Auditoría de confianza en línea y cuadro de honor 2018

Reconocimiento a la excelencia en seguridad, protección al consumidor y prácticas responsables de privacidad.

OTA
Online Trust Alliance
an **Internet Society** initiative

ÍNDICE

Resumen y contexto

Esta auditoría de confianza en línea y cuadro de honor 2018, que toma una instantánea de la adopción de mejores prácticas a finales de 2018, representa el décimo año en que la Online Trust Alliance (OTA) ha llevado a cabo una investigación de referencia para promover las mejores prácticas de seguridad, protección de datos y prácticas responsables de privacidad. Los objetivos principales de este trabajo incluyen elevar el nivel de seguridad y privacidad de los datos y reconocer a las organizaciones que han demostrado excelencia en estos temas. Además del cuadro de honor (Anexo D), esta auditoría incluye una lista de los "Mejores", en la que figuran las 50 mejores organizaciones según la puntuación total obtenida (Anexo C).

Las noticias que recientemente ocuparon los titulares sobre la vulneración de correos electrónicos empresariales (se extrajeron 123 millones de dólares de Facebook y Google), violaciones masivas de datos (383 millones de registros de Marriott) y el tratamiento cuestionable de los datos de los usuarios (varias revelaciones vinculadas con Facebook), así como la entrada en vigor del Reglamento General de Protección de Datos de la Unión Europea (RGPD), refuerzan la necesidad de que las organizaciones adopten las mejores prácticas en todos los ámbitos: seguridad del correo electrónico, seguridad del sitio y prácticas de privacidad. La Encuesta Global sobre Seguridad y Confianza en Internet que CIGI-Ipsos realizó en 2018 describe que la situación de la confianza en línea es desoladora. Más de la mitad de los encuestados se muestran más preocupados por la privacidad que el año anterior y la mayoría desconfía en gran medida de las plataformas de redes sociales, los motores de búsqueda y las empresas de tecnología de Internet.[1][2][3][4][5]

En muchas áreas, las prácticas comerciales están dejando de alinearse con las expectativas de los consumidores. Si esta situación se mantiene, la desconfianza en la privacidad y la seguridad que ofrecen las organizaciones podría tener efectos escalofriantes. Para que la economía de Internet prospere, los usuarios deben poder confiar en que su información personal estará segura, que se respetarán sus preferencias y que se protegerá su privacidad.

Las recomendaciones de la OTA y las mejores prácticas evaluadas en esta auditoría no solo son relevantes para el correo electrónico, los sitios web y las aplicaciones móviles, sino también a la cada vez mayor oferta del Internet de las cosas (IoT, Internet of Things). Además de esta auditoría, los fabricantes de IoT deberían consultar las recomendaciones que el marco de confianza para IoT de OTA hace específicamente para las ofertas de IoT.[6]La auditoría de 2018 se ha mejorado en varias áreas: subsectores adicionales, un nuevo sector importante (atención médica) y criterios ampliados en cada categoría principal, que ahora contemplan más de 100 atributos de datos (Anexo B). De esta forma, se ofrece una visión más completa de la confianza en línea en una mayor variedad de organizaciones competentes. Se han añadido nuevos criterios y se ha actualizado la ponderación para reflejar la evolución del panorama de amenazas, el entorno normativo y las prácticas aceptadas a nivel mundial. Además, se recogieron principios de alto nivel relacionados con el RGPD para crear un punto de referencia para futuras auditorías. Para ayudar a las organizaciones, este informe incluye una lista de verificación de las mejores prácticas (Anexo E) y recursos de implementación (Anexo F).

Es importante señalar que la auditoría se limita a un período de tiempo. Debido a la naturaleza dinámica del sitio web y las configuraciones de las aplicaciones, es posible que las puntuaciones de las organizaciones hayan cambiado desde que se completó la auditoría. Todo el análisis se realizó sin la participación activa de los sitios analizados. Los sitios se seleccionaron en base a su clasificación dentro de sus sectores particulares o listas públicas (o afiliación institucional en Internet Society). En los casos en que se identificó una vulnerabilidad significativa, la OTA siguió las prácticas de divulgación de información concertadas e intentó ponerse en contacto con la entidad "en riesgo" para darle la oportunidad de remediar el problema observado y ser revisada antes de la publicación de este informe.

Resumen ejecutivo y aspectos destacados

La auditoría de confianza en línea y cuadro de honor 2018 evalúa cerca de 1200 organizaciones, examinando prácticas de protección de privacidad, seguridad y protección al consumidor.[7]Las mejoras de la auditoría incluyen la adición de nuevos subsectores en los sectores de Noticias/Medios y Consumidores (noticias deportivas, transmisión de video y servicios de pago), así como un nuevo sector: Atención médica. Este sector incluye a las principales compañías de seguros médicos, farmacias, laboratorios de análisis y cadenas hospitalarias. Los sectores examinados y las organizaciones líderes asociadas incluyen:

"Nos complace ver que, conforme avanza el tiempo, cada vez más organizaciones cumplen con los criterios del cuadro de honor de Online Trust Alliance, aceptando el reto de atender la creciente demanda de la sociedad por una Internet más segura". Neil Daswani, vicepresidente superior, director de seguridad de la información del consumidor, Norton LifeLock

- 500 principales empresas de venta minorista de Internet 2018 (IR 100 e IR 500)[8]
- 100 principales bancos de la reserva federal (Bancos 100)[9]
- 100 principales organizaciones del gobierno federal de EE. UU. (Federal 100)
- 100 principales empresas de servicios al consumidor (Consumidores 100)[10]
- 100 principales organizaciones de noticias y medios de comunicación (Noticias 100)
- 100 principales operadores, proveedores de servicios de Internet (ISP) y proveedores de servicios de hospedaje (ISP/Hosts 100)
- 100 principales organizaciones de atención médica (Salud 100)
- Organizaciones afiliadas a OTA, Internet Society (OTA)[11]

Aunque la mayoría de los segmentos siguen siendo los mismos, la lista de organizaciones auditadas cada año cambia en función de su clasificación de ingresos/tráfico y consolidación en el mercado. Este año, gracias a la incorporación del sector de atención médica y las adiciones o cambios en las organizaciones de las listas clasificadas, para aproximadamente el 30 % de las organizaciones esta es su primera auditoría.

Al igual que en años anteriores, se pueden obtener 100 puntos básicos en cada una de las tres categorías principales de evaluación (protección al consumidor, seguridad del sitio y privacidad). Se suman puntos de bonificación para las mejores prácticas emergentes y se restan puntos de penalización por violaciones de datos, acuerdos judiciales y vulnerabilidades detectadas. Se requiere una puntuación

mínima de 60 en cada una de las tres categorías. Los puntos de bonificación se limitan a un máximo del 20% de la puntuación básica. Los sitios califican para el cuadro de honor al alcanzar una puntuación global de 80 % o superior, siempre que no hayan presentado deficiencias en ninguna de las tres categorías principales.

El año 2018 ha alcanzado cifras récord: el 70 % de las organizaciones han conseguido figurar en el cuadro de honor (el récord anterior fue de 52 % en la auditoría de 2017). Dado que la metodología se renovó para aumentar el nivel de exigencia en las tres categorías de evaluación, este logro es impresionante. Las puntuaciones de los antiguos socios de la OTA no han sido incluidas en los resultados (salvo las puntuaciones máximas generales), ya que sesgarían los resultados (el 98 % logró ubicarse en el cuadro de honor).

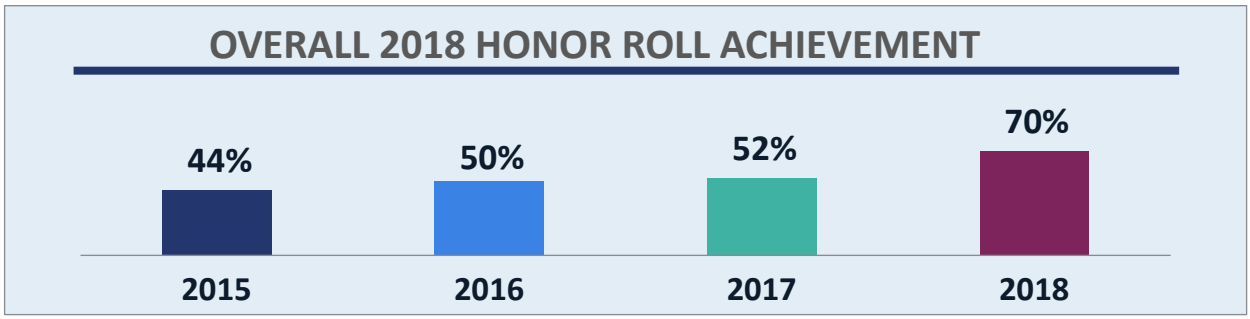


Gráfico 1. Porcentaje general que logró figurar en el cuadro de honor por año, 2015-2018

Como se ilustra en el gráfico 2, el porcentaje de organizaciones que logró ubicarse en el cuadro de honor aumentó en todos los sectores, a pesar de que los criterios de calificación fueron más estrictos en la auditoría de este año.[12] El grupo Federal 100 superó a todos los sectores con un porcentaje del 91 %, sobrepasando a Consumidores 100, que ha sido el sector líder por seis años consecutivos. Las entidades del gobierno federal de EE. UU. también mejoraron en gran medida, seguidas de cerca por Bancos 100 y Noticias 100. En el nuevo sector de Atención médica, solo el 57 % de las organizaciones llegaron al cuadro de honor, ubicándose por debajo de los demás sectores.

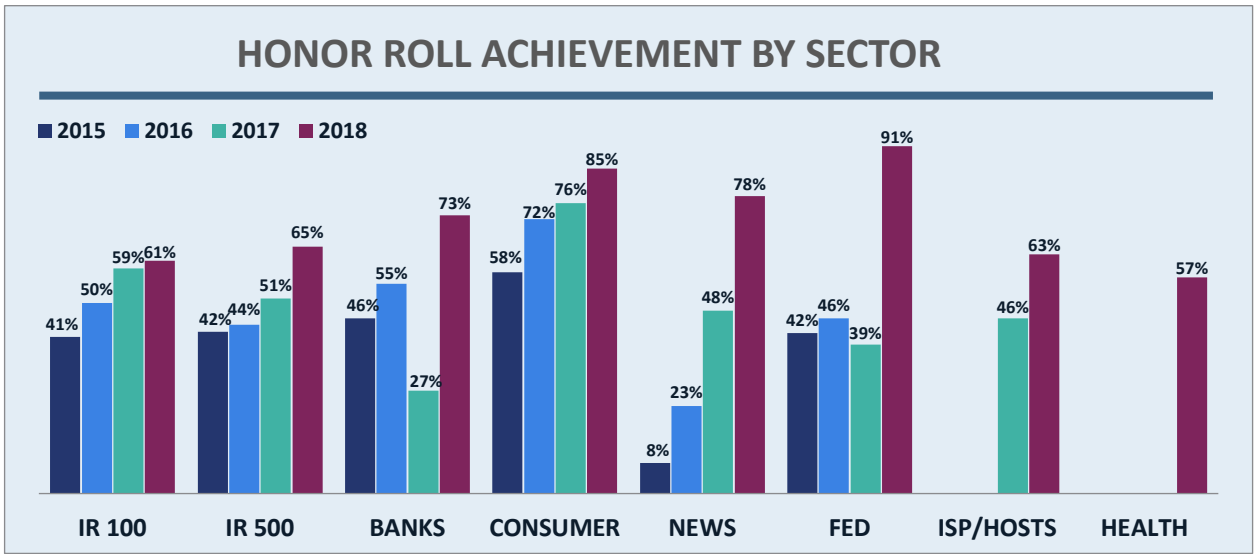


Gráfico 2. Porcentaje que logró figurar en el cuadro de honor por sector, 2015-2018.

