jamf

Manual de estrategias para tecnologías emergentes: Administración, seguridad y ampliación de la empresa moderna

Crecimiento emergente de la tecnología móvil y la empresa

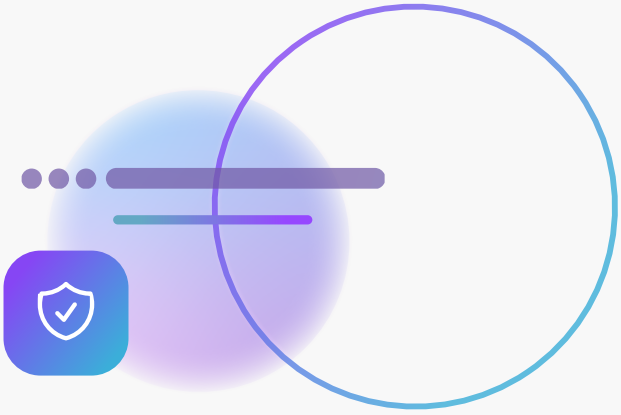
Al igual que han evolucionado los espacios de trabajo, las tecnologías emergentes, como los dispositivos portátiles, la informática espacial y la inteligencia artificial, están cambiando la forma de trabajar. Como herramientas empresariales, están mejorando la experiencia de los usuarios, transformando la productividad y acelerando la innovación a escala mundial en todas las industrias.

Pero para ello, los directivos de las empresas y los equipos de TI y de seguridad deben hacer evolucionar sus estrategias de terminales para que los datos permanezcan seguros, los dispositivos se administren de forma holística y las empresas escalen de forma inteligente para mitigar el riesgo derivado de la ampliación de las superficies de ataque, la fragmentación de la visibilidad y la intensificación de la demanda de recursos operativos.

Este documento no solo explica por qué las organizaciones deben modernizar la administración, sino que también proporciona una guía independiente de la plataforma para construir y poner en práctica una base resiliente, fundamentada en el contexto del mundo real y en medidas prácticas para reducir la complejidad, cerrar las brechas de visibilidad y prepararse para la era de la computación híbrida.

En este documento, aprenderá a:

- Adaptar las estrategias de administración y conformidad con las nuevas tecnologías
- Reconocer por qué los enfoques tradicionales no ofrecen paridad de seguridad
- Aprovechar la automatización y la puesta en práctica continua como estrategias básicas
- Alinear la administración, la identidad, la seguridad y la conformidad con los objetivos empresariales
- Adoptar la confianza cero como principio básico de la seguridad moderna de las terminales



Resumen ejecutivo

Las empresas están ingresando en un periodo definido por los rápidos avances en los modelos informáticos híbridos, incluidos los wearables, el IoT y la IA. Estas tecnologías emergentes están remodelando las operaciones empresariales e impulsando la innovación en todos los sectores, pero también introducen complejidad, fragmentación y nuevas vías de riesgo. A medida que aumenta la diversidad dentro de las flotas de dispositivos, también lo hace la necesidad de una administración holística, políticas de acceso basadas en el contexto, validación continua de la postura y adopción de la confianza cero. Las organizaciones que inviertan en flujos de trabajo automatizados, visibilidad profunda y controles basados en políticas estarán mejor posicionadas para salvaguardar los datos, cumplir las normativas en evolución y ampliar las tecnologías emergentes con garantías.

Principales conclusiones:

- Tasa de Crecimiento Anual Compuesta (CAGR) proyectada para dispositivos de uso rudo al 2028: **8.4%**
- CAGR proyectada de la computación espacial para 2030: **33.16%**
- Adopción empresarial de paradigmas de computación híbrida para 2028: **40%**
- Problemas de servicio al cliente resueltos de forma autónoma para 2029: **80%**
- Envíos de wearables esperado en 2025: **590.7 millones de unidades**

Tecnologías emergentes: 2026 y proyecciones futuras

Una nueva era de la informática se acelera a medida que los wearables, el IoT y la IA pasan de ser programas piloto a herramientas empresariales que ofrecen resultados comerciales. Estas tecnologías están cambiando la forma en que las personas trabajan, aprenden y se relacionan —difuminando las realidades de nuestro mundo físico y los espacios de trabajo digitales— lo que permite alcanzar nuevos niveles de creatividad, productividad, colaboración, visión estratégica y automatización. Las organizaciones que aprovechen este impulso se alinearán estratégicamente, reforzarán su resiliencia, escalarán de forma inteligente y aprovecharán las oportunidades que definan la próxima etapa de la innovación.

