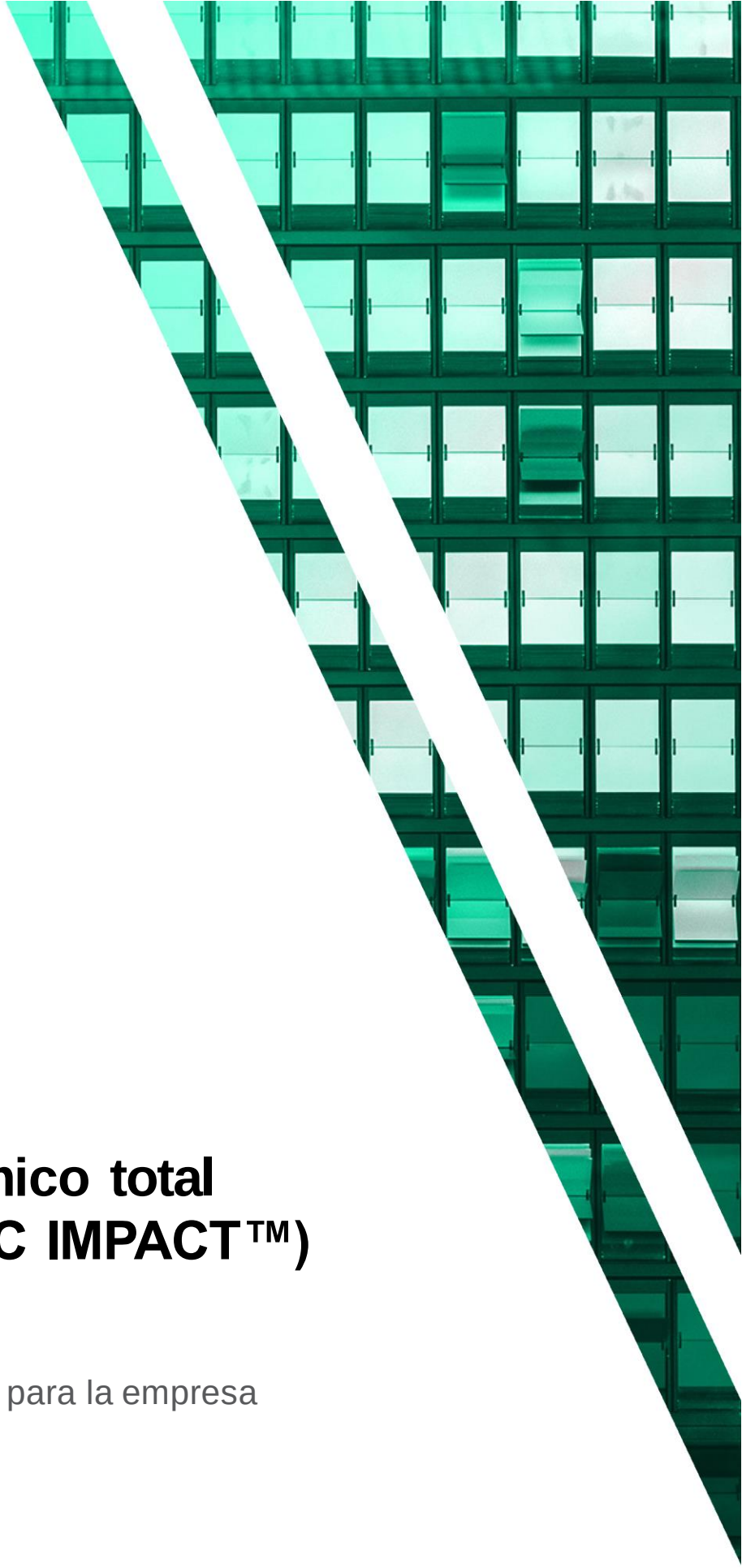
FORRESTER®



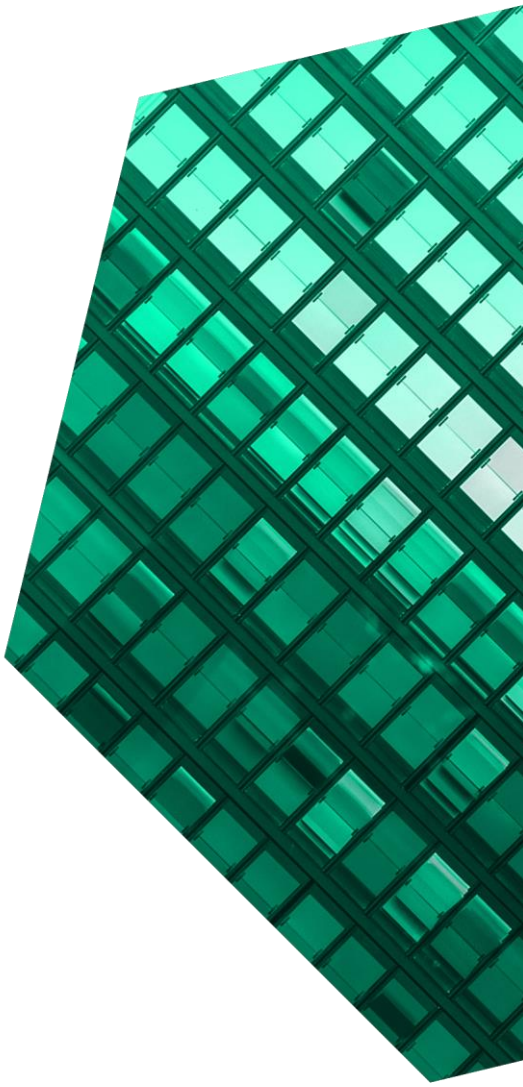
El impacto económico total (TOTAL ECONOMIC IMPACT™) de Cisco Duo

Ahorro de costos y beneficios para la empresa
Facilitado por Duo

FEBRERO, 2023

Índice

Consultora: *Mary Anne North*



SOBRE FORRESTER CONSULTING

Forrester Consulting asesora a líderes de organizaciones de manera independiente y objetiva, con el fin de alcanzar sus objetivos de transformación. Nuestras investigaciones, desarrolladas con un enfoque obsesivo en el cliente, le permiten a nuestros consultores expertos junto con los líderes trabajar en sus prioridades utilizando un modelo único, adaptado a las diferentes necesidades, lo que garantiza unos resultados duraderos. Si desea más información, visite forrester.com/consulting.

Resumen Ejecutivo

La implementación de Duo les ahorró tiempo a los usuarios finales, al personal de los centros de asistencia, a los analistas de seguridad y al resto del personal de TI, comparado con la solución utilizada anteriormente en las organizaciones. Duo también redujo el riesgo en esas organizaciones de sufrir una brecha de seguridad relacionada con las credenciales al proporcionar una mejor inteligencia en torno a todos los intentos de autenticación, simplificar la aplicación exhaustiva y constante de las políticas de seguridad y permitir la identificación proactiva de las vulnerabilidades de autenticación.

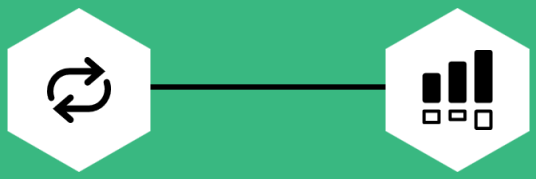
Cisco Secure Access by Duo asegura el acceso a las aplicaciones en la nube o locales mediante autenticación multifactor (MFA), autenticación sin contraseña, inicio de sesión único y comprobaciones de la postura del dispositivo para autenticar la identidad de los usuarios finales que desean acceder a esas aplicaciones. Esto proporciona visibilidad en cada intento de autenticación, incluyendo la postura de seguridad de los distintos dispositivos asociados a la cuenta de cada usuario final. Duo también le simplifica a una organización la aplicación de las políticas de seguridad de acceso en toda la empresa, mientras se adapta a los riesgos de los usuarios, los dispositivos y las aplicaciones.

Cisco le encargó a Forrester Consulting que llevara a cabo un estudio de Total Economic Impact™ (TEI) y examinara el posible retorno de la inversión (ROI) que las empresas pueden obtener con la implementación de Duo.[1] La finalidad de este estudio es poner a disposición del lector un marco para evaluar el posible impacto económico de Duo en su organización.

Para comprender mejor los beneficios, costos y riesgos asociados a esta inversión, Forrester entrevistó a cinco representantes de cuatro organizaciones con experiencia en el uso de Duo. Para los fines de este estudio, Forrester recopiló las experiencias de los entrevistados y combinó los resultados en una única organización compuesta, equivalente a una empresa global con ingresos anuales de 3000 millones $ y 10 000 licencias de Duo.

Antes de implementar Duo, las organizaciones de los entrevistados aseguraban las credenciales (incluyendo la autenticación) con otra solución, o protegían el acceso a las aplicaciones utilizando

ESTADÍSTICAS CLAVE



Retorno de la inversión (ROI)
159 %

Valor actual neto (VAN)
3,23 M$

únicamente contraseñas estáticas. Sin embargo, estos enfoques anteriores producían una inteligencia inadecuada en torno a los intentos de acceso, no protegían suficientemente contra las pérdidas de datos en caso de una brecha de seguridad relacionada con credenciales y generaban costos adicionales. Además, esto disminuía la productividad de los usuarios finales, del personal de los centros de asistencia, de los analistas de seguridad y del resto del personal de TI.

Tras la inversión en Duo, las organizaciones de los entrevistados ahorraron tiempo a los usuarios finales, al personal de los centros de asistencia, a los analistas de seguridad y al resto del personal de TI. También redujeron el riesgo de sufrir una brecha de seguridad relacionada con las credenciales gracias a la información que Duo les proporcionó y a una aplicación más rigurosa de las políticas de seguridad de acceso.

