EMEA

El coste derivado del relleno de credenciales

Patrocinado por **Akamai Technologies**

Elaborado de forma independiente por Ponemon Institute LLC

Fecha de publicación: octubre de 2018

Ponemon INSTITUTE

Informe de investigación de Ponemon Institute©

El coste derivado del relleno de credenciales: EMEA

Ponemon Institute, octubre de 2018

Parte 1. Introducción

Nos complace presentar el informe *El coste derivado del relleno de credenciales: EMEA*[1], patrocinado por Akamai Technologies. El propósito de este estudio es cuantificar el coste potencial de la prevención, la detección y la reparación de los daños causados por los ataques de relleno de credenciales. El estudio también detalla a qué consecuencias financieras pueden enfrentarse las empresas si los atacantes consiguen utilizar las credenciales robadas para efectuar compras o transacciones fraudulentas.

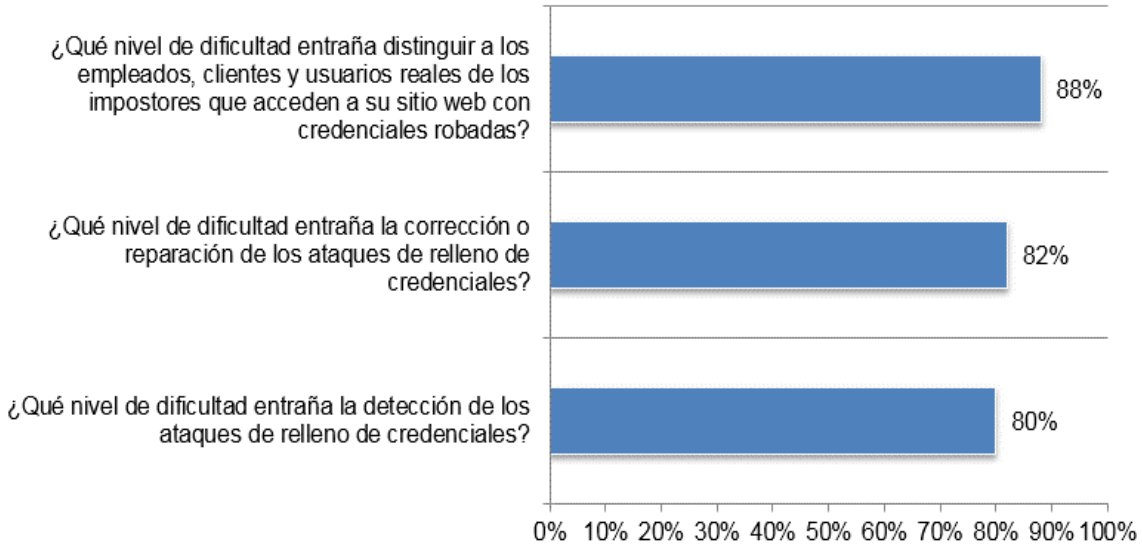
Ponemon Institute encuestó a 544 profesionales de la seguridad de TI, responsables de la protección del sitio web de su empresa y familiarizados con los ataques de relleno de credenciales. Según los encuestados, estos ataques causan costosos tiempos de inactividad de las aplicaciones y la pérdida de clientes, y, además, exigen la participación de los equipos de seguridad de TI, con unos costes que pueden ascender, de media, a 1,2 millones[2], 1,6 millones y 1,2 millones de dólares al año, respectivamente.

Además, las empresas representadas en este análisis estiman que el coste monetario del fraude derivado de ataques de relleno de credenciales puede oscilar desde un promedio de 227 550 dólares, si el 1 % de todas las cuentas pirateadas sufre pérdidas económicas, hasta los 22,8 millones de dólares, si lo hace el 100 %.

Tal como se muestra en la figura 1, casi todos los encuestados creen que resulta difícil identificar a los impostores y criminales que acceden a su sitio web con credenciales robadas (88 %), reparar los daños causados por ataques de relleno de credenciales (82 %) y detectar dichos ataques (80 %).

Figura 1. ¿En qué grado es difícil detectar y reparar los daños causados por los ataques de relleno de credenciales e identificar a los impostores?

Se han combinado las respuestas “muy difícil”, “difícil” y “algo difícil”.



[1] Europa, Oriente Medio y África.
[2] Las divisas locales se han convertido a dólares estadounidenses.

En el contexto de este estudio, se entiende por relleno de credenciales la acción mediante la cual un estafador compra en la Dark Web listas de credenciales robadas, como nombres de usuario y contraseñas, y utiliza una botnet para validar dichas listas en la página de inicio de sesión de una organización. El resultado final es normalmente un robo de cuentas, en el que los estafadores usan las credenciales robadas validadas para tomar el control de las cuentas y cometer fraudes. El objetivo clave de este delito puede ser la realización de compras fraudulentas, la participación en transacciones financieras fraudulentas y el robo de información confidencial adicional.

Las infiltraciones que sufrió Yahoo en 2016 son un ejemplo de la seriedad con la que debe abordarse esta amenaza. Estos delitos supusieron el robo de un total de 1500 millones de credenciales que se compartieron en Internet, y que se encontraban protegidas por el débil algoritmo criptográfico MD5. Los robos se produjeron en 2012 y 2013, por lo que los criminales contaron con hasta cuatro años para deshacer estas débiles defensas.[3]

Los siguientes hallazgos de la investigación revelan por qué son vulnerables las empresas a los ataques de relleno de credenciales.

- Cada mes, las empresas son víctimas de una media de unos 11 ataques de relleno de credenciales, en los que el atacante identifica qué credenciales son válidas.
- El volumen y la gravedad de los ataques de relleno de credenciales van en aumento.
- Resulta complicado distinguir a los criminales de los clientes, empleados y usuarios reales que tienen acceso a los sitios web de las empresas.
- La migración a la nube es una estrategia de TI importante, pero los participantes en el estudio sostienen que aumenta el riesgo de ataques de relleno de credenciales.
- Actualmente, las empresas no cuentan con soluciones o tecnologías suficientes para prevenir o mantener a raya los ataques de relleno de credenciales.

[3] "Credential Stuffing: A Successful and Growing Attack Methodology" (Relleno de credenciales: un método de ataque exitoso y en aumento), de Kevin Townsend, Security Week, 17 de enero de 2017.

Parte 2. Principales conclusiones

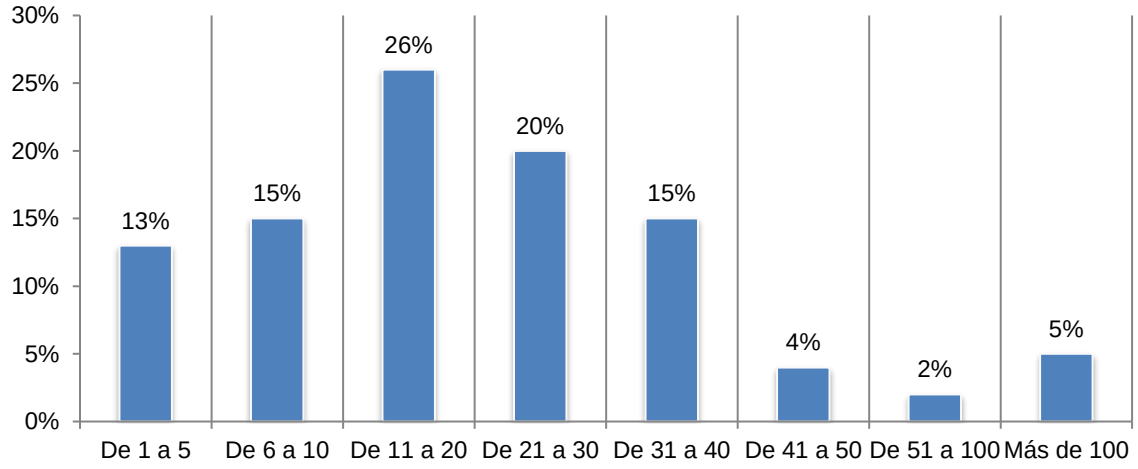
En este apartado, presentamos un análisis de los principales resultados. Los resultados auditados completos se presentan en el apéndice de este informe. Los resultados de la investigación están organizados según los siguientes temas:

- Retos organizativos y de las aplicaciones
- Capacidad para prevenir, detectar y reparar los daños causados por ataques de relleno de credenciales
- Cuantificación de los ataques de relleno de credenciales
- Consecuencias y coste del relleno de credenciales

Retos organizativos y de las aplicaciones

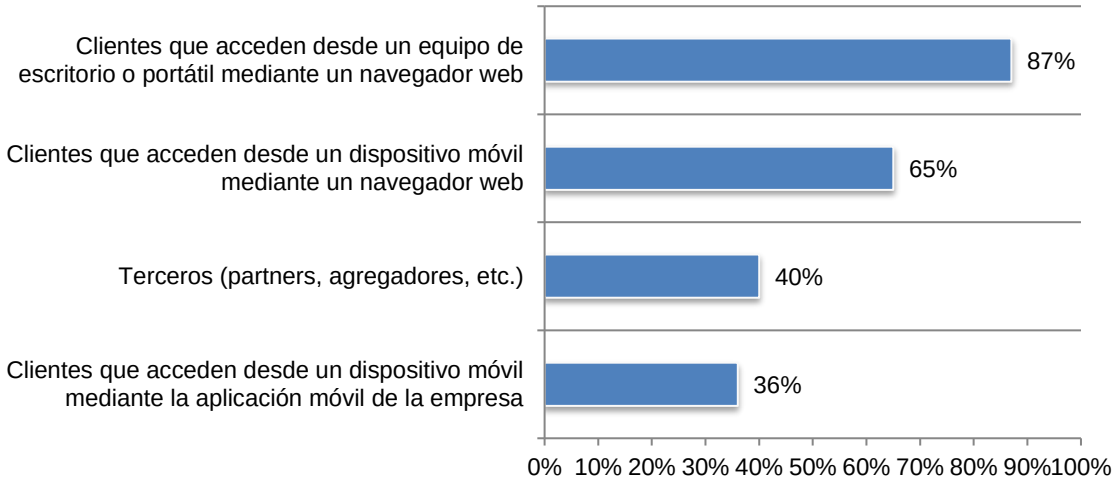
Las organizaciones tienen una superficie de ataque compleja en materia de abuso de credenciales. Esta complejidad agrava el desafío que supone ofrecer protección frente a ataques de relleno de credenciales. Tal y como se muestra en la figura 2, las empresas cuentan con una media de 26,5 sitios web orientados al cliente o para el cliente en fase de producción.

