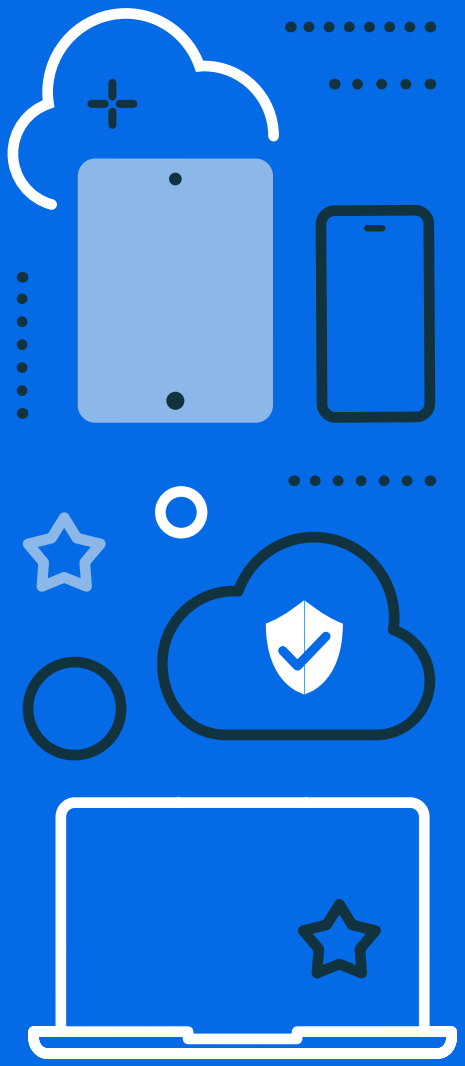


# Política de datos y administración

## para principiantes

jamf

Ahora más que nunca, las empresas apoyan a los trabajadores remotos e híbridos y necesitan algo más que los fundamentos de la administración de dispositivos. Los dispositivos móviles de la empresa proporcionan la libertad de trabajar en cualquier momento y lugar, pero esta flexibilidad conlleva el desgaste que el uso y el comportamiento personal tienen en los dispositivos de la empresa, incluso en los dispositivos habilitados personalmente en su plan de telefonía móvil.

Jamf Data Policy ayuda a las organizaciones a habilitar y mantener el trabajo a distancia, garantizando que los usuarios sigan siendo productivos, independientemente de su ubicación y de los dispositivos que utilicen al pasar a entornos híbridos y remotos.

Al sacar el máximo partido a las siguientes tecnologías, las organizaciones pueden:

- Aplicar políticas personalizables para garantizar el cumplimiento
- Configurar los umbrales de limitación de datos y de alertas
- Filtrar el contenido inapropiado
- Ampliar las políticas a todas las comunicaciones de la red
- Controlar y eliminar el equipo de IT de respaldo
- Administrar el uso en tiempo real

**Aprenda lo que necesite saber para establecer una política de uso aceptable y administrar los datos y dispositivos de su empresa de forma que se ajusten a las necesidades de ésta y de los usuarios finales.**

La administración de dispositivos se considera a menudo una tarea muy científica. Una vez respaldada por todo tipo de datos para llegar al nivel de administración óptimo que garantice que los dispositivos, los usuarios y los datos estén protegidos y sigan estándolo. Y aunque este hecho no se discute aquí, hay un poco de "magia" en ser un administrador de éxito. Algo que proviene de la experiencia y de un profundo conocimiento de las necesidades únicas de su red. Al fin y al cabo, a pesar de los estándares y las mejores prácticas, cada red es realmente su propia isla que opera bajo las políticas específicas de su organización.