Como en años anteriores, los resultados fueron casi bimodales, donde la mayoría de los sitios calificaron para el cuadro de honor o fallaron en una o más áreas. Como se ilustra en el gráfico 3, solo el 3 % del total no falló ni calificó para el cuadro de honor. Este valor oscila entre 0 y 7 % en los sectores individuales.

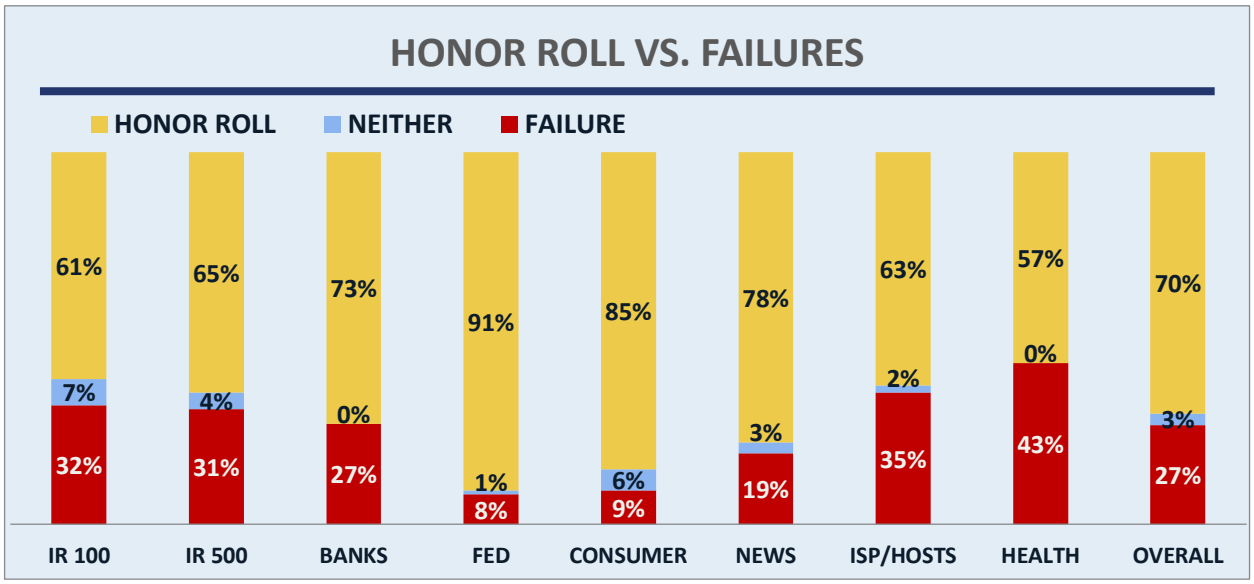


Gráfico 3. Distribución del cuadro de honor frente a quienes no lograron entrar en el mismo por sector.

En la auditoría de 2017 se creó una categoría de los "Mejores", en la que figuran los 50 mejores puntajes generales. Este año, todos los sectores están representados en los 50 Mejores, como se muestra en la siguiente tabla (tenga en cuenta que debido a que varias organizaciones pertenecen a diversos sectores, el total es mayor de 100 %). El mayor cambio en los 50 Mejores se produjo en el sector federal, que se duplicó del 12 % en 2017 al 26 % este año. El sector bancario, que no tuvo presencia en 2017, consiguió tener a tres organizaciones en los 50 Mejores este año. Puede encontrar el listado completo de las 50 mejores organizaciones en el Anexo C.

RENDIMIENTO DE CADA SECTOR EN LOS 50 MEJORES

Código	Sector	% de los 50 Mejores
C	Servicios al consumidor	40 %
F	Gobierno federal de EE. UU.	26 %
R	Minoristas de Internet	14 %
O	Miembros de OTA (Internet Society)	12 %
B	Bancos	6 %
H	Atención médica	4 %
I	Operadores, proveedores de servicios de Internet (ISP) y proveedores de servicio de hospedaje	4 %
N	Noticias/Medios	4 %

Gráfico 4. Rendimiento de los 50 Mejores por sector.

Google News obtuvo la máxima puntuación global en la auditoría, que también fue la máxima puntuación en el sector de Noticias/Medios. Otros ganadores de cada sector fueron 23andMe (Atención

médica), Agencia Federal para Manejo de Emergencias (FEMA, Federal Emergency Management Agency; Gobierno federal de EE. UU.), First National Bank of Omaha (Bancos), Google Cloud (ISP/Hosts), Google Play (Minoristas de Internet), Online Trust Alliance (miembros de OTA Internet Society) y PayPal (Consumidores).

Los resultados generales en cuanto a quienes fallaron, como se muestra en el gráfico 5, indican que la privacidad fue la causa más recurrente de fallas en todos los sectores con un 15 %, seguida de la protección al consumidor con un 13 % y la seguridad del sitio con solo un 3 %.Las fallas en la categoría de protección al consumidor se redujeron drásticamente en comparación con el 33 % de 2017. Esto se debió principalmente a la mayor adopción del mecanismo de autenticación de correo electrónico DomainKeys Identified Mail (DKIM). Las fallas variaron ampliamente por sector (gráfico 6). En general, el 27 % de los sitios fallaron en una o más áreas (una disminución en comparación con el 47 % en 2017). Las causas más recurrentes de fallas fueron la falta de autenticación de correo electrónico en los sectores de Atención médica e ISP/Hosts, seguida de las declaraciones de privacidad inadecuadas en los sectores de Minoristas de Internet e ISP/Hosts. Por otro lado, los sectores Federal y de Noticias no tuvieron fallas en la seguridad del sitio, y los sectores Federal y Consumidores llevaron la delantera en materia de privacidad, con solo un 2 % de fallas.

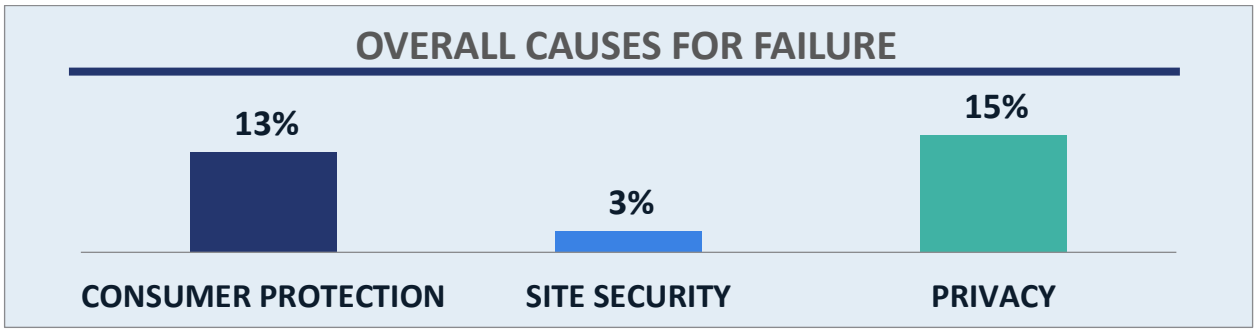


Gráfico 5. Causas de fallas por categoría de la auditoría.

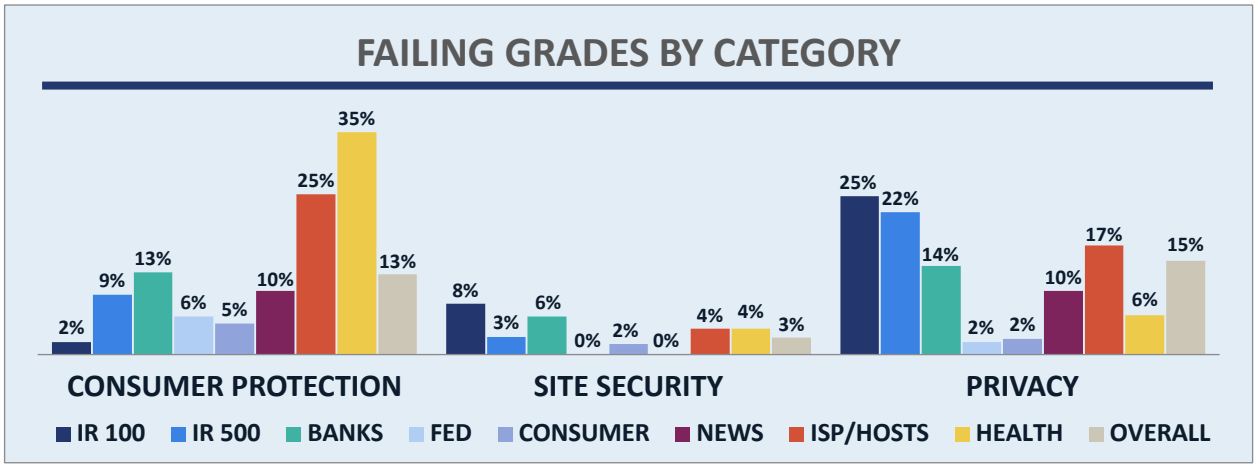


Gráfico 6. Porcentaje de empresas que no pasaron la auditoría por sector y categoría.

Se puede obtener información adicional normalizando los 300 puntos básicos a una escala de 100 puntos (denominada "Índice de confianza en línea") y comparando los índices alto, bajo y medio de los sectores. Durante varios años, el valor medio en la mayoría de los sectores rondaba el umbral del 80 %

del cuadro de honor, lo que significa que muchas organizaciones estaban "en la burbuja" del logro del cuadro de honor. El gráfico 7 muestra que este año el valor medio para todos los sectores está por encima del umbral del 80 %, y en muchos casos supera el 90 %.