Computación espacial

El juego Virtual Reality (VR) Vortex, que se encontraba en los salones recreativos de finales de la década de 1990, sirvió a muchos como primera incursión en las experiencias de realidad alternativa. Esta tecnología —que incluye la Realidad Aumentada (RA) y la Realidad Extendida (RX)—, ha evolucionado hasta formar una Realidad Mixta (RM), que tiende un puente entre nuestra comprensión de los mundos físico y lógico.

Conocida colectivamente como computación espacial, representa la próxima evolución del aprendizaje y la productividad, con **una tasa de crecimiento anual compuesto (TCAC) estimada de 33.16% para 2030**.

A pesar de que la computación espacial está relativamente en pañales, los matices de esta incipiente tecnología **se dejan sentir en múltiples industrias de todo el mundo**, como la educación, la fabricación y la salud, por citar algunas.

Algunos casos de uso de la informática espacial en el mundo real:

- **Optimización de la incorporación:** Los empleados se familiarizan recorriendo y explorando los espacios de trabajo para orientar mejor a los recién contratados desde el primer día.
- **Creación rápida de prototipos:** Los ingenieros desarrollan e iteran productos con mayor rapidez, al mismo tiempo que los manipulan para probar su integridad y colaborar en tiempo real.
- **Capacitación especializada:** Los cirujanos practican en entornos realistas mientras se utilizan superposiciones 3D para crear una simulación inmersiva para aprender procedimientos y aumentar la precisión.
- **Mejora de las experiencias:** Los clientes minoristas utilizan sus teléfonos inteligentes para escanear y visualizar productos en casa o probarse ropa, atendiendo a los clientes en el lugar donde estén.
- **Solución de problemas justo a tiempo:** Los operadores de máquinas utilizan Apple Vision Pro para identificar problemas y realizar análisis para resolverlos desde la planta de producción.

Wearables

Considere lo siguiente: un Apple Watch contiene los componentes de hardware, aunque miniaturizados, que antes solo eran posibles en las computadoras de escritorio de la clase Pentium 4.

Con procesamiento multinúcleo, motores neuronales, toda una serie de sensores microscópicos y la capacidad de funcionar de forma independiente como su propia fuente de computación, son posibles el trabajo (y el juego) hoy en día en un diseño capaz y energéticamente eficiente envuelto ya sea en su cara, mano, dedo y/o muñeca.

He aquí algunos casos de uso para los **590.7 millones de wearables vendidos en 2025**:

- **Relojes:** Simplifican los viajes (nacionales e internacionales) con smartwatches con GPS + Cellular para mantenerse en comunicación con la oficina y sus seres queridos sin tener que lidiar con confusos o costosos planes de itinerancia de datos.
- **Rastreadores:** Obtenga información sanitaria actualizada al minuto para controlar de forma proactiva sus signos vitales, mantenerse en el camino de sus objetivos o responder rápidamente a accidentes e incidentes relacionados con la salud para recibir una atención que puede salvar vidas.
- **Auriculares**: La tecnología de cancelación de ruido limita las distracciones externas para ayudar a enfocarse en lo importante; además, cuando se emparejan con un smartphone, es posible la traducción en directo para entender varios idiomas que se hablen en tiempo real.
- **Gafas**: Tome fotos y videos cuando responda a mensajes urgentes, mientras sigue las indicaciones para llegar al lugar de su reunión: manos libres con el asistente de IA integrado que le ayuda a conseguir más en menos tiempo.

Internet de las Cosas (IoT)

La eficiencia es un motor de la continuidad empresarial. Y puesto que la automatización es un cimiento básico de la eficiencia, no es de extrañar que la confianza en los dispositivos IoT para generar inteligencia empresarial, como en los flujos de procesos, sea esencial para el tipo de toma de decisiones basada en datos que se utiliza para agilizar las operaciones empresariales a gran escala.

Además, la combinación de sensores y automatización **permite ahorrar entre un 20% y un 30% de energía** en determinados modelos de negocio. Asimismo, se puede conseguir **una reducción de los costos de mantenimiento de hasta el 50%**, gracias a un cambio estratégico, como el mantenimiento predictivo, que favorezca un enfoque proactivo (en lugar de reactivo) para recortar los tiempos de inactividad imprevistos.