PRINCIPALES CONCLUSIONES

Beneficios cuantificados. Estos son algunos de los beneficios, cuantificados en valor actual (VA) ajustado por riesgo a tres años para la organización compuesta:

- **Reducción del riesgo de brechas de seguridad relacionadas con las credenciales, valorada en 792 000 $.** Al implementar Duo, la organización compuesta reduce su riesgo de sufrir una brecha de seguridad relacionada con las credenciales gracias a la información que Duo proporciona en torno a los intentos de autenticación, la amplia capacidad con la que cuenta Duo para asegurar cada autenticación y la facilidad para aplicar políticas de seguridad relacionadas con la autenticación en toda la organización.
- **Ahorro de 671 000 $ gracias a la mejora de la productividad de los analistas de seguridad.** Gracias a la facilidad de navegación en Duo, a su integración con otras aplicaciones y a la detallada información que proporciona sobre cada intento de autenticación, los analistas de seguridad de la organización compuesta le dedican menos tiempo a solucionar e investigar posibles vulnerabilidades derivadas de intentos sospechosos de inicio de sesión.
- **Ahorro de tiempo a los usuarios finales gracias a una autenticación simplificada, valorado en 3,2 M$.** Duo le ahorra tiempo a los usuarios finales de la organización compuesta en cada solicitud de autenticación comparado con la solución anterior.
- **Ahorro de 235 000 $ en costos de las soluciones de autenticación anteriores que ahora se evitan.** Al cambiar a Duo, se eliminan los gastos recurrentes de la organización compuesta, incluyendo las cuotas anuales de mantenimiento y soporte de la solución anterior, así como los costos de compras periódicas de nuevos dispositivos para los usuarios finales.
- **Ahorro de 326 000 $ en costos de gestión y asistencia de una solución anterior que ahora se evitan.** Puesto que en Duo es más sencillo de gestionar y dar soporte que en la solución anterior de la organización compuesta, el personal de la organización le dedica menos tiempo a administrar la solución, implementar funcionalidades adicionales, añadir nuevos casos de uso y optimizar el uso de Duo. También elimina gastos en servicios profesionales que eran necesarios para cubrir brechas de conocimiento a nivel interno.
- **Ahorro de 57 000 $ gracias a las mejoras en la productividad del centro de asistencia y de los usuarios finales como consecuencia de la reducción del número de incidentes relacionados con la autenticación.** Duo simplifica el proceso de autenticación de los usuarios finales y elimina la necesidad de que dispongan de un dispositivo de autenticación separado. Como resultado, ocurren menos incidentes relacionados con la autenticación, lo que le ahorra tiempo tanto a los usuarios finales como al propio personal del centro de asistencia.

Beneficios no cuantificados. Entre los beneficios que aportan valor para la organización compuesta, pero que no están cuantificados en este estudio se encuentran:

- **Una mejor experiencia para el usuario final.** Los entrevistados señalaron que para los usuarios finales Duo era fácil de usar y les ahorraba tiempo y frustraciones en cada autenticación comparado con sus soluciones anteriores de autenticación.
- **Facilidad para mejorar aún más la experiencia del usuario con el inicio de sesión único (SSO**) de Duo. Las organizaciones de los entrevistados que optaron por utilizar el inicio de sesión único (SSO) proporcionaron a los usuarios de Duo una experiencia de inicio de sesión simple y armonizada para todas las aplicaciones integradas con Duo**.**

- **Eficiencias en auditoría y cumplimiento normativo.** Los datos de auditoría de Duo y los informes de actividad de los usuarios permitieron automatizar algunos informes de auditoría.
- **Mayor capacidad para atraer nuevos clientes o socios.** El reconocimiento de la marca Duo le proporcionó confianza a clientes y socios.
- **Consolidación de proveedores**. Los entrevistados cuyas organizaciones ya habían utilizado otros productos de Cisco valoraron no tener que añadir y gestionar otro proveedor.
- **La moderada curva de aprendizaje de Duo y el valor del apoyo de primera calidad de Duo Care.** Tanto los usuarios finales como el personal de TI consideraron que Duo es fácil de usar y que Duo Care es un recurso útil.

Costos. Estos son algunos de los costos en valor actual (VA) ajustado por riesgo a tres años para la organización compuesta:

- **Las tarifas de Cisco ascendieron a 1,7 M$.** Las tarifas de Cisco incluyen las cuotas de suscripción a la versión Access de Duo, y las cuotas de Duo Care para servicios adicionales que no incluye el soporte estándar de Duo.
- **La implementación, gestión y asistencia requiere un esfuerzo a nivel interno de 340 000 $.** La organización compuesta implementa Duo y lo gestiona y optimiza de forma continua utilizando un equipo de TI interno junto con la orientación de un equipo de Duo Care.

Con base en las entrevistas con los representantes y del análisis económico, se concluyó que una organización compuesta obtiene un beneficio equivalente a 5,26 M$ a tres años frente a un costo de 2,03 M$, lo que aporta un valor actual neto (VAN) de 3,23 M$ y un retorno de la inversión (ROI) del 159 %.

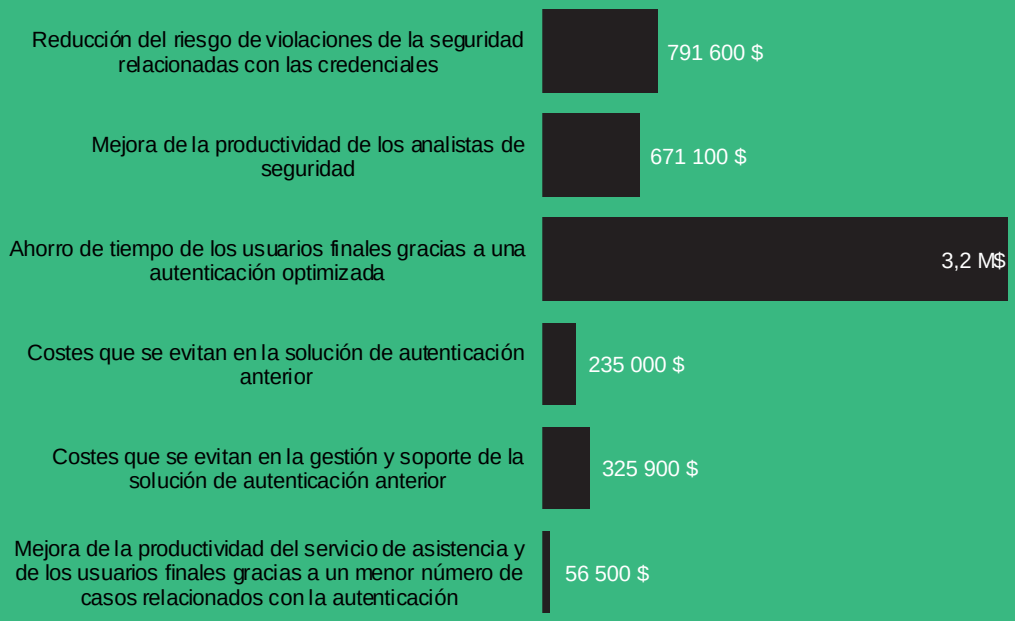
ROI
159 %

VALOR ACTUAL DE LOS BENEFICIOS
5,26 M$

VAN
3,23 M$

RECUPERACIÓN DE LA INVERSIÓN
<6 meses

Beneficios (tres años)



«El enfoque por capas de Duo con respecto a la seguridad y las políticas de seguridad proporciona unas prestaciones que nuestro producto anterior no ofrecía. Los datos mucho más detallados que ahora podemos analizar mejoran mucho nuestra seguridad.»

- Técnico de seguridad, servicios profesionales

MARCO Y METODOLOGÍA TEI

A partir de la información obtenida en las entrevistas, Forrester elaboró un marco del impacto económico total (Total Economic Impact™) para aquellas organizaciones que planean invertir en Duo.

La finalidad de este marco es identificar los factores de costo, beneficio, flexibilidad y riesgo que repercuten en la decisión de invertir. Forrester adoptó una estrategia de múltiples pasos para evaluar el impacto que Duo puede tener en una organización.

Forrester Consulting encargó una encuesta en línea con 351 líderes en ciberseguridad de empresas globales que se llevó a cabo en Estados Unidos, Reino Unido, Canadá, Alemania y Australia. Entre los participantes de la encuesta había gerentes, directores, vicepresidentes y ejecutivos de alto rango encargados de tomar decisiones, dirigir las operaciones y generar informes en el área de ciberseguridad. Con las preguntas planteadas a los participantes, se pretendía evaluar las estrategias de ciberseguridad de estos líderes, con respecto a cualquier brecha de seguridad que se hubiera producido dentro de sus organizaciones. Los participantes accedieron voluntariamente a la encuesta a través de un panel de investigación externo que llevó a cabo el trabajo de campo en nombre de Forrester en noviembre del 2020.

AVISOS

Los lectores deben tener en cuenta lo siguiente:

Este estudio ha sido encargado por Cisco y realizado por Forrester Consulting. No pretende ser un análisis competitivo.

Forrester no hace suposiciones sobre el posible ROI que obtendrán otras organizaciones. Forrester recomienda encarecidamente que los lectores utilicen sus propias estimaciones dentro del marco proporcionado en el estudio para determinar la idoneidad de invertir en Duo.

Cisco ha revisado el contenido y le ha aportado información a Forrester, pero este último mantiene el control editorial sobre el estudio y sus conclusiones, y no acepta cambios que contradigan las conclusiones a las que ha llegado o que confundan su significado.

Cisco proporcionó los nombres de los clientes para las entrevistas, pero no participó en ellas.

DILIGENCIA DEBIDA

Se entrevistó a partes interesadas de Cisco y a analistas de Forrester para recoger datos relacionados con Duo.

