos y beneficios favorable, es posible que no se pueda llevar a cabo una mejora que requiera un importante desembolso de capital inicial.

En la actualidad, muchas SMB utilizan sistemas obsoletos para sus operaciones diarias. Por desgracia, algunas plataformas no disponen de la tecnología necesaria para soportar una solución de inicio de sesión moderna y escalable. Para implementar una solución de SSO, puede ser necesario desmantelar partes o todo el entorno informático existente. Este tipo de actualización podría percibirse como una implementación lenta que supondría una carga innecesaria para las operaciones diarias de la organización. La reticencia a llevar a cabo una revisión significativa del entorno podría retrasar u obstaculizar la adopción del SSO y cualquier otra nueva tecnología (Teo et al., 2003).

7 Conclusión

Tanto la revisión bibliográfica como los esfuerzos de la CISA que incluyeron grupos focales y debates técnicos de seguimiento identifican varios conjuntos de beneficios, desafíos y otras consideraciones asociadas con la adopción del SSO por parte de las SMB.

Beneficios del SSO

Para aprovechar al máximo las ventajas del SSO, las SMB deben comprender que mejora la productividad al minimizar la cantidad de intentos de inicio de sesión necesarios para acceder a múltiples sistemas. Además, este método fortalece las medidas de seguridad al reducir la exposición de las contraseñas. Normalmente, las personas suelen reutilizar la misma contraseña en varios sistemas, lo que se considera un comportamiento riesgoso. Este comportamiento se puede abordar mediante la implementación del SSO. Las SMB también pueden aprovechar los beneficios de este método al administrar eficazmente las cuentas de usuario desde una ubicación centralizada, lo que agiliza la gestión de usuarios y minimiza el riesgo de las cuentas no gestionadas. Además, el SSO es un habilitador para otras tecnologías y el comercio electrónico. Simplifica el proceso de gestión de las identidades de los usuarios finales en línea. Para muchas SMB, las aplicaciones de comercio electrónico pueden traducirse en una fuente adicional de ingresos.

Desafíos de las SMB al implementar el SSO

Implementar soluciones de SSO puede representar todo un desafío para las SMB. Tanto los costos financieros como las cargas no financieras asociadas al cambio a una nueva solución tecnológica constituyen obstáculos clave que dificultan la implementación de este método. El costo de entrada es un factor importante, ya que implica una inversión inicial elevada. La capacitación plantea un desafío adicional para muchas SMB que necesitan más experiencia técnica para administrar una solución de SSO de forma independiente. Además, algunas de estas empresas que ya se han comprometido a un contrato a largo plazo o cerrado con un proveedor específico pueden tener dificultades para cambiar de proveedor sin penalizaciones ni problemas de integración. Por último, la falta de conocimientos técnicos entre las SMB puede impedir la implementación de una solución de SSO, sobre todo a la hora de garantizar la interoperabilidad con las infraestructuras existentes.

Prácticas comerciales de proveedores

Varios proveedores ofrecen descuentos para atraer a los clientes a la compra de varios programas y servicios de software. Una estrategia eficaz consiste en ofrecer descuentos escalonados en función de los servicios agrupados. Además, el objetivo de los proveedores es establecer un sistema de gestión de relaciones con el cliente para mejorar la satisfacción de los clientes de las SMB. Al analizar los datos recopilados a través del sistema de gestión de relaciones con el cliente, los proveedores pueden obtener información más profunda sobre las necesidades específicas de dichas empresas y proporcionar soluciones personalizadas en consecuencia.

Necesidades de las SMB

Las SMB buscan atributos específicos en una solución de SSO. Tiene que ser escalable para que pueda alojar a más usuarios a medida que la empresa crece. La asequibilidad es crucial para dichas empresas a corto y largo plazo, por lo que se considera importante un costo inicial bajo. Las SMB valoran mucho la facilidad de uso de una solución de SSO, ya que a menudo necesitan más habilidades para gestionarla. Estas empresas clasificaron la atención al cliente como una de las funcionalidades más importantes de este método. Como dichas empresas suelen tener una experiencia técnica limitada, prefieren evitar modificar la solución y confiar en el proveedor para obtener orientación y asistencia durante la fase inicial de implementación del SSO.