Varios ejemplos de los beneficios de IoT en la empresa son:

- **Control y seguimiento de activos y red logística:** Simplifique el monitoreo de inventarios y, cuando se combina con análisis predictivos, mejore la planificación de la capacidad y el pronóstico de existencias.
- **Personalización de la experiencia de los clientes:** Refuerce la fidelidad a la marca con interacciones personalizadas que satisfagan mejor las necesidades únicas de los clientes y mejoren al mismo tiempo la prestación de servicios.
- **Administración de edificios e instalaciones:** Reduzca la huella energética al mismo tiempo que aumenta la eficiencia de las funciones del edificio, automatizando la climatización, la iluminación y la seguridad.
- **Interconexión de sistemas sofisticados:** Obtenga valor añadido de los sistemas existentes integrando sensores e IoT, para permitir nuevos servicios y oportunidades de ingresos.

Inteligencia Artificial (IA)

La promesa que sostiene la IA afecta por igual a usuarios empresariales y particulares. Con aplicaciones que abarcan industrias de todo el mundo, las ventajas transformadoras de GenAI para las empresas parecen ilimitadas:

- **Mayor valor:** Los empleados pueden enfocar sus habilidades en el trabajo estratégico, mientras que las tareas repetitivas se realizan automáticamente.
- **Aumentar el ROI:** La optimización de los recursos y una mayor eficiencia optimizan los procesos y reducen los costos operativos, además de los beneficios cualitativos derivados de la innovación y la mejora de las experiencias de los clientes.
- **Agilización de procesos:** Maximice los recursos visualizando conceptos, resumiendo contenidos o desarrollando código de muestra rápidamente.
- **Potenciación del análisis:** Obtenga una visión estratégica valiosa, realice análisis de tendencias y tome decisiones proactivas basadas en datos, reduciendo los tiempos de salida al mercado (GTM).

Además, la IA agéntica (toma de decisiones sin interacción humana) ofrece ventajas clave que amplían los beneficios enumerados anteriormente. Por ejemplo, el estudio de Gartner estima que **el 80% de los problemas comunes de atención al cliente se resolverán de forma autónoma en 2029**. Otras ventajas clave residen en su capacidad proactiva (caza de amenazas) y adaptativa (aprendizaje en tiempo real). Uno de los segmentos en los que está a punto de revolucionar procesos empresariales cruciales es el del software de ciberseguridad. Las soluciones de seguridad basadas en la IA agéntica monitorean y evalúan continuamente los factores de riesgo mientras toman medidas para mitigar las amenazas rápidamente y sin necesidad de intervención humana, lo que reduce los tiempos de respuesta y mantiene la capacidad de recuperación.

Computación híbrida

Las empresas de todo el mundo se enfrentan a retos de eficiencia y administración de cargas de trabajo, aprovisionamiento de recursos y escalamiento, junto con requisitos normativos y gastos de capital que los modelos informáticos tradicionales, como los locales o las nubes públicas o privadas, por sí solos no pueden abordar con eficacia. Incluso los modelos de latencia aún más baja que procesan datos más cerca del dispositivo para agilizar la respuesta, como la computación en el borde (edge computing), siguen sin resolver todas las inquietudes de un entorno digital en constante cambio.

La computación híbrida es un nuevo paradigma que se amplía para incluir no solo las tecnologías emergentes, sino que mezcla los modelos informáticos existentes para resolver los obstáculos mencionados, como:

- **Agilidad**: El aprovechamiento de múltiples modelos informáticos permite a las organizaciones optimizar la administración del tráfico, impulsar los tiempos de respuesta y reducir la latencia de forma económica en momentos de picos inesperados.
- **Rendimiento**: Consiga mejoras de productividad implementando herramientas y automatización basadas en IA para distribuir de forma inteligente las cargas de trabajo en el entorno más eficiente.
- **Conformidad**: La geopatriación da a las organizaciones el control sobre dónde residen los datos y las aplicaciones, garantizando la soberanía y cumpliendo al mismo tiempo las exigencias de privacidad y reglamentación.
- **Resiliencia**: Agilice la continuidad para garantizar que las operaciones empresariales se mantengan durante las interrupciones, aprovechando la integración de sistemas en la nube, locales y heredados.

Para 2028, Gartner predice que **más del 40% de las empresas líderes habrán adoptado arquitecturas de paradigma informático híbrido** en los flujos de trabajo empresariales críticos, frente al 8% actual.