ENTREVISTAS

Se entrevistó a un total de cinco representantes de cuatro organizaciones que utilizaban Duo con el fin de recoger datos sobre los costos, beneficios y riesgos.

ORGANIZACIÓN COMPUESTA

Se diseñó una organización compuesta basada en las características de las organizaciones de los entrevistados.

MARCO DE MODELO ECONÓMICO

Se elaboró un modelo económico con base en las entrevistas mediante la metodología TEI, y se ajustó por riesgo dicho modelo de acuerdo los problemas e inquietudes que manifestaron los entrevistados.

CASO PRÁCTICO

Se emplearon cuatro elementos fundamentales de la metodología TEI a la hora de modelar el impacto de la inversión: beneficios, costos, flexibilidad y riesgos. Gracias a la creciente sofisticación de los análisis del retorno de las inversiones en TI, la metodología TEI de Forrester proporciona una perspectiva integral del impacto económico total de las decisiones de compra. Para obtener más información sobre la metodología TEI, consulten al Anexo A.

La trayectoria del cliente de Cisco Duo

Motivos para invertir en Duo

Entrevistas

Cargo	Sector	Área geográfica	Cuentas protegidas con Duo
Director sénior de seguridad informática	Sanitario	Con sede en Norteamérica; operaciones regionales	11 000
Técnico de seguridad	Servicios profesionales	Con sede en Norteamérica; operaciones globales	6800
Especialista en apoyo informático	Servicios de información	Con sede en Norteamérica; operaciones globales	1225
Analista de ciberseguridad	Sanitario	Con sede en Norteamérica; operaciones nacionales	12 000
Director del centro de operaciones de ciberdefensa	Sanitario	Con sede en Norteamérica; operaciones nacionales	12 000

PRINCIPALES DIFICULTADES

Antes de implementar Duo, las organizaciones de los entrevistados aseguraban las credenciales con otra solución de autenticación, o protegían el acceso a las aplicaciones utilizando únicamente contraseñas.

Los entrevistados señalaron que sus organizaciones se enfrentaban a retos comunes, como:

- **Alto riesgo de brechas de seguridad relacionadas con las credenciales.** Antes de Duo, las organizaciones de los entrevistados tenían un riesgo elevado de sufrir una brecha de seguridad relacionada con las credenciales porque carecían de protección multicapa, les resultaba difícil aplicar y actualizar de forma sistemática las políticas de seguridad y solo obtenían información limitada sobre los intentos de autenticación y la postura de seguridad de los dispositivos de los usuarios finales.
- **Productividad del analista de seguridad en torno a la investigación de intentos sospechosos de inicio de sesión.** Al disponer de pocos datos para respaldar sus investigaciones sobre intentos sospechosos de inicio de sesión, los analistas de seguridad de las organizaciones de los entrevistados tenían que revisar manualmente los registros para obtener esa información. Un técnico de seguridad de una empresa de servicios profesionales afirmó: «En el pasado, nuestras investigaciones sobre intentos de inicio de sesión tenían que basarse en registros super-genéricos. Los analistas tenían que iniciar sesión y analizar cada caso individualmente. Rastrear todo esto, tener listos los inicios de sesión, etc., me llevaba una o dos horas para cada caso.»
- **Una experiencia deficiente para el usuario final, incluyendo el tiempo que tarda cada autenticación.** Los entrevistados cuyas organizaciones ya empleaban una solución de autenticación explicaron la frustración de los usuarios finales respecto al tiempo necesario para autenticarse y tener que depender de un dispositivo adicional para hacerlo.

«Antes de Duo, actuábamos sin mucha información sobre los intentos de acceso. Era difícil determinar si alguien realmente se autenticaba o desde qué región lo hacía.»

Analista de ciberseguridad, sector sanitario

- **Esfuerzo necesario por parte de los administradores de seguridad y otro personal de TI para gestionar y dar soporte a la solución previa de autenticación.** Los entrevistados afirmaron que sus soluciones anteriores eran complejas y mantenerlas y optimizarlas requería de mucho tiempo, por ejemplo, para añadir un nuevo empleado, proteger aplicaciones adicionales o establecer y actualizar las políticas de seguridad. Un técnico de seguridad de una empresa de servicios profesionales afirmó: «Mantener lo que teníamos e incorporar nuevas funcionalidades significaba un gran esfuerzo con nuestra solución anterior. Integrar esa solución con otras aplicaciones solo era posible con ayuda externa y conocimientos muy secretos sobre la solución, etc. No era sencillo.»

  Un analista de ciberseguridad de una organización sanitaria afirmó: «Nuestra solución anterior era muy complicada: no puedes olvidarte de hacer esto o aquello. Y cuando nos encontrábamos con problemas, parecía que se tardaba mucho o teníamos que recurrir a los ingenieros más veteranos del proveedor.»
- **La productividad del centro de asistencia y de los usuarios finales se ve afectada por los incidentes de autenticación.** Los procesos de inicio de sesión más complejos de los usuarios finales y la necesidad de utilizar un dispositivo separado provocaban un número significativo de casos de asistencia técnica en organizaciones que utilizaban otros tipos de soluciones de autenticación. Resolver esos casos representaba una molestia para los usuarios finales y requería tiempo tanto del personal del centro de asistencia como de los propios usuarios finales.
- **Problemas técnicos con las soluciones anteriores de autenticación.** Los entrevistados señalaron tiempo de inactividad, inestabilidad, integraciones problemáticas con otras aplicaciones y otros problemas técnicos con sus soluciones anteriores.

ORGANIZACIÓN COMPUESTA

Con base en las entrevistas, Forrester ha elaborado un marco TEI, una empresa compuesta y un análisis de ROI que ilustra en qué áreas hay un impacto económico. La organización compuesta es representativa de las organizaciones de los cinco entrevistados y se utiliza en la próxima sección para presentar el análisis económico agregado. La organización compuesta tiene las siguientes características:

Descripción de la organización compuesta. La organización compuesta es una empresa global con unos ingresos de 3000 mil $ y 10 000 licencias de Duo. Implementa Duo en todas las cuentas que se utilizan para acceder de forma remota a las aplicaciones. La mayoría de dichas cuentas están asociadas a empleados, y el resto las utilizan contratistas u otros terceros que necesitan acceso a los sistemas de la organización. Los dispositivos que se utilizan para acceder a estas aplicaciones son una mezcla de dispositivos móviles y computadores portátiles o de escritorio. Los dispositivos móviles y computadores portátiles se utilizan con frecuencia de forma remota. Las aplicaciones de la organización compuesta son una mezcla de aplicaciones en la nube y locales, y el porcentaje en la nube está aumentando. Antes de implementar Duo, la

Suposiciones clave

- **3000 millones de dólares de ingresos anuales**
- **Operaciones mundiales**
- **10 000 licencias de Duo**
- **Uso de aplicaciones en la nube y locales**
- **Acceso a las aplicaciones a través del móvil y computadores portátiles o de escritorio**
- **Acceso remoto frecuente**

organización compuesta utilizaba otro sistema de autenticación multifactor.

Características de la implementación.
La organización compuesta adquiere la versión Access de Duo y selecciona Duo Care, un soporte prémium que ofrece Cisco. Implementa Duo utilizando una combinación de servicios profesionales de su equipo Duo Care y recursos internos de su personal de TI. Como parte de la implementación, proporciona una breve formación a todos los usuarios de cuentas que tienen Duo instalado. Una vez que la funcionalidad de Duo se ha implementado y está plenamente disponible, el personal de TI de la organización invierte tiempo de forma continua para ampliar su uso y adopción, lo que también incluye nuevas funciones, a medida que se van introduciendo.

Análisis de beneficios

Datos de beneficios cuantificados aplicados a la organización compuesta

Beneficios totales

Ref.	Beneficio	Año 1	Año 2	Año 3	Total	Valor actual
Atr	Reducción del riesgo de brechas de seguridad relacionadas con las credenciales	267 943 $	331 579 $	364 737 $	964 259 $	791 649 $
Btr	Mejora de la productividad de los analistas de seguridad	240 259 $	282 872 $	291 368 $	814 499 $	671 105 $
Ctr	Ahorro de tiempo para el usuario final gracias a una autenticación optimizada	1 243 120 $	1 280 307 $	1 318 557 $	3 841 985 $	3 178 866 $
Dtr	Costos evitados de la solución anterior de autenticación	94 500 $	94 500 $	94 500 $	283 500 $	235 008 $
Etr	Costos evitados en la gestión y soporte de la solución anterior de autenticación	128 845 $	131 184 $	133 588 $	393 616 $	325 914 $
Ftr	Mejoras en la productividad del centro de asistencia y de los usuarios finales como consecuencia del menor número de incidentes de autenticación	22 094 $	22 757 $	23 437 $	68 288 $	56 502 $
	Beneficios totales (ajustados por riesgo)	1 996 760 $	2 143 199 $	2 226 187 $	6 366 147 $	5 259 044 $

REDUCCIÓN DEL RIESGO DE BRECHAS DE SEGURIDAD RELACIONADAS CON LAS CREDENCIALES

Evidencia y datos. Los entrevistados afirmaron que al implementar Duo, sus organizaciones redujeron el riesgo de sufrir brechas de seguridad relacionadas con las credenciales. Atribuyeron esa reducción de riesgo a las capacidades de Duo que van más allá del propio método de autenticación, a la información que Duo proporciona sobre cada autenticación, a las amplias capacidades de Duo para proteger cada autenticación y a la facilidad con la que podían aplicar de forma sistemática y exhaustiva las políticas de seguridad relacionadas con la autenticación en toda la organización.