8 Recomendaciones

A partir de lo que la CISA averiguó en este estudio, identificó recomendaciones generales para SMB, proveedores de SSO, organismos gubernamentales y organizaciones sin fines de lucro destinadas a animar a dichas empresas a adoptar soluciones de dicho método, ayudándolas a garantizar una implementación exitosa y sin inconvenientes, a la vez que brindan mayor seguridad y acceso simplificado a los usuarios.

Recomendaciones para las SMB

La aplicación de un enfoque sistemático para el SSO facilitará su implementación en entornos de SMB. Recomendamos que estas empresas utilicen un enfoque como el siguiente. Comience analizando las necesidades de la organización, como la cantidad de usuarios, las aplicaciones y los requisitos de seguridad. Esta evaluación ayudará a determinar la solución de SSO más adecuada. Busque opciones asequibles (por ejemplo, soluciones basadas en la nube que no requieran una infraestructura extensa). Compare las características y la compatibilidad de diferentes las soluciones proporcionadas por los numerosos proveedores del mercado. Evalúe qué tan bien se integran con la infraestructura y las aplicaciones existentes. Realice un proyecto piloto para minimizar los riesgos y probar la eficacia de la solución antes de implementarla en toda la organización. Capacite al personal y proporcione pautas claras para la gestión de contraseñas y prácticas de seguridad. Supervise continuamente la solución de SSO para reforzar la postura general de seguridad.

Recomendaciones para los proveedores

Según los comentarios de los usuarios, los proveedores pueden mejorar significativamente sus ofertas de servicios mediante la implementación de las siguientes recomendaciones. Los proveedores deben (a) recopilar los requisitos de los clientes y ofrecer soluciones personalizadas que satisfagan sus necesidades, y al mismo tiempo eliminar los servicios innecesarios; (b) ofrecer umbrales o requisitos de acceso más flexibles; y (c) mejorar la precisión e integridad de los materiales de asistencia para su conjunto esencial de servicios, como el SSO.

En primer lugar, los servicios básicos y esenciales, como el SSO, deberían desvincularse de los paquetes con servicios prémium. Los proveedores deben evitar las técnicas de venta adicional, mediante las cuales venden servicios innecesarios a las SMB. Si bien la agrupación de productos es una estrategia de precios reconocida para extraer el máximo beneficio del consumidor, la necesidad de servicios cibernéticos esenciales para proteger y defender infraestructuras críticas y organizaciones pobres en cibernética y ricas en objetivos no debe aprovecharse para vender servicios prémium que pueden no tener el mismo atractivo o valor añadido. Por el contrario, debería animar a los clientes a solicitar servicios adicionales para mejorar su situación general de seguridad cuando sea necesario.

En segundo lugar, los proveedores deberían proporcionar un calendario más flexible de umbrales o requisitos de acceso que permitan una personalización significativa del servicio en función del tamaño de la organización. Específicamente, para las SMB, debe prestarse especial atención a la agrupación de licencias de SSO a nivel de proveedor de servicios gestionados o a nivel de grupo de dichas empresas, en lugar de hacerlo a nivel de organización de abonado individual.

En tercer lugar, es fundamental que los proveedores ofrezcan a las SMB la asistencia y capacitación necesarias. Para reducir el número de llamadas y la cantidad de asistencia técnica que necesitan dichas empresas para implementar y mantener correctamente el SSO, debería mejorarse significativamente la calidad de las instrucciones que se dan a los usuarios por adelantado. En sus comentarios sobre la experiencia de usuario, los usuarios subrayan sistemáticamente que las instrucciones son incompletas, vagas y a menudo imprecisas. Este último factor es un obstáculo no solo para la adopción de dicho método, sino que también se manifiesta cuando los usuarios existentes intentan migrar de plataforma. En conjunto, estos tres factores (es decir, la inclusión del SSO en paquetes con servicios prémium, umbrales y requisitos de acceso inflexibles, e instrucciones inexactas e incompletas) dan como resultado una experiencia de usuario negativa, que influye negativamente en las decisiones de adopción de los posibles adoptantes de este método.