Retos para la TI empresarial

Cuando los dispositivos quedan fuera del ámbito de administración, surgen lagunas de visibilidad que limitan la capacidad de:

- Evaluar las medidas de seguridad
- Responder rápidamente a las amenazas
- Mantener la seguridad de los datos

La diversidad de plataformas y dispositivos, junto con los distintos modelos de propiedad y los entornos de trabajo híbridos, introducen variables que amplían la superficie de ataque de una organización. Además, aumenta la presión sobre los equipos ya responsables de mitigar el riesgo de un panorama de amenazas en evolución. La evolución de las normativas y la fragmentación de los estándares en torno a la IA y el IoT, respectivamente, aumentan la importancia de la gobernanza y la adopción responsable a escala mundial, tanto para las organizaciones como para las industrias en los que operan.

Implementación y aprovisionamiento

Una estrategia integral de administración y seguridad comienza con la inscripción de dispositivos y sigue con la capacidad de dotar a los dispositivos de las herramientas y configuraciones necesarias para que las organizaciones sigan cumpliendo la normativa, salvaguardando los datos y manteniendo la productividad de los empleados. Estas buenas prácticas están integradas en flujos de trabajo informáticos holísticos y son objeto de numerosas normas e infraestructuras de implementación.

Cuando los dispositivos no se registran con las suites de administración o no se aprovisionan con las herramientas de las que dependan sus usuarios para realizar las tareas, se desencadena una lenta pero constante cadena de acontecimientos que introduce riesgos:

- Usabilidad del dispositivo
- Confidencialidad de los datos
- Integridad de la comunicación
- Privacidad del usuario
- Disponibilidad de las terminales

Cada factor de riesgo afecta a la prestación de servicios y al cumplimiento de la normativa y, en última instancia, se traduce en repercusiones agravadas para la continuidad de la actividad.

Carencias en las políticas y la visibilidad

La visión estratégica de los dispositivos es la piedra angular de cualquier estrategia de seguridad. La imposibilidad de ver o analizar el estado de las terminales significa que los equipos de TI y seguridad no pueden ver lo que ocurre en los dispositivos tecnológicos emergentes que se conectan, se comunican y solicitan y utilizan recursos de la empresa dentro de su infraestructura.

Debido a los puntos ciegos de la telemetría, puede haber una gran cantidad de problemas que los administradores no puedan mitigar sin saber primero qué amenazas pueden existir ni cómo se deben priorizar los recursos, en vista de los recursos limitados y/o las opciones de mitigación.

Algunos ejemplos comunes que contribuyen a las carencias de visibilidad son:

- Múltiples plataformas de OS
- Manipulación física
- Modelos de propiedad mixta
- Tipos de dispositivos no compatibles
- Mala configuración de los dispositivos

Amenaza y mitigación de riesgos

Aunque las amenazas dirigidas a hardware y software en busca de puntos de entrada no son nada nuevo para la ciberseguridad, el reto de reducir el riesgo se ve agravado por los entornos híbridos, y los distintos tipos de dispositivos —cada uno de los cuales ejecuta múltiples plataformas de software— introducen una variedad de riesgos para la organización.

La mezcla de sistemas y tipos de dispositivos de código abierto, propietarios y cerrados supone una mayor presión para los equipos de TI y seguridad encargados de administrar y proteger las terminales. Cuando se combinan con la falta de visibilidad del estado de las terminales y la capacidad limitada para configurar de forma segura los dispositivos a escala, los siguientes retos aumentan exponencialmente la dificultad de mantener seguros los recursos de la empresa:

- Seguridad de los datos
- Explotación de vulnerabilidades
- Resiliencia de la red
- Administración de parches
- Superficies de ataque ampliadas

Presiones normativas y de conformidad

A diferencia de los sistemas existentes o heredados, las tecnologías emergentes se enfrentan a una serie de diversos retos y en rápida evolución en todo el panorama mundial. En algunos casos, dada la naturaleza fragmentada de tecnologías como IoT, la falta de una norma unificada fomenta muchos problemas de seguridad de los datos. En lo que respecta a la IA, muchos están de acuerdo en los beneficios de rendimiento de la utilización de la tecnología, pero pocos parecen comprender o ponerse de acuerdo posteriormente sobre las implicaciones de su uso para la humanidad o el medio ambiente.