Referente a la versión Access de Duo que utilizaban todos los entrevistados, las organizaciones que anteriormente disponían de una solución de autenticación no se limitaron a cambiar la forma de autenticarse de sus usuarios finales, sino que también añadieron nuevas capacidades que redujeron el riesgo de sufrir brechas de seguridad relacionadas con las credenciales. Duo le permitió a las organizaciones de los entrevistados identificar mejor aquellos sistemas vulnerables a ataques que afectan a las credenciales (por ejemplo, mediante el análisis del contexto y la inspección continua de la postura de seguridad de cada dispositivo en cada intento de acceso), y también les permitió implementar políticas de autenticación más minuciosas, como proporcionar detalles adicionales sobre quién accedió a qué y cómo (por ejemplo, restringiendo el acceso desde ciertas ubicaciones o limitando el acceso desde dispositivos que no cumplan ciertas condiciones).

Un técnico de seguridad de una empresa de servicios profesionales afirmó: «Cuantos más datos tengas, más cosas podrás detectar. Ahora disponemos de mejor información en torno a cada autenticación multifactor, y la hacemos valer. Podemos detectar desde dónde está emitiendo alguien una autenticación multifactor, detectar qué dispositivo está utilizando y comportamientos extraños, cosas que no cuadran.»

Ese mismo técnico de seguridad también afirmó lo siguiente: «Incluso nuestras interacciones con el centro de asistencia técnica son más seguras ahora. Si alguien se pone en contacto con nuestro centro de asistencia, tenemos un procedimiento por defecto mediante el cual Duo enviará al cliente un mensaje

tipo push y este deberá verificar su identidad con esta autenticación multifactor. Esto no era posible con nuestra solución anterior.»

Un especialista en soporte informático de una empresa de servicios de información afirmó: «Ahora tenemos un único panel de cristal a través del cual podemos ver todas nuestras aplicaciones protegidas y hacer un seguimiento de las tendencias. Eso nos ahorra algo de tiempo, pero lo más importante es que disponemos de nueva información relevante de la que no disponíamos antes de implementar Duo... Y Duo tiene una función genial que nos permite identificar y abordar vulnerabilidades como la de alguien que está utilizando un sistema operativo obsoleto o un navegador que ha llegado al final de su vida útil o que necesita un parche. Aunque tenemos otros portales que muestran algo de eso, Duo lo muestra todo en un solo lugar.»

Los entrevistados atribuyeron parcialmente la reducción de su riesgo a otras medidas de seguridad que integraron de forma simultánea a la implementación de Duo, como una mejor formación en seguridad de los usuarios finales, una mejora de las políticas y procesos de seguridad y la ampliación del uso de la autenticación multifactor para un conjunto más amplio de aplicaciones y casos de uso.

«Además de la autenticación, Duo dispone de información y capacidades fantásticas. Podemos determinar la versión actual del software del dispositivo desde el que se está solicitando la autenticación, y si tiene parches de seguridad obsoletos. Podemos configurar nuestras políticas y decir: "Si no ha actualizado su dispositivo, ya no podrá autenticarse a través de él."»

Técnico de seguridad, servicios profesionales

Modelado y supuestos. Para la organización compuesta, Forrester aplica las siguientes suposiciones:

- Las organizaciones experimentan en promedio tres brechas de seguridad al año.[2]
- El treinta por ciento de las brechas de seguridad se deben a la vulnerabilidad de credenciales.
- El costo estimado de subsanar una filtración de datos (dimensionado en función del número de usuarios finales de la organización compuesta) es de 605 274 $ durante el primer año y aumenta un 10 % cada año debido a nuevas normas y a otros factores en evolución constante.[3]
- Tras la implementación de Duo, el riesgo de una brecha de seguridad relacionada con las credenciales disminuye en un 80 % en el primer año y en un 90 % en el segundo y tercer año.
- El setenta por ciento de esa reducción es atribuible a Duo.

Riesgos. La reducción del riesgo de brechas de seguridad relacionadas con las credenciales varía en función de:

- La prevalencia, el tipo y el costo promedio de las filtraciones de datos en el sector de una organización.
- El volumen y el tipo de datos vulnerados.
- El territorio de las operaciones.
- Las medidas reglamentarias y normas que debe seguir la organización.
- La situación anterior y el grado de madurez de la organización con respecto a las operaciones de seguridad.
- El software de autenticación previo.
- La medida en que la organización se ha valido de las capacidades de Duo.

Resultados. En consideración de estos riesgos, Forrester ajustó el beneficio un 15 % a la baja, con lo que obtuvo un valor actual (VA) total ajustado por riesgo a tres años (con un descuento del 10 %) de 792 000 $.

Reducción en el riesgo de brechas de seguridad relacionadas con las credenciales					
Ref.	**Parámetro**	**Fuente**	**Año 1**	**Año 2**	**Año 3**
A1	Promedio de brechas de la seguridad durante un año	Investigación de Forrester	3	3	3
A2	Porcentaje del total que se debe a la vulneración de credenciales	Suposición de Forrester	30 %	30 %	30 %
A3	Costo estimado de subsanar una única filtración de datos	Investigación de Forrester	605 274 $	665 801 $	732 382 $
A4	Subtotal: Costo promedio anual de las brechas relacionadas con las credenciales	A1*A2*A3	562 905 $	619 195 $	681 115 $
A5	Reducción en el riesgo de brechas de seguridad relacionadas con las credenciales tras la implementación de Duo	Entrevistas	80 %	90 %	90 %
A6	Porcentaje de esa reducción atribuido a Duo	Entrevistas	70 %	70 %	70 %
At	Reducción en el riesgo de brechas de seguridad relacionadas con las credenciales	A4*A5*A6	315 227 $	390 093 $	429 102 $
	Ajuste por riesgo	↓15 %			
Atr	Reducción en el riesgo de brechas de seguridad relacionadas con las credenciales (ajustada por riesgo)		267 943 $	331 579 $	364 737 $
	Total de tres años: 964 259 $		**Valor actual de tres años: 791 649 $**		

MEJORA DE LA PRODUCTIVIDAD DE LOS ANALISTAS DE SEGURIDAD

Evidencia y datos. Para los analistas de seguridad de las organizaciones a las que pertenecen los entrevistados, Duo supuso un ahorro de tiempo en la resolución de problemas y la investigación de posibles problemas de seguridad derivados de los intentos de inicio de sesión. Los entrevistados atribuyeron este ahorro de tiempo a la facilidad de navegación en Duo, a su integración con otras aplicaciones y a la disponibilidad de información detallada sobre cada intento de autenticación.

Un analista de ciberseguridad de una organización sanitaria afirmó: «Duo es una gran ayuda para nuestro equipo 24/7 porque sus integrantes confían en Duo para ayudarles a determinar si un usuario se ha autenticado o no, si el usuario está realmente en esa determinada región [protocolo de Internet] (IP) o no, o si el usuario pertenece a un determinado grupo autorizado a autenticarse y acceder a una aplicación. Duo es uno de sus principales recursos para investigar las autenticaciones. Como gran parte de la información se encuentra en Duo y no es necesario mirar en muchas herramientas distintas, resulta fácil examinar la actividad de registro y determinar dónde está el problema para luego trasladárselo fácilmente a otros equipos.»

Un especialista en soporte informático de una empresa de servicios de información afirmó: «Antes de implementar Duo, teníamos que mirar los registros de distintas aplicaciones para verificar lo que estaba sucediendo. Duo ahorra mucho tiempo en comparación con eso, porque podemos ver todas

«Ahora, cuando nuestro [centro de operaciones de seguridad] (SOC) recibe una alerta, dispone de datos mucho más pormenorizados con los que trabajar y los obtiene de tal forma que se ahorra tiempo. Así que, investigaciones que llevaban horas, ahora requieren solo minutos.»

Técnico de seguridad, servicios profesionales

nuestras aplicaciones protegidas dentro de un solo panel y ver cuándo un empleado accede a algo, cuánto tiempo estuvo allí y qué estuvo haciendo.»

Un técnico de seguridad de una empresa de servicios profesionales afirmó que sus analistas de seguridad ahorraron tiempo de investigación gracias a la facilidad (a través de las API) para extraer los registros de Duo en la gestión de eventos e información de seguridad (SIEM) de la organización para proporcionar más contexto a los analistas de seguridad.

Modelado y suposiciones. Para la organización compuesta, Forrester aplica las siguientes suposiciones:

- Cada año hay que investigar 3500 alertas relacionadas con la autentificación.
- Antes de implementar Duo, un analista de seguridad le dedicaba en promedio 90 minutos a investigar cada alerta.
- Con Duo, un analista de seguridad le dedicaba en promedio 20 minutos a investigar cada alerta en el primer año, y 10 minutos en el segundo y tercer año.
- Los analistas de seguridad utilizan de forma productiva el 90 % del tiempo que ahorran.

Riesgos. La mejora de la productividad de los analistas de seguridad varía en función de:

- El tipo de incidentes de seguridad de la organización y el tiempo que los analistas tienen que dedicar a los incidentes.
- La situación anterior de la organización.
- El tipo de solución de autenticación previa.
- Cómo otros sistemas se integran con Duo.
- El volumen de alertas de autenticación.
- Experiencia y capacidades de los analistas de seguridad.
- La madurez de las operaciones de seguridad de la organización.
- La medida en que la organización se ha valido de las capacidades de Duo.
- Tasas de retribución locales vigentes.

Resultados. En consideración de estos riesgos, Forrester ajustó el beneficio un 15 % a la baja, con lo que obtuvo un valor actual (VA) total ajustado por riesgo a tres años de 671 000 $.

