proofpoint.

LIBRO ELECTRÓNICO

# Cómo medir el impacto de un programa de concienciación en seguridad para una eficacia a largo plazo

## Guía para CISO y responsables de TI

proofpoint.com/es

# El 85 %

de los CFO de EE. UU. afirmaron que sus consejos de administración habían tenido un debate formal sobre ataques de ciberseguridad recientes y las secuelas de los incidentes[1].

# Introducción

Para los responsables de la seguridad y de TI, la nueva década ha comenzado cargada de desafíos y cambios. Desde las prisas por conectar de forma segura a los teletrabajadores debido a la pandemia al repunte de ataques de phishing que aprovecha el caos, 2020 marcó el comienzo de una complicada nueva era para la ciberseguridad.

En una entrevista reciente entre profesionales de tecnología, el 57 % afirmó que su organización sufrió un ataque de phishing en 2020, un 55 % más que el año anterior[2]. Y el bombardeo no cesa. El creciente repunte de importantes ataques de ransomware y fugas de datos está forzando a las empresas a limitar los riesgos a los que se exponen.

Los compromisos son dolorosos para las víctimas, pero pueden generar conversaciones muy necesarias entre los ejecutivos y el consejo de administración sobre la ciberseguridad y el papel que juegan los empleados en la protección de la empresa.

Las mayoría de las ciberamenazas requieren la intervención humana. Esa es la razón por la que los programas de concienciación sobre seguridad eficaces (y los cambios en el comportamiento) pueden jugar un gigantesco papel en la reducción de riesgos[3]. Muchos responsables de seguridad son perfectamente conscientes de esta situación. Pero medir el impacto de su programa de concienciación en seguridad y comunicárselo a los cargos directivos no siempre se produce de manera natural.

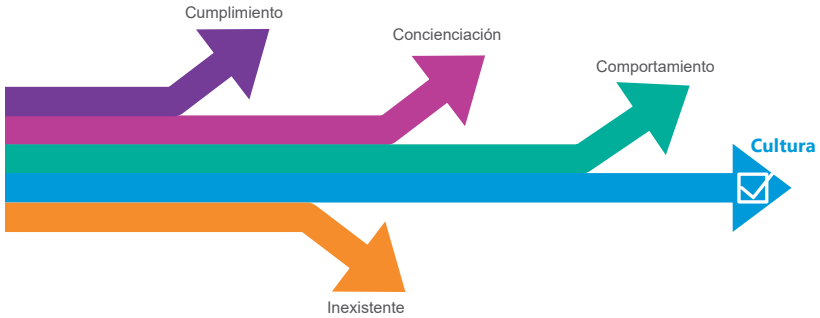
Este libro electrónico analiza los pormenores de los programas de concienciación en seguridad para que sean eficaces a largo plazo. Describe las estrategias para defender, medir y conseguir la aceptación de las partes interesadas. Y le explica cómo aprovechar al máximo esta inversión crítica.

[1] CNBC. "CNBC Global CFO Council Survey" (Encuesta del Global CFO Council de la CNBC) Julio de 2021.
[2] Proofpoint. "State of the Phish 2021". Febrero de 2021
[3] Proofpoint. "Protegiendo al usuario final". Febrero de 2019

# El estado de la concienciación en seguridad

La concienciación en seguridad no suele tener el peso a nivel presupuestario que tienen los controles técnicos. Pero no tendría que ser así. Con indicadores atractivos y una narrativa eficaz, puede conseguir dos objetivos. En primer lugar, puede reducir los riesgos de manera palpable. E igual de importante, puede demostrar a los CISO y a otras partes interesadas por qué la concienciación en seguridad es una herramienta tan crítica dentro del conjunto de estrategias de seguridad de organización.

Las preocupaciones de la dirección dependerán del estado y los objetivos del programa de seguridad existente. Los programas orientados al cumplimiento normativo, por ejemplo, se centrarán en marcar casillas para cumplir las normas. Los programas basados en los comportamientos, por su parte, medirán el éxito en función de indicadores como la tasa de clics y la tasa de denuncias durante los ataques de phishing simulados.




**Etapas de madurez de los programa de concienciación en seguridad**

## Itinerario para la instauración de una cultura de seguridad

La mayoría de las organizaciones (98 %) cuentan con un programa de formación para concienciar en materia de seguridad[4]. Sin embargo, el 64 % solo realizan sesiones formales de formación (presenciales o virtuales), por lo que desaprovechan otras oportunidades de refuerzo de la concienciación en seguridad. Solo el 23 % utilizan una combinación de todos los medios disponibles de evaluación, educación y comunicación.

