Microsoft

Seis pasos para crear una estrategia de seguridad integral con Microsoft 365

Tabla de contenido

Seis pasos para crear una estrategia de seguridad integral con Microsoft 365

Proteger los datos y los sistemas es una prioridad esencial para las organizaciones. Pero cumplir este reto resulta cada vez más difícil, ya que los ataques son más sofisticados, los empleados usan una variedad más amplia de dispositivos y aplicaciones, y los datos entran y salen de tu empresa de más maneras.

Los líderes tienen que equilibrar estos retos con la necesidad de colaborar, innovar y hacer crecer una empresa. Necesitas un enfoque de seguridad de varios frentes que proteja de forma continua todos los puntos de conexión, identifique los indicios tempranos de una infracción y responda cuando se produzcan daños. Y, no importa lo buenas que sean tus defensas: las medidas de prevención ya no son suficientes y también necesitas adoptar una postura de "dar por hecho la infracción" en la que se incluya también la detección y las medidas de respuesta.

La administración de riesgos es ahora una obligación para muchos directores de seguridad de la información. Trata de minimizar el posible impacto de los ataques cada vez más sofisticados al proteger de forma más eficaz un creciente número de usuarios, dispositivos, aplicaciones, datos e infraestructura con menos personas.

Los directores de seguridad de la información en la actualidad, necesitan marcos de seguridad ágiles que permitan la transformación digital, apoyada por estrategias integrales que se integren en las tecnologías, los procesos y los programas de aprendizaje. En este e-book conocerás las estrategias y los procedimientos recomendados de directores de seguridad de la información que consiguieron que la seguridad fuera la piedra angular del éxito de su negocio.

> *Necesitas estar preparado cada hora del día. Y eso significa que necesitas adoptar esta posición de seguridad operativa de forma continuada.*
>
> **Satya Nadella,**
> *consejero delegado de Microsoft*

Microsoft 365 Enterprise es una solución completa e inteligente (en la que se incluye Office 365, Windows 10 Enterprise y Enterprise Mobility + Security) que permite a todos los empleados ser creativos y colaborar de forma segura.

Microsoft 365 cuenta con soluciones de seguridad contra correo no deseado de terceros, cifrado, administración de dispositivos móviles y otros problemas integrados. Microsoft Intelligent Security Graph aplica análisis avanzado a los miles de millones de señales de amenaza que recibimos de todos nuestros productos (como Exchange, Windows y Azure) para ofrecer información más útil que permita a tu organización identificar ataques y responder rápidamente ante ellos. Este nivel de seguridad está integrado en todos los niveles de Microsoft 365 (físico, de red, de infraestructura y de aplicaciones) para que te resulte más fácil proteger a las personas, los datos y los dispositivos, sin que esto afecte a la productividad.

01 Integración y respuesta rápida

Los actores de las amenazas han evolucionado desde ataques de "robo con fuerza" hasta poner en peligro los sistemas para mantener una presencia persistente y a largo plazo. Ahora, los atacantes usan una amplia variedad de vectores y diferentes herramientas y técnicas cada vez más avanzadas: el robo de credenciales, la instalación de malware que se elimina a sí mismo para evitar la detección, la modificación de procesos internos y el redireccionamiento de datos de red, estafas de ingeniería social e incluso ataques dirigidos a los teléfonos móviles y dispositivos del hogar de los empleados.

Por supuesto, las organizaciones implementan cada vez más herramientas de seguridad contra este panorama que evoluciona rápidamente. Aunque intentan dar solución a problemas específicos, estas soluciones rara vez funcionan correctamente entre sí. En muchas se usan paneles, consolas y registros de propiedad. La dificultad de la integración hace que resulte complicado obtener una vista general y clasificar rápidamente amenazas por orden de prioridad, y es un reto aún más difícil cuando se trata de recursos que están tanto en la nube como entornos locales. Como resultado, puede que los ataques no se identifiquen pueden durante 140 días.[1]

[1] "Panorama de amenazas: Números". FireEye, 2016.
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/Infographic-mtrends2016.pdf

De media, una gran empresa usa 75 productos de seguridad.[2]

El método tradicional es poner en correlación información de una amplia variedad de herramientas con soluciones de Administración de eventos e información de seguridad (SIEM). Pero la detección necesita que los equipos de seguridad procesen fuera de banda registros y datos y que, después, clasifiquen por orden de prioridad los incidentes y los investiguen. La recopilación y conciliación de datos resultan difíciles, y la falta de una vista unificada complica la respuesta y la administración. A medida que la respuesta y detección rápidas son cada vez más importantes, surgieron estos procedimientos recomendados:

- Obtén una vista integral de toda tu red, incluidos los entornos híbridos y de nube.
- Crea un ecosistema de plataformas y productos de seguridad que se integren entre sí y que proporcionen información sobre una amplia variedad de plataformas.
- Asóciate con proveedores de tecnología que colaboren y compartan información en todo el sector de la seguridad.
- Combina perspectivas sobre los datos con inteligencia humana de analistas de seguridad, investigadores y cazadores de amenazas para mejorar aún más la capacidad de evaluar los eventos rápidamente y clasificarlos por orden de prioridad.