Mejora de la productividad de los analistas de seguridad

Ref.	Parámetro	Fuente	Año 1	Año 2	Año 3
B1	Cantidad de alertas anuales relacionadas con la autenticación que requieren investigación	Entrevistas	3500	3500	3500
B2	Tiempo que los analistas de seguridad le dedicaban a investigar cada alerta antes de implementar Duo (minutos)	Entrevistas	90	90	90
B3	Tiempo que los analistas de seguridad le dedican a investigar cada alerta con Duo (minutos)	Entrevistas	20	10	10
B4	Subtotal: Ahorro anual de tiempo (en horas)	(B1*(B2-B3))/60	4083	4667	4667
B5	Recuperación de la productividad	Estándar TEI	90 %	90 %	90 %
B6	Retribución por hora (incluyendo todos los gastos) de un analista de seguridad	Estándar TEI	76,92 $	79,23 $	81,61 $
Bt	Mejora de la productividad de los analistas de seguridad	B4*B5*B6	282 658 $	332 790 $	342 786 $
	Ajuste por riesgo	↓15 %			
Btr	Mejora de la productividad de los analistas de seguridad (ajustada por riesgo)		240 259 $	282 872 $	291 368 $
	Total de tres años: 814 499 $			**Valor actual de tres años: 671 105 $**	

AHORRO DE TIEMPO PARA EL USUARIO FINAL GRACIAS A UNA AUTENTICACIÓN OPTIMIZADA

Evidencia y datos. Los entrevistados afirmaron que sus usuarios finales ahorraron tiempo gracias a los procesos de autenticación simples de Duo en comparación con los que utilizaban anteriormente para la autenticación.

Un técnico de seguridad de una empresa de servicios profesionales afirmó: «Con Duo, nuestros usuarios finales se toman menos tiempo en cada solicitud de autenticación. Ya no tienen que escribir números y esperar una respuesta».

Modelado y supuestos. Para la organización compuesta, Forrester aplica las siguientes suposiciones:

- Cada uno de sus 10 000 usuarios finales se autentica en promedio 500 veces al año.
- Antes de implementar Duo, un usuario final tardaba 1,5 minutos en autenticarse.
- Con Duo, un usuario final se autentica en 0,5 minutos.
- Los usuarios finales utilizan de forma productiva el 50 % del tiempo que ahorran.

Riesgos. El ahorro de tiempo para el usuario final gracias a una autenticación optimizada varía en función de:

- La cantidad de usuarios finales.
- El promedio de autenticaciones anuales por usuario final.
- El tipo de solución de autenticación previa.
- Tasas vigentes de retribución locales.

Resultados. En consideración de estos riesgos, Forrester ajustó el beneficio un 15 % a la baja, con lo que obtuvo un VA total ajustado por riesgo a tres años de 3,2 M$.

Ahorro de tiempo para el usuario final gracias a una autenticación optimizada

Ref.	Parámetro	Fuente	Año 1	Año 2	Año 3
C1	Cantidad de usuarios finales	Organización compuesta	10 000	10 000	10 000
C2	Promedio de autenticaciones por usuario final al año	Entrevistas	500	500	500
C3	Tiempo que tardaba el usuario final en autenticarse antes de implementar Duo (en minutos)	Entrevistas	1,5	1,5	1,5
C4	Tiempo que tarda el usuario final en autenticarse con Duo (en minutos)	Entrevistas	0,5	0,5	0,5
C5	Subtotal: Ahorro total anual de tiempo para el usuario final (en horas)	(C1*C2*(C3-C4))/60	83 333	83 333	83 333
C6	Tarifa por hora de los usuarios finales combinados (incluyendo todos los gastos)	Estándar TEI	35,10 $	36,15 $	37,23 $
C7	Recuperación de la productividad del usuario final	Estándar TEI	50 %	50 %	50 %
Ct	Ahorro de tiempo para el usuario final gracias a una autenticación optimizada	C5*C6*C7	1 462 494 $	1 506 244 $	1 551 244 $
	Ajuste por riesgo	↓15 %			
Ctr	Ahorro de tiempo para el usuario final gracias a una autenticación optimizada (ajustada por riesgo)		1 243 120 $	1 280 307 $	1 318 557 $
	Total de tres años: 3 841 985 $			**Valor actual de tres años: 3 178 866 $**	

COSTOS EVITADOS DE LA SOLUCIÓN ANTERIOR DE AUTENTICACIÓN

Evidencia y datos. Al pasarse a Duo, las organizaciones de los entrevistados que antes utilizaban otra solución de autenticación eliminaron sus gastos recurrentes en esas soluciones. Aunque se trata de un beneficio neto, ya que ahora las organizaciones pagan por Duo.

Modelado y suposiciones. Para la organización compuesta, Forrester aplica las siguientes suposiciones:

- El anterior proveedor de soluciones cobra una cuota anual de mantenimiento y asistencia de 2,50 $ por cada dispositivo de autenticación de usuario final en uso.
- Cada año se reemplaza el 25 % de los dispositivos de autenticación de los usuarios finales.
- Un nuevo dispositivo de autenticación de usuario final cuesta 25 $.
- El costo de envío en promedio de un nuevo dispositivo a un usuario final es de 7 $.

Riesgos. Los costos ahorrados en la infraestructura de las soluciones de autenticación anteriores varía en función de:

- El número de usuarios finales.
- El enfoque previo de la organización en materia de autenticación.
- Las cuotas del proveedor por el costo inicial y el mantenimiento y soporte posterior.

Resultados. En consideración de estos riesgos, Forrester ajustó el beneficio un 10 % a la baja, con lo que obtuvo un valor actual (VA) total ajustado por riesgo a tres años de 235 000 $.

Costos evitados de la solución de autenticación anterior

Ref.	Parámetro	Fuente	Año 1	Año 2	Año 3
D1	Número de usuarios finales	Organización compuesta	10 000	10 000	10 000
D2	Cuota anual de mantenimiento y soporte que se paga al proveedor de la solución por dispositivo de autenticación de usuario final	Entrevistas	2,50 $	2,50 $	2,50 $
D3	Subtotal: Cuotas anuales de mantenimiento y asistencia que se pagan al proveedor de la autenticación	D1*D2	25 000 $	25 000 $	25 000 $
D4	Porcentaje de dispositivos de autenticación de usuario final sustituidos al año	Entrevistas	25 %	25 %	25 %
D5	Coste por dispositivo nuevo	Entrevistas	25 $	25 $	25 $
D6	Coste del envío del nuevo dispositivo al usuario final	Entrevistas	7 $	7 $	7 $
D7	Subtotal: Costos anuales de la sustitución de dispositivos	D1*D4*(D5+D6)	80 000 $	80 000 $	80 000 $
Dt	Costos evitados de la solución de autenticación anterior	D3+D7	105 000 $	105 000 $	105 000 $
	Ajuste por riesgo	↓10 %			
Dtr	Costos evitados de la solución de autenticación anterior (ajustados por riesgo)		94 500 $	94 500 $	94 500 $
	Total de tres años: 283 500 $			**Valor actual de tres años: 235 008 $**	

COSTOS EVITADOS EN LA GESTIÓN Y SOPORTE DE LA SOLUCIÓN DE AUTENTICACIÓN ANTERIOR

Evidencia y datos. Debido a que las organizaciones de los entrevistados consideraron que Duo es más sencillo de gestionar y dar soporte que sus soluciones anteriores, pagaron menos por ello comparado con sus soluciones anteriores. Redujo el tiempo que el personal le dedicaba a asegurarse de que la solución funcionaba correctamente, a responder preguntas, a instalar funciones adicionales, a añadir nuevos casos de uso y, en general, a optimizar su uso, y también resultó en ahorros gracias a la eliminación de los honorarios por servicios profesionales que antes se pagaban para cubrir las brechas de conocimiento a nivel interno.

Las actividades de gestión y apoyo incluían la promulgación y el ajuste de las políticas de autenticación, la adición de nuevos usuarios y la gestión de las credenciales de los usuarios finales, la integración de la solución de autenticación con otras inversiones en seguridad y con todas las aplicaciones, la inscripción y activación de nuevos usuarios, y el perfeccionamiento de la experiencia del usuario.

Un especialista en soporte informático de una empresa de servicios de información afirmó: «Es la opción más sencilla para la autenticación multifactor en un entorno empresarial.» Un técnico de seguridad de una empresa global de servicios profesionales afirmó: «El ahorro de tiempo del personal ha representado un gran beneficio. Duo es muy ágil y hemos podido eliminar muchas horas de ingeniería que nuestro equipo le dedicaba a mantener la solución anterior.»

Ese mismo especialista en soporte informático también afirmó: «Ya no le pagamos a una empresa de servicios profesionales porque podemos gestionar Duo con nuestro propio equipo de seguridad. Con la solución anterior, le pagábamos constantemente a un proveedor externo para que estuviera a nuestra disposición y le ayudara a nuestros ingenieros especializados que trabajaban en la solución. Ahora, en lugar de tener que asignar personal para dar soporte a la solución, todos los miembros de nuestro equipo de seguridad están más o menos formados hasta el nivel de poder manejar Duo.»

> **«Ha sido muy fácil aprender a usar, navegar y trabajar con Duo, en comparación con nuestra solución anterior. Requiere menos gestión.»**
>
> *Analista de ciberseguridad, sector sanitario*

Un analista de ciberseguridad de una organización sanitaria afirmó: «Duo nos ha beneficiado mucho en muchos aspectos: inscripción, dotación, seguridad, actividad de registro, investigaciones, establecimiento de políticas, creación de procesos y normas para ayudar a los equipos internos. Todo es muy fácil. Algunos de los propietarios de aplicaciones con los que trabajo no son muy expertos en tecnología, pero después de trabajar con ellos, explicarles Duo y mostrárselo, ya no me piden ayuda... Con nuestro producto anterior, a menudo teníamos que ponernos en contacto con el proveedor para obtener asistencia porque era un sistema muy complicado. Duo le ha ayudado mucho a nuestro entorno.»