La interacción continua y permanente a través de una amplia variedad de canales mejorará la retención y los resultados del programa de concienciación en seguridad. Por esa razón recomendamos utilizar la mayor cantidad de canales posible.

Un elemento clave para mejorar el programa de concienciación en seguridad es la instauración de una cultura que haga los usuarios crean en los beneficios de una seguridad robusta no solo para la organización, sino también para ellos mismos. Esto se pueden conseguir a través de la combinación de actividades para generar concienciación, cambiar comportamientos e inculcar una dedicación a combatir a los ciberdelincuentes por el bien común. Esto significa hacer de la formación un elemento relevante y útil para los usuarios, de manera constante, no solo una o dos veces al año.

### Enfoques actuales de la concienciación en seguridad[5]:

**El 29 %** usan exclusivamente pruebas de phishing simulado

**El 41 %** usan exclusivamente sesiones de formación formal

**El 7 %** usan exclusivamente contenido informativo

**El 23 %** usan una combinación de tipos de contenido

[4] Proofpoint. "State of the Phish 2021". Febrero de 2021

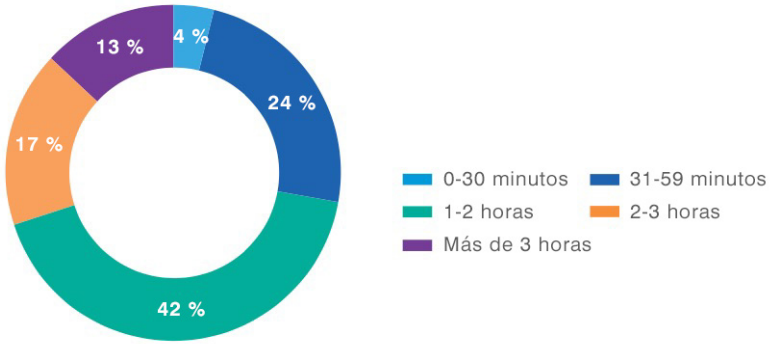
[5] Ibid.

# Cómo ejecutar un programa que consiga resultados

Cuanto más tiempo invierta una organización en sus esfuerzos de concienciación en seguridad, mayores posibilidades tendrá de obtener buenos resultados.

**Tiempo que dedican las organizaciones a la concienciación en seguridad**

La mayoría de las organizaciones dedican menos de dos horas por usuario al año para obtener resultados positivos.




**Cada año son más las empresas que incrementan la frecuencia de las actividades de concienciación en seguridad.**

## Céntrese en los usuarios vulnerables

En ocasiones, puede encontrar reticencias a la hora de ampliar su programa de concienciación en materia de seguridad. Los más escépticos pueden tener miedo a que el programa sobrecargue a muchos usuarios, sobre todo a los que no presentan un riesgo alto.

Centrarse en los usuarios vulnerables con mayor regularidad en lugar de seguir un enfoque general que imponga más formación a todos, puede ayudar a disipar algunas preocupaciones. Con un enfoque dirigido, las partes interesadas saben que están justificadas las sesiones de formación y esfuerzos de concienciación en seguridad adicionales. Y los usuarios tienen el contexto por el que la reciben.

A otros puede preocuparle menos el número de personas afectadas que la cantidad de tiempo que lleva la formación. Afortunadamente, puede impulsar la concienciación de formas que no hagan perder tiempo a los usuarios.

**Considere el uso de boletines de noticias, tablones de anuncios, páginas wiki y notificaciones de correo electrónico para ofrecer un programa de concienciación en seguridad eficiente en cuanto a tiempo.**

# ¿Sabe quiénes son sus usuarios más vulnerables?

En Proofpoint, utilizamos el término VAP (Very Attacked People™ o personas muy atacadas) para describir a la categoría de usuarios que los ciberdelincuentes atacan con una intensidad inusual. Puede tratarse de grandes volúmenes de ataques, amenazas muy dirigidas, tácticas avanzadas, o todas a la vez. Aunque todos los usuarios reciben ataques, los VAP son objetivos preciados por sus exclusivos contactos profesionales y acceso con privilegios a los datos, sistemas y otros recursos.