[2] Según Balaji Yelamanchili, vicepresidente ejecutivo y director general de negocio de seguridad empresarial de Symantec, como se cita en: Symantec. "Symantec introduce la nueva era de protección contra amenazas avanzada". 27 de octubre de 2015. https://www.symantec.com/en/in/about/newsroom/press-releases/2015/symantec_1027_01

Soluciones de administración de la seguridad de Microsoft

Para obtener visibilidad y control sobre tu seguridad, Microsoft 365 ofrece un enfoque integral de seguridad, desde proteger la puerta principal a proteger tus datos en cualquier lugar, e incluso identificar y solucionar ataques. Esto te permite consolidar herramientas, a la vez que garantizas que tus equipos especializados en seguridad tengan la flexibilidad y la libertad de dar solución a sus cargas de trabajo específicas.

Puntos de referencia más importantes

- **La falta de integración entre los productos de seguridad dificulta que los equipos de seguridad puedan ver y combatir las amenazas de forma global y rápida.**
- **Busca productos diseñados para integrarse con otros.**

02

La necesidad de controles de seguridad en un número cada vez mayor de puntos de conexión

Las empresas saben que una infracción de datos puede tener costes inmensos y, aun así, se enfrentan al reto real de establecer suficientes controles de seguridad para obtener la visibilidad que necesitan de amenazas y ataques. También tienen que admitir el TI de consumo, donde los empleados ya no trabajan de forma exclusiva con dispositivos corporativos y con un control estricto, y pueden trabajar desde cualquier lugar, con cualquier dispositivo y desde cualquier plataforma, independientemente de que el equipo de TI de la compañía lo autorizara o no.

En este mundo, las estrategias de seguridad basadas en identidad vinculan el acceso a la identidad, por lo que la organización puede ir más allá de los dispositivos y aplicar controles basados en roles y necesidades, sin importar cómo se conecte el usuario. Este enfoque en la autenticación y administración de usuarios cuando obtienen acceso a activos corporativos también permite a las organizaciones proteger sus datos, sin importar dónde estén, cómo se obtenga acceso o con quién se compartan.

Vale la pena mencionar otras dos tecnologías: las soluciones de administración de acceso e identidad (IAM), y las soluciones de administración de aplicaciones móviles con prevención de pérdida de datos (DLP). Estas dos tecnologías reducen los riesgos, ya que protegen el acceso a las aplicaciones y los datos que se encuentran en recursos corporativos y en la nube. IAM puede eliminar la necesidad de usar varias credenciales, ya que asigna a los empleados una única identidad para obtener acceso a recursos locales y en la nube. Los sistemas de IAM basados en la nube también pueden usar análisis e inteligencia sobre amenazas del proveedor de tecnología para mejorar la detección de comportamientos de inicio de sesión inusuales y responder automáticamente en consecuencia.

Multi-Factor Authentication (MFA) ofrece otro nivel de protección, ya que exige que un usuario presente algo que conoce (la contraseña) y algo que tiene (una autenticación secundaria con un dispositivo, una huella

digital o el reconocimiento facial). Otras tácticas seguras son basar el acceso en el riesgo de usuarios, el riesgo de dispositivos, el riesgo de aplicaciones e incluso el riesgo de ubicaciones. Estas funciones pueden, de forma automática, permitir, bloquear o exigir MFA a un usuario en tiempo real basándose en las directivas que establezcas, lo que permite a las organizaciones mejorar la protección en su propia puerta principal.

Estas herramientas modernas también ofrecen una seguridad de punto de conexión antes de que se produzcan infracciones. Las mejores soluciones permiten cifrar dispositivos en todos los niveles, desde hardware a aplicaciones, y proporciona visibilidad en toda la empresa de la dinámica de ataques. Otras herramientas más avanzadas ofrecen un nivel de protección posterior a la infracción, como información sobre las técnicas de los adversarios y la similitud con ataques conocidos con herramientas integradas para bloquear, poner en cuarentena o borrar rápidamente los datos de la compañía.