***"¡La magia no existe!"*** *— Tío Vernon*

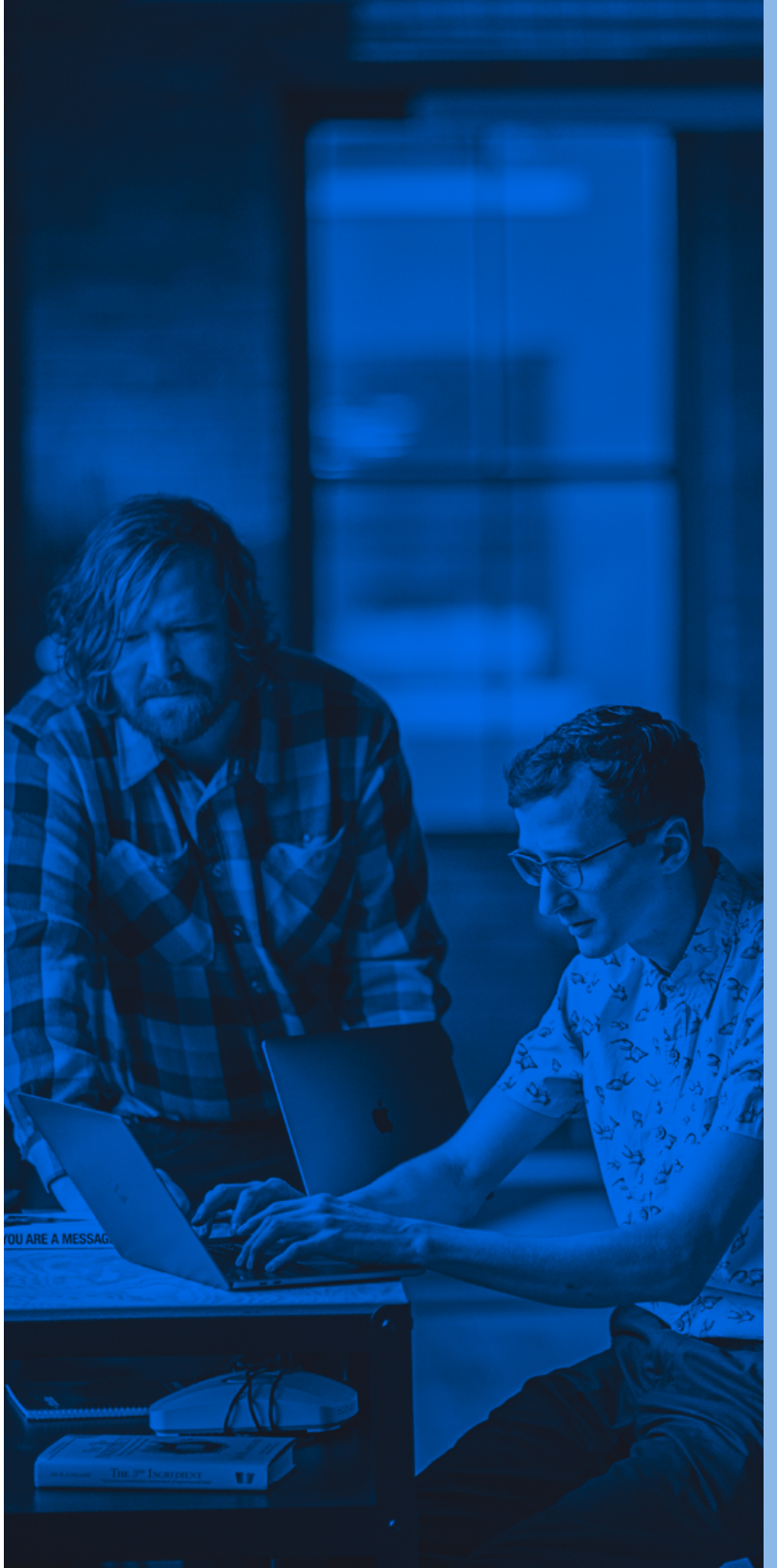
**¿No le parece mágico cuando sus dispositivos funcionan de forma óptima?**

Que los datos estén seguros, las aplicaciones corporativas y los recursos sean accesibles, pero estén protegidos. Y los usuarios estén contentos, con la capacidad de utilizar dispositivos seguros para realizar tareas laborales y personales, sin que las prácticas de administración de mano dura les impidan ser productivos o disfrutar de su tiempo de inactividad. ¿Qué sucede cuando se detectan problemas aunque se mitigue el riesgo mediante la automatización, sin que el departamento de IT tenga que mover un dedo ni el usuario final se vea afectado negativamente?

Ese es el tipo de magia que es ejercida por los administradores de los dispositivos móviles que impulsan Jamf Data Policy. Más allá de los fundamentos, Jamf Data Policy ayuda a las organizaciones a dar soporte a las prácticas empresariales en entornos de trabajo a distancia e híbridos. Independientemente del tipo de dispositivo o de si se trata de dispositivos personales como parte de una iniciativa BYOD (trae tu propio dispositivo) o de una flota de propiedad corporativa que permite la flexibilidad de utilizar dispositivos para tareas laborales y personales, es esencial contar con una política de uso aceptable y con un lugar, así como con los medios para administrarla y hacerla cumplir.

Aquí tiene un punto de partida para crear o evaluar su política de uso aceptable. Considere cómo su organización puede:

- Facultar a sus administradores a monitorear el consumo de datos con análisis en tiempo real y reportes granulares
- Forzar la aplicación de políticas de uso aceptable
- Eliminar el equipo de IT de respaldo
- Filtrar contenidos
- Implementar políticas de protección personalizadas para satisfacer las necesidades de sus usuarios y de su organización
- Apoyar su red de forma integral, independientemente del dispositivo o del tipo de propiedad