Aunque muchas de estas preocupaciones se están resolviendo en tiempo real, en el caso de las leyes que se han puesto al día con la tecnología, las estrictas protecciones de datos como la Ley de Privacidad del Consumidor de California (CCPA) y el Reglamento General de Protección de Datos de Europa (GDPR) añaden un inmenso escrutinio a la manera en que se utiliza la tecnología emergente. Otras consideraciones que requieren una evaluación metódica por parte de los responsables de las empresas para determinar si pueden utilizarse y dónde son:

- Residencia de datos
- Resiliencia operativa
- Administración de riesgos de terceros
- Factores de gobernanza
- Consideraciones éticas

Soluciones a futuro y buenas prácticas

Cuando llega la hora de resolver los retos que plantea la implantación de tecnologías emergentes, las empresas deben anclar su enfoque en las mejores prácticas probadas para optimizar la reducción de riesgos. Este enfoque disciplinado admite una administración de terminables escalable y resistente, a medida que las flotas se diversifican y evolucionan nuevos casos de uso que benefician más específicamente a las crecientes necesidades empresariales.

Inventario de terminales

Antes de que una empresa pueda evaluar los riesgos de forma exhaustiva, primero necesita saber cómo es la infraestructura. Y la mejor manera de hacerse una idea de lo que hay es realizar un inventario completo de todo el hardware, el software, los servicios y los procesos. Un conocimiento detallado de:

- Todos los dispositivos
- Sus dependencias
- Los flujos de trabajo y políticas

Identificar cada componente y cómo se interconectan ofrece una visión holística de toda la infraestructura, cómo se comunica y con qué dispositivos, lo que proporciona a las empresas una base sólida para implantar soluciones con visión de futuro.

Evaluación de riesgos

El siguiente paso es evaluar los factores de riesgo para determinar su gravedad. El objetivo durante esta fase no es solo reducir el riesgo, sino alinear cada uno de ellos con la tolerancia o apetito general de riesgo de la organización.

La combinación de métodos cualitativos y cuantitativos permite elaborar un índice programático de riesgos cibernéticos, que proporciona a los responsables de la toma de decisiones una visión general basada en datos y en indicadores clave de ataques, como:

- **Vectores:** La ruta o método utilizado para ejecutar un ataque o comprometer un sistema.
- **Complejidad:** La habilidad y los recursos necesarios para que un adversario explote una debilidad.
- **Impacto:** Las consecuencias empresariales y operativas de un ataque exitoso.
- **Exposición:** las debilidades o lagunas que dejan un entorno abierto a la explotación.
- **Gravedad:** Medida de la probabilidad de una amenaza y de lo perjudicial que podría ser.
- **Solución:** Si existe una solución, en qué consiste y con qué rapidez puede implementarse.

Modelado de amenazas

El tercer paso es un enfoque proactivo para identificar y priorizar los riesgos en dispositivos, sistemas y aplicaciones. Más específicamente, la realización de modelos de amenazas antes de las pruebas de penetración (hablamos más sobre esto en la siguiente sección) se centra en priorizar los riesgos de mayor a menor gravedad. A su vez, esto ayuda no solo a reducir el riesgo de los dispositivos, sino también a mantener una postura de seguridad organizativa reforzada.

Existen múltiples modelos de amenazas y pueden utilizarse para evaluar tipos específicos de riesgo, o como un enfoque integrado para encontrar y cuantificar sistemáticamente las amenazas; o dicho de otro modo, la mejor manera de mitigar a un atacante es pensar como uno.

Las metodologías comunes de modelado de amenazas y sus usos son (por sus siglas en inglés):

STRIDE:
Suplantación, manipulación, repudio, revelación de información, denegación de servicio y elevación de privilegios.
QUÉ HACE:
Este modelo clasifica el riesgo en función de su comportamiento en cada una de las seis categorías.

DREAD:
Potencial de daño, reproducibilidad, explotabilidad, usuarios afectados y facilidad de ser descubiertas.
QUÉ HACE:
Este modelo produce una puntuación media basada en los cinco factores para clasificar la gravedad del riesgo. (A menudo se utiliza junto con STRIDE para priorizar la mitigación de las amenazas de alto riesgo).

LINDDUN:
Vinculación, identificación, no repudio, detección, divulgación de datos, desconocimiento e incumplimiento.
QUÉ HACE:
Este modelo proporciona un método estructurado para identificar y mitigar las amenazas basadas en la privacidad, basándose en el análisis de cómo fluyen los datos dentro de las aplicaciones y sistemas.

PASTA:
Proceso de simulación de ataques y análisis de amenazas.
QUÉ HACE:
Este modelo se centra en el impacto del riesgo para las empresas, incluidos los requisitos técnicos (por ejemplo, definir objetivos y alcance, analizar vulnerabilidades y simular ataques), para el desarrollo de estrategias de mitigación de riesgos.