Microsoft 365 funciona con una infraestructura existente (unifica la administración de TI de usuarios, dispositivos, aplicaciones, datos y servicios) para que tu equipo de TI pueda consolidar y simplificar soluciones, y ahorrar dinero. También es compatible con entornos híbridos, lo que te ofrece la flexibilidad de integrar soluciones locales y en la nube.

Centro de operaciones de defensa cibernética: Cómo defiende Microsoft su plataforma

El Centro de Operaciones de Defensa Cibernética (CDOC) de Microsoft reúne a expertos en respuestas de seguridad de toda la compañía para ayudar a proteger, identificar y responder ante amenazas de seguridad contra nuestra infraestructura y nuestros servicios en tiempo real.

La administración de la seguridad inteligente y simplificada permite obtener visibilidad y control sobre la seguridad

La clave para el éxito de un director de seguridad de la información no es usar una única consola para todo, sino facilitar la integración siempre que tenga más sentido. No necesitas todas las soluciones específicas de administración de puntos de datos para proteger los dispositivos de tus usuarios finales y las redes en expansión. Microsoft 365 ofrece administración de la seguridad inteligente con controles especializados basados en las necesidades de tus equipos de seguridad, visibilidad siempre que la necesites y una guía de cómo mejorar la posición de seguridad de tu organización basándose en inteligencia inigualable. Esto te permite beneficiarte de la flexibilidad y la libertad para administrar fácilmente la seguridad con controles integrados, además de aprovechar directrices e inteligencia de seguridad para mejorar tu posición de seguridad y defenderte ante las amenazas.

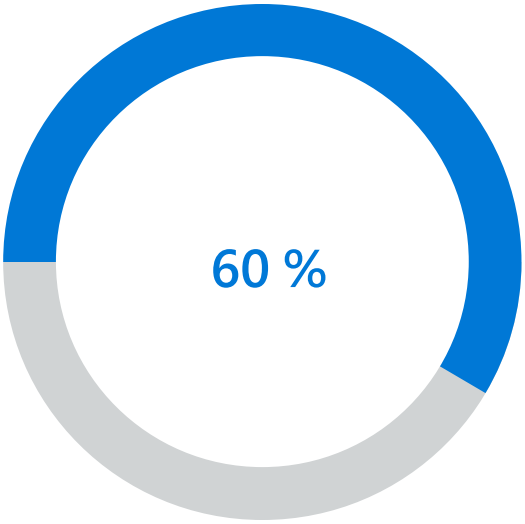
- Comprende tu posición de seguridad: obtén información sobre tu estado de seguridad y los riesgos en los recursos de tu organización para ofrecer una detección y respuesta efectivas.

- Define la protección de datos que necesitas: crea y personaliza directivas de seguridad coherentes, y establece controles, algo esencial para la administración de la seguridad inteligente.

- Ponte al día con la inteligencia de seguridad: usa directrices, recomendaciones e inteligencia integrada para mejorar la seguridad de tu organización.

Aumentar la seguridad con controles de acceso e identidad

Las soluciones de administración de acceso e identidad de Microsoft te permiten proteger las identidades de usuario y controlar el acceso a recursos valiosos según el nivel de riesgo de los usuarios. Microsoft 365 Enterprise ofrece protección de identidad (Windows Hello, Touch ID, Credential Guard, Acceso condicional, Azure Active Directory), aplicaciones y datos (DLP de Office, Azure Information Protection, Cloud App Security) y dispositivos (Device Guard, Intune).



El 60 % de las infracciones se producen debido a un punto de conexión en peligro.[3]

Soluciones de administración de acceso e identidad de Microsoft

Vuelve a centrar tus esfuerzos para proteger las identidades y la información. Las soluciones de administración de acceso e identidad de Microsoft permiten proteger las identidades de los usuarios y ofrecen acceso seguro a aplicaciones y datos, mientras que nuestras soluciones de protección de la información ayudan a garantizar que la información siempre esté segura en cualquier lugar, incluso en movimiento.

Puntos de referencia más importantes

- Establecer controles de administración de acceso e identidad
- El 60 % de las infracciones se producen debido a un punto de conexión en peligro.[3]
- Una estrategia de seguridad basada en identidad cambia de centrarse en el seguimiento de un número cada vez mayor de puntos de conexión, a administrar los usuarios que tienen acceso a datos corporativos.
- Una protección de puntos de conexión más sólida ofrece información posterior a las infracciones sobre las técnicas de los adversarios.

[3] Ibídem. Reed, 2017.