Figura 2. Número de sitios web de cliente u orientados al cliente
Valor extrapolado = 26,5



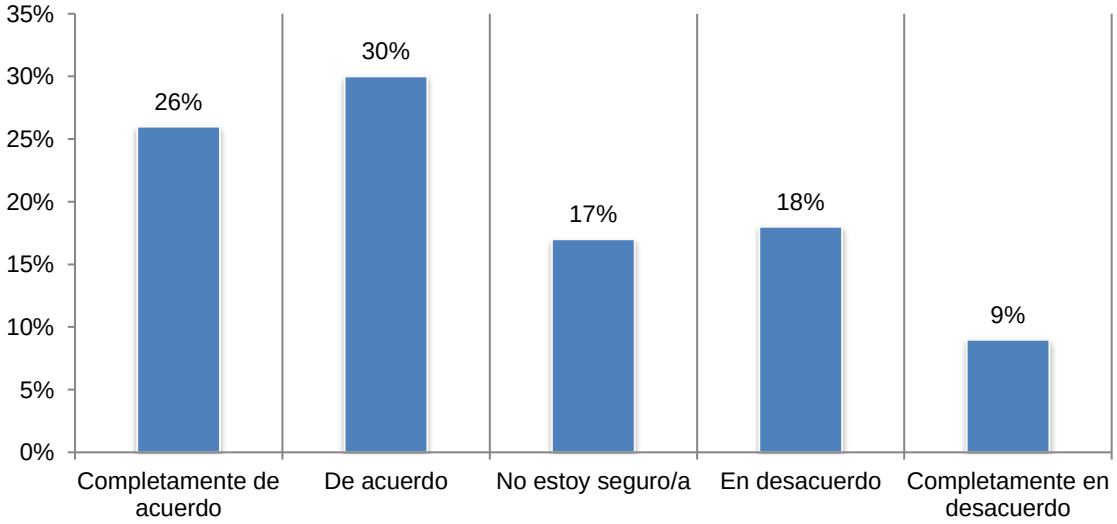
Por lo general, las organizaciones tienen que proporcionar acceso de inicio de sesión a distintos tipos de clientes. Los clientes tipo que inician sesión se muestran en la figura 3. Si bien los dos primeros tipos de clientes son usuarios de equipos de escritorio o portátiles que utilizan navegadores web (el 87 % de los encuestados) y usuarios de dispositivos móviles que utilizan navegadores móviles (el 65 % de los encuestados), las API usadas en aplicaciones móviles (el 36 % de los encuestados) y los recursos de terceros (el 40 % de los encuestados) también son una fuente importante de tráfico de inicio de sesión. Además, se espera que el tráfico móvil aumente a lo largo del tiempo. Por ejemplo, eMarketer prevé que las ventas de comercio de retail móvil crezcan del 34,5 % de 2017 a un 53,9 % en 2021.

Figura 3. Tipos de clientes de sitios web
Se admite más de una respuesta.



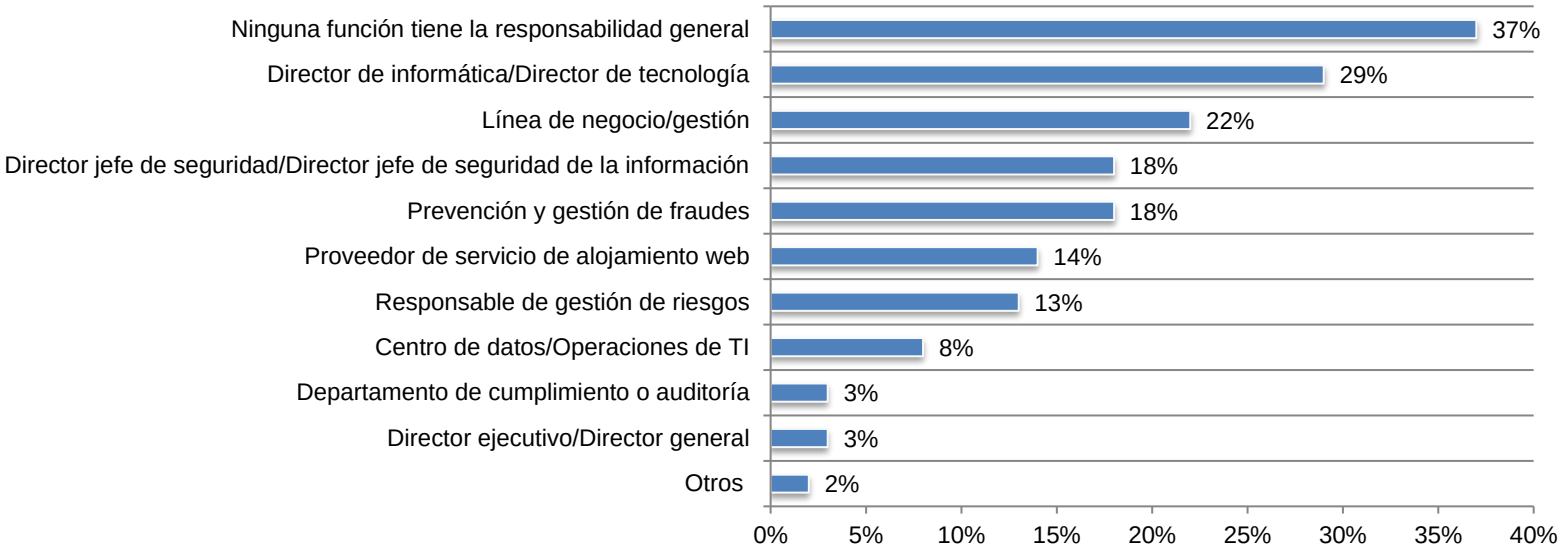
La nube aumenta el riesgo de sufrir ataques de relleno de credenciales. Según se muestra en la figura 4, el 56 % los encuestados coincide en que la migración de aplicaciones a la nube aumenta el riesgo planteado por los ataques de relleno de credenciales. Como sucede con muchos aspectos de la seguridad, la amplitud de la estrategia en la nube de una organización podría afectar a la capacidad de un equipo de seguridad de proteger el número creciente de aplicaciones (y los terminales que dan servicio a los distintos clientes) en distintas plataformas informáticas.

Figura 4. La migración a la nube ha aumentado el riesgo de ataques de relleno de credenciales



La responsabilidad de prevenir los ataques de relleno de credenciales pasa de unos a otros en la organización. Como se muestra en la figura 5, la responsabilidad de hacer frente a los ataques de relleno de credenciales se suele asignar a distintos responsables en la organización. Sin embargo, el 37 % de los encuestados afirma que no hay ninguna función que asuma plenamente esa responsabilidad. En algunas organizaciones, los equipos de gestión y los encargados de las aplicaciones son los responsables últimos del impacto. El 29 %, el 22 % y el 18 % de los encuestados afirman que los mayores responsables son, respectivamente, los directores de tecnología o informática, las líneas de negocio o gestión y los directores jefe de seguridad o seguridad de la información.

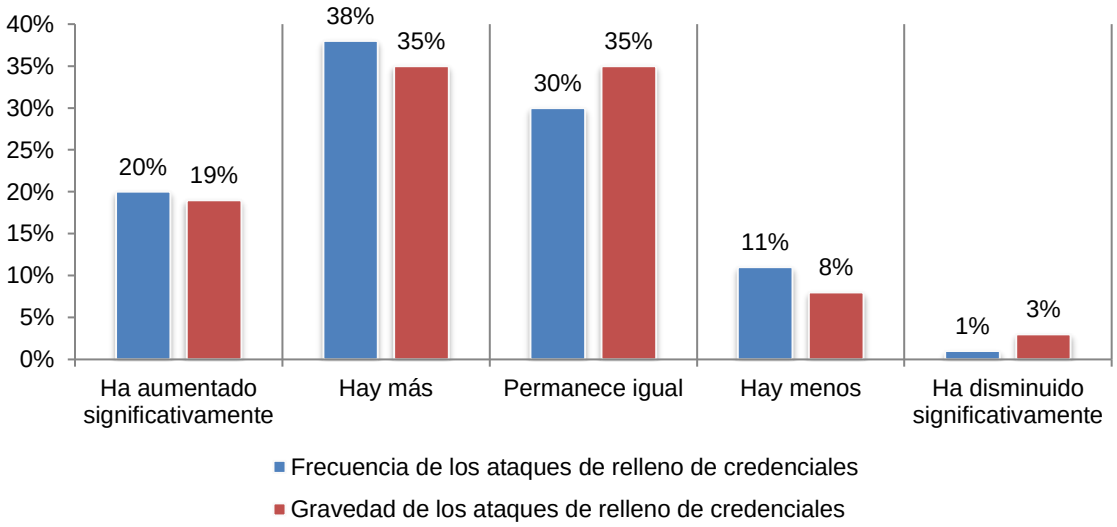
Figura 5. ¿Quién es el máximo responsable de limitar los ataques de relleno de credenciales en los sitios web de la empresa?
Dos respuestas como máximo.