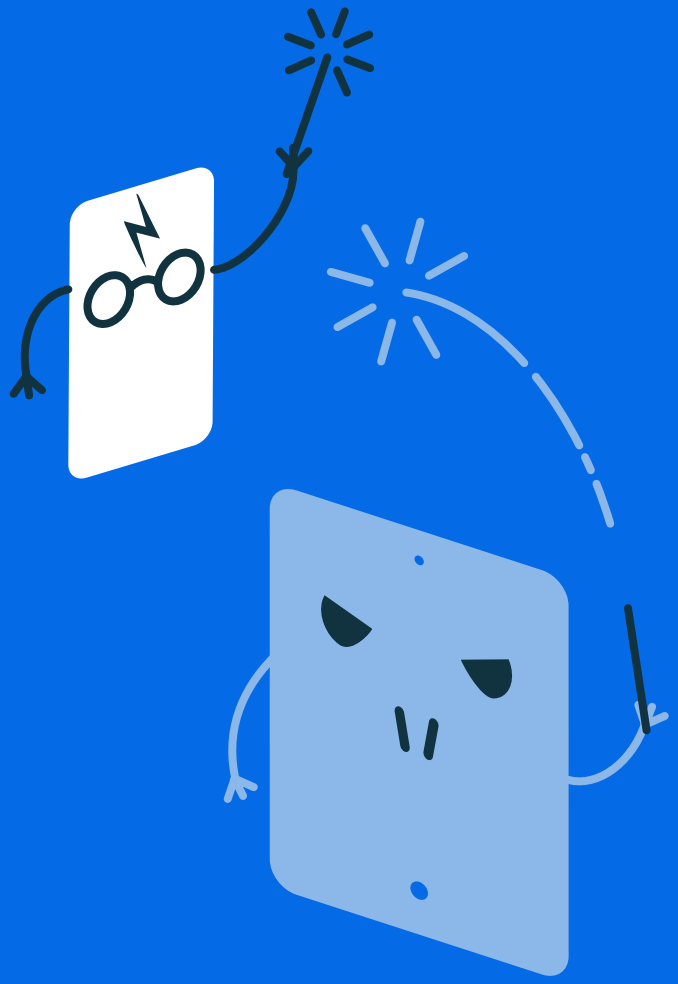


# HARRY POTTER CONTRA VOLDEMORT

Antes de profundizar en las características de Jamf Data Policy, vamos a tocar algunas de las razones por las que es necesario ayudar a su organización a administrar la flota de dispositivos móviles de su red. Y qué mejor manera de describir el caso de uso que invocando al más grande de los magos modernos, ¡Harry... Potter, así es!

En la serie de libros escritos por la autora J.K. Rowling, los magos del universo Pottermore comparten similitudes con los administradores de IT en el sentido de que se les presenta una opción: ser como Voldemort o ser como Harry: quedarse con nosotros.

Si elige el camino de Voldemort, su organización gobernaría con puño de hierro, obligando a los usuarios a adaptarse a sus políticas, a pesar de sus necesidades o de las consecuencias no deseadas.



Pero si elige emular a Harry, su organización funcionaría con equidad, optando por errar en el lado de la zona de riesgos mientras se trabaja conjuntamente para resolver el problema mayor.

***"Todos debemos enfrentarnos a la elección entre lo que es correcto y lo que es fácil".*** *– Albus Dumbledore*

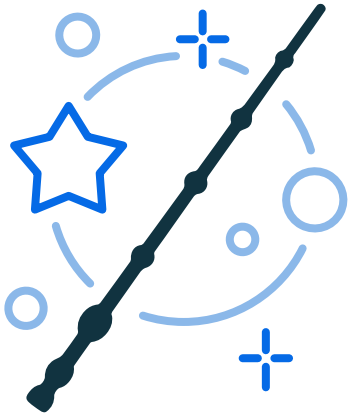
Aunque es fácil para los informáticos elegir el camino de Voldemort en nombre de la seguridad y la protección de los usuarios, la triste realidad es que, a menudo, este último camino presenta más opciones para lograr la seguridad de los datos y proteger a los usuarios, ya que todos los interesados trabajan juntos para lograr este objetivo común y no luchan contra controles excesivos o restrictivos que no hacen más que ahogar la productividad y, en última instancia, enemistarse con los usuarios.