03

Velocidad y agilidad de los actores de amenazas

Los hackers saben que todas las organizaciones tienen varios puntos de entrada. Usan estafas de suplantación de identidad, ataques de malware y spyware, vulnerabilidades de seguridad de exploradores y software, acceso con dispositivos perdidos y robados, ingeniería social y otras tácticas para minar tu seguridad. Se necesita una vigilancia constante para seguir viendo todas las amenazas que conoces y ser consciente de las vulnerabilidades emergentes.

Algunas herramientas pueden ayudar a mantener un enfoque de seguridad siempre disponible, pero un enfoque más amplio tiene más sentido. Las herramientas tradicionales se centran en la prevención, pero eso ya no es suficiente. Las organizaciones tienen que dar por hecho que ya se produjo una infracción o que pronto se producirá una y, después, necesitan buscar formas de reducir significativamente el tiempo necesario para identificarlas y recuperarse ante ellas.

De media, una gran empresa tiene que analizar 17 000 alertas de malware a la semana.[4]

[4] Ponemon Institute. “El coste de la contención de malware”. Patrocinado por Damballa. 2015. https://www.ponemon.org/local/upload/file/Damballa%20Malware%20Containment%20FINAL%203.pdf

Muchas aplicaciones de seguridad usan funciones de aprendizaje automático y análisis integrado para obtener información sobre incidentes, actividades y los pasos que realizaron los atacantes. Esto sigue siendo una vista al pasado que puede que no agilice la reacción y la recuperación. Existen soluciones de análisis y seguridad más avanzadas que aprovechan esa información y que actúan automáticamente para impedir infracciones similares y responderán ante ellas, lo que reduce significativamente el tiempo de mitigación. Estas soluciones cuentan con una enorme envergadura de señal e inteligencia y, al combinarlas con la experiencia y el conocimiento de expertos humanos, pueden convertirse en herramientas realmente útiles contra los actores de las amenazas que avanzan rápidamente.

Los líderes de seguridad tienen que trabajar con directores ejecutivos y la junta para comprender y mantener un nivel aceptable de riesgos, así como para equilibrarlo con el presupuesto de seguridad. No existe una solución válida para cada caso y para todas las organizaciones, pero un enfoque de administración de riesgos puede ayudarte a decidir dónde y cómo invertir basándose en lo que sea más adecuado para tu organización.

Soluciones de protección contra amenazas de Microsoft

Protégete contra amenazas avanzadas y recupérate rápidamente después de un ataque.

Microsoft cree que la protección contra amenazas tiene que permitir a las organizaciones protegerse contra ciberataques avanzados. También tiene que proporcionar soluciones que puedan ayudar a identificar comportamientos sospechosos dentro de la organización. Por último, como no hay ninguna solución de seguridad que sea efectiva al 100 %, es necesario implementar procesos y herramientas para responder rápidamente ante amenazas que permitan controlar los daños y limitar los efectos derivados de un ataque.

Las soluciones de protección contra amenazas de Microsoft ofrecen una combinación de métodos tradicionales (como protección antimalware) e innovaciones, como el análisis de comportamiento de usuarios y entidades (UEBA) y la detección y respuesta de puntos de conexión (EDR). Microsoft invierte tanto en la prevención de los ataques como en la detección y respuesta posteriores a una infracción.

Puntos de referencia más importantes

- **Adopta un método de "dar por hecho una infracción" en tu seguridad.**
- **Selecciona soluciones que reduzcan el tiempo necesario para identificar una infracción y recuperarte ante esta.**
- **Toma una postura de administración de riesgos hacia la seguridad para que te resulte más fácil decidir dónde invertir.**

04 Migrar a la nube de forma segura

Cada organización se encuentra en una fase distinta de su viaje hacia la nube. Los requisitos de cumplimiento, las normativas locales y otros retos de migración hacen que no todas las organizaciones estén preparadas para migrar cargas de trabajo críticas a la nube.

Pero migrar a la nube no tiene por qué significar una salida de tus sistemas y procesos existentes. En un entorno de TI híbrido e integrado por completo, la nube se convierte en una extensión de tu centro de datos y las directivas con que lo controlas. Las estrategias de nube híbrida también ofrecen a los líderes de seguridad un método medido para migrar a la nube, lo que les permite migrar funciones empresariales a la nube solo cuando estén seguros de que los servicios ofrezcan la cantidad de control adecuada.

Los modelos de servicios en la nube afectan a la forma en que los proveedores de servicios y los clientes comparten responsabilidades. Esto genera problemas para los directores de seguridad de la información a medida que salvan los retos de renunciar a algunos de los controles de las soluciones locales para obtener una mayor seguridad de la que los proveedores de servicios en la nube pueden proporcionar.