Capacidad para prevenir, detectar y reparar los daños causados por ataques de relleno de credenciales

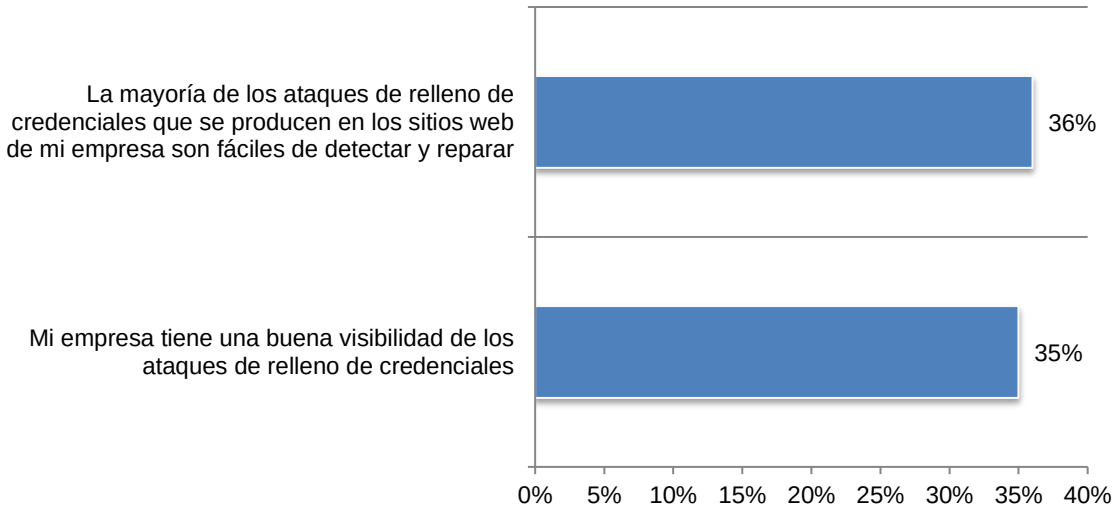
Los ataques de relleno de credenciales son cada vez más frecuentes y graves. Según los datos de la figura 6, el 88 % de los encuestados declara que los ataques registran un volumen y una frecuencia estables o crecientes. Además, el 89 % de los encuestados afirma que los ataques son igual de graves o más.

Figura 6. El aumento en el volumen o frecuencia y la gravedad de los ataques de relleno de credenciales



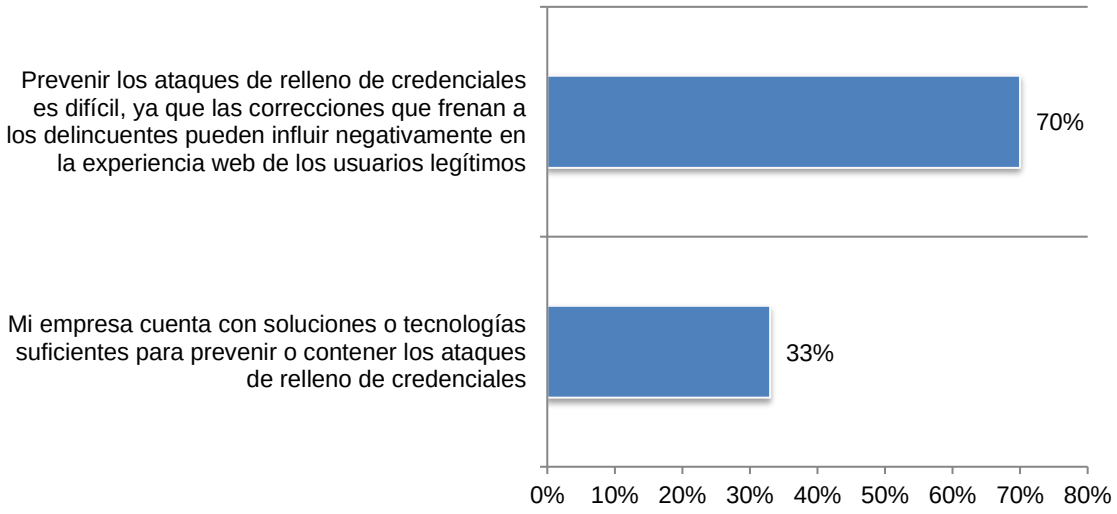
Las organizaciones tienen dificultades para reaccionar a los ataques de relleno de credenciales. Se pidió a los encuestados que indicaran en qué grado estaban de acuerdo con las declaraciones de la figura 7, con respuestas que iban desde “completamente de acuerdo” hasta “completamente en desacuerdo”. La figura compila las respuestas “de acuerdo” y “completamente de acuerdo”. Tal como se muestra, solo el 35 % de los encuestados afirma tener una buena visibilidad de los ataques de relleno de credenciales, y solo el 36 % cree que los ataques de relleno de credenciales perpetrados contra sus sitios web son fáciles de detectar y reparar.

Figura 7. ¿Qué nivel de eficacia revelan las empresas al enfrentarse a los ataques de relleno de credenciales?
Se combinan las respuestas “completamente de acuerdo” y “de acuerdo”.



Las organizaciones se enfrentan a un sinfín de retos a la hora de prevenir y mantener a raya los ataques de relleno de credenciales. Como se muestra en la figura 8, la mayoría (70 %) de los encuestados está de acuerdo con la afirmación de que prevenir los ataques de relleno de credenciales es difícil, ya que las correcciones que frenan esas acciones delictivas pueden influir negativamente en la experiencia web de los usuarios legítimos. Solo el 33 % considera que su empresa cuenta con soluciones y tecnologías suficientes para prevenir o contener ataques de relleno de credenciales.

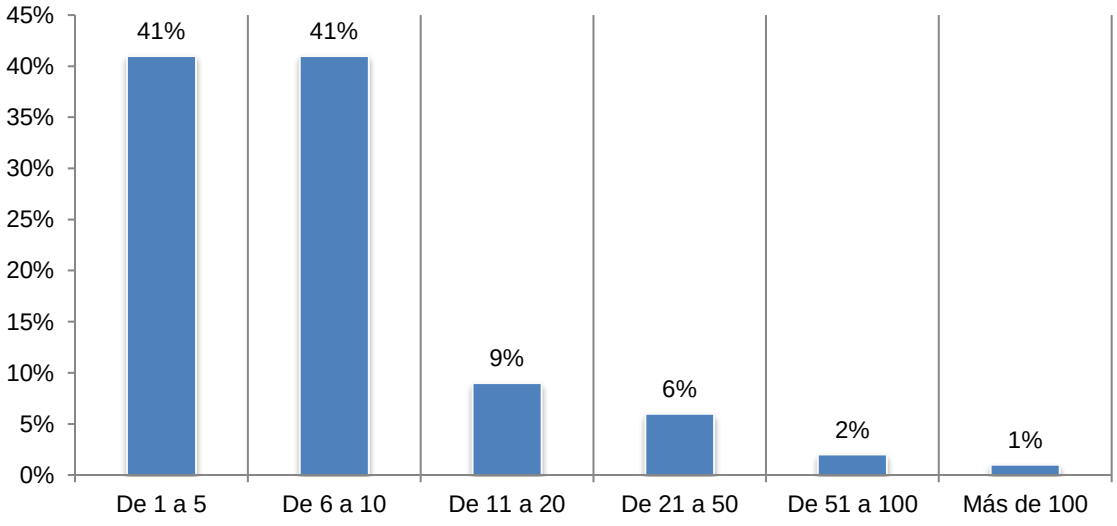
Figura 8. Retos a la hora de enfrentarse a los ataques de relleno de credenciales
Se combinan las respuestas "completamente de acuerdo" y "de acuerdo".



Cuantificación de los ataques de relleno de credenciales

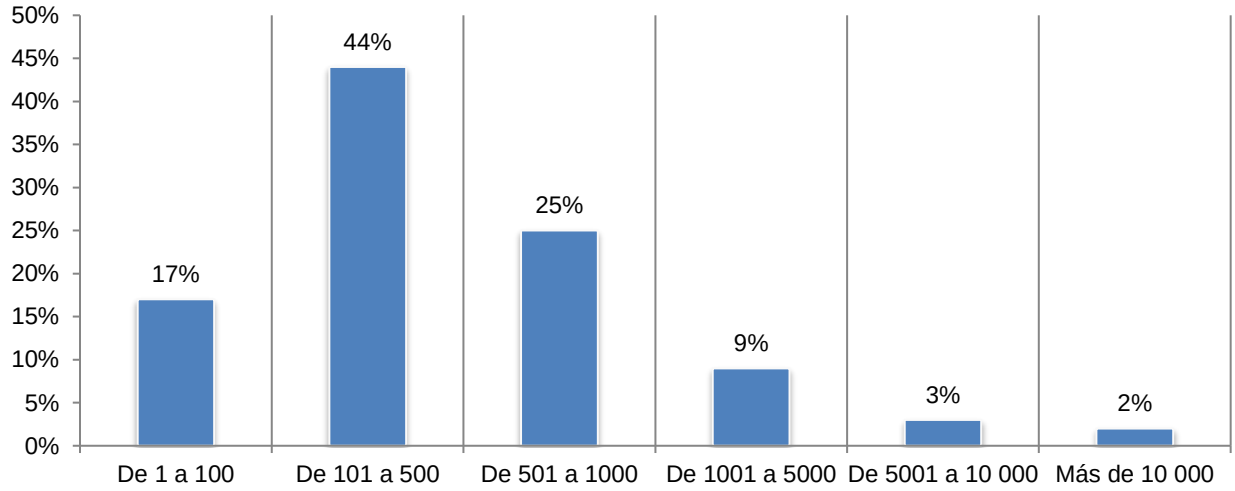
El relleno de credenciales supone un desafío persistente y continuo. Las empresas que han participado en el estudio sufren un promedio de 10,96 ataques de relleno de credenciales al mes, tal como se muestra en la figura 9. Además, un porcentaje significativo de los ataques pasa inadvertido, registrando estimaciones del 27,5 % de media.