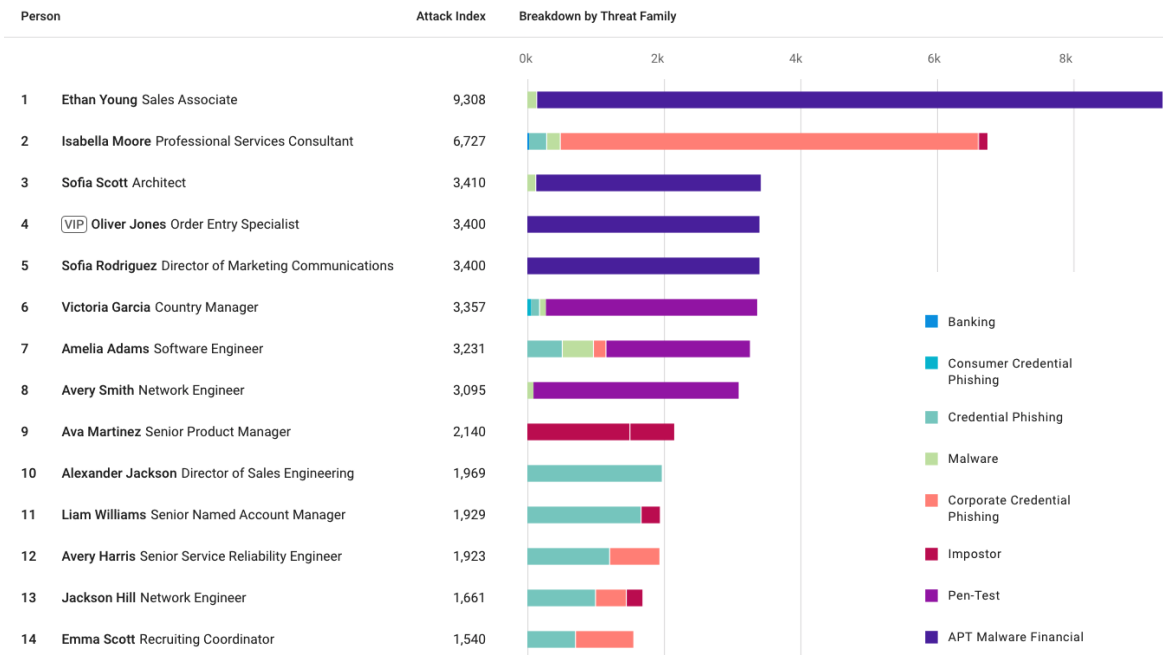
Los VAP reciben
**3-12 veces**
más ataques que
con otros usuarios

Hemos descubierto que los VAP no son siempre los VIP de una organización, como los altos directivos. Pueden formar parte de los recursos humanos, relaciones públicas, marketing o equipos de investigación. Cualquier empleado con el tipo de acceso adecuado puede ser un objetivo de alto valor.

Una vez que ha identificado a sus VAP, es fundamental cubrir las lagunas de conocimientos en seguridad con educación enormemente dirigida. Por ejemplo, considere el envío de ataques de phishing simulados a los VAP víctimas de phishing de credenciales. Si no consiguen superar las pruebas de la simulación, ofrézcales formación opcional. Esta secuencia es una forma dirigida de reducir los riesgos basados en las personas conocidos sin hacer perder tiempo a los usuarios.

La concienciación en seguridad no es un proceso que pueda aplicarse una sola vez y olvidarse. Necesita una formación completa y permanente que esté a la altura de las ciberamenazas a las que se enfrentan los usuarios. Este proceso incluye:

- Evaluaciones periódicas
- Formación
- Actividades de refuerzo
- Medición




Para realizar un seguimiento y poner de acuerdo a las partes interesadas, considere la creación de un calendario que describa las actividades, canales, mensajes y temas para su programa.

# Cómo medir la excelencia de su programa de concienciación en seguridad

Muchos programas miden el éxito en función exclusivamente de la realización de las sesiones de formación (por razones de cumplimiento) y la tasa a la que los usuarios se dejan engañar por los ataques simulados. Sin embargo, para cambiar de verdad el comportamiento de los usuarios y reducir los riesgos de phishing, debe ir un paso más lejos.