"Los proveedores de servicios en la nube pública ofrecen mejor seguridad de lo que una pequeña empresa o incluso una gran empresa puede alcanzar. Esto es debido a las inversiones que realizan los proveedores de servicios en la nube para crear y mantener su infraestructura de nube".[5]

La norma general para la seguridad de la nube es que se trata de una responsabilidad compartida. Los proveedores de servicios en la nube necesitan contar con cifrado y seguridad de última generación, pero los clientes tienen que asegurarse de que los servicios que compran son realmente seguros y que integran las directivas de seguridad necesarias en sus nuevos recursos en la nube. Busca transparencia al planear una migración a la nube: los proveedores tienen que publicar información detallada sobre la seguridad, la privacidad y el cumplimiento de sus servicios. También necesitan producir informes de auditoría y otros materiales para ayudarte a comprobar sus afirmaciones y a comprender dónde terminan sus responsabilidades y empiezan las tuyas.

[5] Trotter, Paul. "Principales miedos de la seguridad de la nube y cómo los afrontan los directores ejecutivos". 20 de mayo de 2015. http://www.cio.com/article/2924390/cloud-security/top-cloud-security-fears-and-how-the-c- suite-is-tackling-them.html

Preguntas que realizar a tu proveedor de servicios en la nube

Evaluar a los proveedores de servicios en la nube no es simplemente elegir un servicio, es seleccionar a quién confiar tus datos. Estas son algunas preguntas críticas sobre la seguridad y el control de acceso:

- ✓ ¿Están protegidos tus datos por tecnología de última generación y seguridad avanzada?
- ✓ ¿Incorporas la privacidad en el diseño y permites el control de tus datos en nuestra nube empresarial?
- ✓ ¿Realizas amplias inversiones en procesos de cumplimiento sólidos e innovadores para ayudar a mi organización a alcanzar sus necesidades de cumplimiento?
- ✓ ¿Dónde se almacenarán mis datos, quién tendrá acceso a ellos y por qué?
- ✓ ¿Está sujeto el proveedor de servicios en la nube a revisiones anuales por terceros?
- ✓ ¿Rechazará el proveedor de servicios en la nube cualquier solicitud de divulgación de datos personales de clientes que no sean vinculantes legalmente? ¿Se adhiere el proveedor de servicios en la nube a las normas reglamentarias y de cumplimiento de diferentes países y ubicaciones?

La nube de confianza

Las personas solo usan tecnología en la que confían. Podrás migrar a la nube de forma segura cuando tengas información sobre tu proveedor de servicios en la nube en relación con la seguridad, privacidad, cumplimiento y transparencia. Microsoft Cloud se basa en estos cuatro principios y Trusted Cloud Initiative impulsa un conjunto de directrices, requisitos y procesos para ofrecer estrictos niveles de ingeniería, cumplimiento y aspectos jurídicos de nuestros servicios en la nube.

Obtén rentabilidad con mayor rapidez con Microsoft Cloud y FastTrack

FastTrack ya ayudó a más de 40 000 clientes a maximizar la rentabilidad de la inversión, agilizar la implementación e impulsar la adopción.

- Migra el correo electrónico y el contenido, y pon en marcha los servicios de Microsoft 365, incluida la guía de evaluación y corrección para preparar tu infraestructura para la nube
- Implementa y administra de forma segura dispositivos, incluidos dispositivos con tecnología de Microsoft 365
- Facilita tu negocio y alcanza la adopción de los usuarios finales

Los ingenieros de Microsoft ofrecen FastTrack para que te resulte más fácil migrar a la nube a tu propio ritmo y que puedas obtener acceso a partners cualificados si necesitas servicios adicionales.

Puntos de referencia más importantes

- Migrar a la nube no tiene por qué significar abandonar tus sistemas y procesos existentes.
- Una nube híbrida ofrece un método medido para la migración a la nube.
- Al evaluar los proveedores de servicios en la nube, asegúrate de que cumplan con normas internacionales.
- Busca proveedores que publiquen información detallada sobre cómo operan sus servicios y administran los datos.