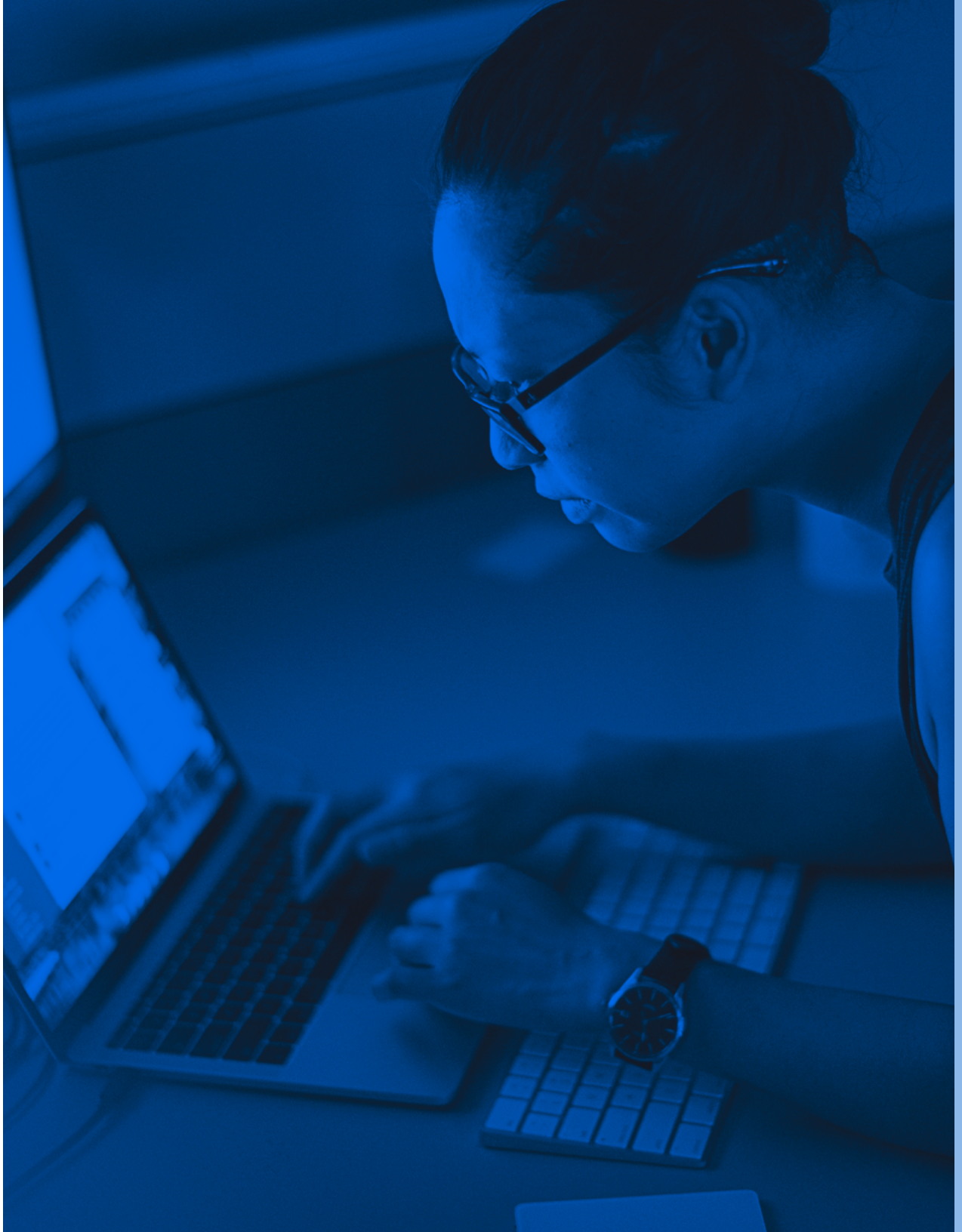
Como ya se ha dicho, cada red es diferente y se adhiere a un conjunto de normas, políticas, leyes y reglamentos distintos a los de la siguiente, por lo que, en lo que respecta a las políticas y la administración de datos, no hay una respuesta única para todos. Pero teniendo esto en cuenta, administrar los dispositivos según el método Voldemort seguramente no hará más que encasillar a los equipos de IT, eliminando de hecho la fluidez necesaria para supervisar, detectar, responder y remediar cualquier problema potencial que se encuentre en el dinámico mundo de la tecnología de la información. ¿Está de acuerdo?

# LA VARITA DE SAUCO

Al igual que Harry Potter, los administradores de IT son solo personas. Personas comunes y corrientes con habilidades que, aunque formidables, necesitan una forma de ser canalizadas para ser utilizadas eficazmente. Harry tenía la Varita de Sauco. Usted tiene Jamf Data Policy.

En concreto, profundizaremos en dos características que proporcionan a las organizaciones las protecciones defensivas necesarias para administrar en forma integral sus dispositivos móviles de manera constante y eficiente.





## CONTROL DE POLÍTICAS EN TIEMPO REAL

La configuración de políticas de límites para el uso de datos y su aplicación cuando se alcanzan los umbrales, que definen a cuáles sitios web, servicios y apps se puede acceder y la visibilidad del uso con controles basados en categorías, además de su personalización para activar la automatización de la aplicación de las políticas, ofrecen una visión de cómo se pueden seleccionar las políticas de IT de la organización para restringir el acceso a contenidos y apps inapropiados que no se consideran críticos para la empresa.

Más del 50% del uso de datos de las empresas no es crítico para la empresa, según Jamf. Este nivel de visibilidad sin precedentes sobre el uso de los datos permite a las organizaciones configurar de forma granular los grupos de datos y el uso del tráfico basado en la red, de modo que los dispositivos móviles se utilicen como herramientas y no como objetos de los que se puede abusar por falta de conocimientos o controles.