Duo también le ahorró tiempo al personal gracias a:

- **La sencillez para establecer políticas de autenticación.** Un analista de ciberseguridad de una organización sanitaria afirmó: «Duo nos beneficia porque es muy fácil configurar una política e implementarla en una de nuestras aplicaciones dentro de Duo, entonces todo el mundo queda dentro de la política. Con nuestro producto anterior era más complicado.»
- **La facilidad de integración de Duo con otras aplicaciones.** Un técnico de seguridad de una empresa de servicios profesionales afirmó: «Duo tiene una gran documentación para casi todos los proveedores de [software como servicio] (SaaS). Sea lo que sea, lo que se haya que obtener por Internet, prácticamente se puede garantizar que Duo dispone de una integración bien documentada y sencilla que podemos utilizar sin más recursos, y la sencillez de los procesos de incorporación nos viene bastante bien. Aplicamos la autenticación Duo a todos

nuestros proveedores de SaaS en la nube y valoramos muy positivamente la excelente documentación que se proporciona para todas estas integraciones.»

Un especialista en soporte informático de una empresa de servicios de información afirmó: «Hoy en día, muchas aplicaciones de terceros están integradas con Duo. Ya reconocen a Duo como una de las mejores MFA. «Entonces, ¿estás utilizando Duo? Aquí tienes la integración para MFA con Duo. No tienes que ponerte a buscar, está ahí mismo.»

Modelado y suposiciones. Para la organización compuesta, Forrester aplica las siguientes suposiciones:

- Para gestionar y dar soporte a la solución previa de autenticación, dos miembros del personal de TI a tiempo completo (ETC) trabajan un total combinado de 4160 horas al año.
- Para gestionar y dar soporte a Duo, el personal de TI trabaja un total combinado de 312 horas al año.
- El personal de TI utiliza de forma productiva el 50 % del tiempo ahorrado.

Riesgos. Los costos ahorrados en la gestión y soporte de la solución anterior de autenticación varían en función de:

- El tipo de solución de autenticación que tenían anteriormente.
- Experiencia y capacidades del personal de TI.
- La madurez de las operaciones de seguridad de la organización.
- La medida en que la organización se ha valido de las capacidades de Duo.
- Tasas de retribución locales vigentes.

Resultados. En consideración de estos riesgos, Forrester ajustó el beneficio un 15 % a la baja, con lo que obtuvo un valor actual (VA) total ajustado por riesgo a tres años de 326 000 $.

Costos evitados en la gestión y soporte de la solución de autenticación anterior

Ref.	Parámetro	Fuente	Año 1	Año 2	Año 3
E1	Personal de TI a tiempo completo (ETC) necesario para gestionar y dar soporte de forma continua a la solución previa de autenticación	Entrevistas	2	2	2
E2	Cantidad de horas que trabaja cada empleado (ETC) al año	Estándar TEI	2080	2080	2080
E3	Tiempo del personal de TI necesario para gestionar y dar soporte de forma continua a Duo (en horas)	Entrevistas	312	312	312
E4	Subtotal: Tiempo del personal de TI ahorrado con Duo (en horas)	(E1*E2)-E3	3848	3848	3848
E5	Recuperación de la productividad	Estándar TEI	50 %	50 %	50 %
E6	Retribución por hora del personal de TI combinado (incluidos todos los gastos)	Estándar TEI	47,60 $	49,03 $	50,50 $
E7	Tarifas ahorradas en servicios profesionales	Entrevistas	60 000 $	60 000 $	60 000 $
Et	Costos evitados en la gestión y soporte de la solución previa de autenticación	(E4*E5*E6)+E7	151 582 $	154 334 $	157 162 $
	Ajuste por riesgo	↓15 %			
Etr	Costos evitados en la gestión y soporte de la solución previa de autenticación (ajustados por riesgo)		128 845 $	131 184 $	133 588 $
	Total de tres años: 393 616 $			**Valor actual de tres años: 325 914 $**	

MEJORAS EN LA PRODUCTIVIDAD DEL CENTRO DE ASISTENCIA Y DE LOS USUARIOS FINALES COMO CONSECUENCIA DE LA DISMINUCIÓN EN INCIDENTES DE AUTENTICACIÓN

Evidencia y datos. Dado que Duo simplifica el proceso de autenticación del usuario final y elimina la necesidad de un dispositivo aparte, los centros de asistencia de las organizaciones de los entrevistados recibieron menos casos relacionados con la autenticación. Esto ahorró tiempo al personal del servicio de asistencia y a los usuarios finales.

Un técnico de seguridad de una empresa de servicios profesionales afirmó: «Pasamos de 20 llamadas semanales a quizás una o dos. La cantidad de llamadas disminuyó porque la aplicación es más intuitiva y menos problemática para los usuarios finales. La aplicación antigua no era tan sencilla, la gente a veces no tenía el código, etc. También tenemos comentarios muy buenos por parte del centro de asistencia en cuanto a la verificación durante las llamadas que están haciendo con Duo, la cual está funcionando sin ningún problema.»

«Los usuarios tienen menos problemas con la autenticación, y los registros de Duo son de gran ayuda para resolver los problemas de los usuarios que llegan a nuestro centro de asistencia.»

Analista de ciberseguridad, sector sanitario

Modelado y suposiciones. Para la organización compuesta, Forrester aplica las siguientes suposiciones:

- Antes de implementar Duo, el centro de asistencia atendía cada año 1500 incidentes de autenticación.
- Con Duo, se elimina el 90 % de esos incidentes.
- El personal del centro de asistencia invierte 0,4 horas en resolver cada incidente de autenticación.
- El personal del centro de asistencia utiliza de forma productiva el 100 % del tiempo que ahorra.
- Los usuarios finales tardan 0,4 horas en resolver los incidentes de autenticación.
- Los usuarios finales utilizan de forma productiva el 50 % del tiempo que ahorran.

Riesgos. La mejora de la productividad del centro de asistencia y del usuario final debido a la disminución de incidentes de autenticación varía en función de:

- El tipo de solución de autenticación que tenían anteriormente.
- Experiencia y capacidades del personal del centro de asistencia.
- La medida en que la organización se ha valido de las capacidades de Duo.
- Tasas de retribución locales vigentes.

Resultados. En consideración de estos riesgos, Forrester ajustó el beneficio un 10 % a la baja, con lo que obtuvo un VA total ajustado por riesgo a tres años de 57 000 $.

Mejoras en la productividad del centro de asistencia y de los usuarios finales como consecuencia de la disminución de incidentes de autenticación					
Ref.	**Parámetro**	**Fuente**	**Año 1**	**Año 2**	**Año 3**
F1	Incidentes de autenticación que llegaban al centro de asistencia antes de implementar Cisco Duo	Entrevistas	1500	1500	1500
F2	Porcentaje de reducción de incidentes tras implementar Duo	Entrevistas	90 %	90 %	90 %
F3	Subtotal: Reducción de incidentes con Duo	F1*F2	1350	1350	1350
F4	Tiempo del centro de asistencia por incidente (en horas)	Entrevistas	0,4	0,4	0,4
F5	Tarifa por hora del personal del centro de asistencia (incluidos todos los gastos)	Estándar TEI	27,91 $	28,75 $	29,61 $
F6	Recuperación de la productividad del centro de asistencia	Estándar TEI	100 %	100 %	100 %
F7	Subtotal: Mejora de la productividad del centro de asistencia	F3*F4*F5*F6	15 071 $	15 525 $	15 989 $
F8	Tiempo del usuario final por incidente (en horas)	Entrevistas	0,4	0,4	0,4
F9	Tarifa por hora de los usuarios finales combinados (incluyendo todos los gastos)	Estándar TEI	35,10 $	36,15 $	37,23 $
F10	Recuperación de la productividad del usuario final	Estándar TEI	50 %	50 %	50 %
F11	Subtotal: Mejora en la productividad de los usuarios finales	F3*F8*F9*F10	9477 $	9761 $	10 052 $
Ft	Mejoras en la productividad del centro de asistencia y de los usuarios finales como consecuencia de la disminución de incidentes de autenticación	F7+F11	24 548 $	25 286 $	26 041 $
	Ajuste por riesgo	↓10 %			
Ftr	Mejoras en la productividad del servicio de asistencia y de los usuarios finales como consecuencia de la disminución de incidentes de autenticación (ajustado por riesgo)		22 094 $	22 757 $	23 437 $
	Total a tres años: 68 288 $			**Valor actual a tres años: 56 502 $**	

BENEFICIOS NO CUANTIFICADOS

Los entrevistados mencionaron los siguientes beneficios adicionales que sus respectivas organizaciones experimentaron, pero que no pudieron cuantificar:

- **Una mejor experiencia para el usuario final.** A los usuarios finales les resultó fácil empezar a utilizar Duo, y posteriormente se ahorraron tiempo (en cada autenticación y en tiempo de inactividad) y frustración.

  Un técnico de seguridad de una empresa de servicios profesionales afirmó: «La facilidad de uso de Duo ha sido muy bien recibida en nuestra organización. Con Duo, recibes la notificación push y solo tienes que dar un solo toque al dispositivo. Comparado con el método anterior, en el que todos tenían pequeños tokens y debían marcar un número en un tiempo determinado... Desde que incorporamos a Duo, no hemos tenido tiempo de inactividad debido a incidentes de seguridad relacionados con la autenticación.»

  Un director de seguridad informática de alto nivel de una organización sanitaria afirmó: «El cambio a Duo mejoró la experiencia del usuario final un 100 %. En primer lugar, no tienes que llevar un dispositivo físico y estar pendiente de él, comparado con el teléfono que ya llevo conmigo. Y segundo, en lugar de tener que intentar leer los números del token y luego teclearlos en el dispositivo, simplemente pulsas 'Aceptar'.»
  Un analista de ciberseguridad de una organización sanitaria afirmó: «Incluso nuestro autorregistro es bastante sencillo para los usuarios finales.»