Figura 9. Número de ataques de relleno de credenciales al mes
Valor extrapolado = 10,96



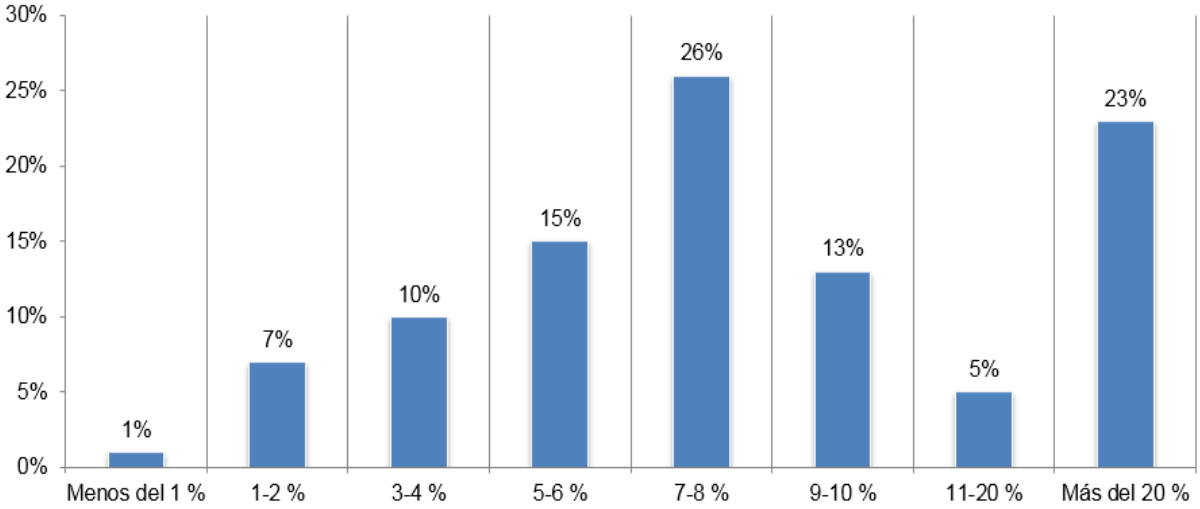
Los ataques afectan a un gran número de cuentas de usuario. Como podemos ver en la figura 10, los encuestados declararon que cada ataque de relleno de credenciales tiene como blanco un promedio de 1041 cuentas de usuario.

Figura 10. Número de cuentas de usuario afectadas por ataque
Valor extrapolado = 1041



Los atacantes tienen éxito con demasiada frecuencia. Según los encuestados, en promedio, el 10,97 % de los intentos de ataques de relleno de credenciales permite identificar correctamente las credenciales válidas de los usuarios, como se muestra en la figura 11.

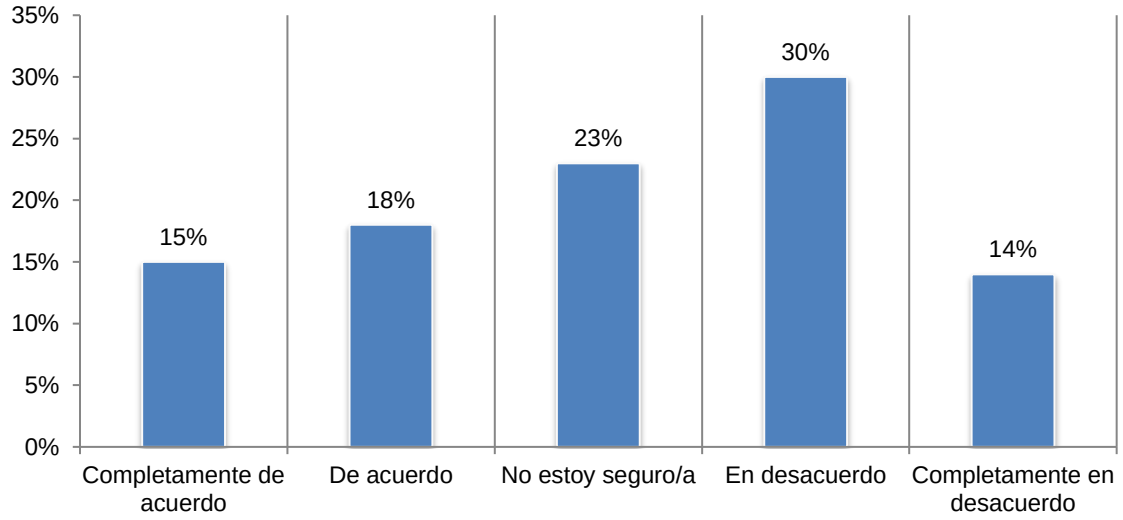
Figura 11. Porcentaje de intentos de ataques de relleno de credenciales que cumplen su objetivo
Valor extrapolado = 10,97 %



Consecuencias y coste de los ataques de relleno de credenciales

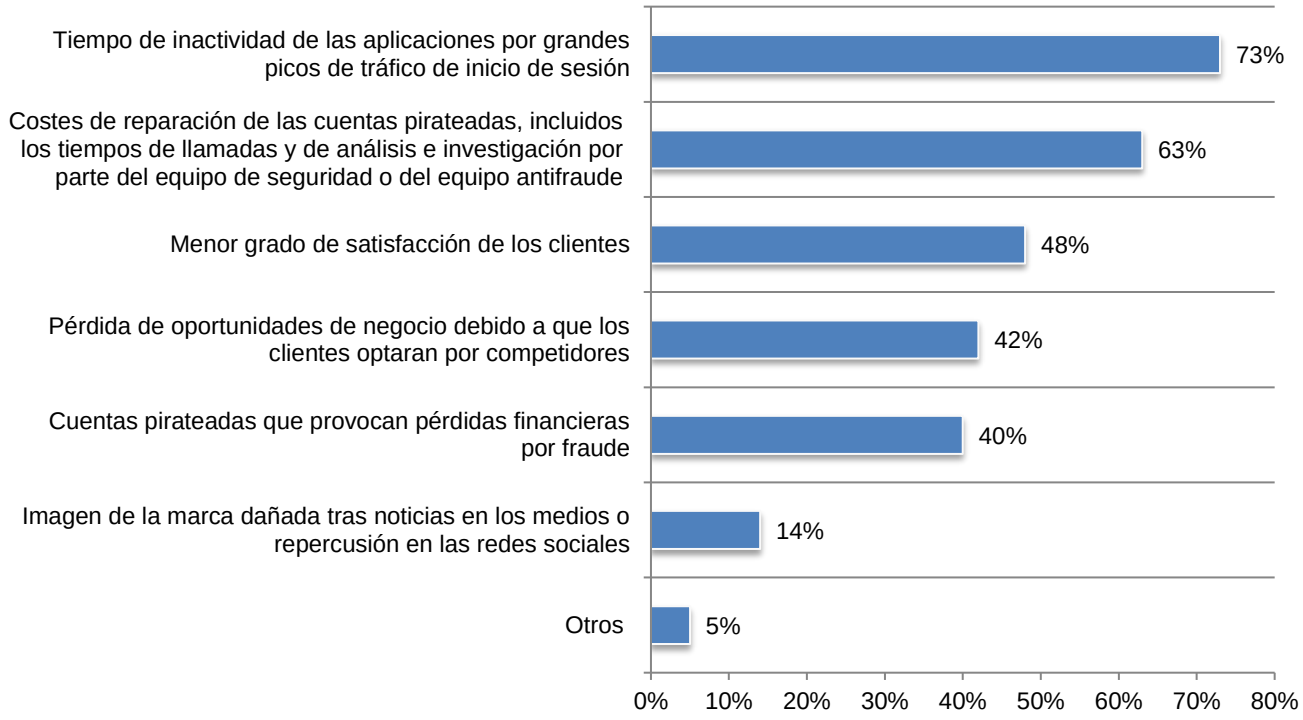
Las organizaciones no asignan suficiente presupuesto para abordar el problema. Como se muestra en la figura 12, solamente el 33 % de los encuestados coincide en que los presupuestos para seguridad de su compañía son suficientes para prevenir o contener los ataques de relleno de credenciales. El 23 % no lo tiene claro, y el 44 % no está de acuerdo con la afirmación o está completamente en desacuerdo.

Figura 12. El presupuesto de seguridad existente es suficiente para prevenir o contener los ataques de relleno de credenciales



Si bien las organizaciones podrían no estár asignando suficiente presupuesto para enfrentarse correctamente a los ataques de relleno de credenciales, los encuestados declaran que estas ofensivas tienen un impacto financiero importante en muchísimas áreas. En términos de frecuencia, la figura 13 muestra que las consecuencias negativas más comunes son el tiempo de inactividad de las aplicaciones (según el 73 % de los encuestados) y los costes derivados de la reparación de las cuentas pirateadas, incluidos los tiempos de llamadas y de análisis e investigación por parte del equipo de seguridad o del equipo antifraude (según el 63 % de los encuestados).