05 El riesgo de shadow IT

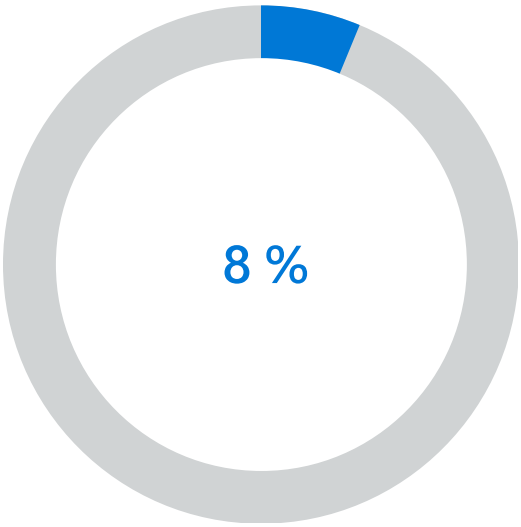
Incluso si tu organización no usa soluciones basadas en la nube, es probable que tus empleados lo hagan. Esta tendencia, conocida como shadow IT, es mucho más importante de lo que se piensa. De hecho, solo el 8 % de las compañías conocen el alcance de shadow IT en sus organizaciones[6], y el número de servicios en la nube usados por empleados corporativos supera rápidamente a los cálculos de TI internos.

> *En 2022, un tercio de los ataques con éxito que reciban las empresas se producirán en sus recursos de shadow IT.*[7]
>
> Diez principales predicciones de seguridad para 2016 de Gartner

El shadow IT expone tu organización a enormes riesgos de TI y la administración de aplicaciones, la seguridad y el cumplimiento.

[6] "Informe sobre una encuesta de procedimientos de adopción de la nube y prioridades". Cloud Security Alliance. Enero de 2015. https://downloads.cloudsecurityalliance.org/initiatives/surveys/capp/Cloud_Adoption_Practices_Priorities_Survey_Final.pdf

[7] Gartner, Smarter With Gartner, "Diez principales predicciones de seguridad para 2016 de Gartner". 15 de junio de 2016. http://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/



Solo el 8 % de las compañías conocen el alcance de shadow IT en sus organizaciones.[12]

Los usuarios finales suelen aceptar términos y condiciones sin leerlos y sin comprender en su totalidad a lo que conceden su acceso. Las soluciones de seguridad de red tradicionales no están diseñadas para proteger datos en aplicaciones SaaS y no pueden proporcionar visibilidad a TI sobre cómo usan la nube los empleados.

Al mismo tiempo, bloquear el shadow IT es una solución poco eficaz, ya que los empleados siempre encontrarán formas de eludir las restricciones. Un control demasiado estricto afecta a la innovación, entra en conflicto con requisitos de tecnología exigentes y sin planear, merma la productividad y puede reducir la implicación y aumentar la rotación entre el talento de alto calibre.

Por último, todos tenemos que aceptar que el shadow IT ya es algo habitual. Permitir que los usuarios finales y los equipos usen las aplicaciones en la nube que sean más adecuadas para su tipo de trabajo permite impulsar la productividad y la innovación. Obtener visibilidad, control y protección contra amenazas de las aplicaciones SaaS de shadow IT son los primeros pasos para administrar el riesgo y facilitar la transformación digital que ya se inició en tu compañía.

Los agentes de seguridad de acceso a la nube (CASB) proporcionan a las organizaciones una imagen detallada de cómo sus empleados usan la nube:

- ¿Qué aplicaciones de nube usan los empleados?
- ¿Qué riesgos implican para la organización el uso de estas aplicaciones?
- ¿Cómo se obtiene acceso a estas aplicaciones?
- ¿Qué tipos de datos se envían y se comparten desde estas aplicaciones?
- ¿Qué apariencia tiene el tráfico de carga o descarga?
- ¿Existen anomalías en el comportamiento del usuario, como viajes imposibles, intentos de inicio de sesión incorrectos o direcciones IP sospechosas?

Una mayor visibilidad y control sobre estas aplicaciones y servicios permite a los líderes de seguridad desarrollar y exigir directivas de SaaS razonables y efectivas sin sacrificar la seguridad y el cumplimiento que exige la organización.

Soluciones de protección de la información de Microsoft

Tu organización puede usar la nube sin poner en riesgo la información confidencial. Las soluciones de protección de la información de Microsoft pueden ofrecerte visibilidad y extender tus directivas de seguridad a la nube. Microsoft Cloud App Security te permite:

- Descubrir y evaluar riesgos: identifica aplicaciones de nube en tu red, obtén visibilidad sobre el uso de shadow IT y recibe evaluaciones de riesgo y análisis continuados

- Controla el acceso en tiempo real: administra y limita el acceso a aplicaciones de nube basándose en condiciones y en contextos de sesión, como la identidad del usuario, el dispositivo y la ubicación.

- Protege tu información: obtén un control granular sobre los datos y usa directivas integradas o personalizadas para el uso compartido de datos y la prevención de pérdida de datos.