***"El tiempo no se ralentizará cuando surja algo desagradable más adelante".***

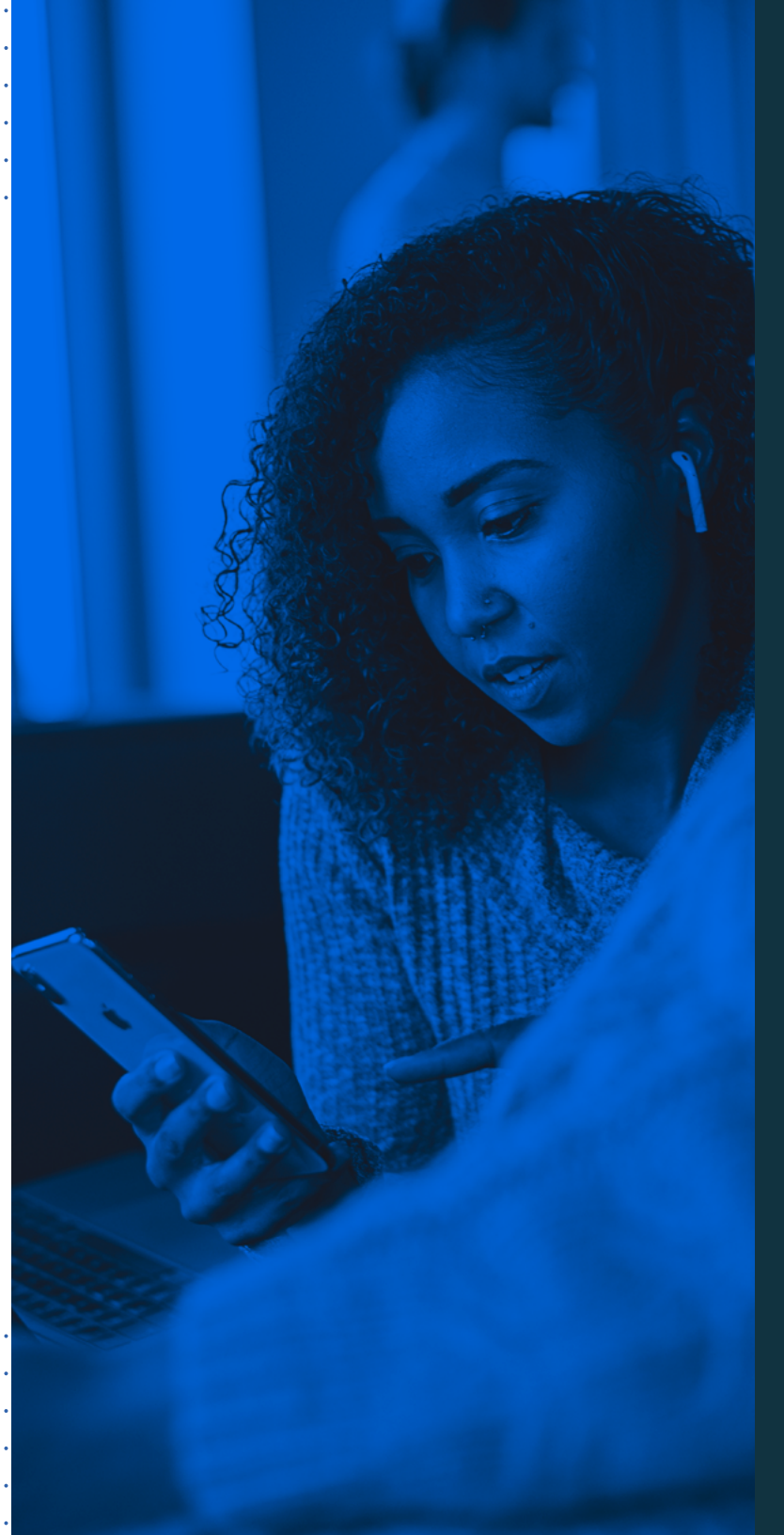
*– Harry Potter y el Cáliz de Fuego*

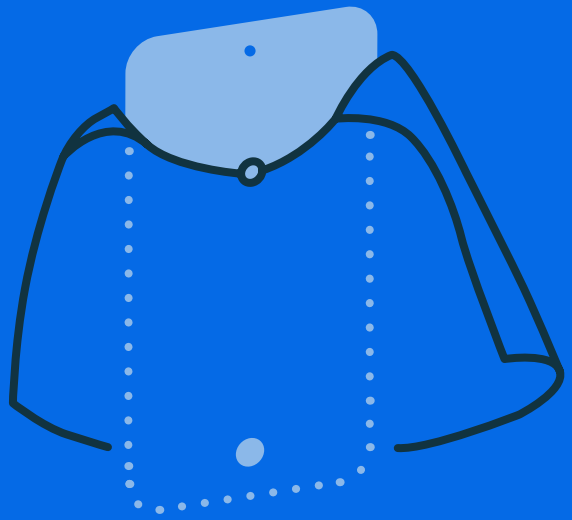
## CUALQUIER DISPOSITIVO MÓVIL, CUALQUIER MODELO DE PROPIEDAD

Programa "Trae tu propio dispositivo" (BYOD) CYOD. COPE. Esta diversidad de siglas se refiere a los programas de dispositivos móviles que indican diversos grados de apoyo según el modelo de programa. Si averiguar qué modelo de propiedad apoyar no era ya lo suficientemente difícil por sí solo, la variedad de tipos de dispositivos móviles, proveedores y transportadoras seguramente servirá para complicar aún más las cosas, ¿verdad?