Puede ir a un nivel más profundo con perfiles de alto riesgo más completos. A continuación incluimos los indicadores clave que le ayudan a cuantificar el impacto real de la seguridad:

## Tasa de denuncias de las simulaciones

Este indicador proporciona información sobre los usuarios que adoptan buenos comportamientos, y no solo que evitan los malos. Esto significa poner en práctica su formación para concienciar en materia de seguridad cuando detectan algo sospechoso.

## Tasa de clics real

La solución de protección avanzada del correo electrónico de Proofpoint le permite ver la tasa de clics de contenido realmente inseguro, incluso si se bloquea o reescribe la URL por razones de seguridad. Este indicador deja bien a las claras el conocimiento del mundo real que tienen los usuarios. Con estos datos, puede determinar si los usuarios mejoran a la hora de detectar contenido malicioso real.

## Tipos de mensajes denunciados

Gracias a un add-in de correo electrónico, los usuarios pueden denunciar el contenido potencialmente malicioso, de una forma muy similar a como utilizan un buzón de correo malicioso. Proofpoint Targeted Attack Protection (TAP) le muestra la clasificación que realizó de los distintos tipos de correo electrónico (malicioso, spam, bajo riesgo, etc.). Puede ver los usuarios que mejoran con el tiempo a la hora de denunciar mensajes que podrían causar daños a la organización.

## Impactos reales

Este es sin duda el indicador más importante de todos. Realiza un seguimiento de lo que los usuarios hacen realmente: si se enfrenta a menos ataques de phishing, compromisos de credenciales, incidentes de origen interno y malware. Ese es el indicador máximo de la excelencia. Y lo que es más importante, es fundamental para conseguir una aceptación a largo plazo de los programas de concienciación sobre seguridad.

### Responder a la pregunta: ¿cuál debería ser nuestra tasa de clics y de denuncias?

**Proofpoint recomienda**

**<5 %**
tasa de fallos/ clics

**>70 %**
tasa de denuncias

# Comunicación eficaz con su CISO y los principales interesados

A la hora de informar a la dirección y las partes interesadas, el recurso al miedo, la incertidumbre y la duda no le llevarán muy lejos. No cabe duda de que es necesario hacer frente a las ciberamenazas, pero cuando se hace un uso excesivo de tácticas alarmistas y se exageran las amenazas, se corre el riesgo de generar el clásico escenario de "Pedro y el lobo", que hace más daño que bien.

## Principales formas de comunicar el rendimiento del programa de concienciación en seguridad

### Cuantitativa

El contexto importa. Y por eso es fundamental el conocimiento del rendimiento general y de su posición con respecto a otras empresas. Al realizar la comparación con otras empresas, céntrese en los indicadores positivos en lugar de exclusivamente en la tasa de clics en las simulaciones.

Ejemplos de indicadores positivos son:

- Las tasas de denuncias de los usuarios de los mensajes de phishing simulado han aumentado.
- Las evaluaciones de conocimientos de concienciación sobre seguridad han mejorado.
- La precisión de los mensajes maliciosos reales denunciados por los usuarios ha aumentado.
- Las tasas de participación de los usuarios en actividades de concienciación en seguridad han aumentado.

### Cualitativa

Estas historias, combinadas con datos ayudan a demostrar que la concienciación sobre seguridad es mucho más que una actividad de cumplimiento impuesta. Estos relatos ayudan a demostrar cómo el comportamiento de los usuarios está cambiando; que la cultura cambia de forma activa a medida que los usuarios comprenden los riesgos; y que el esfuerzo es ayudar a proteger la empresa.

Ejemplos de narrativa:

- Un usuario detuvo un ataque de phishing sofisticado real.
- Los usuarios valoraron positivamente el programa de concienciación en una encuesta de satisfacción.
- Un miembro del equipo directivo o un empleado conocido organización compartió algo sobre concienciación en seguridad con el personal.