- **Facilidad para mejorar aún más la experiencia del usuario con el inicio de sesión único (SSO) de Duo.** Las organizaciones que optaron por utilizar la funcionalidad SSO de Duo mejoraron aún más la experiencia del usuario final al proporcionar a los usuarios de Duo una experiencia de inicio de sesión simple y armonizada entre todas las aplicaciones que están integradas con Duo, ya sean locales o en la nube. El SSO basado en la nube de Cisco para Duo está diseñado para complementar la solución de autenticación multifactor de Duo, aunque Duo también se integra con decenas de SSO de terceros y de herramientas de identidad.

  Un analista de ciberseguridad de una organización sanitaria que utiliza el SSO de Duo afirmó: «El SSO de Duo es fácil de configurar y gestionar. A la mayoría de los empleados con los que he hablado les encanta lo fácil que es utilizarlo. El SSO de Duo ahorra tiempo a los usuarios finales porque ahora, después de iniciar sesión en una aplicación, no tienen que utilizar el multifactor en cada una de las aplicaciones siguientes.»
- **Eficiencias en auditoría y cumplimiento de normas.** Un técnico de seguridad de una empresa de servicios profesionales afirmó: «Con los mejores datos de auditoría que proporciona Duo y los informes de actividad de los usuarios podemos ejecutar informes de auditoría totalmente automatizados. Eso no era posible con nuestra solución anterior.»
- **Mayor capacidad para atraer nuevos clientes o socios.** Un especialista en soporte informático de una empresa de servicios de información afirmó: «Creo que el uso de Duo nos ayuda a atraer nuevos clientes y socios, o a obtener más ingresos de nuestros clientes actuales, una vez que saben que utilizamos Cisco Duo. Tiene reconocimiento de marca en algunos de los mercados en los que estamos, y eso les da cierto grado de confianza.»
- **Consolidación de proveedores.** Un director de seguridad informática de alto nivel de una organización sanitaria afirmó: «Tenía sentido elegir una empresa con la que ya trabajábamos y así limitar el número de personas a las que tenemos que llamar.» Un especialista en soporte informático de una empresa de servicios de información afirmó: «La facilidad de integración de Duo con nuestros productos de seguridad existentes del mismo proveedor resultó atractiva.»
- **La moderada curva de aprendizaje de Duo y el valor del soporte de primera calidad de Duo Care.** Un técnico de seguridad de una empresa de servicios profesionales afirmó: «Nuestra curva de aprendizaje fue baja. El producto se explica por sí mismo y la atención al cliente es excelente.» Un especialista en soporte informático de una empresa de servicios de información afirmó: «Cisco nos facilitó mucho la incorporación y todos los demás aspectos.»

  Un analista de ciberseguridad de una organización sanitaria afirmó: «Nuestro equipo de Duo Care nos ha ayudado mucho a aprender cómo hacer las cosas y nos ha proporcionado los recursos necesarios para resolver el problema. O si queríamos implementar un determinado diseño, nos han ayudado mucho a averiguar cómo hacerlo.»

FLEXIBILIDAD

Cada cliente asigna su propio valor a la flexibilidad. Hay muchas situaciones en las que un cliente puede descubrir usos y oportunidades empresariales adicionales tras implementar Duo, por ejemplo:

- **Aprovechar aún más las capacidades de Duo.** Los entrevistados mencionaron el amplio alcance de las capacidades de Duo y su intención de aprovechar más esa funcionalidad. Un analista de ciberseguridad de una organización sanitaria afirmó: «Podemos sacarle mucho más provecho a Duo. Estamos deseando probar más funcionalidades.»
- **Protección de aplicaciones adicionales con Duo.** Las organizaciones de los entrevistados suelen implementar Duo inicialmente en sus aplicaciones de máxima prioridad (especialmente aquellas a las que se accede con frecuencia de forma remota) y posteriormente le van aplicando Duo a otras aplicaciones, incluyendo las aplicaciones y servicios internos. Un especialista en soporte informático de una empresa de servicios de información afirmó: «Añadir otra

aplicación no cambia lo que pagamos por Duo. Cuantas más aplicaciones pueda proteger con Duo, más valor obtendré de él.»

- **Ampliar fácilmente el uso de Duo a entidades adquiridas.** Un analista de ciberseguridad de una organización sanitaria afirmó: «Pronto se nos unirán muchos más empleados debido a una adquisición, pero Duo nos lo pone fácil.»

La flexibilidad también se cuantificó al evaluarse en el marco de un proyecto específico (esto se describe más a detalle en el Anexo A).

Análisis de costos

Datos de costos cuantificados aplicados a la organización compuesta

Costos totales

Ref.	Coste	Inicial	Año 1	Año 2	Año 3	Total	Valor actual
Gtr	Tarifas de Cisco	0 $	680 400 $	680 400 $	680 400 $	2 041 200 $	1 692 054 $
Htr	Esfuerzo a nivel interno que requiere la implementación, gestión y asistencia	218 691 $	47 596 $	49 023 $	50 489 $	365 798 $	340 408 $
	Costos totales (ajustados por riesgo)	218 691 $	727 996 $	729 423 $	730 889 $	2 406 998 $	2 032 462 $

TARIFAS DE CISCO

Evidencia y datos. Las tarifas de Duo reflejaban las cuotas de suscripción a la versión Access de Duo, y las cuotas de Duo Care para servicios adicionales que no incluye la asistencia estándar de Duo.

Dado que los factores específicos de cada cliente determinan las tarifas de suscripción y de Duo Care, deberá consultar con Cisco los posibles costos específicos para su organización cuando realice su análisis. Las cuotas de su organización pueden diferir de las de la organización compuesta.

Modelado y suposiciones. Para la organización compuesta, Forrester aplica las siguientes suposiciones:

- La organización implementa la versión Access de Duo con 10 000 licencias.
- La organización opta por suscribirse a Duo Care.

Riesgos. Las tarifas de Cisco varían en función de:

- La cantidad de licencias de Duo.
- La versión de Duo que elige la organización.
- Si la organización opta por Duo Care.

Resultados. En consideración de estos riesgos, Forrester ajustó el costo un 5 % al alza, con lo que obtuvo un VA total ajustado por riesgo a tres años (con un descuento del 10 %) de 1,7 millones $.

Tarifas de Cisco

Ref.	Parámetro	Fuente	Inicial	Año 1	Año 2	Año 3
G1	Cuotas de suscripción a Duo Access	Organización compuesta		540 000 $	540 000 $	540 000 $
G2	Cuotas de Duo Care	Organización compuesta		108 000 $	108 000 $	108 000 $
Gt	Tarifas de Cisco	G1+G2	0 $	648 000 $	648 000 $	648 000 $
	Ajuste por riesgo	↑5 %	·			
Gtr	Tarifas de Cisco (ajustadas por riesgo)		0 $	680 400 $	680 400 $	680 400 $
	Total a tres años: 2 041 200 $			**Valor actual a tres años: 1 692 054 $**		

ESFUERZO A NIVEL INTERNO QUE REQUIERE LA IMPLEMENTACIÓN, GESTIÓN Y ASISTENCIA

Evidencia y datos. Los entrevistados explicaron que la instalación de Duo fue relativamente sencilla. Las organizaciones de los entrevistados implementaron Duo utilizando recursos internos que incluían un director de proyecto, administradores de redes y servidores, administradores de seguridad, así como la orientación por parte de su equipo de Duo Care. La configuración técnica implicó determinar los requisitos (por ejemplo, en torno a los usuarios remotos que se conectan a las aplicaciones internas) y, a continuación, la configuración, implementación y pruebas de Duo y sus integraciones con las aplicaciones clave.

El personal de formación interno de las organizaciones de los entrevistados elaboró documentación y materiales de formación para los usuarios finales basándose en las plantillas y la orientación que les proporcionó su equipo de Duo Care y, a continuación, apoyó a los usuarios finales durante la salida en vivo de Duo en sus organizaciones. Los usuarios finales se familiarizaron con Duo leyendo material o viendo un vídeo y consultando con el personal de formación si era necesario y, posteriormente, registraron sus dispositivos en Duo.

De forma continua, el personal de TI encargado de la seguridad gestionó y dio soporte de Duo (incluyendo el interfaz con Cisco y una evaluación continua sobre cómo optimizar aún más su uso de Duo). Además, se encargó de proyectos como incorporar nuevas funciones o nuevos casos de uso en Duo. Los usuarios finales recién contratados se formaron utilizando los materiales de formación y consultaron con el personal del centro de asistencia cuando fue necesario.

Modelado y suposiciones. Para la organización compuesta, Forrester aplica las siguientes suposiciones:

- El personal de TI dedica un total combinado de 180 horas a lo largo de un mes a la implementación técnica.
- El personal de formación dedica un total combinado de 340 horas durante la implementación desarrollando y distribuyendo materiales y orientando a los usuarios finales.

> **«Pasar a Duo fue sencillo. Duo nos lo puso muy fácil: solo tienes que enchufar y listo. La documentación, las actualizaciones y el soporte son muy buenos.»**
>
> *Analista de ciberseguridad, sector sanitario*

- El personal de TI dedica un total de 312 horas al año a la gestión y asistencia.
- El personal del centro de asistencia dedica un total combinado de 75 horas al año a matricular nuevos usuarios en Duo.
- Todos los usuarios finales reciben formación durante la implementación; los nuevos empleados reciben formación a medida que son contratados.
- Cada usuario final dedica 0,5 horas a familiarizarse con Duo y a registrar su dispositivo.
- La rotación anual de personal es del 15 %.