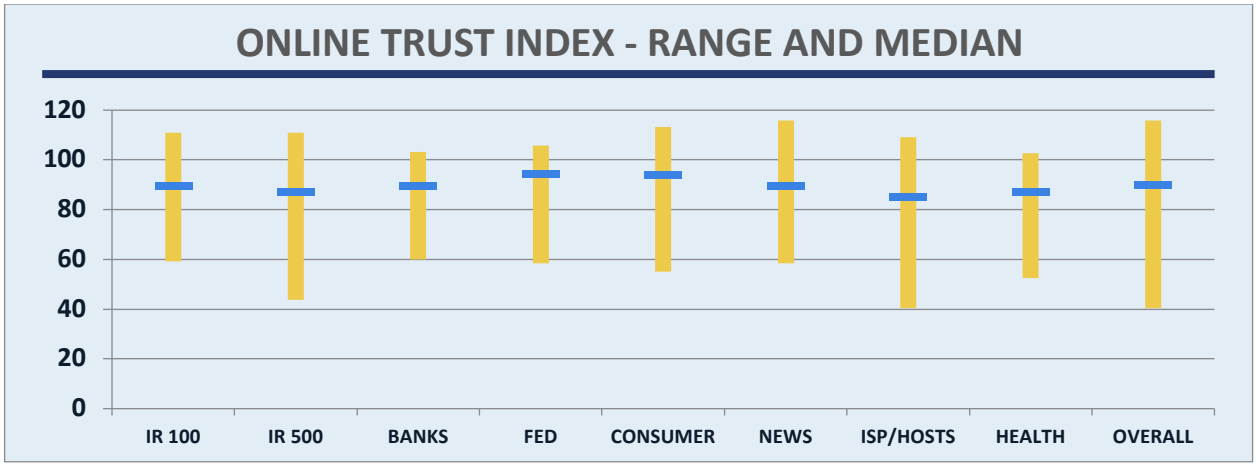


Gráfico 7. Rango y valor medio de los puntajes del índice de confianza en línea por sector.

Aspectos destacados de las mejores prácticas

A continuación se presenta un resumen de las mejores prácticas auditadas recomendadas por la OTA. Se proporcionan detalles adicionales en las secciones respectivas: 1) Dominio, marca y protección al consumidor; 2) Seguridad del sitio, el servidor y la infraestructura, y 3) Privacidad, transparencia y declaraciones.

Protección al consumidor

Autenticación de correo electrónico. La metodología se actualizó en 2017 para garantizar que los registros del Marco de directivas de remitente (SPF, Sender Policy Framework) y la Autenticación de mensajes, informes y conformidad basada en dominios (DMARC) cumplieran con las especificaciones publicadas. Los registros que mostraron falta de cumplimiento recibieron un puntaje parcial o fueron descalificados por completo. El 3 % de todas las organizaciones tenía un registro de SPF inválido y el 13 % tenía errores que provocaron que recibieran un puntaje parcial. De igual manera, el 2 % de los registros de DMARC se consideraron inválidos. Esto subraya la necesidad de que los sitios monitoreen constantemente sus registros para maximizar la protección de la marca y de los consumidores. De no hacerlo, las marcas pueden tener una falsa sensación de seguridad porque algunos proveedores de servicios de Internet y redes receptoras pueden pasar por alto dichos registros "inválidos".

- En general, el uso de la autenticación de correo electrónico ha alcanzado niveles récord. La adopción del SPF en el dominio de primer nivel aumentó del 77 al 89 %, mientras que la adopción de DKIM en el dominio de primer nivel creció más drásticamente, del 56 al 83 %.
- El uso de los registros de DMARC creció del 34 al 50 %.El estándar DMARC se usa junto con registros SPF y firmas digitales DKIM para defenderse de correos electrónicos con remitentes falsos que se usan en los ataques de vulneración de correos electrónicos empresariales y de suplantación de identidad tipo "spear phishing".
- La adopción de registros de rechazo o cuarentena de DMARC en el dominio de primer nivel creció del 15 al 24 %.Esta política de "aplicación" le indica a los receptores de correo electrónico bloquear o poner en cuarentena los mensajes que fallen la autenticación para proteger a los consumidores de correos fraudulentos.

TLS oportunista. Encripta los mensajes entre servidores de correo. Su adopción continuó creciendo del 65 al 73 %.(Puntos de bonificación)

Extensiones de seguridad del sistema de nombres de dominio (DNSSEC). La adopción se redujo ligeramente, del 12 al 10 %. Esto puede atribuirse a los cambios en las listas de los sectores. (Puntos de bonificación)

IPv6. La adopción se redujo ligeramente, del 14 al 12 %, principalmente a causa de los criterios más estrictos (los sitios web tenían que ser accesibles a través de IPv6; en años anteriores, solo el servicio de nombres debía ser compatible con IPv6). A pesar de la mayor exigencia, la adopción creció en algunos sectores (Bancos del 0 al 6 %, Consumidores del 12 al 15 %, y Minoristas de Internet del 5 al 7 %). (Puntos de bonificación)

Seguridad del sitio

Seguridad de transporte estricta de HTTP (HSTS), Always on SSL o HTTPS Everywhere. Este elemento se convirtió en parte de la puntuación básica este año (previamente aseguraba puntos de bonificación). La adopción dio otro gran salto, llegando al 93 % (en comparación con el 30 % en 2016 y 52 % en 2017). El crecimiento se atribuye al mayor interés generado por el cifrado en línea como la "norma" en la comunicación por Internet debido al temor de que terceros y el gobierno estén monitoreando las actividades en la red. En auditorías anteriores, el 99 % de los sitios admitían sistemas de cifrado, pero a menudo solo se aplicaba a las páginas de inicio de sesión o de transacciones financieras en lugar de a toda la sesión web.

Puntuaciones globales de seguridad del sitio. Las puntuaciones globales cayeron ligeramente del 91 al 89 (sobre 100) debido al aumento en la ponderación de la reputación de la dirección IP, los parches de software y las puntuaciones de seguridad de los encabezados de los sitios web. Varios sitios aún no establecen una política de seguridad de contenidos ni tampoco configuran encabezados de seguridad web para limitar la exposición a las vulnerabilidades que introducen las cookies y otros contenidos de terceros. La mayor parte de la puntuación de seguridad del sitio sigue vinculada a la configuración SSL/TLS, y en realidad las puntuaciones mejoraron un 2 % en este aspecto, dado que más sitios están usando configuraciones adecuadas de protocolos y conjuntos de cifrado. Aquellos sitios con puntuaciones desaprobatorias tuvieron los mismos problemas observados en años anteriores: conjuntos de cifrado débiles o inseguros, use de protocolos inseguros y cadenas de certificados incompletas que los hacían vulnerables a amenazas, como el ataque ROBOT. Los bancos tuvieron el mayor índice de fallas (6 %). El uso de nuevos protocolos TLS siguió evolucionando: el 29 % de los sitios no admite versiones anteriores al protocolo TLS 1.2 y el 7 % ya admite la versión TLS 1.3, que fue publicada oficialmente por el Grupo de trabajo de ingeniería de Internet (IETF) en agosto de 2018.[13]

"Esta es la auditoría de OTA más extensa hasta la fecha y hemos visto un aumento récord en la adopción de prácticas clave, como la autenticación de correo electrónico y el cifrado de un extremo a otro", dijo Olaf Kolkman, director de tecnología de Internet, Internet Society. "Esto es alentador y esperamos que motive a todas las organizaciones a hacer lo mismo. Las prácticas que auditamos hacen posible que los consumidores confíen y aumentan la confianza, no solo en una organización individual, sino en la Internet en su conjunto".

Autorización de la Autoridad de Certificación (CAA, Certificate Authority Authorization). Permite a los sitios publicar una lista de autoridades de certificación autorizadas a emitir certificados para su dominio, limitando así el abuso. Este punto se añadió a la auditoría de 2018 porque el Foro de navegador/autoridad de certificación (CA/B) ordenó que las autoridades de certificación debían comprobar la existencia de CAA antes de emitir o renovar certificados a partir de septiembre de 2017. Desafortunadamente, solo el 6 % de los sitios está aprovechando esta capacidad, principalmente en los sectores de Consumidores (20 %) e ISP/Hosts (13 %). La adopción en todos los demás sectores es inferior al 6 %. (Puntos de bonificación)

Programas/mecanismos de divulgación de vulnerabilidades. Esto fue añadido en 2017 y es reconocido como una mejor práctica por la Administración Nacional de Telecomunicaciones e Información (NTIA), el Instituto Nacional de Estándares y Tecnología (NIST), la Comisión Federal de Comercio (FTC) y la OTA. La adopción creció del 6 al 11 % en los sitios que tenían mecanismos de informes visibles en el sitio o que ofrecían recompensas a terceros por encontrar fallas. El sector de Consumidores superó a todos los demás con un 43 % de adopción, seguido de ISP/Hosts con un 25 %, Noticias/Medios con un 9 % y

Bancos con un 6 %.Contar con tales mecanismos es fundamental para responder eficazmente a los informes de los usuarios e investigadores externos y es relativamente sencillo de implementar. (Puntos de bonificación)

Vulnerabilidades de scripts de sitios (XSS, Cross Site Scripting). Después de aumentar del 27 % en 2016 al 50 % en 2017, la presencia de vulnerabilidades XSS cayó significativamente al 21 % en esta auditoría. Los sitios de Noticias tuvieron el porcentaje más alto (43 %), mientras que los Bancos tuvieron el más bajo (5 %). Varios sectores se acercaron al promedio general en el rango del 21 al 23 %.

Tendencias de privacidad

Las puntuaciones combinadas (declaración de privacidad y uso de rastreadores de terceros) cayeron este año, de 73 a 70, debido principalmente a la calificación más estricta de algunos de los criterios clave de declaración de privacidad.

Declaración de privacidad. En general, las puntuaciones por declaración de privacidad cayeron de 31 en 2017 a 27 en 2018. Se observaron cambios importantes en el texto sobre retención de datos (una caída del 49 al 2 % porque ahora el RGPD exige indicar un tiempo de retención específico), la presentación de información en capas (creció del 29 al 47 %) y el sometimiento de los proveedores externos a las mismas prácticas de privacidad que la organización (creció del 48 al 57 %). Además, el criterio de intercambio de datos se dividió en dos partes: lenguaje básico (p. ej., "no compartimos datos salvo con terceros que entregan el servicio"; el 67 % tiene una declaración de este tipo, un incremento ligero en comparación del 63 % en 2017) y un lenguaje de "afiliados" (p. ej., "no compartimos con afiliados ni con otros terceros"; solo el 20 % tiene esta restricción). Esto significa que el 80 % comparte o podría compartir datos con terceros. La preocupación relacionada con la excepción del intercambio de datos con afiliados es que a menudo permite el uso de marketing dirigido y otras actividades que el usuario puede no esperar.