- Identifica las amenazas y protégete contra estas: identifica usos de alto riesgo y detecta actividades de usuario inusuales con las funciones de detección de anomalías y análisis de comportamiento de Microsoft.

Los usuarios suelen obtener acceso a aplicaciones donde se puede almacenar información confidencial de la empresa o los clientes. La capacidad de controlar lo que ocurre después de que se obtenga acceso a los datos es crítico, así como llevar la seguridad de tus sistemas locales a la nube, con una mayor visibilidad, controles de datos granulares y una mejor protección contra amenazas.

- Nuestras funciones de administración de aplicaciones móviles (MAM) y las directivas de protección de aplicaciones pueden ayudarte a proteger los datos en el nivel de las aplicaciones, como autenticación de nivel de aplicación, control de copiar y pegar, y control de guardar como.

- Las directivas configurables te proporcionan un control específico de lo que pueden hacer los usuarios con los datos a los que obtienen acceso.

- Puedes aplicar directivas en las aplicaciones para proteger los datos (tanto si se inscribe o no el dispositivo para su administración), lo que te permitirá proteger la información corporativa sin la intromisión en la vida personal de los usuarios.

- Puedes cifrar los datos de la compañía en las aplicaciones con el máximo nivel de cifrado de dispositivo proporcionado por iOS y Android.

- También puedes proteger los datos de tu compañía al exigir directivas de credenciales o código PIN.

Puntos de referencia más importantes

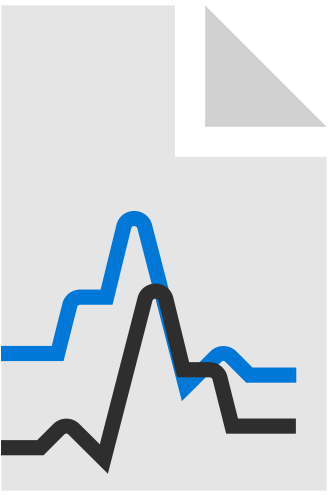
En lugar de bloquear el shadow IT, busca soluciones que te permitan supervisar y evaluar el riesgo.

Los CASB pueden ofrecerte una imagen detallada de cómo usar la nube los empleados.

Con una mejor visibilidad, podrás establecer directivas que realicen un seguimiento y controlar la forma en que los empleados usan estas aplicaciones.

06 Equilibrar la protección de la información integral y la productividad

Los datos dejan de estar en tu control ahora más que nunca a medida que tus empleados, partners y clientes los comparten. Esto impulsa la productividad y la innovación, pero puede tener consecuencias importantes si la información confidencial cae en las manos equivocadas. Los líderes de seguridad tienen que administrar y proteger los datos almacenados en varias ubicaciones y compartidos más allá de fronteras internacionales. Las organizaciones que operen en la UE tienen que dar prioridad a la protección de datos antes de que entre en vigor el Reglamento general de protección de datos (RGPD) el 25 de mayo de 2018. El reglamento RGPD tendrá un impacto importante en la forma en que las compañías almacenan y administran los datos de clientes, informan sobre infracciones, comunican directivas e invierten en recursos internos.



Los empleados tolerarán esas molestias antes de encontrar soluciones alternativas para los requisitos de seguridad. Clasificar y cifrar los datos son las mejores formas de mantenerlos a salvo, a la vez que se facilita la productividad y el uso compartido de la información. Esperar que los empleados recuerden los datos que es necesario proteger y cómo clasificarlos correctamente puede dar pie a errores y retrasos, por lo que recomendamos clasificar y etiquetar los datos a medida que se creen. Se pueden evitar los errores humanos si se automatiza la clasificación de datos. Las herramientas pueden comprender el contexto de los datos, como los números de tarjetas de crédito en un archivo, o la confidencialidad de los datos basada en su origen. Después del etiquetado, las marcas visuales (como encabezados, pies de página y marcas de agua) y la protección (como el cifrado, la autenticación y los derechos de uso) se pueden aplicar automáticamente en la información confidencial.

Los equipos de seguridad también tienen que ser capaces de realizar un seguimiento de la actividad en archivos compartidos altamente confidenciales o con un gran impacto empresarial y, si es necesario, revocar el acceso. Esta protección persistente viaja con los datos y los protege en todo momento, independientemente de dónde se almacenen o con quién se compartan.