Recomendaciones para los organismos gubernamentales

Los organismos gubernamentales, como el Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology), la CISA y la Administración de Servicios Generales (General Services Administration), pueden ayudar a resaltar las prácticas recomendadas, brindar orientación y producir guías para compradores relacionadas con tecnologías, como el SSO, que se alineen con las recomendaciones de seguridad actuales. Además, el Gobierno podría considerar la posibilidad de ofrecer incentivos que fomenten la adopción de tecnologías de seguridad, como el SSO. Un estudio exhaustivo de incentivos realizado por un grupo de trabajo integrado del Departamento de Seguridad Nacional de Estados Unidos (2013) contiene un análisis detallado de las posibles opciones.

Recomendaciones para las organizaciones sin fines de lucro

Las organizaciones sin fines de lucro relevantes dedicadas a mejorar la ciberseguridad (por ejemplo, la Alianza Cibernética Global [Global Cyber Alliance] y la Alianza Nacional de Ciberseguridad [National Cybersecurity Alliance]) pueden interactuar con el público sobre el tema de las soluciones del SSO como parte de su participación comunitaria. Esta participación comunitaria desempeña una función vital a la hora de capacitar a las SMB sobre las ventajas de la tecnología de SSO. Además, durante sus interacciones habituales con SMB, estas organizaciones sin fines de lucro recopilan información valiosa sobre los requisitos de dichas empresas, que se puede utilizar para ofrecerles servicios y conjuntos de herramientas personalizados.

Apéndice: metodología de participación de las partes interesadas

La CISA eligió una muestra de conveniencia[1] de proveedores de SSO basándose en el Magic Quadrant de Gartner,[2] las relaciones industriales existentes y una investigación de mercado más amplia. La lista de participantes se amplió mediante un muestreo de bola de nieve, en el que los participantes iniciales identificaron otros contactos de interés. Dicha agencia utilizó una técnica similar para identificar proveedores de servicios gestionados, auditores de red experimentados y SMB con experiencia en la adopción del SSO.

Luego, la CISA llevó a cabo grupos focales con varios grupos de partes interesadas involucradas en el SSO. Entre los participantes en estos debates se encontraban proveedores del SSO, auditores de redes informáticas experimentados y SMB, que tienen un gran interés en fomentar la adopción de dicho método y han experimentado de primera mano tanto los obstáculos como los catalizadores. En este estudio, se analizan los factores que influyen en la adopción mediante el examen de las pautas y tendencias reveladas durante estos debates. La participación de las partes interesadas y los debates técnicos continuaron hasta que se abordó un conjunto básico de consideraciones hasta que ya no se presentó nueva información adicional en la divulgación posterior.

Diseño de la investigación

La CISA utilizó un diseño de investigación cualitativa para obtener un conocimiento profundo de los catalizadores y los obstáculos para la adopción del SSO. Las conversaciones individuales ayudaron a dicha agencia a obtener información de los participantes y comprender sus experiencias a través de debates semiestructurados que permitieron una investigación más profunda sobre temas específicos, al tiempo que se mantenía un marco uniforme en todos los debates.

Método de recopilación de datos

La CISA recopiló datos a través de conversaciones individuales con cada participante, ya sea cara a cara, por teléfono o por videoconferencia, según su disponibilidad y preferencia. Dicha agencia transcribió las conversaciones y revisó las notas para su posterior análisis. Además, sintetizó y agregó los hallazgos de una manera que preserva el anonimato y evita la reidentificación en la medida de lo posible.