Por primera vez en esta auditoría, se tomó en cuenta el sello con la fecha de la declaración de privacidad, dado que era un dato de interés ya que el RGPD entró en vigor en mayo de 2018. En general, el 31 % de los sitios no tenía sello con la fecha, el 11 % tenía una fecha anterior a 2017, el 11 % tenía una fecha de 2017 y el 47 % tenía una fecha posterior al 1 de enero de 2018. El sector de Consumidores tuvo las declaraciones de privacidad más "actuales" (el 71 % con fecha posterior al 1 de enero de 2018), mientras que el sector de Atención médica tuvo las menos actuales (solo el 19 % con fecha posterior al 1 de enero de 2018).

Alineamiento con el RGPD. Dado que el RGPD entró en vigor a mediados de 2018, se capturaron diversos datos relacionados con este reglamento para crear una referencia. Se concedieron puntos de bonificación a las organizaciones que incluyeron principios clave relacionados con el RGPD en su declaración de privacidad. Se otorgaron puntos de bonificación (en lugar de básicos) porque la mayoría de las organizaciones auditadas (y sitios relacionados) evaluadas están en Estados Unidos, por lo que el RGPD no aplica necesariamente. En análisis demostró lo siguiente:

- El 32 % de las declaraciones de privacidad eran fáciles de leer (por lo que casi el 70 % necesitaba mejorar).
- El 95 % de las declaraciones de privacidad expresaron adecuadamente los datos que recopilan y por qué motivo.
- Menos del 1 % mencionó las categorías de terceros con los que comparten los datos.
- El 70 % señaló un medio para contactar al responsable de la protección de datos.

- Solo el 1% indica cómo se trata la información personal confidencial (p. ej., datos biométricos, origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, etc.) que terceros recopilan (esta divulgación solo es necesaria si se manejan este tipo de datos).
- El 50 % describe el proceso que los usuarios deben seguir para solicitar a la organización los datos que ha recopilado sobre ellos.

Rastreadores de terceros. En general, las puntuaciones relacionadas con los rastreadores problemáticos permanecieron estables, aumentando ligeramente de 42,0 en 2017 a 42,4 en 2018. Se conoce que estos rastreadores comparten datos con terceros (sin incluir los datos capturados para las métricas anónimas o seudónimas de los sitios). El número de rastreadores únicos observados en todos los sitios osciló entre 0 y 40. El sector de Noticias/Medios tuvo más del doble del promedio de todos los sectores, lo que refleja su dependencia en la publicidad y la redestinación de los usuarios del sitio.

Incidentes de pérdida de datos y vulneraciones. Tras una medición realizada entre junio de 2017 y diciembre de 2018, el 15 % de los sitios tuvo uno o más incidentes (en comparación del 12 % en 2017). El sector de Consumidores tuvo el porcentaje más alto (34 %) seguido del de Atención médica (30 %). El sector de Bancos, que tuvo el mayor porcentaje en la auditoría de 2017, siguió con el 20 %. Las organizaciones con vulneraciones de más de 1000 registros recibieron una penalización, la cual este año se incrementó en función de la dimensión de la vulneración.[14]

Acuerdos y multas normativas. Dieciocho organizaciones recibieron una penalización por demandas o acuerdos este año (en comparación con 21 en 2017). La mayoría de ellas forma parte del sector de Consumidores (14). Los datos incluyen acciones de la Oficina de Protección Financiera del Consumidor (CFPB, Consumer Financial Protection Bureau), de las oficinas del procurador general del estado, demandas colectivas y agencias internacionales, así como de la Comisión Federal de Comercio (FTC, Federal Trade Commission). Para los fines de la auditoría, el enfoque se centra en las acciones de protección del consumidor relacionadas con la seguridad y la privacidad, y no incluyen acuerdos relacionados con fusiones, adquisiciones o cuestiones laborales.

Protección al consumidor, dominio y marca

Al utilizar la autenticación de correo electrónico (SPF y DKIM), las organizaciones pueden ayudar a proteger sus marcas y evitar que los consumidores reciban correos electrónicos falsificados. La autenticación de correo electrónico permite a los remitentes especificar quién está autorizado a enviar correos electrónicos en su nombre. Basándose en los protocolos de autenticación de correo electrónico, las políticas DMARC indican a los receptores qué hacer con los correos que fallan las verificaciones. El cifrado TLS oportunista permite encriptar los mensajes entre servidores de correo, protegiendo tanto a la marca como al consumidor. El bloqueo de dominio garantiza que la titularidad del dominio no puede transferirse sin la autorización del propietario. Las extensiones de seguridad del sistema de nombres de dominio (DNSSEC) añaden seguridad e integridad al DNS, ayudando a prevenir ataques de intermediarios (MitM, Man in the Middle), envenenamiento de caché y otros ataques relacionados con el DNS. El IPv6 amplía el número de direcciones IP únicas, apoyando así el crecimiento de Internet, incluida la demanda de nuevas direcciones IP impulsada por el IoT.[15][16]

Las mejores prácticas incluyen:

- Implementar SPF y DKIM en dominios de primer nivel, dominios "aparcados" (que no sea usan para el correo electrónico) y cualquier subdominio importante que sea vea en los sitios web o se use para correo electrónico.
- Optimizar los registros SPF con no más de 10 búsquedas de DNS.
- Implementar DMARC, inicialmente en modo "monitor" para obtener retroalimentación de los destinatarios y verificar la exactitud de la autenticación de correo electrónico, y finalmente pasar a "ejecución" (indicar una política de "rechazo" o "cuarentena" a los destinatarios).
- Exigir el uso de las capacidades de informe DMARC con informes RUA (agregados) y RUF (forenses).
- Implementar comprobaciones de autenticación de correo entrante y DMARC en todas las redes para ayudar a proteger contra correos electrónicos maliciosos y ataques de suplantación de identidad tipo "spear phishing" que supuestamente provienen de remitentes legítimos.
- Implementar cifrado TLS oportunista para proteger los mensajes en tránsito entre servidores de correo.
- Asegurar que los dominios estén bloqueados para evitar que alguien tome control de ellos.
- Implementar DNSSEC para ayudar a proteger la infraestructura DNS del sitio web.
- Utilizar IPv6.
- Implantar tecnologías y procesos de mitigación de ataques de denegación de servicio distribuido (DDoS).
- Implementar una autenticación multifactor (AMF).

Autenticación de correo electrónico

Las tecnologías de autenticación, a saber SPF y DKIM, ayudan a evitar el phishing (suplantación de identidad) y el spam. La OTA recomienda el uso de autenticación de correo electrónico en el dominio de nivel superior (TLD) (o "corporativo") así como en cualquier otro dominio que se use para enviar correos electrónicos o que pueda ser utilizado para engañar a los consumidores. Se añadió telemetría adicional en la auditoría de 2017 para evaluar la validez de los registros SPF y DMARC. La autenticación en el TLD recibió una mayor ponderación por tercer año consecutivo.

El gráfico 8 muestra la adopción de registros SPF y DKIM en el dominio de nivel superior (TLD) corporativo y el uso combinado de SPF y DKIM en cualquier nivel, incluidos los subdominios. En general, la adopción de SPF es mayor que la de DKIM. Concluimos que esto se debe principalmente a la facilidad de su implementación, aunque la brecha sigue reduciéndose. El uso de tanto SPF como DKIM permite a los destinatarios detectar y bloquear correos electrónicos maliciosos, a la vez que se reduce el riesgo de falsos positivos.

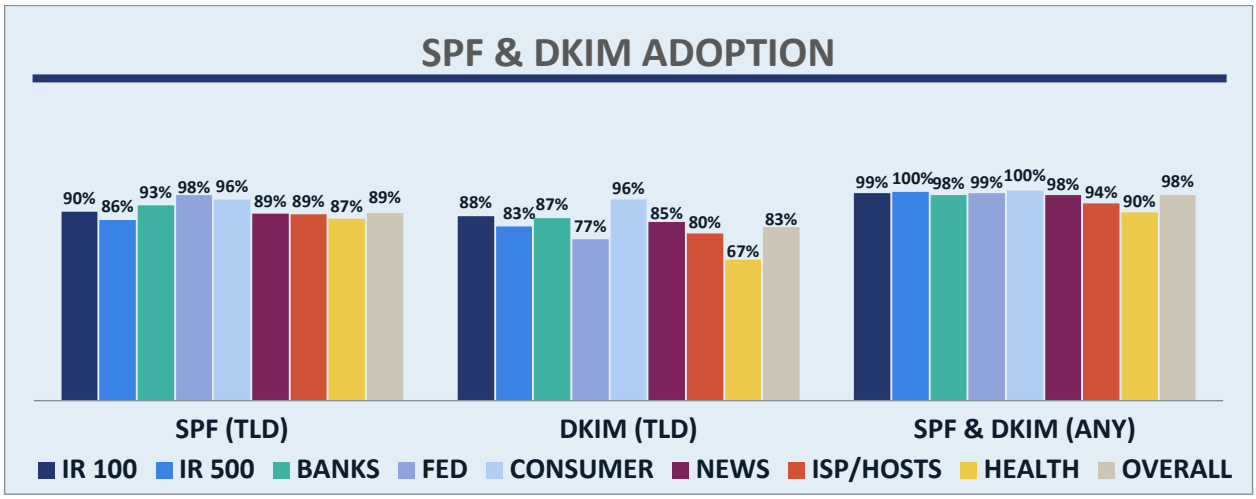


Gráfico 8. Autenticación de correo electrónico y adopción de DMARC por sector.

El gráfico 9 muestra un crecimiento en todos los sectores, y varios están cerca de alcanzar una adopción total del 100 %.Se observaron incrementos significativos en el sector Federal (del 46 al 94 %, atribuidos en gran medida a la Directiva DHS 18-01) y el sector Bancos (del 60 al 87 %).[17] Los sectores de Atención médica e ISP/Hosts quedan rezagados con el 65 y 75 % respectivamente. Aunque las brechas se están cerrando, en algunos sectores todavía hay una falta significativa de apoyo a la autenticación de correos electrónicos en los dominios de nivel superior (nótese la brecha entre "DKIM TLD" y "SPF y DKIM" en el gráfico 8). Esto subraya que se necesitan mayores esfuerzos para impulsar la implementación de DKIM y proteger los dominios de nivel superior y de nivel superior corporativo contra el abuso.