Pero eso no ocurrirá con Jamf Data Policy.

La única decisión que debe tomar su organización es elegir qué dispositivos son los mejores para su empresa. Independientemente del tipo de dispositivo, el modelo de propiedad o el sistema operativo, Jamf es compatible con toda la gama de estas opciones, lo que permite al departamento de IT centrarse en la administración de los dispositivos móviles prestando la máxima atención a las políticas de seguridad y cumplimiento, sin preocuparse de encajar la clavija cuadrada en el agujero redondo que suele corresponder a la administración de sistemas heterogéneos.





# LA CAPA DE INVISIBILIDAD

Desde el punto de vista de la informática, tener una capa que lo haga invisible podría ser útil cuando se reciben demasiados tíckets a la vez. ¿Se imagina bajar la cabeza y centrarse únicamente en resolver los problemas en lugar de atender una oleada tras otra de correos electrónicos, mensajes de texto, llamadas y "preguntas rápidas"?

Pues bien, si esto le dice algo, hay un par de características más en Jamf Data Policy que pueden ser interesantes para ayudar a frenar el maremágnum de solicitudes mediante la estandarización del uso de los recursos, exigiendo el cumplimiento y el establecimiento de las expectativas de los usuarios.

## TOTALMENTE PERSONALIZABLE

No hay dos redes iguales, ya que no hay dos organizaciones que administren su infraestructura ni que identifiquen los mismos requisitos para la continuidad del negocio. En gran medida, esto dependerá del apetito de riesgo de la organización. Y al igual que las empresas modifican su postura de seguridad para hacer frente a los riesgos, también Jamf Data Policy permite la personalización integral de las políticas y su aplicación para la administración.

Desde la adaptación de las categorías de filtrado de contenidos hasta la personalización de las listas de permitidos y bloqueados, las políticas pueden aplicarse de forma holística (la organización en su conjunto) o de forma granular, aplicándose a un solo usuario —o a través de la pertenencia a un grupo—, las opciones son flexibles y funcionan para satisfacer las necesidades de su organización. Y lo más importante, la elección es suya.

## FILTRADO DE CONTENIDOS

Jamf descubrió que las apps y servicios para adultos y de juegos de azar son significativamente más propensos a depender de conexiones no cifradas que pueden exponer potencialmente a las organizaciones a riesgos por fugas de datos y cumplimiento de los organismos reguladores. Más allá de las categorías señaladas, acceder a contenidos que contengan armas, discursos de odio u otras formas de material incendiario puede ocasionar consecuencias civiles y/o penales reales para los usuarios y/o la organización.

Esto, por no hablar de las amenazas a la seguridad que provienen de los contenidos basados en la web, como los sitios web de phishing y otras formas de malware que se instalan en las cuatro esquinas de la inmensa Internet. El filtrado de contenidos no consiste únicamente en mantener fuera la maldad. Si se utiliza de forma proactiva, puede tratarse de permitir solo la entrada de los datos autorizados, asegurándose de que se puede acceder a sitios web, servicios y apps aceptables.

Además, es esencial reducir la exposición a los litigios mediante la administración y el mantenimiento de un uso de datos que cumpla los estándares y la supervisión para el bloqueo del acceso a los servicios no autorizados, servicios como las IT de respaldo que pueden socavar la postura de seguridad de sus dispositivos y su red al exponer inadvertidamente datos corporativos sensibles.

# LA PIEDRA FILOSOFAL

Lamentablemente, en esta sección no se hablará de la fórmula para elaborar el elíxir de la vida ni de cómo convertir los metales comunes en oro, pero sí se hablará de la siguiente mejor opción: dos características más de Jamf Data Policy que, a su manera, hacen su propia magia al recopilar información en tiempo real, permitiendo a los administradores de IT convertir esos datos en tareas procesables utilizadas para adaptarse y administrar mejor su flota de dispositivos.