OCTAVE:
Evaluación de amenazas, activos y vulnerabilidades críticos desde el punto de vista operativo.
QUÉ HACE: Este modelo también se centra en el riesgo empresarial que alinea la ciberseguridad con los objetivos empresariales a través de tres fases: construcción de perfiles de amenazas basados en activos, identificación de vulnerabilidades de infraestructura y desarrollo de estrategias de administración de riesgos.

Prueba de penetración

Podría decirse que la tarea de evaluación de riesgos más común es la prueba de penetración (pentest), que suele realizarse para encontrar y priorizar vulnerabilidades en dispositivos y software. La decisión de incluir esto último en la lista se remonta a la sección anterior sobre modelado de amenazas. Cuando se realiza después del modelado de amenazas, la pentest añade una capa de eficiencia y eficacia al proceso de evaluación de riesgos.

Esto se consigue en el primer caso:

- Al permitir enfocarse a los pentesters en los riesgos de mayor gravedad (ya que el modelado de amenazas probablemente identificó amenazas de menor riesgo)
- Al facilitar la mitigación de riesgos por parte de las TI en una fase más temprana del proceso de evaluación

Para este último:

- El pentesting valida las medidas correctivas aplicadas anteriormente
- Se añade otra capa de escrutinio para encontrar vulnerabilidades que puedan haber pasado desapercibidas anteriormente

Estado de seguridad del dispositivo y acceso que dé prioridad a la identidad (hacia el modelo Zero Trust)

Las tecnologías emergentes requieren estrategias que den prioridad a la identidad y una validación continua de la postura de los dispositivos para salvaguardar los datos confidenciales y mantener la integridad operativa. La modernización de la administración para seguir prestando apoyo a flotas cada vez más diversificadas debe automatizar el cumplimiento de la normativa, reducir los gastos operativos y ampliar sin problemas la confianza cero.

Las siguientes soluciones proporcionan herramientas variables para ayudar a TI en la administración del ciclo de vida de las tecnologías emergentes:

- **Administración de dispositivos móviles (MDM)**: Integra la administración de dispositivos e identidades, junto con la seguridad de terminales de forma integral, **desde la implementación sin contacto hasta la eliminación segura**, en las instalaciones o en la nube.
- **Administración unificada de terminales (UEM)**: En las instalaciones o en la nube, ofrece compatibilidad entre plataformas, pero a menudo se intercambia por un ámbito de capacidades más reducido.
- **Servicios Web de Amazon (AWS):** Modelo basado en la nube que ofrece una capacidad de administración y seguridad limitada a tecnologías específicas, como dispositivos IoT y compatible con varios proveedores.
- **Administración autónoma de terminales (AEM):** El futuro de la UEM basada en la nube, que reduce los costos operativos mediante la automatización e impone la confianza cero validando y corrigiendo continuamente la postura de los dispositivos —para flotas diversificadas— a escala.

Controles de apps y datos

Cuando se reducen a su nivel básico, independientemente del tipo de dispositivo o del sistema operativo que utilice, los datos son datos. La protección de los datos sigue estando en el núcleo de cada control, proceso y tarea realizados al servicio de la administración y la seguridad de la tecnología emergente.

La implementación de configuraciones es un método eficaz para proteger los dispositivos y los datos procesados y contenidos en ellos. Aunque los métodos admitidos dependerán en gran medida de la plataforma del sistema operativo, el objetivo es establecer configuraciones seguras basadas en las mejores prácticas, como normas e infraestructuas, que se traduzcan más allá de las fronteras de los sistemas operativos para mantener los datos a salvo.

Algunos ejemplos de herramientas utilizadas para crear configuraciones seguras son:

- **Android**: **OEMConfig** y **Android Open Source Project** (AOSP)
- **Apple**: **Apple Configurator**, **Jamf Pro** y **Declarative Device Management** (DDM)
- **Linux**: Scripts Bash, **SOTI MobiControl** y **Microsoft Intune**
- **Propietario:** Revise el sitio de soporte del fabricante para obtener información sobre dónde obtener herramientas específicamente adaptadas a la tecnología

Monitoreo y respuesta

La visibilidad del estado de las terminales es un componente esencial de la ciberseguridad proactiva. Cuanto antes se identifiquen los problemas, más rápido podrá la respuesta ante incidentes mitigar el riesgo o remediar la amenaza. La supervisión activa de las terminales dentro de la infraestructura de su empresa no solo es muy recomendable, sino que es un componente crucial de la arquitectura de confianza cero.