Fuentes de datos

La CISA eligió participantes de diversos orígenes para obtener una perspectiva amplia y equilibrada de la adopción del SSO. La muestra estuvo formada por representantes de proveedores de SSO, auditores de redes informáticas con amplia experiencia en auditorías de dicho método y SMB que adoptaron o contemplan adoptar estas soluciones.

Validez y fiabilidad

La CISA utilizó varias estrategias para mejorar la validez y fiabilidad de los hallazgos. Primero, seleccionó participantes con experiencia relevante en el dominio del SSO. El muestreo intencional es una técnica ampliamente utilizada en la investigación cualitativa para la identificación y selección de casos con mucha información para el uso más eficaz de recursos limitados. Luego, dicha agencia adoptó técnicas de verificación de miembros, donde los participantes recibieron un resumen de los hallazgos con la oportunidad de recibir comentarios o aclaraciones de los demás asistentes. Además, la CISA celebró sesiones informativas entre investigadores para revisar el proceso de análisis de datos y garantizar una interpretación precisa de los hallazgos. Asimismo, tiene previsto un compromiso de seguimiento y extensión a la comunidad de SMB a través de la Alianza Cibernética Global. Además, la CISA tiene previsto organizar mesas de debate y grupos focales para validar los hallazgos de este estudio con un conjunto más amplio de usuarios actuales y potenciales del SSO.

[1] Una muestra de conveniencia es un tipo de muestra en el que se utilizará la primera fuente de datos primaria disponible para la investigación sin requisitos adicionales.

[2] El Magic Quadrant de Gartner es una serie de informes de investigación de mercado publicados por la firma de consultoría informática Gartner que se basan en métodos patentados de análisis de datos cualitativos para demostrar las tendencias del mercado, como la dirección, la madurez y los participantes (Teixeira et al., 2022).

Limitaciones

El hecho de que este estudio se base en una muestra de conveniencia de participación voluntaria tiene limitaciones reconocidas. En concreto, como en cualquier debate voluntario, existe una muestra limitada de participantes con un sesgo de autoselección inherente, por lo que la inferencia estadística de los resultados de la muestra sobre el resto de la población (más allá de los encuestados reales) no es apropiada. Por lo tanto, los resultados no se pueden generalizar para toda la población de SMB. Es posible que el tamaño y la composición de la muestra no representen con precisión todos los aspectos del ecosistema de SSO. Además, la información recopilada depende de las experiencias personales de los participantes, por lo que se asume que se presentan relatos honestos y precisos de sus experiencias con la adopción de dicho método. El hecho de que este estudio se centre en datos cualitativos relativos a una solución de ciberseguridad específica (es decir, el SSO) podría limitar la generalizabilidad en otros contextos.

Referencias

Armando, A., Carbone, R., Compagna, L., Cuéllar, J., Pellegrino, G., & Sorniotti, A. (2013). An authentication flaw in browser-based Single Sign-On protocols: Impact and remediations. *Computers & Security*, 33, 41–58. https://doi.org/10.1016/j.cose.2012.08.007

Blili, S., & Raymond, L. (1993). Information technology: Threats and opportunities for small and medium-sized enterprises. *International Journal of Information Management*, *13*(6), 439–448. https://doi.org/10.1016/0268-4012(93)90060-H

Bracken, B. (2023, November 30). *Okta Breach Widens to Affect 100% of Customer Base*. DarkReading. https://www.darkreading.com/application-security/otka-breach-widens-entire-customer-base

Bradbury, D. (2023, October 20). *Tracking unauthorized access to Okta's support system*. Okta. https://sec.okta.com/articles/2023/10/tracking-unauthorized-access-oktas-support-system

Chang, C.-C., & Lee, C.-Y. (2012). A secure single sign-on mechanism for distributed computer networks. *IEEE Transactions on Industrial Electronics*, *59*(1), 629–637. https://doi.org/10.1109/TIE.2011.2130500