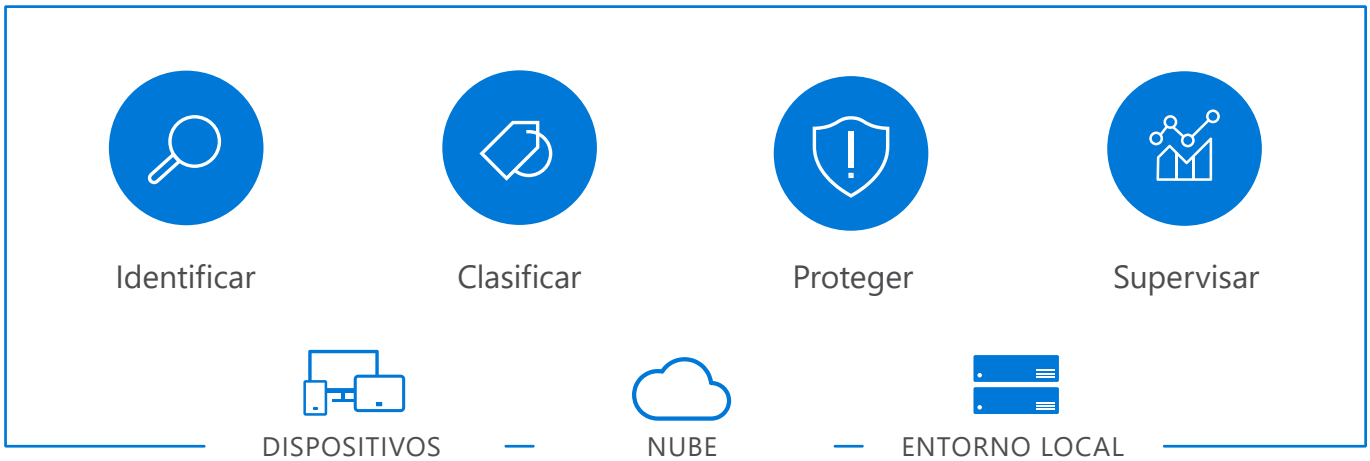
Soluciones de protección de la información de Microsoft

Evita las pérdidas de datos y el uso indebido por error al proteger la información, sin importar dónde esté.

Las soluciones de protección de la información de Microsoft ayudan a proteger la información confidencial en todo el ciclo de vida: en dispositivos, aplicaciones, servicios en la nube y entornos locales

El método de Microsoft para la protección completa de la información confidencial en todo el ciclo de vida (tanto dentro como fuera de la organización) es identificar, clasificar, proteger y supervisar datos críticos, sin importar dónde se encuentren o a dónde viajen. Microsoft 365 proporciona un método más coherente e integrado para la clasificación, el etiquetado y la protección en todas nuestras tecnologías de protección de la información básicas.

Consulta el siguiente gráfico:



Tenemos que volver a pensar en cómo vamos a proteger los datos en este mundo que da prioridad a la nube y a la movilidad. La realidad es que nadie posee la experiencia, el tiempo y los recursos necesarios para hacer esto por su cuenta.

Brad Anderson, *vicepresidente corporativo de Microsoft para Enterprise Mobility*

Puntos de referencia más importantes

- **Los líderes de seguridad necesitan centrarse en la seguridad en el nivel de los datos.**
- **El cifrado y la clasificación de datos son cada vez más importantes. El etiquetado y la clasificación de datos tienen que producirse en el momento de la creación, y los equipos de seguridad tienen que ser capaces de supervisar las actividades realizadas en los archivos y tomar medidas rápidamente.**

Conclusión

La naturaleza polifacética de las amenazas informáticas hace que solucionar algunos de sus retos de seguridad ya no sea suficiente. Usar varias soluciones puede proteger puntos de conexión críticos, identificar infracciones y limitar los daños; pero la naturaleza persistente de las amenazas informáticas actuales exige el uso de defensas persistentes de manera uniforme, lo que, a su vez, exige un enfoque de seguridad más integral.

Proteger los datos y los sistemas es ahora una prioridad esencial para todas las organizaciones. Las necesidades de seguridad de cada compañía son únicas, pero las compañías se enfrentan a los mismos retos y comparten la misma responsabilidad para proteger sus datos, empleados y sistemas, a la vez que facilitan la innovación y el crecimiento. Necesitas marcos de seguridad ágiles que faciliten la transformación digital, apoyados por estrategias de seguridad integrales que se integren en las tecnologías, los procesos y los programas de aprendizaje. Microsoft 365 Enterprise ofrece una solución completa e inteligente que facilita tu transformación digital con funciones de seguridad y cumplimiento integradas en todos los niveles.

Para obtener más información sobre cómo Microsoft puede ayudarte con tu estrategia de seguridad integral, visita la **página principal de Microsoft 365.**