Figura 13. Consecuencias negativas resultantes de un ataque de relleno de credenciales
Se admite más de una respuesta.



El coste total anualizado de los ataques de relleno de credenciales, excluido el fraude, asciende a 3,9 millones de dólares. La tabla 1 presenta el coste que supone que un equipo de seguridad lidie con este tipo de ataque. La tabla 2 muestra el coste derivado de los tiempos de inactividad de las aplicaciones, y en la tabla 3 se desglosan los costes que supone el abandono de los clientes.

Tabla 1. Tiempo dedicado a la prevención y detección del relleno de credenciales, y a la reparación de los daños asociados	**Promedio de horas dedicadas a la semana**	**Coste semanal***
Enfoques de organización y planificación para detectar y contener el abuso de credenciales	69	3146 $
Análisis e investigación de posibles ataques de relleno de credenciales	136	6202 $
Realización de análisis forenses en cuentas con sospechas de pirateo mediante relleno de credenciales	71	3238 $
Documentación o presentación de informes sobre incidentes de relleno de credenciales	59	2690 $
Contención y reparación de ataques basados en credenciales	151	6886 $
Total semanal	486	22 162 $
Total anual	25 272	1 152 403 $

*En la región de EMEA, la tarifa salarial total horaria para los equipos de TI y de seguridad de TI es de 45,60 $ (fuente: Ponemon Institute).

Tabla 2. Coste del tiempo de inactividad	**Mensual**	**Anual**
Promedio de tiempo (en horas) al mes incurrido por todas las organizaciones	7,33	87,96
Coste medio por hora de tiempo de inactividad de la aplicación	13 842 $	13 842 $
Coste total al año	101 462 $	1 217 542 $

Tabla 3. Coste del abandono de clientes	**Pregunta de la encuesta**	**Cálculo**
A = Valor promedio del cliente	P24	1204 $
B = Porcentaje de clientes que abandonan a consecuencia de un ataque de relleno de credenciales	P23	8,63 %
C = Número promedio de las cuentas de usuario que suelen atacarse	P6	1041
D = Porcentaje de éxito de los ataques de relleno de credenciales	P7	10,97 %
E = Número medio de ataques de relleno de credenciales al mes	P4	10,96
F = (A x B x C x D x E)	Mensual	130 048 $
G = F x 12	Anual	1 560 581 $

Los tres componentes = Coste total anualizado de los ataques de relleno de credenciales, excluido el fraude	Total general	3 930 527 $

El coste monetario del fraude por ataques de relleno de credenciales oscila entre los 227 550 dólares y los 22,8 millones de dólares al año. El coste derivado del fraude puede ser a menudo difícil de predecir, ya que los atacantes que acometen las ofensivas de relleno de credenciales suelen ser intermediarios, que revenden las credenciales de las cuentas de usuario validadas a terceros que se apropian de ellas para efectuar transacciones fraudulentas. Por lo tanto, una cuenta pirateada no conduce necesariamente a una pérdida derivada del fraude.

El coste previsto dependerá de qué porcentaje de todas las cuentas pirateadas experimenta pérdidas monetarias a lo largo del año. Por lo tanto, si la tasa de fraude monetario es de un 1 %, el coste monetario total extrapolado para ese año sería de 227 550 dólares. Si esta tasa fuera del 100 %, es decir, si todas las cuentas pirateadas sufrieran pérdidas económicas, el coste monetario total del fraude sería de 22 754 954 dólares. Téngase en cuenta que estas cifras se basan en la empresa media del grupo analizado.

Tabla 4. Coste monetario del fraude	**Pregunta de la encuesta**	**Cálculo**
Frecuencia de ataques de relleno de credenciales detectados al mes	P4	10,96
Porcentaje de ataques de relleno de credenciales no detectados	P5	27,5 %
Frecuencia ajustada de ataques de relleno de credenciales al mes	11/(1 - P5)	15,17
Número de cuentas por ataque de relleno de credenciales	P6	1041
Porcentaje de ataques de relleno de credenciales con los que se identifican credenciales válidas	P7	10,97 %
Frecuencia de cuentas pirateadas al mes	15 x 1041 x 11 %	1732
Cantidad de dinero perdido al mes por fraude derivado de cuentas pirateadas	P9	1095 $
Cantidad de dinero perdido al año por fraude derivado de cuentas pirateadas	P9 x 12	13 140 $
Porcentaje de cuentas pirateadas que ocasionaron pérdidas económicas = 100 %	13 140 $ x 1732 x 100 %	22 754 954 $
Porcentaje de cuentas pirateadas que ocasionaron pérdidas económicas = 75 %	13 140 $ x 1732 x 75 %	17 066 215 $
Porcentaje de cuentas pirateadas que ocasionaron pérdidas económicas = 50 %	13 140 $ x 1732 x 50 %	11 377 477 $
Porcentaje de cuentas pirateadas que ocasionaron pérdidas económicas = 25 %	13 140 $ x 1732 x 25 %	5 688 738 $
Porcentaje de cuentas pirateadas que ocasionaron pérdidas económicas = 10 %	13 140 $ x 1732 x 10 %	2 275 495 $
Porcentaje de cuentas pirateadas que ocasionaron pérdidas económicas = 5 %	13 140 $ x 1732 x 5 %	1 137 748 $
Porcentaje de cuentas pirateadas que ocasionaron pérdidas económicas = 1 %	13 140 $ x 1732 x 1 %	227 550 $

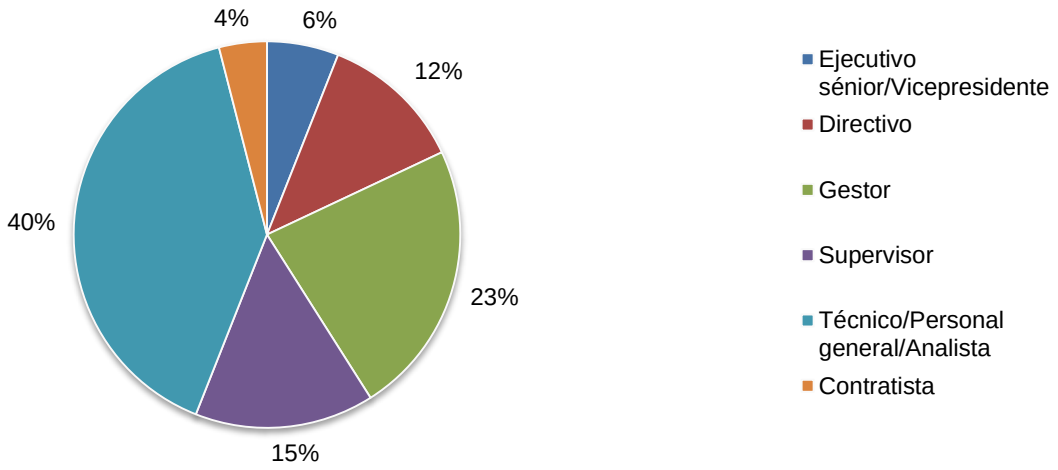
Parte 3. Metodología

En el estudio, se seleccionaron participantes de un marco de muestreo formado por 14 351 profesionales de seguridad de TI, residentes en la región de EMEA, que conocen los ataques de relleno de credenciales y que son responsables de la seguridad de los sitios web de sus empresas. La tabla 5 muestra que se rellenaron 603 encuestas en total. Tras el filtrado y los controles de fiabilidad, se eliminaron 59 encuestas. La muestra final consta de 544 encuestas, lo que quiere decir que se registró una tasa de respuesta del 3,8 %.

Tabla 5. Respuesta de la muestra	Frec.	%
Marco de muestreo	14 351	100,0 %
Respuestas totales	603	4,2 %
Encuestas rechazadas o descartadas	59	0,4 %
Muestra final	544	3,8 %

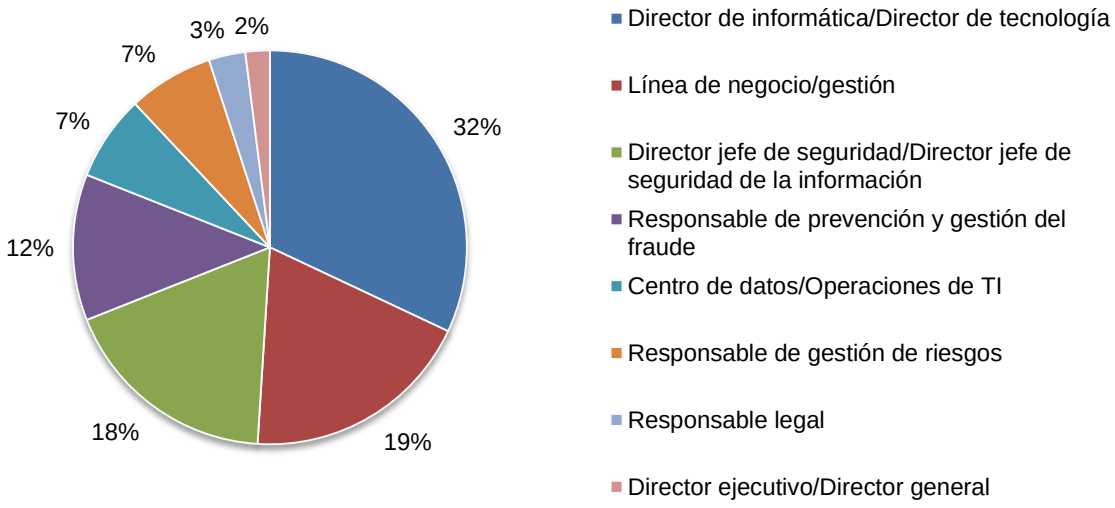
El gráfico circular 1 muestra el nivel profesional de los encuestados en sus respectivas empresas. De acuerdo con los fines y el diseño del estudio, algo más de la mitad de los encuestados (56 %) se sitúa en cargos de supervisión o superiores.