Chwelos, P., Benbasat, I., & Dexter, A. S. (2001). Research report: Empirical test of an EDI adoption model. *Information Systems Research*, *12*(3), 304–321. https://doi.org/10.1287/isre.12.3.304.9708

Cusack, B., & Ghazizadeh, E. (2016). Evaluating single sign-on security failure in cloud services. *Business Horizons*, *59*(6), 605–614. https://doi.org/10.1016/j.bushor.2016.08.002

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, *35*(8), 982–1003. https://doi.org/10.1287/mnsc.35.8.982

D'Costa-Alphonso, M.-M., & Lane, M. (2010). The adoption of single sign-on and multifactor authentication in organisations – A critical evaluation using TOE framework. *Issues in Informing Science and Information Technology Education*, *7*, 161–189. https://doi.org/10.28945/1199

Dreyer, M., & Nygaard, K. (2020, June 15). Governments encourage SMEs to adopt new technology. Yale School of Management. https://som.yale.edu/blog/governments-encourage-smes-to-adopt-new-technology

Esmaeilpour, M., Hoseini, S. Y., & Jafarpour, Y. (2016). An empirical analysis of the adoption barriers of E-commerce in small and medium sized enterprises (SMEs) with implementation of Technology Acceptance Model. *Journal of Internet Banking and Commerce*, *21*(2).

Fink, D. (1998). Guidelines for the successful adoption of information technology in small and medium enterprises. *International Journal of Information Management*, *18*(4), 243–253. https://doi.org/10.1016/S0268-4012(98)00013-9

Ghobakhloo, M., Hong, T. S., Sabouri, M. S., & Zulkifli, N. (2012). Strategies for successful information technology adoption in small and medium-sized enterprises. *Information*, *3*(1), 36–67. https://doi.org/10.3390/info3010036

Goodstein, J. D. (1994). Institutional pressures and strategic responsiveness: Employer involvement in work-family issues. *The Academy of Management Journal*, *37*(2), 350–382.

Govindaraju, R., & Chandra, D. R. (2011). E-commerce adoption by Indonesian small, medium, and micro enterprises (SMMEs): Analysis of goals and barriers. *2011 IEEE 3rd International Conference on Communication Software and Networks*, 113–117. https://doi.org/10.1109/ICCSN.2011.6014861

Herzallah, F., & Mukhtar, M. (2015). The impact of internal organization factors on the adoption of e-commerce and its effect on organizational performance among Palestinian small and medium enterprise. *International Conference on E-Commerce (IcoEC) 2015*.

Herzallah, F., & Mukhtar, M. (2016). The impact of perceived usefulness, ease of use and trust on managers' acceptance of e-commerce services in small and medium-sized enterprises (SMEs) in Palestine. *International Journal on Advanced Science Engineering and Information Technology*, *6*(6), 922–929.

Hoque, M. R., Ali, M. A., & Mahfuz, M. A. (2015). An empirical investigation on the adoption of e-commerce in Bangladesh. *Asia Pacific Journal of Information Systems*, *25*(1), 1–24. http://doi.org/10.14329/apjis.2015.25.1.001

Joshi, U., Cha, S., & Esmaili-Sardari, S. (2018). Towards adoption of authentication and authorization in identity management and Single Sign On. *Advances in Science, Technology and Engineering Systems Journal*, *3*(5), 492–500. https://doi.org/10.25046/aj030556

Komorowski, M., Coppens, P., Van den Broeck, W., & Braet, O. (2016). Lowering the barriers for online cross-media usage: Scenarios for a Belgian single sign-on solution. *Telematics and Informatics*, *33*(4), 916–924. https://doi.org/10.1016/j.tele.2016.02.005

Mamun, A. A. (2018). Diffusion of innovation among Malaysian manufacturing SMEs. *European Journal of Innovation Management*, *21*(1): 113–141. https://doi.org/10.1108/EJIM-02-2017-0017