# Visibilidad de la concienciación en seguridad en un panel

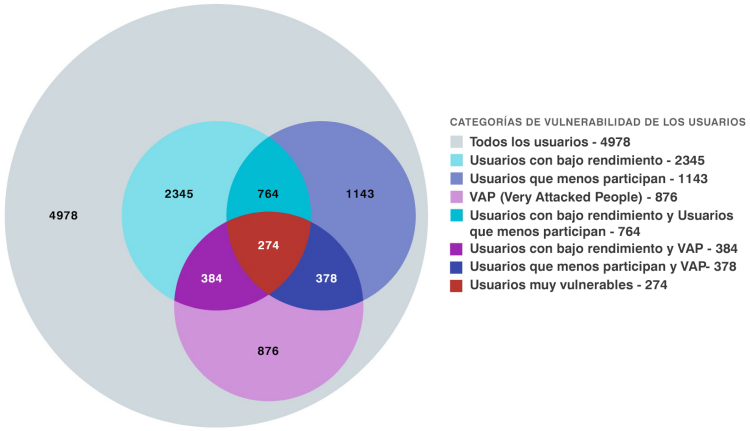
La concienciación en seguridad es una de las medidas más importantes que puede aplicar para proteger su organización. Esa es una de las razones por las que creamos un panel de CISO para la concienciación en seguridad de Proofpoint. Gracias a este panel, los equipos de TI y de seguridad tienen acceso a indicadores clave que demuestran que los programas de concienciación en seguridad cambian comportamientos y crean una cultura. Con estos indicadores de éxito, la rentabilidad de la inversión (y la razón para la inversión futura), es mucho más obvia.

Gracias al panel de CISO de Proofpoint, tiene acceso a indicadores como la vulnerabilidad de los usuarios y su calificación en el programa de concienciación en seguridad.

## Vulnerabilidad de los usuarios

Vea los usuarios con bajo rendimiento, los que menos participan, junto con los que hacen clic en mensajes maliciosos reales. Si los usuarios son identificados como VAP por Proofpoint Targeted Attack Protection, esos datos se integran también para conocer mejor el perfil de riesgo global de ese usuario.

**274 usuarios muy vulnerables (de un total de 4978 usuarios)**
**82 usuarios muy vulnerables menos en los últimos 90 días**

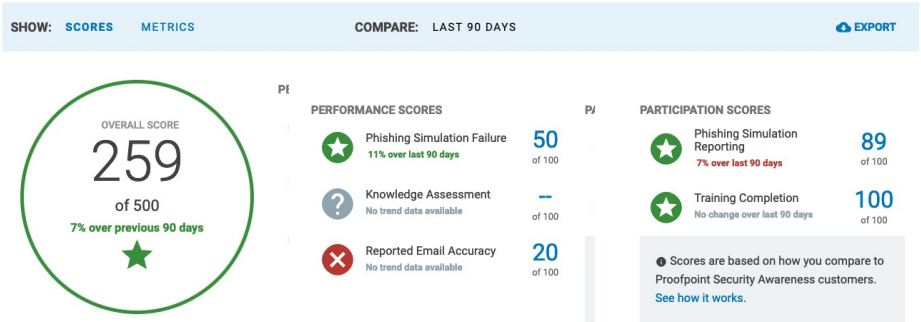



**Resumen de la vulnerabilidad de los usuarios en el panel de CISO**

## Calificación del programa de seguridad

La calificación de rendimiento y participación muestran el rango percentil de su organización en cada área y cómo ha cambiado la calificación general. Gracias a iconos tipo semáforo, puede conocer su situación en cada área en un abrir y cerrar de ojos y ver las oportunidades de mejora.

**Resumen de calificaciones del programa de seguridad**
Realice un seguimiento del estado de su programa a lo largo del tiempo gracias a la calificación del programa. Haga clic aquí en cada calificación para ver cómo se calcula.



# Visibilidad de la concienciación en seguridad en un panel

## Comparativa del percentil a lo largo del tiempo

Junto a la calificación del programa de seguridad, vea cómo es su percentil en comparación con otras empresas del sector para realizar un análisis de referencia. Puede medir el progreso a lo largo del tiempo.

El objetivo de los ciberataques actuales no es la tecnología, son las personas. Por eso, un enfoque eficaz centrado en las personas de la protección de su organización incluye formación dirigida y actividades que tengan presente la ciberseguridad, sobre todo para los usuarios vulnerables y los VAP.

Gracias al panel de CISO, tiene acceso a los indicadores necesarios para mejorar y hacer avanzar su programa de concienciación en seguridad. La comunicación con su CISO, así como conseguir apoyo permanente y mejorar su programa son más fáciles que nunca.

Para obtener más información sobre cómo puede ayudarle Proofpoint a cambiar el comportamiento de los usuarios y convertir la ciberseguridad en un elemento esencial de su cultura corporativa, visite proofpoint.com/es.

---

**ACERCA DE PROOFPOINT**

Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentran más de la mitad del Fortune 1000, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en **www.proofpoint.com/es**.



proofpoint.

0504-002-01-01 09/21