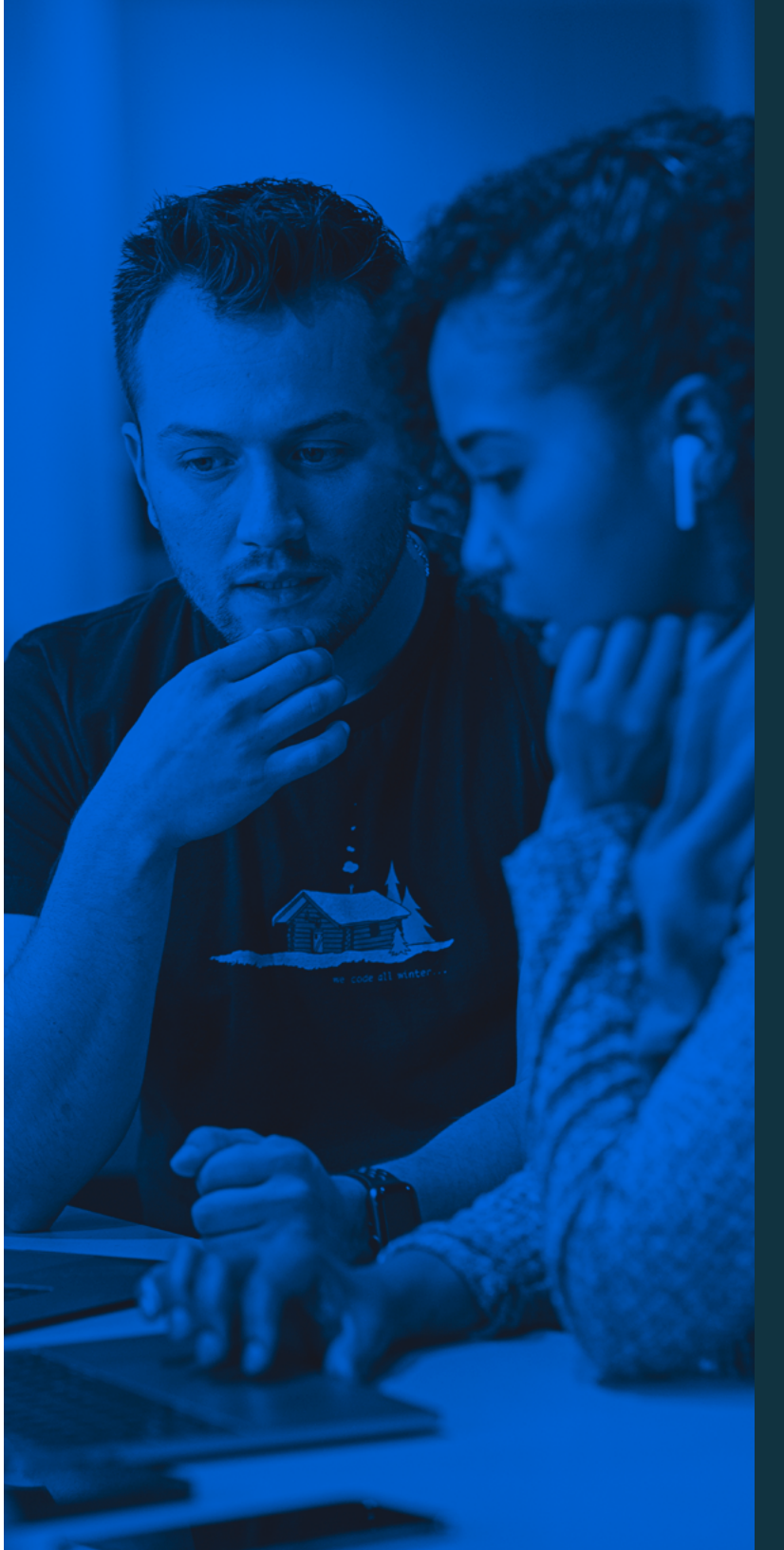
Yendo aún más lejos, las características hacen que las protecciones sean conscientes de la red, lo que significa que, sin importar si se generan nuevas sesiones o se cierran conexiones existentes, sus dispositivos y usuarios seguirán estando protegidos y cumpliendo con todos los tipos de conexión de red.

## CONCIENCIA DE RED

Como ya hemos establecido, una talla única no sirve para todos. Nada abarca más este concepto que las conexiones de red de su dispositivo móvil. Por ejemplo, cuando los usuarios están obligados a utilizar conexiones móviles medidas, a menudo serán más conscientes de los límites de uso debido a los cargos adicionales en los que pueden incurrir por la itinerancia y/o las tarifas por exceso de uso. Sin embargo, si pueden conectarse a un punto de acceso Wi-Fi público, es muy probable que los problemas de ancho de banda no sean una preocupación.

Jamf Data Policy aclara la administración de estas aguas turbias permitiendo a los administradores crear y exigir la aplicación de políticas para los diferentes tipos de conexión de red y de sus variables únicas.

Supongamos que su organización apoya el modelo COPE (propiedad de la empresa, habilitada personalmente) y proporciona dispositivos móviles a sus empleados tanto para el trabajo como para el uso personal, pero el plan de datos del celular forma parte de un conjunto de datos que comparten todos los usuarios. Es posible que su organización quiera restringir el ancho de banda utilizado por los usuarios para que haya suficientes datos para todos mientras estén en el celular, sin establecer una administración del ancho de banda en las conexiones Wi-Fi. Jamf Data Policy permite aplicar políticas que pueden implementarse para hacer precisamente eso: limitar el ancho de banda mientras se está en el celular, pero no en Wi-Fi. Además, las políticas son lo suficientemente inteligentes como para detectar qué conexión se está utilizando en ese momento y se ajustan automáticamente sin necesidad de que el departamento de IT realice aportaciones adicionales o afecte a la experiencia del usuario final.