Las protecciones en el dispositivo y en la red son los dos aspectos de las protecciones de confianza cero. Mientras que la parte de la red se trata en la siguiente sección, aquí hay directrices que se enfocan en las terminales para mantener posturas sólidas de los dispositivos en toda su infraestructura:

- Supervisión activa de la telemetría de la salud del dispositivo y los niveles de cumplimiento
- Integración de las soluciones de administración y seguridad para automatizar la respuesta
- Implementación de la confianza cero para verificar la salud de las terminales antes de conceder acceso a los recursos
- Implementación de actualizaciones del sistema operativo y parches de seguridad y de aplicaciones con regularidad

Seguridad de la red

Las tecnologías emergentes suelen avanzar más rápido que los estándares, lo que dificulta la administración de ciertas terminales o provoca un desalineamiento con los objetivos empresariales. Dado que el riesgo es subjetivo, las estrategias de seguridad no son universales. Esto eleva el enfoque a la seguridad de los datos desde las terminales. Las siguientes soluciones —ya sea instaladas por separado o combinadas— ayudan a maximizar la seguridad de los datos en entornos locales y en la nube:

- **Zonas desmilitarizadas (DMZ)**: Segmenta los dispositivos de alto riesgo, como la IoT, permitiendo solo la comunicación controlada con sistemas internos o redes externas en función de políticas.
- **Red de área local virtual (VLAN):** Aísla el tráfico de red —limitando el movimiento lateral y obligando las comunicaciones de acceso mínimo— lo que proporciona a TI un control granular sobre el tráfico entre dispositivos y sistemas de misión crítica.
- **Orquestación, automatización y respuesta de seguridad (SOAR)**: Unifica las herramientas y los flujos de trabajo de seguridad mediante la automatización para acelerar la detección, respuesta y contención de amenazas.
- **Acceso a la red basado en Zero Trust (ZTNA)**: Aplica una verificación continua de dispositivos basada en el contexto, microtúneles (por solicitud de conexión) y evaluaciones de estado para garantizar que solo los dispositivos que cumplen con las políticas puedan acceder a los recursos protegidos.

Líneas de base y puntos de referencia, normas y marcos

Es importante considerar cada sección como una fase cíclica en lugar de lineal. Los ciclos de vida en TI y seguridad son iterativos —no son un destino, sino un camino sin fin— que informa de lo que viene después y está moldeado por lo que vino antes. Teniendo esto en cuenta, la sinergia entre cada uno de los siguientes elementos es primordial para mantener la seguridad, mientras se introducen tecnologías emergentes en la pila tecnológica de su entorno informático:

- **Líneas de base:** Conjunto de controles y procesos que **definen una postura de seguridad fundacional.**
- **Puntos de referencia:** Métricas de rendimiento utilizadas para **medir el cumplimiento de las mejores prácticas de seguridad.**
- **Normas:** Mejores prácticas mundialmente reconocidas que identifican cómo se debe **proteger el hardware, el software y/o los servicios para cumplir un requisito específico**.
- **Marcos:** Directrices estructuradas que detallan cómo los controles, las políticas, los procesos y las normas **deben desplegarse para minimizar los riesgos** y maximizar la seguridad.

Conclusión

Una vez comprendidas las tecnologías emergentes y su impacto en los objetivos empresariales, ahora es el momento de que los directivos y los equipos de TI den el siguiente paso para alinear las estrategias de administración y seguridad existentes con las mejores prácticas orientadas al futuro. Actuando ahora, las organizaciones pueden adelantarse a los riesgos emergentes, optimizar las operaciones y abrazar con confianza la próxima era de la innovación.

Lista de control: Próximos pasos para directivos de empresas y responsables de TI

1. Identificar casos de uso empresarial

- Evalúe dónde se alinean las tecnologías emergentes (IA, IoT, computación espacial, wearables) con los objetivos empresariales.
- Determine el posible retorno de la inversión y las mejoras operativas con respecto a los flujos de trabajo existentes.
- Dé prioridad a las iniciativas que ofrezcan resultados empresariales mensurables y preparación para la conformidad.

2. Establecer un equipo de evaluación interfuncional

- Forme un comité con las partes interesadas de TI, seguridad, legal y operaciones.
- Asigne la propiedad de la evaluación de riesgos, la revisión de la conformidad y la administración del ciclo de vida.
- Defina canales de comunicación para una rápida retroalimentación y escalamiento.