Riesgos. El esfuerzo interno necesario para la implementación, gestión y asistencia varía en función de:

- La cantidad de licencias de Duo.
- Experiencia y capacidades del personal de TI.
- La madurez de las operaciones de seguridad de la organización.
- La medida en que la organización se ha valido de las capacidades de Duo.
- Tasas de retribución locales vigentes.

Resultados. En consideración de estos riesgos, Forrester ajustó el coste un 10 % al alza, con lo que obtuvo un VA total ajustado por riesgo a tres años de 34 000 $.

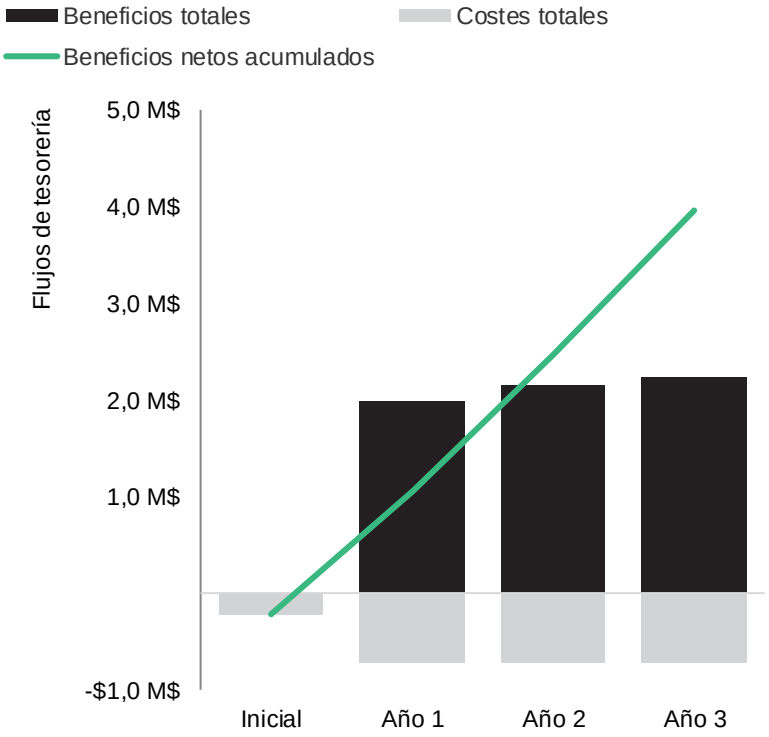
Esfuerzo a nivel interno que requiere la implementación, gestión y asistencia

Ref.	Parámetro	Fuente	Inicial	Año 1	Año 2	Año 3
H1	Horas totales combinadas del equipo de TI necesarias para la implementación técnica inicial, la gestión y el soporte continuos de Duo	Entrevistas	180	312	312	312
H2	Retribución por hora del personal de TI combinado (incluidos todos los gastos)	Estándar TEI	47,60 $	47,60 $	49,03 $	50,50 $
H3	Horas totales combinadas de formadores necesarias para la formación inicial	Entrevistas	340			
H4	Retribución por hora de los formadores combinados (incluidos todos los gastos)	Estándar TEI	43,36 $			
H5	Tiempo del centro de asistencia para matricular a nuevos usuarios (en horas)	Entrevistas		75	75	75
H6	Retribución por hora del personal del centro de asistencia (incluidos todos los gastos)	Estándar TEI		27,91 $	28,75 $	29,61 $
H7	Usuarios finales nuevos a Duo	Organización compuesta	10 000	1500	1500	1500
H8	Tiempo que cada usuario final nuevo a Duo le dedica a familiarizarse con el sistema y registrar sus dispositivos (en horas)	Entrevistas	0,5	0,5	0,5	0,5
H9	Retribución por hora de los usuarios finales combinados (incluidos todos los gastos)	Estándar TEI	35,10 $	35,10 $	36,15 $	37,23 $
Ht	Esfuerzo a nivel interno que requiere la implementación, gestión y asistencia	(H1*H2)+(H3*H4)+ (H5*H6)+(H7*H8*H9)	198 810 $	43 269 $	44 566 $	45 899 $
	Ajuste por riesgo	↑10 %	·			
Htr	Esfuerzo a nivel interno que requiere la implementación, gestión y asistencia (ajustado por riesgo)		218 691 $	47 596 $	49 023 $	50 489 $
	Total a tres años: 365 798 $			**Valor actual a tres años: 340 408 $**		

Resumen de los aspectos económicos

PARÁMETROS CONSOLIDADOS A TRES AÑOS AJUSTADOS POR RIESGO

Gráfica del flujo de tesorería (ajustada por riesgo)



Los resultados financieros calculados en los apartados de beneficios y costos se pueden emplear para determinar el ROI, VAN y el plazo de recuperación de la inversión de la organización compuesta. En este análisis, Forrester aplica la suposición de una tasa de descuento anual del 10 %.

Estos valores de ROI, VAN y plazos de recuperación de la inversión ajustados por riesgo se determinan mediante la aplicación de factores de ajuste de riesgo a los resultados brutos de cada sección de beneficios y costos.

Análisis del flujo de tesorería (estimaciones ajustadas por riesgo)

	Inicial	Año 1	Año 2	Año 3	Total	Valor actual
Costos totales	(218 691 $)	(727 996 $)	(729 423 $)	(730.889 $)	(2 406 998 $)	(2 032 462 $)
Beneficios totales	0 $	1 996 760 $	2 143 199 $	2 226 187 $	6 366 147 $	5.259 044 $
Beneficios netos	(218 691 $)	1 268 765 $	1 413 777 $	1 495 298 $	3 959 148 $	3 226 582 $
ROI						159 %
Recuperación de la inversión						<6 meses

Anexo A: Total Economic Impact

Total Economic Impact™ (TEI) es una metodología desarrollada por Forrester Research que mejora los procesos de toma de decisiones tecnológicas de una empresa y le ayuda a los proveedores a comunicarle a sus clientes la propuesta de valor de sus productos y servicios. La metodología TEI le ayuda a las empresas a demostrar, justificar y constatar el valor tangible de las iniciativas de TI, tanto a los altos directivos como a otros actores clave de la empresa.

ENFOQUE MEDIANTE LA METODOLOGÍA TOTAL ECONOMIC IMPACT

Los beneficios representan el valor que obtiene la empresa derivados del producto. La metodología TEI otorga el mismo peso a la medida de los beneficios y a la de los costos, lo que permite examinar plenamente el efecto de la tecnología en toda la organización.

Los costos representan todos los gastos necesarios para obtener el valor o beneficios propuestos con el producto. Dentro de la metodología TEI, la categoría de costos registra el aumento en costos que representa la solución comparado con el entorno de costos recurrentes que existen actualmente.

La flexibilidad representa el valor estratégico que se puede obtener de una inversión adicional futura sobre la base de la inversión inicial ya realizada. Contar con la capacidad de registrar ese beneficio conlleva un VA que se puede estimar.

Los riesgos son una medida de la incertidumbre de los estimados de beneficios y costos basada en: 1) la probabilidad de que los estimados coincidan con las proyecciones originales y 2) la probabilidad de que se haga un seguimiento de los estimados a lo largo del tiempo. En la metodología TEI, los factores de riesgo se basan en una «distribución triangular».

La columna correspondiente a la inversión inicial contiene los costos en los que se ha incurrido en el «momento 0» o al comienzo del primer año y que no se descuentan. Los demás flujos de tesorería se descuentan aplicando la tasa de descuento al final del año. Se facilitan cálculos de VA para cada estimación de costos y beneficios totales. Los cálculos de VAN en las tablas de resumen consisten en la suma de la inversión inicial y los flujos de tesorería descontados cada año. Las sumas y cálculos de valor actual de las tablas de beneficios totales, costos totales y flujo de tesorería podrían no dar resultados exactos debido al redondeo de cifras.

VALOR ACTUAL (VA)

El valor actual o presente de las estimaciones (con descuento aplicado) de los costos y beneficios materializados según un tipo de interés (la tasa de descuento). El VA de los costos y beneficios se contabiliza en el VAN total de los flujos de tesorería.

VALOR ACTUAL NETO (VAN)

El valor actual o presente de los futuros flujos de tesorería netos (con descuento aplicado) según un tipo de interés (la tasa de descuento). Un VAN positivo para un proyecto suele indicar que la inversión es aconsejable excepto en caso de que otros proyectos obtengan un VAN superior.

RETORNO DE LA INVERSIÓN (ROI)

La rentabilidad prevista de un proyecto expresada como un valor porcentual. El ROI se calcula dividiendo los beneficios netos (beneficios menos costos) entre los costos.

TASA DE DESCUENTO

El tipo de interés que se emplea en el análisis del flujo de tesorería para contabilizar el valor monetario del tiempo. Las organizaciones suelen aplicar tasas de descuento de entre el 8 % y el 16 %.

PLAZO DE RECUPERACIÓN DE LA INVERSIÓN

El tiempo que se tarda en recuperar el monto de una inversión. En el momento en que se cumple este plazo, los beneficios netos (beneficios menos costos) equivalen a la inversión o coste inicial.

Anexo B: Notas

[1] Total Economic Impact™ (TEI) es una metodología desarrollada por Forrester Research que mejora los procesos de toma de decisiones tecnológicas de una empresa y le ayuda a los proveedores a comunicarle a sus clientes la propuesta de valor de sus productos y servicios. La metodología TEI le ayuda a las empresas a demostrar, justificar y constatar el valor tangible de las iniciativas de TI, tanto a los altos directivos como a otros actores clave de la empresa.

[2] Fuente: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q1 2021.

[3] Fuente: Ibid.


FORRESTER®