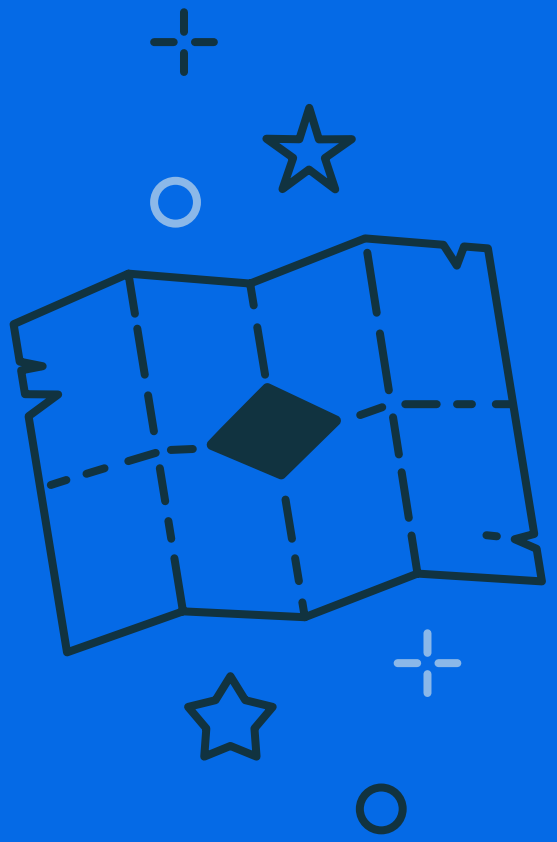
## DATOS EN TIEMPO REAL

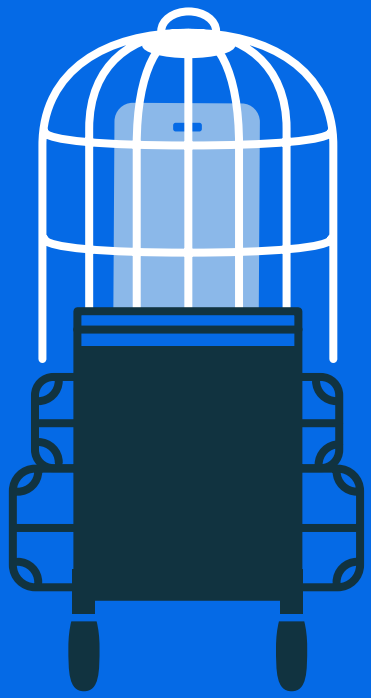
***"Juro solemnemente que no estoy tramando nada bueno".*** *— Harry Potter*

Pregunte a cualquier administrador si prefiere saber cuándo se va a descomponer o fallar algo antes de que ocurra (proactivo) o después de que ocurra (reactivo), y la respuesta probablemente será siempre la misma: quieren saberlo de antemano.

Si se le diera la opción, cualquiera desearía tener un aviso previo. Si no es para intentar frenar que ocurra el suceso, al menos para mitigarlo lo antes posible.

¡Hurra! La información en tiempo real de Jamf Data Policy proporciona precisamente eso: un aviso preventivo a través de informes granulares que proporcionan transparencia al equipo de IT sobre la forma en que los dispositivos están utilizando sus datos y sobre qué conexiones. Los administradores pueden modificar de forma proactiva las políticas que necesiten ser más (o menos) restrictivas, hacer cambios en los grupos de datos existentes, configurar el filtrado de contenidos para habilitar/deshabilitar el acceso a determinadas apps y servicios, o simplemente vigilar la postura de seguridad de un dispositivo.





# AHORA SUBAMOS AL ANDÉN 9¾

Tener inscrita en Jamf Pro su flota de dispositivos móviles o los dispositivos personales de los usuarios es una base excelente para la administración de dispositivos. Pero en los modernos entornos de trabajo actuales, que se centran en el trabajo híbrido o a distancia, la simple administración del dispositivo físico requiere una herramienta más especializada.

Jamf Data Policy es esa herramienta:

- Administra la forma en que se envían y reciben los datos en el propio dispositivo a través de políticas inteligentes que son conscientes de la red
- Se adhiere a las normas de cumplimiento a través de cualquier conexión de red
- Filtra el contenido con 70 plantillas diseñadas de forma inteligente para evitar que los dispositivos se conecten a sitios web, apps y servicios vulnerables, comprometidos y maliciosos, además del contenido no aprobado

Por último, Jamf Data Policy simplifica el trabajo del departamento de IT eliminando la IT de respaldo y aplicando políticas de uso aceptables para todos los dispositivos —sin importar el nivel de propiedad—, no solo para asegurar los datos, sino también los dispositivos y los usuarios, sin interrumpir la experiencia de los interesados.

## Solicite una prueba

Empiece hoy mismo con una prueba gratuita, o comuníquese con su distribuidor Apple preferido.