TANTO SPF COMO DKIM

	2015	2016	2017	2018
100 mejores minoristas de Internet	90 %	92 %	92 %	98 %
500 mejores minoristas de Internet	78 %	85 %	83 %	95 %
Bancos 100	63 %	69 %	60 %	87 %
Federal 100	48 %	58 %	46 %	94 %
Consumidores 100	76 %	86 %	88 %	95 %
Noticias 100	56 %	75 %	77 %	94 %
ISP/Hosts 100	-	-	55 %	75 %
Salud 100	-	-	-	65 %

Gráfico 9. Adopción tanto de SPF como DKIM por sector.

A partir de 2017, los registros SPF se analizaron con mayor detenimiento y solo recibieron una puntuación parcial o se consideraron inválidos si contenían errores que podrían hacerlos inservibles o

ineficaces. Esto afectó al 16 % de las organizaciones y fue más predominante para los minoristas (20 %). El sector Federal tuvo el índice de error más bajo (4 %). Los principales motivos por los que solo se otorgaron puntos parciales fueron búsquedas excesivas e "incluir" referencias a registros SPF inexistentes o inválidos de otros dominios.[18]Las principales razones por la que los registros se consideraron inválidos fueron el uso de múltiples registros SPF y errores de sintaxis que hacen que los registros sean inservibles. Además, se observó el uso de una directiva "+all" o "?all", que instruye a los destinatarios (en ISP y redes corporativas) que permitan que cualquier dirección IP envíe correo o ignoren el registro. Estos registros también se consideraron inválidos. Muchas de estas organizaciones pueden tener un falso sentido de seguridad, ya que no saben que sus registros SPF no están protegiendo eficazmente sus dominios.

Aunque está fuera del alcance o capacidad de esta auditoría, todas las organizaciones deberían implementar comprobaciones de autenticación entrante y aplicar las políticas de DMARC. Como práctica recomendada de mitigación de riesgo, se debería exigir a los proveedores clave, socios comerciales y proveedores de servicios que adopten la autenticación de un extremo a otro, como SPF, DKIM y DMARC.

Autenticación de mensajes, informes y conformidad basada en dominios (DMARC)

DMARC se basa en los resultados de SPF y DKIM, permite generar informes de retroalimentación y añade visibilidad a los destinatarios sobre cómo procesar los mensajes que no pasan la autenticación. Se añadió a la puntuación básica en 2013 y en 2016 se incrementó la ponderación al uso de políticas DMARC de rechazo y cuarentena, con un máximo de puntos para las de rechazo. Este año se incrementó la ponderación para el uso de políticas de rechazo.

Como se ilustra en los gráficos 10 y 11, la adopción de DMARC creció en la mayoría de los sectores, particularmente en los sectores Federal (del 20 al 93 % a causa de la directiva 18-01), Bancos (del 39 al 70 %) y Noticias (del 29 al 50 %). Se observaron registros DMARC inválidos en casi el 2 % de todas las organizaciones, pero en mayor medida en el sector ISP/Hosts (5 %). Las razones principales para invalidar un registro fueron registros "descubiertos" (p=ninguno y falta de informes RUA o RUF) y enviar los informes a dominios que no podían aceptarlos.

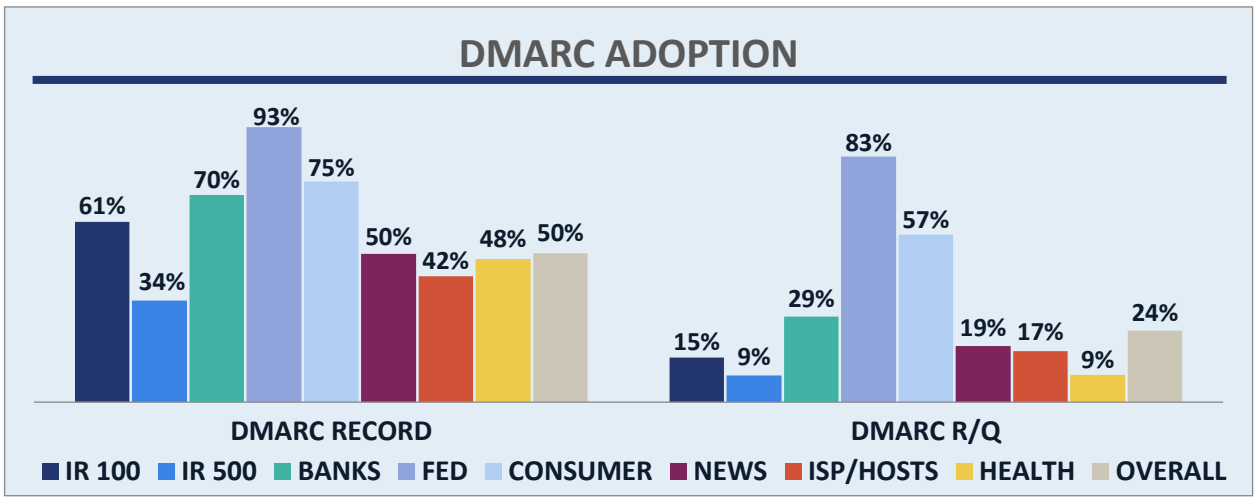


Gráfico 10. Adopción y políticas de DMARC.

ADOPCIÓN DE DMARC						
	2015 Registro	2016 Registro	2017 Registro	2018 Cualquier registro	2018 Registro válido	2018 R o C*
100 mejores minoristas de Internet	20 %	30 %	50 %	61 %	61 %	15 %
500 mejores minoristas de Internet	8 %	21 %	33 %	34 %	33 %	9 %
Bancos 100	24 %	33 %	39 %	70 %	70 %	29 %
Federal 100	14 %	20 %	20 %	93 %	93 %	83 %
Consumidores 100	48 %	64 %	62 %	75 %	74 %	57 %
Noticias 100	10 %	21 %	29 %	50 %	48 %	19 %
ISP/Hosts 100	-	-	25 %	42 %	37 %	17 %
Salud 100	-	-	-	48 %	47 %	9 %

Gráfico 11. Adopción de DMARC por sector.*R o C = Política de rechazo o de cuarentena

Seguridad de la capa de transporte (TLS, Transport Layer Security) oportunista para correo electrónico

En la auditoría de 2015, se añadió el rastreo de TLS oportunista para correo electrónico con el fin de abordar las crecientes preocupaciones de confidencialidad relacionadas con el monitoreo de correos electrónicos en tránsito. TLS cifra los mensajes en tránsito de un servidor a otro y los descifra sin problemas antes de que lleguen al usuario. La adopción de TLS se encuentra en crecimiento constante, aumentando del 65 % en 2017 al 73 % este año. El sector Federal sigue rezagado con el 51 %, mientras que los sectores de Consumidores y Noticias llevan la delantera con un 83 % de adopción. El crecimiento se atribuye a la demanda generalizada de cifrado por parte de decenas de organizaciones, como Internet Society, Google y Twitter, que proporcionan datos sobre el uso de TLS oportunista. Desde principios de 2016, Gmail también ha resaltado los mensajes sin TLS con un candado rojo desbloqueado.[19]

Bloqueo de dominios

El bloqueo de dominios se incorporó a los criterios de calificación en 2013 debido a su importancia para prevenir que extraños tomen control de los dominios (se asigna una penalización si el dominio no está bloqueado). Más del 95 % de las organizaciones en todos los sectores bloquean sus dominios. El sector Federal lidera el grupo con una adopción del 100 %, seguido de cerca por los sectores de Consumidores (98 %) y Atención médica (97 %). Los sectores de Minoristas, Bancos, Noticias e ISP/Hosts están en el rango de 93-94 %.

Extensiones de seguridad del sistema de nombres de dominio (DNSSEC)

Las DNSEEC añaden seguridad a la búsqueda de DNS. Están diseñadas para ayudar a combatir los ataques de intermediarios ("Man in the Middle", MitM) y envenenamiento de caché al autenticar el origen de los datos de DNS y verificar su integridad mientras se mueven por Internet. Las DNSSEC han sido implementadas en extensiones .com, .gov, .org, .net y más de 135 otros TLD, y admitiendo potencialmente más de 90 millones de registros de nombres de dominio en todo el mundo solo con la extensión.com.[20]La adopción de DNSSEC cayó del 12 % en 2017 al 10 % este año debido a los cambios en la lista de organizaciones auditadas. El sector Federal lidera la adopción (87 %) en gran medida debido a

una orden de 2008, seguido por los sectores de Bancos (10 %) e ISP/Hosts (8 %).[21] La aplicación más amplia de DNSSEC sigue viéndose obstaculizada por los sistemas existentes y la falta de infraestructura de ecosistemas.

Protocolo de Internet versión 6 (IPv6)

IPv6 es la versión más reciente del protocolo de Internet (IP), el protocolo de comunicaciones que proporciona un sistema de identificación y localización a las computadoras a través de Internet, y amplía significativamente el número de direcciones disponibles. La OTA apoya una implementación mayor, otorgando puntos de bonificación por su adopción. La adopción en todo el mundo está creciendo. Actualmente, más del 26 % de los 1000 mejores sitios web de Alexa pueden accederse a través de IPv6, un aumento del 2 % desde 2017.[22] La adopción general en la auditoría de la OTA cayó del 14 % en 2017 al 12 % este año debido a la mayor exigencia. Los sitios web debían poder ser accesibles a través de IPv6, mientras que en años anteriores solo el servicio de nombres debía ser compatible con IPv6. El sector Federal lidera con un 46 % de adopción, seguido por ISP/Hosts con un 20 % y las organizaciones de Consumidores con un 15 %.

Autenticación multifactor (MFA)

Agregar otra capa de autenticación además de un nombre de usuario y contraseña es una forma eficaz para ayudar a prevenir el acceso no autorizado a las cuentas, que alguien extraño tome control de las cuentas o que se restablezcan las contraseñas. La autenticación multifactor (AMF) requiere credenciales adicionales más allá del nombre de usuario y contraseña para obtener acceso a una aplicación, sitio o datos. En la autenticación típica de dos factores, un programa de software o un dispositivo de hardware (en posesión del usuario) genera una contraseña o código de único uso para verificar que se autoriza el acceso a la cuenta. A la luz de la ola de ataques de relleno de credenciales (credential stuffing) en 2018 y la enorme base de datos de pares de nombres de usuarios y contraseñas vulnerados, el uso de la autenticación multifactor es una práctica muy recomendada.[23][24] En la auditoría de 2017, se recopilaron datos de autenticación multifactor pero abarcaron menos de la cuarta parte de las organizaciones auditadas. Debido a que solo contamos con datos incompletos, no se ha evaluado la AMF en esta auditoría, pero es nuestra intención incorporarla en la metodología de auditoría cuando se disponga de datos suficientes.