Gráfico circular 1. Nivel profesional dentro de la organización



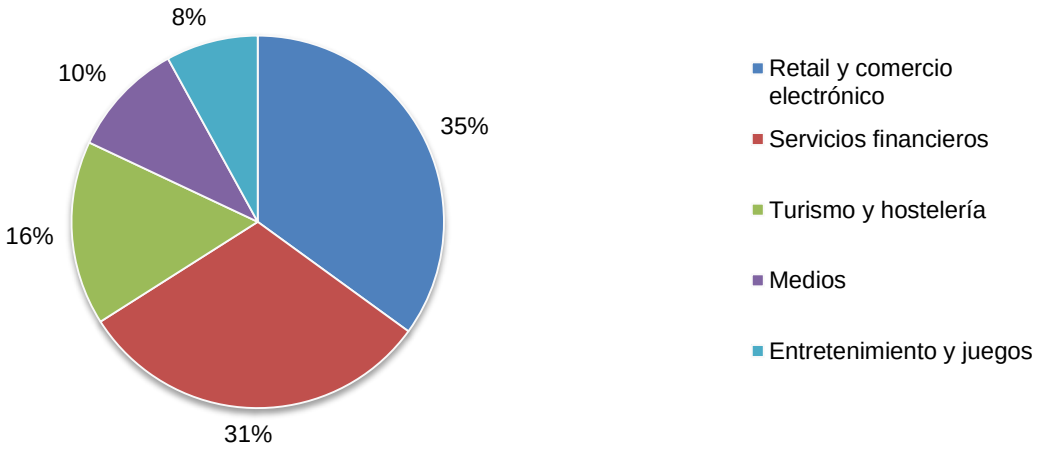
En el gráfico circular 2, podemos ver que el 32 % de los encuestados depende directamente del director de tecnología o informática de la empresa; el 19 %, de la línea de negocio o gestión; el 18 %, del director jefe de seguridad o de seguridad de la información; y el 12 %, del responsable de prevención de fraudes.

Gráfico circular 2. Responsables directos con respecto a los puestos de los encuestados en la organización



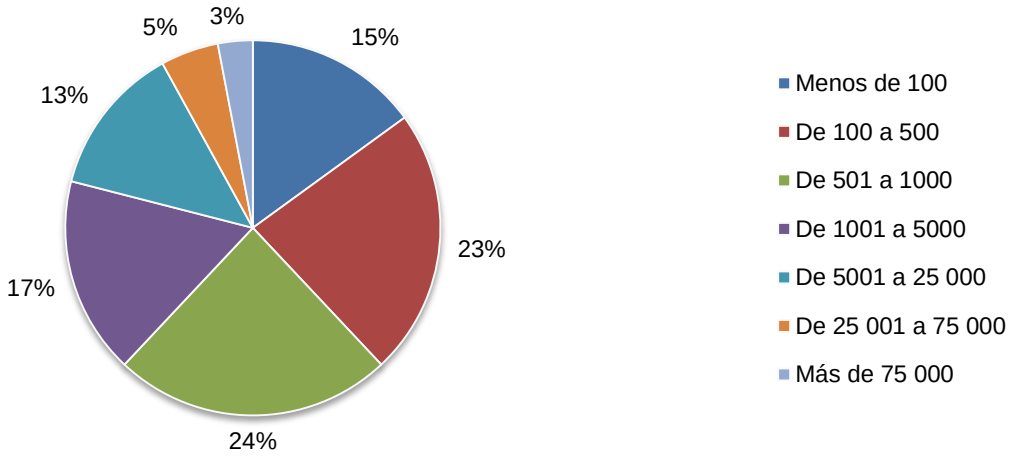
El gráfico circular 3 muestra los sectores de las organizaciones de los encuestados. En este gráfico, el retail y el comercio electrónico (35 %) y los servicios financieros (31 %) se posicionan como los mayores sectores encuestados. Entre las actividades de las organizaciones de servicios financieros se incluyen la banca, los seguros, la gestión de inversiones y el corretaje. El 16 % de los encuestados indicó el turismo y la hostelería como su principal sector, y el 10 %, los medios.

Gráfico circular 3. Principal sector de las organizaciones de los encuestados



Como ilustra el gráfico 4, el 62 % de los encuestados pertenece a organizaciones con una plantilla global de más de 500 empleados.

Gráfico circular 4. Total de empleados a nivel global de las organizaciones de los encuestados



Parte 4. Advertencias

Existen limitaciones inherentes a las investigaciones mediante el proceso de encuesta que conviene tener en cuenta antes de extraer conclusiones de los resultados. A continuación, se indican algunas limitaciones concretas que son relevantes en la mayoría de las encuestas por Internet.

Sesgo de no respuesta: los resultados actuales se basan en una muestra de respuestas. Enviamos las encuestas a una muestra representativa de personas, lo que dio lugar a un gran número de respuestas utilizables. A pesar de las pruebas de no respuesta, siempre es posible que las personas que no participaron en la encuesta tengan opiniones considerablemente distintas de las que sí la completaron.

Sesgo del marco de muestreo: la precisión se basa en la información de contacto y el grado en que la lista es representativa de individuos que son profesionales de la seguridad de TI familiarizados con ataques de relleno de credenciales y responsables de la seguridad del sitio web de su empresa. También reconocemos que los resultados pueden estar sesgados por componentes externos, como la cobertura de medios. Asimismo, reconocemos que existe un sesgo provocado por ofrecer una gratificación por completar la investigación en un plazo de tiempo determinado.

Resultados autoevaluados: la calidad de una investigación efectuada mediante el proceso de encuesta se fundamenta en la integridad de las respuestas recibidas. Aunque se pueden incorporar ciertos mecanismos de control y ponderación en el proceso, existe siempre la posibilidad de que una persona no proporcione respuestas absolutamente fieles.

Apéndice: Resultados detallados de la encuesta

Las tablas siguientes proporcionan la frecuencia o la frecuencia porcentual de las respuestas a todas las preguntas de la encuesta de este estudio. Todas las respuestas de la encuesta se recopilaron entre el 9 de julio de 2018 y el 23 de julio de 2018.

Respuesta a la encuesta	EMEA
Marco de muestreo total	14 351
Respuestas totales	603
Encuestas rechazadas	59
Total	544
Tasa de respuesta	3,8 %

Países de la región EMEA	Frec.
Reino Unido	81
Alemania	79
Francia	65
Italia	55
Países Bajos	45
España	44
Dinamarca	23
Suecia	14
Suiza	15
Israel	21
Turquía	37
Rusia	45
Egipto	20
Total	544

Parte 1. Preguntas de filtrado

F1. ¿Qué grado de familiarización tiene con los ataques de abuso de credenciales y de relleno de credenciales (según se define)?	EMEA
Muy familiarizado	27 %
Familiarizado	39 %
Algo familiarizado	34 %
No tengo ningún conocimiento (fin de la encuesta)	0 %
Total	100 %

F2. Aproximadamente, ¿qué porcentaje de los ingresos de su empresa (ventas brutas) procede de actividades relacionadas con su sitio web?	EMEA
Ninguno (fin de la encuesta)	0 %
1-10 %	11 %
11-20 %	13 %
21-30 %	21 %
31-40 %	16 %
41-50 %	8 %
51-60 %	3 %
61-70 %	3 %
71-80 %	4 %
81-90 %	5 %
91-100 % (prácticamente todas)	16 %
Total	100 %
Valor extrapolado	43 %

F3. ¿Tiene algún tipo de responsabilidad con respecto a la seguridad del tráfico del sitio web de su organización?	EMEA
Sí, plena responsabilidad	21 %
Sí, cierta responsabilidad	56 %
Sí, responsabilidad mínima	23 %
No, ninguna responsabilidad (fin de la encuesta)	0 %
Total	100 %

Parte 2. Atribuciones

P1. Califique cada una de las diez (10) declaraciones siguientes usando la escala de opinión que va desde “completamente de acuerdo” a “completamente en desacuerdo” proporcionada para cada elemento.	
P1a. El relleno de credenciales representa un importante desafío de seguridad para mi empresa.	EMEA
Completamente de acuerdo	25 %
De acuerdo	32 %
No estoy seguro/a	19 %
En desacuerdo	19 %
Completamente en desacuerdo	5 %
Total	100 %

P1b. La mayoría de los ataques de relleno de credenciales que se producen en los sitios web de mi empresa son fáciles de detectar y reparar.	EMEA
Completamente de acuerdo	17 %
De acuerdo	19 %
No estoy seguro/a	30 %
En desacuerdo	23 %
Completamente en desacuerdo	11 %
Total	100 %

P1c. Mi empresa tiene una buena visibilidad de los ataques de relleno de credenciales.	EMEA
Completamente de acuerdo	20 %
De acuerdo	15 %
No estoy seguro/a	24 %
En desacuerdo	32 %
Completamente en desacuerdo	9 %
Total	100 %

P1d. El tráfico de bots maliciosos aumenta debido a los ataques de relleno de credenciales.	EMEA
Completamente de acuerdo	39 %
De acuerdo	33 %
No estoy seguro/a	16 %
En desacuerdo	9 %
Completamente en desacuerdo	3 %
Total	100 %