3. Conducir un inventario completo de activos y dependencias

- Documente todos los dispositivos, software, API y servicios en la nube utilizados en la infraestructura.
- Identifique las dependencias de integración en entornos híbridos (nube, local y periférico).
- Modelos de propiedad de etiquetas (COBO/COPE/BYOD/CYOD) para garantizar la visibilidad y la responsabilidad.

4. Realizar evaluación de riesgos y amenazas

- Utilice métodos cualitativos y cuantitativos para calibrar la tolerancia al riesgo y su impacto.
- Mapee las amenazas utilizando modelos de precisión y coherencia.
- Clasifique las vulnerabilidades por gravedad, explotabilidad y plazos de corrección.

5. Realizar un modelado de amenazas

- Simule posibles rutas de ataque utilizando marcos de modelado de amenazas aceptados.
- Identifique la privacidad, el flujo de datos y los puntos de exposición operativos.
- Documente las mitigaciones para reducir el riesgo antes de la puesta en producción.

6. Validar los requisitos de cumplimiento y gobernanza

- Revise la normativa regional y específica de la industria.
- Confirme la residencia de los datos, la soberanía y la administración de riesgos de proveedores externos.
- Incorpore consideraciones éticas para la IA y las tecnologías basadas en datos.

7. Definir los procesos de inscripción y aprovisionamiento

- Estandarice los flujos de trabajo de incorporación para todos los tipos de dispositivos y modelos de propiedad.
- Automatice la configuración, la cadencia de aplicación de parches y los controles de acceso para minimizar los errores manuales.
- Utilice la inscripción segura y la autenticación basada en la identidad para la verificación de terminales.

8. Integrar estrategias de acceso basadas en la identidad

- Exija la verificación continua de las credenciales y la postura del dispositivo antes de acceder a los recursos.
- Obligue la aplicación de los principios de privilegios mínimos en todas las terminales y aplicaciones.
- Integre la confianza cero y las políticas sensibles al contexto en los sistemas de control de acceso.

9. Establecer controles seguros de configuración y datos

- Defina líneas de base de seguridad para establecer las expectativas de configuración y conformidad.
- Cifre los datos confidenciales en reposo y en tránsito.
- Aplique políticas granulares de clasificación, almacenamiento y uso compartido de datos.

10. Segmentar y reforzar las comunicaciones de red

- Utilice VLAN y DMZ para aislar los dispositivos de alto riesgo, como el IoT y los wearables.
- Aplique la microsegmentación y el acceso de red de confianza cero (ZTNA) para obtener controles de seguridad adaptables dentro de la red.
- Garantizar la seguridad de los datos es fundamental para la seguridad de la red, independientemente del tipo de dispositivo, el modelo de propiedad, la plataforma del sistema operativo o el lugar desde el que trabajen los usuarios.

11. Implementar políticas de monitoreo continuo y respuesta automatizada

- Recopile telemetría de todos las terminales para obtener visibilidad en tiempo real e información sobre su estado.
- Implemente flujos de trabajo automatizados para la detección de anomalías y la respuesta a incidentes.
- Transmita alertas a herramientas centralizadas para automatizar las tareas de detección y corrección de amenazas.

12. Aplicar líneas de base, puntos de referencia y recopile métricas de productividad

- Aplique normas de configuración en la línea de base para una seguridad holística en toda la empresa.
- Utilice puntos de referencia para medir el rendimiento y las posturas de seguridad.
- Revise los KPI para evaluar el estado de cumplimiento y demostrar la reducción de riesgos.

13. Llevar a cabo validaciones periódicas: pruebas de penetración y auditorías

- Programe pruebas de penetración y análisis de vulnerabilidades recurrentes tras la implementación.
- Valide las medidas correctivas identificadas durante el modelado de amenazas.
- Revise los resultados con respecto a las líneas de base establecidas y actualice las políticas en consecuencia.

14. Automatizar la administración del ciclo de vida y la aplicación obligatoria de políticas

- Aproveche los sistemas unificados de terminales o de administración autónoma para la conformidad continua.
- Automatice los procesos de aplicación de parches, las políticas de conformidad y los flujos de trabajo de retirada de dispositivos.
- Adapte continuamente las configuraciones a las infraestructuras y normas en evolución.

15. Documentar los hallazgos y llevar a cabo una capacitación periódica

- Establezca circuitos de retroalimentación para las amenazas emergentes y las lecciones aprendidas.
- Imparta capacitación continua a administradores y usuarios para que reconozcan los riesgos.
- Reevalúe la idoneidad e realice la iteración de controles a medida que evolucionan las tecnologías y las normativas.