Seguridad de sitios, servidores e infraestructura

La confiabilidad de un sitio se define en gran medida por la seguridad de la infraestructura, así como por sus prácticas de privacidad asociadas. Los usuarios necesitan tener la garantía de que tanto el sitio como sus datos están seguros. La implementación adecuada de las mejores prácticas en esta categoría también protege al sitio de ataques. La auditoría de 2018 se ha ampliado con una evaluación más profunda del estado del DNS, la reputación de la IP, la seguridad de las aplicaciones y la gestión de vulnerabilidades (patching cadence). Además, este año se aumentó el nivel de exigencia en la puntuación de seguridad del servidor al combinar los resultados de High-Tech Bridge (ahora ImmuniWeb), Qualys SSL Labs, Observatory de Mozilla y SiteCheck de Sucuri. Las mejores prácticas incluyen:

"Los consumidores merecen saber qué prácticas siguen las empresas para mantener sus datos privados y seguros. La auditoría de confianza en línea proporciona esta transparencia cada año con su auditoría anual. Esta auditoría independiente ayuda a las empresas de todos los tamaños a comprender qué prácticas de privacidad y seguridad aplicar para proteger a sus clientes y a sus negocios". Ashutosh Agrawal, gerente senior de cumplimiento de seguridad y privacidad, 23andMe.

- Optimizar la implementación de SSL/TLS usando información obtenida de herramientas públicas, centrándose en las vulnerabilidades con calificación de "F" o que hayan reprobado (60 puntos o menos) en un subcomponente principal de la calificación (lo que normalmente conduce a una calificación global de "C").[25][26] Esto incluye eliminar el uso de cifrados inseguros y protocolos antiguos e inseguros, así como la vulnerabilidad a los ataques POODLE y ROBOT.[27]
- Implementar una política de seguridad de contenido y encabezados asociados para los contenidos de terceros utilizados en el sitio. Esto puede evitar que contenidos externos introduzcan vulnerabilidades.[28][29][30]
- Revisar las capacidades de las autoridades de certificación para asegurarse de que cumplen con sus requisitos de soporte. Usar certificados SSL con EV para las clases de sitios que se falsifican con frecuencia y en los que los usuarios necesitan tener la seguridad de que están visitando un sitio legítimo.
- Implementar la autorización de la autoridad de certificación (CAA) para evitar que se emitan certificados no autorizados.[31]
- Implementar la Seguridad de Transporte Estricta de HTTP (HSTS), también conocida como Always on SSL (AOSSL) o HTTPS Everywhere, en todas las páginas para maximizar la seguridad de los datos y la privacidad en línea. La HSTS ayuda a garantizar que todos los datos intercambiados entre el sitio y el dispositivo estén cifrados.
- Implementar un cortafuegos de aplicaciones web para monitorear las conversaciones HTTP y bloquear ataques comunes, como los de scripts de sitios (XSS) y las inyecciones de código SQL.
- Analizar los sitios proactivamente para detectar enlaces maliciosos, vulnerabilidades en iFrame, malware (software dañino) y publicidad malintencionada.[32]

- Implantar la detección y mitigación de robots para ayudar a prevenir ataques de fuerza bruta, "web scraping", secuestro de cuentas, análisis de vulnerabilidades no autorizados, el spam y ataques de intermediarios (man-in-the-middle).
- Proporcionar un mecanismo accesible y visible para que los visitantes y terceros puedan informar vulnerabilidades.

Como se ilustra en el gráfico 12, las puntuaciones de seguridad promedio están un rango relativamente estrecho, mientras que la tasa de adopción de las mejoras clave varía ampliamente:

- Las puntuaciones de seguridad del sitio, que representan la mayor parte de la calificación básica en esta categoría, están concentradas alrededor del promedio global de 89 (una disminución en comparación del 92 obtenido en 2017). El sector Federal está a la cabeza con 94, seguido por los sectores de Consumidores y Noticias con 91. El descenso en las puntuaciones se debe en su totalidad al incremento en la ponderación de otros elementos de seguridad: contenido de terceros e implementación de encabezados de seguridad, gestión de vulnerabilidades y reputación de IP.
- La adopción global de "Always on SSL" (ahora parte de la puntuación básica) aumentó significativamente a 93 % (de 30 % en 2016 y 52 % en 2017), y la brecha de adopción se ha reducido, yendo de 82 % en el sector de Atención médica a 100 % en el Federal (frente al rango entre 26 y 91 % en 2017). Los sitios de Noticias mostraron el mayor crecimiento, del 26 al 93 %.
- La adopción de certificados SSL con EV es del 25 % en promedio, pero varía significativamente en cada sector. Es más alta en el sector de Bancos (71 %, que sobrepasa todos los demás sectores en más del doble) y más baja en los sectores de Noticias y Federal (8 %), seguidos de cerca por el de Atención médica (9 %).
- Solo 6 % de los sitios han aprovechado las capacidades del nuevo rastreo de CAA, que permite a los propietarios de dominios publicitar la lista de autoridades de certificación autorizadas a emitir certificados en su nombre, limitando así el abuso. La adopción fue mayor en los sectores de Consumidores (20 %) y Noticias (13 %), y fue menor en el sector de Minoristas en línea (2 %).

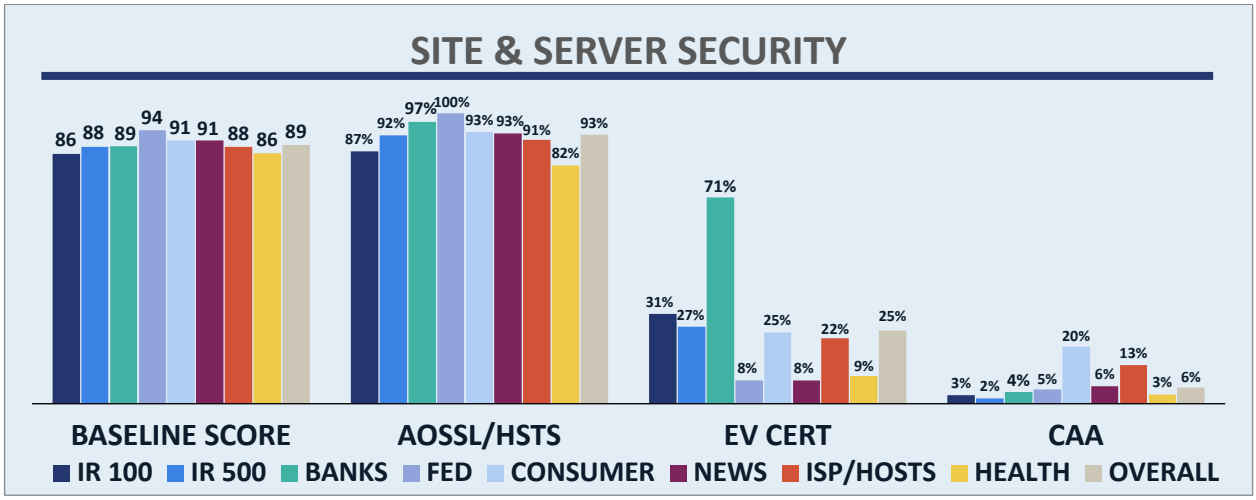


Gráfico 12. Puntuación/adopción de seguridad de sitio y servidor por sector.

Implantación de servidores y análisis de vulnerabilidad

El monitoreo continuo de la configuración SSL/TLS y el uso de configuraciones de seguridad relacionadas es un requisito esencial para optimizar la seguridad y contrarrestar las vulnerabilidades. La auditoría de 2018 amplió el análisis con la adición de nuevas herramientas, como aquellas brindadas por ImmuniWeb, Internet.nl, Mozilla, Sucuri, Symantec y SSL Labs. Los datos se usaron en forma colectiva para evaluar la implementación de SSL/TLS en los sitios, la adopción de SSL con EV, la adopción de CAA, la adopción de AOSSL, la configuración de contenido de terceros, el uso de un cortafuegos de aplicaciones web y la vulnerabilidad a scripts de sitios y de iFrame, malware y enlaces maliciosos.

Como referencia al estado general de la seguridad SSL/TLS, el informe mensual de SSL Pulse del 2 de marzo de 2019 indicó que el 66% de los 139 822 sitios analizados se consideraban seguros, lo que supone un aumento continuo con respecto al 58 % de junio de 2017 y el 43 % de junio de 2016.[33] En comparación, el 83 % de los sitios de la auditoría de la OTA se consideran seguros, lo que indica que la muestra de la auditoría supera significativamente el rendimiento de los sitios web en general. Al analizar las puntuaciones de seguridad del sitio, se observaron varias tendencias:

- El uso de parámetros, protocolos y cifrados de intercambio de claves vulnerables disminuyó, pero muchos sitios siguen siendo compatibles con implementaciones más antiguas. Los problemas que se identificaron más comúnmente fueron el uso de protocolos Diffie-Hellman débiles, cifrados RC4 y protocolos SSL3 o TLS 1.0 (la versión TLS 1.0 se considera obsoleta como parte del estándar PCI a partir de junio de 2018).[34]
- El 29 % de los sitios solo admiten TLS 1.2 o superior, que es la práctica recomendable. Todavía hay problemas de compatibilidad con navegadores antiguos que evitan que las organizaciones eliminen completamente las versiones 1.0 y 1.1 de TLS, pero hay una tendencia a eliminar los protocolos anteriores a TLS 1.2. El 7 % de los sitios admite TLS 1.3, que fue publicado oficialmente en agosto de 2018. Los sectores de ISP/Hosts y Atención médica lideran la lista con 11 %.
- La mayoría de los sitios no están estableciendo una política de seguridad de contenidos ni están aprovechando los encabezados que pueden limitar vulnerabilidades relacionadas con contenidos de terceros, como las cookies. Se puede ver resultados específicos usando el análisis de seguridad del sitio web de ImmuniWeb y Mozilla Observatory.

Se detectó malware en el 2 % de los sitios, especialmente en el sector de Bancos (10 %). Se observaron vulnerabilidades de XSS/iFrame en el 21 % de los sitios, una disminución de más de la mitad en comparación del 50 % observado en 2017. Se penalizó a los sitios si habían tenido un ataque XSS en 2018 o no habían corregido una vulnerabilidad XSS reportada antes de 2018.[35] El sector de Bancos tuvo la menor presencia de vulnerabilidades de XSS/iFrame con un 5 %, pero el 43 % de los sitios de Noticias y más de una quinta parte de los sitios de Consumidores y Federal eran vulnerables. Aunque los resultados muestran una mejoría desde 2017, la presencia de vulnerabilidades es preocupante y refuerza la necesidad de que las organizaciones monitoreen continuamente sus sitios y sistemas de gestión de contenidos.