P1e. El presupuesto de seguridad de mi empresa es suficiente para prevenir o contener los ataques de relleno de credenciales.	EMEA
Completamente de acuerdo	15 %
De acuerdo	18 %
No estoy seguro/a	23 %
En desacuerdo	30 %
Completamente en desacuerdo	14 %
Total	100 %

P1f. Mi empresa cuenta con soluciones o tecnologías suficientes para prevenir o contener los ataques de relleno de credenciales.	EMEA
Completamente de acuerdo	13 %
De acuerdo	20 %
No estoy seguro/a	24 %
En desacuerdo	29 %
Completamente en desacuerdo	14 %
Total	100 %

P1g. La migración a la nube de mi empresa ha aumentado el riesgo de ataques de relleno de credenciales.	EMEA
Completamente de acuerdo	26 %
De acuerdo	30 %
No estoy seguro/a	17 %
En desacuerdo	18 %
Completamente en desacuerdo	9 %
Total	100 %

P1h. La **frecuencia** de los ataques de relleno de credenciales sufridos por mi empresa está en aumento.	EMEA
Completamente de acuerdo	23 %
De acuerdo	30 %
No estoy seguro/a	25 %
En desacuerdo	17 %
Completamente en desacuerdo	5 %
Total	100 %

P1i. La **gravedad** de los ataques de relleno de credenciales sufridos por mi empresa está en aumento.	EMEA
Completamente de acuerdo	25 %
De acuerdo	30 %
No estoy seguro/a	23 %
En desacuerdo	17 %
Completamente en desacuerdo	5 %
Total	100 %

P1j. Prevenir los ataques de relleno de credenciales es difícil, ya que las correcciones que frenan a los delincuentes pueden influir negativamente en la experiencia web de los usuarios legítimos.	EMEA
Completamente de acuerdo	31 %
De acuerdo	39 %
No estoy seguro/a	17 %
En desacuerdo	10 %
Completamente en desacuerdo	3 %
Total	100 %

Parte 3. Antecedentes

P2. Aproximadamente, ¿cuántos sitios web orientados al cliente o consumidor tiene su empresa en fase de producción actualmente? Puede indicar valores aproximados.	EMEA
De 1 a 5	13 %
De 6 a 10	15 %
De 11 a 20	26 %
De 21 a 30	20 %
De 31 a 40	15 %
De 41 a 50	4 %
De 51 a 100	2 %
Más de 100	5 %
Total	100 %
Valor extrapolado	26,5

P3. ¿Qué tipos de clientes inician sesión en su sitio web? Marque todas las opciones que correspondan.	EMEA
Clientes que acceden desde un equipo de escritorio o portátil mediante un navegador web	87 %
Clientes que acceden desde un dispositivo móvil mediante un navegador web	65 %
Clientes que acceden desde un dispositivo móvil mediante la aplicación móvil de la empresa	36 %
Terceros (partners, agregadores, etc.)	40 %
Total	228 %

P4. En un mes habitual, ¿cuántos ataques de relleno de credenciales detecta su empresa? Puede indicar valores aproximados.	EMEA
Ninguno	0 %
De 1 a 5	41 %
De 6 a 10	41 %
De 11 a 20	9 %
De 21 a 50	6 %
De 51 a 100	2 %
Más de 100	1 %
Total	100 %
Valor extrapolado	10,96

P5. ¿Qué porcentaje de ataques de relleno de credenciales cree que no consigue detectar su empresa? Puede indicar valores aproximados.	EMEA
Ninguno	9 %
1-10 %	16 %
11-25 %	33 %
26-50 %	27 %
51-75 %	10 %
76-100 %	5 %
Total	100 %
Valor extrapolado	27,5 %

P6. ¿Cuántas cuentas de usuario suele atacar cada ofensiva de relleno de credenciales? Puede indicar valores aproximados.	EMEA
De 1 a 100	17 %
De 101 a 500	44 %
De 501 a 1000	25 %
De 1001 a 5000	9 %
De 5001 a 10 000	3 %
Más de 10 000	2 %
Total	100 %
Valor extrapolado	1041

P7. ¿Qué porcentaje de intentos de relleno de credenciales se completa con éxito (es decir, con la identificación de credenciales válidas)? Puede indicar valores aproximados.	EMEA
Ninguno	0 %
Menos del 1 %	1 %
1-2 %	7 %
3-4 %	10 %
5-6 %	15 %
7-8 %	26 %
9-10 %	13 %
11-20 %	5 %
Más del 20 %	23 %
Total	100 %
Valor extrapolado	10,97 %

P8. ¿Qué consecuencias negativas resultantes de un ataque de relleno de credenciales ha experimentado? Marque todas las opciones que correspondan.	EMEA
Tiempo de inactividad de las aplicaciones por grandes picos de tráfico de inicio de sesión	73 %
Cuentas pirateadas que provocan pérdidas financieras por fraude	40 %
Costes de reparación de las cuentas pirateadas, incluidos los tiempos de llamadas y de análisis e investigación por parte del equipo de seguridad o del equipo antifraude	63 %
Menor grado de satisfacción de los clientes	48 %
Pérdida de oportunidades de negocio debido a que los clientes optaran por competidores	42 %
Imagen de la marca dañada tras noticias en los medios o repercusión en las redes sociales	14 %
Otra consideración (especifique)	5 %
Total	285 %

Parte 4. Dinero perdido a causa del fraude

P9. Estime la cantidad de dinero que ha perdido por cada cuenta pirateada. Puede utilizar cualquier sistema métrico adecuado para su empresa, como el valor medio de pedidos, el saldo medio de cuentas o cuotas fijas perdidas.	EMEA
Menos de 100 $	33 %
De 100 a 500 $	30 %
De 501 a 1000 $	20 %
De 1001 a 5000 $	11 %
De 5001 a 10 000 $	5 %
Más de 10 000 $	1 %
Total	100 %
Valor extrapolado	1095 $

P10. En los últimos 12 meses, ¿qué porcentaje de los ingresos totales de la empresa (ventas brutas) se ha perdido debido a casos de fraude por Internet? Puede indicar valores aproximados.	EMEA
Ninguno	6 %
Menos del 1 %	9 %
1-2 %	19 %
3-4 %	23 %
5-6 %	18 %
7-8 %	9 %
9-10 %	6 %
Más del 10 %	10 %
Total	100 %
Valor extrapolado	4,5 %

P11. En los últimos 12 meses, ¿qué porcentaje del fraude por Internet que ha sufrido se ha debido a ataques de relleno de credenciales? Puede indicar valores aproximados.	EMEA
Ninguno	6 %
Menos del 5 %	10 %
5-10 %	20 %
11-25 %	30 %
26-50 %	19 %
51-75 %	9 %
76-100 %	6 %
Total	100 %
Valor extrapolado	25,2 %

Parte 5. Estimación del coste de la prevención del fraude

P12. En su organización, ¿cuántos miembros del personal de seguridad o antifraude participan en actividades relacionadas con la **detección y contención** de ataques de relleno de credenciales?	EMEA
Ninguno	5 %
Menos de 5	36 %
De 5 a 10	29 %
De 11 a 15	20 %
De 16 a 20	4 %
De 21 a 25	4 %
Más de 25	2 %
Total	100 %
Valor extrapolado	8,46

P13. En su opinión, ¿cómo ha cambiado en los últimos 12 meses el volumen o la frecuencia de los ataques de relleno de credenciales?	EMEA
Ha aumentado significativamente	20 %
Hay más	38 %
Permanece igual	30 %
Hay menos	11 %
Ha disminuido significativamente	1 %
Total	100 %

P14. En su opinión, ¿cómo ha cambiado en los últimos 12 meses la gravedad de los ataques de relleno de credenciales?	EMEA
Ha aumentado significativamente	19 %
Hay más	35 %
Permanece igual	35 %
Hay menos	8 %
Ha disminuido significativamente	3 %
Total	100 %

P15. Califique la efectividad de cada una de las seis soluciones y capacidades siguientes contra ataques de relleno de credenciales utilizando la escala de 10 puntos proporcionada debajo de cada elemento. Puede ignorar las preguntas que no sean aplicables.	
P15a. Identificación manual de ataques según los picos de intentos de inicio de sesión	EMEA
1 o 2	7 %
3 o 4	15 %
5 o 6	34 %
7 u 8	35 %
9 o 10	9 %
Total	100 %
Valor extrapolado	5,98

P15b. Bloqueo de atacantes individual por dirección IP	EMEA
1 o 2	4 %
3 o 4	15 %
5 o 6	34 %
7 u 8	22 %
9 o 10	25 %
Total	100 %
Valor extrapolado	6,48

P15c. Limitación de velocidad de direcciones IP individuales en función de la cantidad de intentos de inicio de sesión	EMEA
1 o 2	9 %
3 o 4	14 %
5 o 6	25 %
7 u 8	28 %
9 o 10	24 %
Total	100 %
Valor extrapolado	6,38

P15d. Uso de una solución de firewall de aplicaciones web (WAF)	EMEA
1 o 2	8 %
3 o 4	11 %
5 o 6	31 %
7 u 8	32 %
9 o 10	18 %
Total	100 %
Valor extrapolado	6,32

P15e. Uso de una solución específica de detección o mitigación de bots	EMEA
1 o 2	4 %
3 o 4	9 %
5 o 6	16 %
7 u 8	38 %
9 o 10	33 %
Total	100 %
Valor extrapolado	7,24

P15f. Uso de una solución de gestión de identidades para identificar las cuentas pirateadas	EMEA
1 o 2	3 %
3 o 4	11 %
5 o 6	19 %
7 u 8	32 %
9 o 10	35 %
Total	100 %
Valor extrapolado	7,20