National Security Agency & Cybersecurity and Infrastructure Security Agency. (2023, October 4). *Identity and access management: Developer and vendor Challenges*. https://media.defense.gov/2023/Oct/04/2003313510/-1/-1/0/ESF%20CTR%20IAM%20MFA%20SSO%20CHALLENGES.PDF

Newman, L. (2023, November 23). Okta Breach Impacted All Customer Support Users—Not 1 Percent. Wired. https://www.wired.com/story/okta-breach-disclosure-all-customer-support-users/#:~:text=Okta%20upped%20its%20original%20estimate,%2C%20citing%20a%20%E2%80%9Cdiscrepancy.%E2%80%9D&text=In%20late%20October%2C%20the%20identity,of%20its%20customer%20support%20system

Nguyen, T. H. (2009). Information technology adoption in SMEs: an integrated framework. *International Journal of Entrepreneurial Behavior & Research*, *15*(2), 162–186. https://doi.org/10.1108/13552550910944566

Quirt, B; Singh, P; Sparling, C. (2022). SMBs: The next growth opportunity for high tech. https://www.accenture.com/us-en/blogs/high-tech/smbs-the-next-growth-opportunity-for-high-tech

Ramamoorthi, L. S., & Sarkar, D. (2020). Single Sign-On: A solution approach to address inefficiencies during sign-out process. *IEEE Access*, *8*, 195675–195691. https://doi.org/10.1109/ACCESS.2020.3033570

Riches, T. (2007). The challenge of supporting new technology adoption by SMBs. *Database and Network Journal*, *37*(3).

Rogers, E. M. (2010). *Diffusion of innovations* (4th ed.). Simon and Schuster.

Ruivo, P., Oliveira, T., & Neto, M. (2012). ERP use and value: Portuguese and Spanish SMEs. *Industrial Management & Data Systems*, *112*(7), 1008–1025. http://doi.org/10.1108/02635571211254998

Salimon, M. G., Kareem, O., Mokhtar, S. S. M., Aliyu, O. A., Bamgbade, J. A., & Adeleke, A. Q. (2023). Malaysian SMEs m-commerce adoption: TAM 3, UTAUT 2 and TOE approach. *Journal of Science and Technology Policy Management*, *14*(1), 98–126. https://doi.org/10.1108/JSTPM-06-2019-0060

Santini, F. d. O., de Matos, C. A., Ladeira, W. J., Jardim, W. C., & Perin, M. G. (2023). Information technology adoption by small and medium enterprises: a meta-analysis. *Journal of Small Business and Entrepreneurship*, *35*(4), 632–655. https://doi.org/10.1080/08276331.2022.2145787

Sila, I. (2013). Factors affecting the adoption of B2B e-commerce technologies. *Electronic Commerce Research, 13*(2), 199–236. https://doi.org/10.1007/s10660-013-9110-7

Sutanonpaiboon, J., & Pearson, A. M. (2006). E-commerce adoption: Perceptions of managers/owners of small- and medium-sized enterprises (SMEs) in Thailand. *Journal of Internet Commerce*, *5*(3), 53–82. https://doi.org/10.1300/J179v05n03_03

Teixeira, H., Data, A., Kelley, M., Hoover, J., & Guthrie, B. (2022). *Gartner, Magic Quadrant for Access Management*.

Teo, H. H., Wei, K. K., & Benbasat, I. (2003). Predicting intention to adopt interorganizational linkages: An institutional perspective. *MIS Quarterly*, *27*(1), 19–49. https://doi.org/10.2307/30036518

Urueña, M., Muñoz, A., & Larrabeiti, D. (2014). Analysis of privacy vulnerabilities in single sign-on mechanisms for multimedia websites. *Multimedia Tools and Applications*, *68*(1), 159–176. https://doi.org/10.1007/s11042-012-1155-4

U.S. Department of Homeland Security Integrated Task Force. (2013, June 12). *Executive Order 13636: Improving critical infrastructure cybersecurity*. https://www.cisa.gov/sites/default/files/2023-01/19_1115_dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf

U.S. Small Business Administration. (2023). *Frequently Asked Questions About Small Business.* Office of Advocacy. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjPqMKXvMeDAxUYD1kFHZkHApcQFnoECA4QAw&url=https%3A%2F%2Fadvocacy.sba.gov%2Fwp-content%2Fuploads%2F2023%2F03%2FFrequently-Asked-Questions-About-Small-Business-March-2023-508c.pdf&usg=AOvVaw1q6D9GShZFxP4KyOUe0oEq&opi=89978449

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3) 425–478. https://doi.org/10.2307/30036540

Vu, N. H., Bui, T. A., Hoang, T. B., & Pham, H. M. (2022). Information technology adoption and integration into global value chains: Evidence from small- and medium-sized enterprises in Vietnam. *Journal of International Development*, *34*(2), 259–286. https://doi.org/10.1002/jid.3591

Yousafzai, S. Y., Foxall, G. R., & Pallister, J. G. (2007). Technology acceptance: A meta-analysis of the TAM: Part 1. *Journal of Modelling in Management*, *2*(3), 251–280. https://doi.org/10.1108/17465660710834453

Glosario

Autenticación: validación de una identidad como verdadera o falsa, generalmente utilizada para verificar que un usuario es quien dice ser. Por lo general, se logra mediante una combinación de nombre de usuario y contraseña, pero el mismo principio se aplica a otras formas de autenticación, como preguntas secretas, enlaces secretos e identificación biométrica.

Comercio electrónico: compra y venta de bienes y servicios en línea.

Falsificación de solicitud entre sitios: ataque que obliga a los usuarios autenticados a enviar una solicitud a una aplicación web en la que están autenticados en ese momento. Los ataques de falsificación de solicitud entre sitios explotan la confianza que una aplicación web tiene en un usuario autenticado.

Gestión de accesos: administración de los inicios de sesión y las contraseñas de los usuarios en una variedad de aplicaciones y recursos, generalmente contenidos dentro de una única organización.

Inicio de sesión único (SSO): método de identificación que permite a los usuarios iniciar sesión en múltiples aplicaciones y sitios web con un solo conjunto de credenciales.

Pequeñas y medianas empresas (SMB): si bien la Administración de Pequeñas Empresas (SBA, por sus siglas en inglés) tiene una definición establecida de pequeña empresa, el límite de empleados y de ingresos varía según el sector. En general, la Oficina de Defensa (Office of Advocacy) de la SBA define una pequeña empresa como una empresa independiente con menos de 500 empleados[3]. Para conocer los estándares de tamaño de las pequeñas empresas a nivel industrial utilizados en los programas y contratos gubernamentales, consulte la Tabla de estándares de tamaño en https://www.sba.gov/document/support-table-size-standards. No existe una definición fija de mediana empresa. Sin embargo, según los comentarios del sector, una empresa con menos de 100 empleados suele considerarse pequeña, mientras que una con entre 100 y 999 empleados se considera mediana.

Proveedor de identidades: sitio web, aplicación o servicio responsable de coordinar las identidades entre usuarios y clientes. Un proveedor de identidades puede proporcionar a un usuario información de identificación y compartir esa información con servicios cuando el usuario solicita acceso.

Seguridad de la información: práctica de proteger la información mediante la mitigación de sus riesgos. Forma parte de la gestión de riesgos de la información.

Tecnología de la información (IT): uso de computadoras para crear, procesar, almacenar, recuperar e intercambiar datos e información.

[3] U.S. Small Business Administration. (2023). *Frequently Asked Questions About Small Business.* Office of Advocacy. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjPqMKXvMeDAxUYD1kFHZkHApcQFnoECA4QAw&url=https%3A%2F%2Fadvocacy.sba.gov%2Fwp-content%2Fuploads%2F2023%2F03%2FFrequently-Asked-Questions-About-Small-Business-March-2023-508c.pdf&usg=AOvVaw1q6D9GShZFxP4KyOUe0oEq&opi=89978449