PUNTUACIÓN DE SEGURIDAD DEL SITIO				
	2015	2016	2017	2018
100 mejores minoristas de Internet	85,7	89,6	91,1	86,0
500 mejores minoristas de Internet	85,3	88,3	90,6	88,4
Bancos 100	83,0	88,3	87,7	88,6
Federal 100	83,6	91,6	95,2	94,2
Consumidores 100	86,1	89,9	93,1	81,2
Noticias 100	83,0	85,0	88,8	90,6
ISP/Hosts 100	-	-	92,9	88,4
Salud 100	-	-	-	86,3

Gráfico 13. Puntuación de seguridad del sitio promedio por sector, 2015-2018.

Como se muestra en el gráfico 13, los puntajes de seguridad han disminuido con respecto al año anterior en la mayoría de los sectores (a excepción de Bancos y Noticias). Las puntuaciones cayeron debido al incremento en la ponderación de factores de configuración que no son SSL/TLS, y principalmente debido a las bajas puntuaciones observadas en el análisis de seguridad del sitio de ImmuniWeb y Mozilla Observatory. El sector Federal está a la cabeza por tercer año consecutivo, con una puntuación de 94,2. Al igual que con los ataques XSS y el *malware*, la configuración e implementación de SSL/TLS y otros elementos de seguridad del sitio relacionados requieren de monitoreo continuo porque aparecen nuevas vulnerabilidades con frecuencia. Según la experiencia de la OTA, es posible efectuar cambios de una manera rápida y económica cuando quienes toman las decisiones están comprometidos.

Tipos de certificados SSL/TLS

Tras reconocer la importancia de los certificados de confianza y la creciente preocupación por la adquisición de certificados para sitios fraudulentos que pretenden ser destinos populares entre los consumidores, la OTA empezó a rastrear tipos de certificados en 2015. Existen tres tipos principales de certificados: validación de dominio (DV), validación de organización (OV) y validación extendida (EV), que tienen diferentes métodos para validar la identidad de la entidad que recibe el certificado. El nombre oficial y la ubicación de las entidades que compran los certificados OV y EV se verifican y confirman directamente con la entidad por medio de autoridades de certificación y se incluyen en el certificado. Por el contrario, los certificados DV se verifican mediante un proceso automatizado, por lo que son más eficientes y menos costosos de adquirir, lo que da lugar a un gran aumento en el uso de TLS. Siguiendo esta tendencia, los ciberdelincuentes también los han utilizado para ataques de suplantación de identidad y para crear dominios y contenidos similares.[363738]

Los certificados SSL con EV brindan un mayor nivel de verificación, lo que requiere de un proceso de auditoría exhaustivo. El certificado SSL con EV proporciona una diferenciación al mostrar el nombre de la entidad y un indicador de confianza verde en la barra de direcciones o el visor del navegador, aunque esta diferenciación ha disminuido en los últimos años y no está presente en muchas implementaciones de navegadores móviles. Los certificados SSL con EV son obligatorios en algunos sectores (p. ej., proveedores de declaración electrónica del IRS).[39]

Recientemente ha habido un intenso debate en la industria sobre el valor de los diferentes tipos de certificados. Algunos argumentan que cualquier cosa más allá del nivel DV no añade valor.[40] Otros argumentan que vale la pena pagar más por los certificados EV y OV debido a la diferenciación mostrada en el navegador (EV) o el apoyo adicional en la gestión de grandes lotes de certificados o la revocación de certificados afectados.

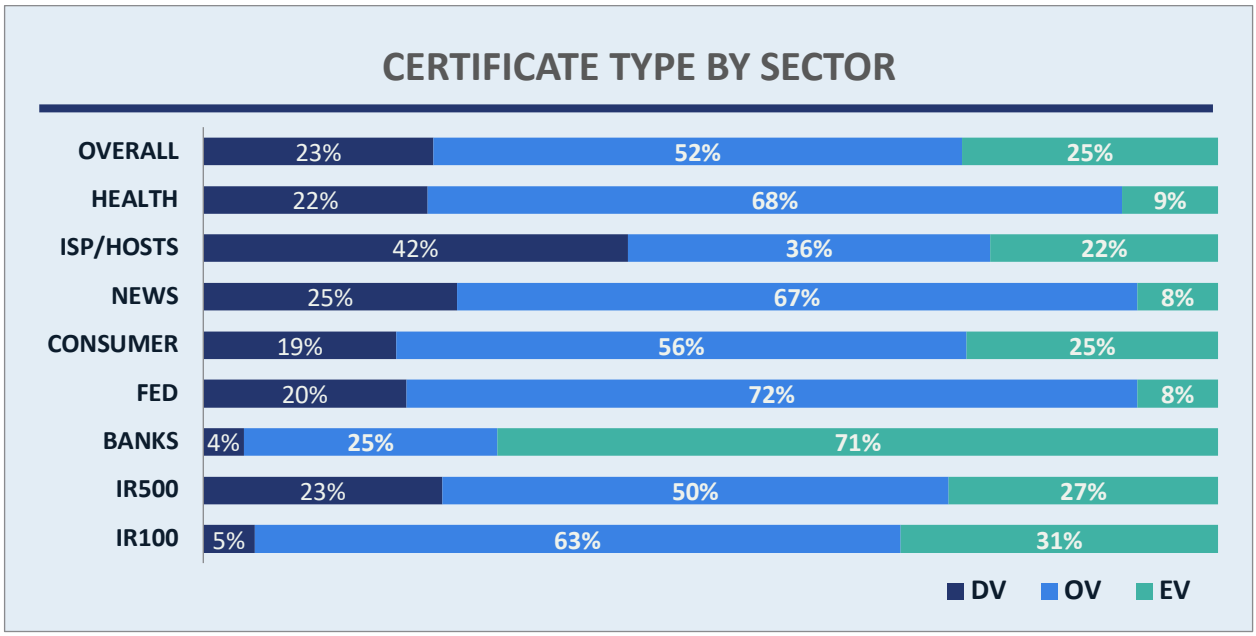


Gráfico 14. Tipo de certificado SSL/TLS por sector, 2018.

El gráfico 14 muestra las tasas de adopción de cada tipo de certificado por sector. Las tasas varían significativamente por sector. El de Bancos se inclina hacia los certificados EV (71 %), los sitios de los sectores Federal, Atención médica y Noticias hacia los certificados OV (67-72 %) y los sitios de ISP/Hosts hacia los certificados DV (42 %). El gráfico 15 muestra que con el tiempo ha habido una ligera disminución en la adopción de certificados EV dando preferencia a los certificados DV, mientras que los OV han permanecido estables.[41] Al elegir qué autoridades de certificación y tipo de certificado usar, los propietarios de dominios deberían examinar la situación de manera integral y tomar en cuenta la asistencia y los servicios además de la emisión básica de certificados.

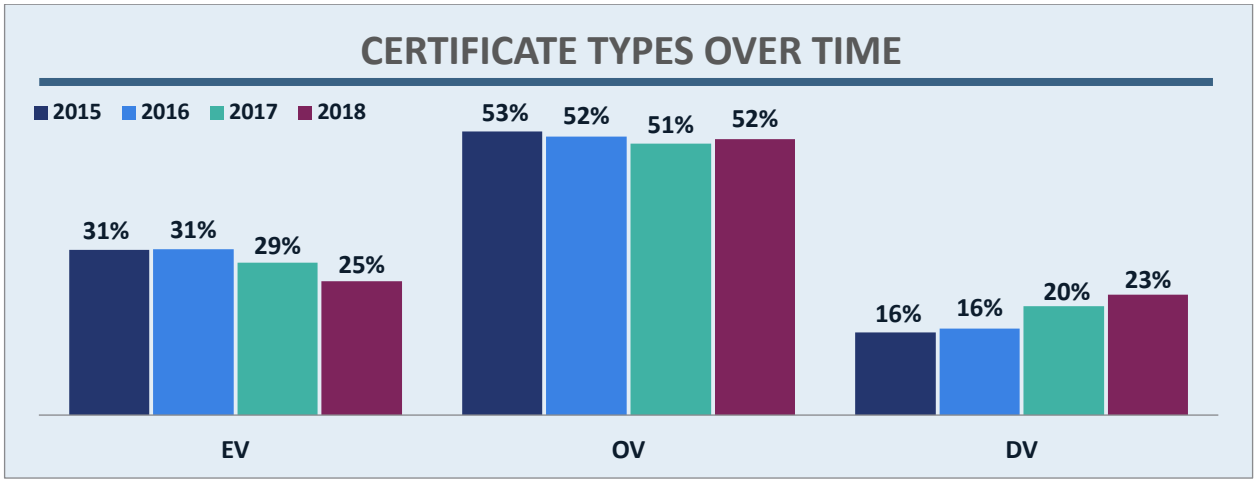


Gráfico 15. Tipo de certificado SSL/TLS, 2015-2018.

Mitigación de DDoS

Aunque está fuera del alcance de la metodología de la auditoría de este año, las organizaciones necesitan implementar medidas que les ayuden a detectar y mitigar el impacto de un ataque de DDoS. Según Kaspersky Labs, hubo un 13 % menos actividad de DDoS en 2018 que en 2017, aunque la duración promedio de los ataques se incrementó de 95 minutos en el primer trimestre de 2018 a 218 minutos en el cuatro trimestre.[42] En todo el mundo, estos ataques siguen siendo impredecibles y persistentes, y varían ampliamente en cuanto a volumen, velocidad y complejidad. Para combatir estos incidentes, es cada vez más importante monitorear constantemente las amenazas para optimizar la estrategia de mitigación. La OTA recomienda cortafuegos locales y dispositivos DDoS dedicados (o servicios equivalentes en la nube) para ayudar a detener el tráfico malicioso. Cuando se configuran correctamente, es posible bloquear y eliminar el tráfico malicioso antes de que llegue a los servidores que busca atacar.