P16. Aproximadamente, ¿cuántas horas a la semana se dedican a **organizar y planificar** las iniciativas de la organización para detectar y contener el abuso de credenciales? Estime las horas totales que dedican los equipos de TI y de operaciones de seguridad de TI (SecOps) y los equipos antifraude.	EMEA
Menos de 5	7 %
De 5 a 10	14 %
De 11 a 25	20 %
De 26 a 50	23 %
De 51 a 100	16 %
De 101 a 250	16 %
De 251 a 500	4 %
Más de 500	0 %
Total	100 %
Valor extrapolado	68,87

P17. Aproximadamente, ¿cuántas horas a la semana se dedican a **analizar e investigar posibles** ataques de relleno de credenciales? Estime las horas totales que dedican los equipos antifraude y de operaciones de seguridad de TI (SecOps).	EMEA
Menos de 5	0 %
De 5 a 10	0 %
De 11 a 25	19 %
De 26 a 50	21 %
De 51 a 100	23 %
De 101 a 250	20 %
De 251 a 500	12 %
Más de 500	5 %
Total	100 %
Valor extrapolado	136,47

P18. Aproximadamente, ¿cuántas horas a la semana se dedican a la realización de **análisis forenses** de las cuentas que se cree que han sufrido ataques de relleno de credenciales? Estime las horas totales que dedican los equipos antifraude y de operaciones de seguridad de TI (SecOps).	EMEA
Menos de 5	8 %
De 5 a 10	10 %
De 11 a 25	12 %
De 26 a 50	25 %
De 51 a 100	23 %
De 101 a 250	21 %
De 251 a 500	1 %
Más de 500	0 %
Total	100 %
Valor extrapolado	70,70

P19. Aproximadamente, ¿cuántas horas a la semana se dedican a la **documentación o presentación de informes** sobre incidentes de relleno de credenciales de conformidad con las directivas y los reglamentos de cumplimiento? Estime las horas totales que dedican los equipos antifraude y de operaciones de seguridad de TI (SecOps).	EMEA
Menos de 5	2 %
De 5 a 10	9 %
De 11 a 25	20 %
De 26 a 50	35 %
De 51 a 100	20 %
De 101 a 250	13 %
De 251 a 500	1 %
Más de 500	0 %
Total	100 %
Valor extrapolado	59,30

Parte 6. Estimación del coste de reparación por los daños sufridos en las cuentas pirateadas

P20. ¿Qué esfuerzos de reparación se llevan a cabo cuando se descubre que se ha pirateado una cuenta? Marque todas las opciones que correspondan.	EMEA
Enviar al propietario de la cuenta un correo electrónico de restablecimiento de contraseña	91 %
Llamar al propietario de la cuenta para explicarle la situación	15 %
Bloquear la cuenta	72 %
Investigar el historial de la cuenta para identificar fraudes no detectados anteriormente	51 %
Otra consideración (especifique)	3 %
Total	232 %

P21. Aproximadamente, ¿cuántas horas a la semana se dedican a **contener y reparar** los daños de ataques basados en credenciales? Estime las horas totales que dedican los equipos antifraude y de seguridad de TI (SecOps).	EMEA
Menos de 5	0 %
De 5 a 10	3 %
De 11 a 25	12 %
De 26 a 50	20 %
De 51 a 100	27 %
De 101 a 250	17 %
De 251 a 500	14 %
Más de 500	7 %
Total	100 %
Valor extrapolado	151,30

Parte 7. Estimación de otros costes derivados de los ataques de relleno de credenciales

P22a. En un mes habitual, ¿cuánto tiempo de inactividad de las aplicaciones sufre como consecuencia de ataques de relleno de credenciales? Marque su respuesta con respecto a todos los sitios web orientados al cliente (en conjunto).	EMEA
Ninguno	6 %
Menos de 1 hora	12 %
De 1 a 2 horas	14 %
De 3 a 5 horas	20 %
De 6 a 10	27 %
De 11 a 24 horas	16 %
Más de 24 horas	5 %
Total	100 %
Valor extrapolado (horas)	7,33

P22b. En promedio, ¿cuál es el coste total en el que incurre su organización por una (1) hora de tiempo de inactividad de aplicaciones debido a ataques de relleno de credenciales? Puede indicar valores aproximados.	EMEA
Menos de 100 $	0 %
De 100 a 500 $	9 %
De 501 a 1000 $	16 %
De 1001 a 5000 $	29 %
De 5001 a 10 000 $	23 %
De 10 001 a 50 000 $	16 %
De 50 001 a 100 000 $	4 %
Más de 100 000 $	3 %
Total	100 %
Valor extrapolado	13 842 $

P23. ¿Qué porcentaje de clientes abandona o se pasa a la competencia al saber que se han robado sus credenciales? Puede indicar valores aproximados.	EMEA
Ninguno	21 %
Menos del 5 %	32 %
5-10 %	25 %
11-20 %	17 %
21-50 %	2 %
51-75 %	2 %
76-100 %	1 %
Total	100 %
Valor extrapolado	8,63 %

P24. ¿Cuál es el valor promedio por cliente? Puede utilizar cualquier sistema métrico adecuado para su empresa, como el valor medio de pedidos, el saldo medio de cuentas o cuotas fijas perdidas. Puede indicar valores aproximados.	EMEA
Menos de 100 $	26 %
De 101 a 500 $	26 %
De 501 a 1000 $	27 %
De 1001 a 5000 $	15 %
De 5001 a 10 000 $	6 %
Más de 10 000 $	0 %
Total	100 %
Valor extrapolado	1204 $

Parte 8. Otras preguntas

P25a. En su opinión, ¿qué nivel de dificultad entraña la **detección** de los ataques de relleno de credenciales?	EMEA
Muy difícil	31 %
Difícil	26 %
Algo difícil	23 %
Nada difícil	10 %
Fácil	10 %
Total	100 %

P25b. En su opinión, ¿qué nivel de dificultad entraña la **corrección o reparación** de los ataques de relleno de credenciales?	EMEA
Muy difícil	28 %
Difícil	33 %
Algo difícil	21 %
Nada difícil	14 %
Fácil	4 %
Total	100 %

P25c. En su opinión, ¿qué nivel de dificultad entraña distinguir a los empleados, clientes y usuarios “reales” de los impostores que acceden a su sitio web con credenciales robadas?	EMEA
Muy difícil	28 %
Difícil	30 %
Algo difícil	30 %
Nada difícil	9 %
Fácil	3 %
Total	100 %

P26. ¿Quiénes son los **máximos responsables** de limitar los ataques de relleno de credenciales en los sitios web de la empresa? Seleccione un máximo de dos opciones.	EMEA
Director ejecutivo/Director general	3 %
Director de informática/Director de tecnología	29 %
Director jefe de seguridad/Director jefe de seguridad de la información	18 %
Responsable legal	0 %
Departamento de cumplimiento o auditoría	3 %
Centro de datos/Operaciones de TI	8 %
Prevención y gestión de fraudes	18 %
Responsable de gestión de riesgos	13 %
Línea de negocio/gestión	22 %
Ninguna función tiene la responsabilidad general	37 %
Proveedor de servicio de alojamiento web	14 %
Otra consideración (especifique)	2 %
Total	167 %

Parte 9. Su función y organización

D1. ¿Qué nivel describe mejor su puesto actual dentro de la empresa?	EMEA
Ejecutivo sénior/Vicepresidente	6 %
Directivo	12 %
Gestor	23 %
Supervisor	15 %
Técnico/Personal general/Analista	40 %
Contratista	4 %
Otros	0 %
Total	100 %

D2. Marque quién es su responsable directo o el de su jefe en la organización.	EMEA
Director ejecutivo/Director general	2 %
Director de informática/Director de tecnología	32 %
Director jefe de seguridad/Director jefe de seguridad de la información	18 %
Centro de datos/Operaciones de TI	7 %
Responsable de cumplimiento o auditoría	0 %
Responsable de prevención y gestión del fraude	12 %
Responsable legal	3 %
Responsable de gestión de riesgos	7 %
Línea de negocio/gestión	19 %
Total	100 %

D3. ¿Qué sector describe mejor la actividad de su empresa?	EMEA
Entretenimiento y juegos	8 %
Servicios financieros	31 %
Medios	10 %
Retail y comercio electrónico	35 %
Turismo y hostelería	16 %
Otros	0 %
Total	100 %

D4. ¿Cuántos empleados tiene su empresa en todo el mundo?	EMEA
Menos de 100	15 %
De 100 a 500	23 %
De 501 a 1000	24 %
De 1001 a 5000	17 %
De 5001 a 25 000	13 %
De 25 001 a 75 000	5 %
Más de 75 000	3 %
Total	100 %

Póngase en contacto con research@ponemon.org o llámenos al 800.887.3118 si tiene alguna pregunta.

Ponemon Institute

Impulsando una gestión responsable de la información

Ponemon Institute se dedica a la investigación independiente y a la educación, fomentando prácticas de gestión responsable de la información y de la privacidad a escala empresarial y gubernamental. Nuestra misión se centra en la producción de estudios empíricos de gran calidad sobre los principales problemas que afectan a la gestión y seguridad de la información confidencial sobre personas y empresas.

Como miembro del **Consejo de Organizaciones Estadounidenses de Investigación por Encuestas (CASRO)**, defendemos unas normas estrictas de confidencialidad de los datos, privacidad e investigación ética. No recopilamos información identificable de personas (o información identificable de empresas en nuestra investigación empresarial). Asimismo, seguimos unas estrictas normas de calidad para garantizar que no se hagan preguntas superfluas, irrelevantes o inadecuadas.