Mecanismos de informes de vulnerabilidad

Se agregaron a la metodología en 2017. Se otorgaron puntos de bonificación a las organizaciones que tienen un mecanismo para enviar informes de vulnerabilidades directamente en su sitio o por medio de programas externos de recompensas por encontrar fallas. Se agregó en parte porque es una práctica reconocida por NTIA, NIST y FTC. La adopción de esta práctica casi se duplicó, de un 6 % en 2017 a un 11 % en 2018, pero aún es bastante baja. El sector de Consumidores lleva la delantera con un 43 % de adopción, seguido de ISP/Hosts con un 25 %, Noticias/Medios con un 9 % y Bancos con un 6 %.Se reconoce que contar con tales mecanismos es fundamental para responder eficazmente a los informes de los investigadores externos, y es relativamente sencillo de implementar. La OTA recomienda que los sitios tengan un mecanismo de informe de vulnerabilidades alojado en su sitio (como el formulario en línea diseñado por la OTA) o por medio de uno de los programas externos que ofrecen una recompensa por encontrar fallas.[43]

Publicidad malintencionada (malvertising)

Los ciberdelincuentes han reconocido que el ecosistema de publicidad es vulnerable y usan su complejidad para distribuir mensajes engañosos y anuncios con códigos maliciosos para afectar los dispositivos de los usuarios y los sistemas de las empresas. La publicidad malintencionada o "malvertising" representa una amenaza creciente para todos los que acceden a contenidos y servicios financiados con publicidad. En el último año, se han usado nuevas técnicas para ocultar anuncios maliciosos, y una firma estima que la publicidad malintencionada le está costando a la industria publicitaria más de mil millones de dólares al año.[44] A fines de 2018, Amazon demandó a los operadores de un sitio que usaba publicidad malintencionada para redirigir a los usuarios a su sitio fraudulento.[45] Aunque no se hizo un seguimiento de los incidentes de publicidad malintencionada en la auditoría, las organizaciones deben entender el ecosistema de entrega de anuncios para sus sitios y las protecciones que existen para bloquear los anuncios maliciosos.

Privacidad, transparencia y divulgación

Nota: En auditorías anteriores, el término "política de privacidad" se usó para referirse a la representación de las prácticas de privacidad de un sitio. Para alinearse con la nomenclatura global, el

término se ha cambiado a "declaración de privacidad". También se debe tener en cuenta que la auditoría evalúa las afirmaciones que la organización hace en su declaración de privacidad, mas no sus prácticas reales, las cuales pueden ser muy diferentes de las políticas declaradas porque la auditoría solo las examina externamente.

La auditoría de 2018 mostró ligeros incrementos en la transparencia y claridad de las declaraciones de privacidad publicadas, por lo que aún hay mucho que mejorar. Cada vez más declaraciones presentan la información por capas, las divulgaciones son más completas y el lenguaje usado está más dirigido a los consumidores en vez de parecer un contrato redactado para personas versadas en temas jurídicos. Parte de esto se puede deber al mayor conocimiento y cumplimiento del Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

Con la llegada del RGPD, ahora es más importante que nunca que las organizaciones protejan los datos. Además, las organizaciones necesitan conocer otras normas transfronterizas, como el Sistema de Reglas de Privacidad Transfronteriza de APEC. Este es un conjunto de normas de privacidad voluntarias pero aplicables que permiten el flujo de datos en la región Asia-Pacífico.[46] En 2020, la Ley de Privacidad del Consumidor de California (CCPA), que se basa en gran medida en los principios del RGPD, entrará en vigor, obligando a las organizaciones estadounidenses a implementar medidas adicionales de protección de la privacidad si desean operar en el mercado más grande de EE. UU.[47] La OTA ha estado promoviendo la mayor transparencia y accesibilidad de las declaraciones de privacidad desde 2009, y ha recomendado que se divulguen las prácticas de recopilación, uso, intercambio y retención de los datos. Las mejores prácticas incluyen:

Elementos básicos de divulgación/notificación

- Asegurarse de que la declaración de privacidad tenga un enlace y sea fácil de encontrar en la página de inicio.
- Colocar la fecha de revisión de la declaración en la parte superior de la página.
- Brindar acceso a las versiones archivadas de la declaración para que los usuarios puedan ver qué ha cambiado.
- Usar un aviso de capa simple o corto diseñado para ayudar a los consumidores a entender la declaración.
- Usar íconos para ayudar a los consumidores a consultar las declaraciones de privacidad junto con avisos cortos presentados por capas.
- Escribir declaraciones adecuadas para la audiencia y el grupo demográfico al que se dirige el sitio. Considerar la posibilidad de brindar versiones en diferentes idiomas para los visitantes que no hablen inglés.

Declarar claramente las políticas de cumplimiento más importantes

- Cumplimiento de la Ley de Protección de la Privacidad Infantil en Internet (COPPA) o normas relacionadas.[48]
- Divulgar si el sitio acata la configuración de "no rastrear" (Do Not Track, DNT) del navegador y de preferencia hacerlo.

- Brindar un resumen de la política de retención de datos, incluyendo un plazo específico y el motivo por el cual se retienen los datos.

Proteger la privacidad y definir el uso compartido protegido

- No compartir datos personales con un tercero salvo que sea necesario para prestar el servicio al usuario. Brindar una declaración clara que detalle si comparte datos, qué datos comparte y con qué fines.
- Exigir que sus proveedores cumplan con la normativa por medio de un contrato y notificar a los consumidores que los proveedores de servicios tienen prohibido usar o compartir sus datos con cualquier fin que no sea la prestación de servicios en nombre del sitio.
- Divulgar si hace seguimiento de los usuarios a través de distintos dispositivos (cross-device tracking).
- Usar sistemas de gestión de etiquetas o soluciones de privacidad para gestionar los rastreadores de terceros.
- Divulgar si compartirá datos para cumplir con sus obligaciones legales y hacer todo lo posible para notificar a los consumidores si terceros solicitan sus datos debido a requisitos legales.

En 2017, los 100 puntos básicos se reasignaron de 50 a 55 % para los elementos de la declaración de privacidad y de 50 a 45% para el uso de rastreadores. La puntuación de privacidad promedio este año fue de 70, menor que la de 2017 (73). Esto se debió principalmente a la mayor exigencia en la calificación. Las puntuaciones oscilaron de 67 para los sitios de Minoristas de Internet hasta 76 para los de Consumidores. Mientras que los puntajes de la mayoría de los sectores se redujeron, el de los Bancos se elevó de 65 a 69, y el de las Noticias de 70 a 71.

En general, un número menor de organizaciones recibió calificaciones reprobatorias en privacidad (16 % en comparación de 15 % el año anterior), aunque los resultados variaron ampliamente por sector. En el caso de los Minoristas de Internet, el porcentaje de reprobados creció del 16 % al 23 %, mientras que disminuyó del 34 % al 14 % para los Bancos, y del 19 % al 10 % para las Noticias. Como se muestra en el gráfico 16, las puntuaciones para el componente de declaración de privacidad (que valía 55 puntos) se encontraban en un rango bastante estrecho, de 25 a 33. Desgraciadamente, el promedio de 27 indica que la mayoría de las organizaciones solo está recibiendo la mitad de los puntos disponibles. Las puntuaciones por seguimiento fueron mucho más alentadoras, dado que los sectores obtuvieron más del 87 % de los 45 puntos disponibles.

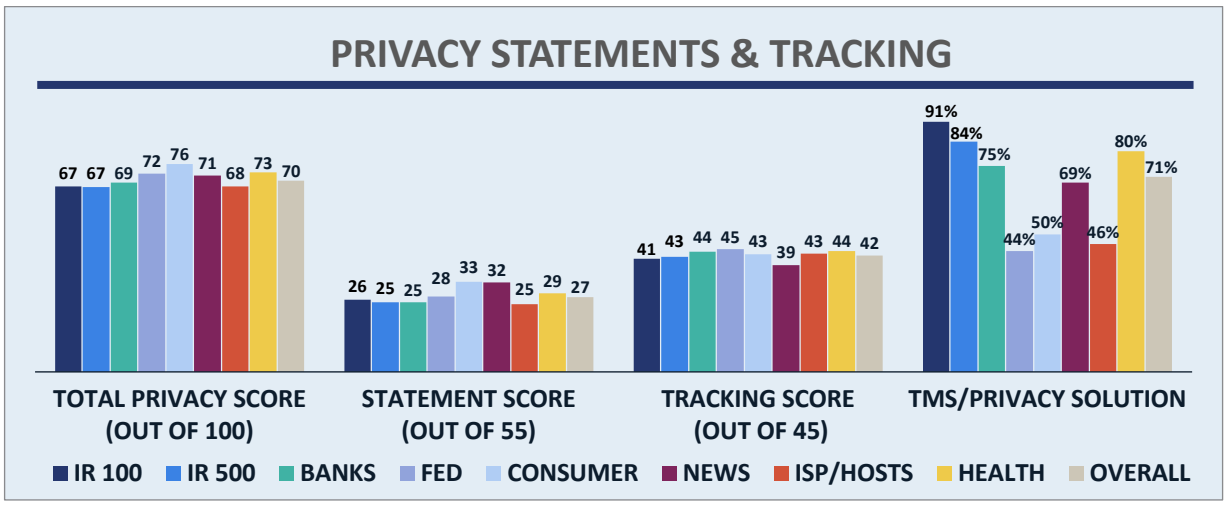


Gráfico 16. Puntuaciones de declaración de privacidad y seguimiento por sector.

Los sitios que dependen de la publicidad y los análisis de terceros se enfrentan al reto de gestionar el seguimiento de terceros. El creciente desafío de los propietarios de sitios es conocer las prácticas de intercambio de datos de sus socios y el "efecto dominó" de los datos que puede producirse cuando se divulgan datos personales. Los sistemas de gestión de etiquetas y las soluciones de privacidad ayudan a monitorear la recopilación y el intercambio de datos por parte de terceros en tiempo real. Se otorgaron puntos de bonificación si estaban presentes.[49] La adopción general aumentó a 71 % a comparación del 69 % de 2017, y se está considerando incluir este elemento en la puntuación base en auditorías futuras. Los Minoristas de Internet lideraron la adopción (84 %). El sector Federal tuvo la tasa de adopción más baja (44 %), que se atribuye al bajo número de etiquetas empleadas y al hecho de que no dependen de ingresos por publicidad ni intercambio de datos.

Transparencia

Proporcionar un aviso claro de las modificaciones a la declaración de privacidad con fecha en la parte superior de la página y un enlace para acceder a las versiones archivadas ayuda a maximizar la transparencia. Ambos elementos forman parte de la calificación base en la auditoría de 2018. En general, el 47 % de las organizaciones tenía una fecha en la parte superior de la página (un poco más que el 46 % de 2017), pero la adopción varió ampliamente, de solo 2 % en el sector Federal a 74 % en el de Noticias. Por primera vez se registraron las fechas de las declaraciones de privacidad. El 31 % de ellas no tenía fecha, mientras que el 11 % tenía una fecha anterior a 2017, el 11 % tenía una fecha de 2017 y el 47 % tenía una fecha posterior al 1 de enero de 2018. Las declaraciones de privacidad del sector de Consumidores son las más "actualizadas" (el 71 % tiene fechas de 2018 o posteriores), mientras que el sector de la Atención médica tiene las declaraciones más antiguas (solo el 19 % con fechas de 2018 o posterior). El uso de seguimiento de versiones para comparar las declaraciones de privacidad históricas disminuyó del 6 % en 2017 al 3 % este año, principalmente debido a cambios en la lista de organizaciones auditadas. Los sectores líderes en este sentido fueron el de Consumidores (12 %) e ISP/Hosts (10 %).

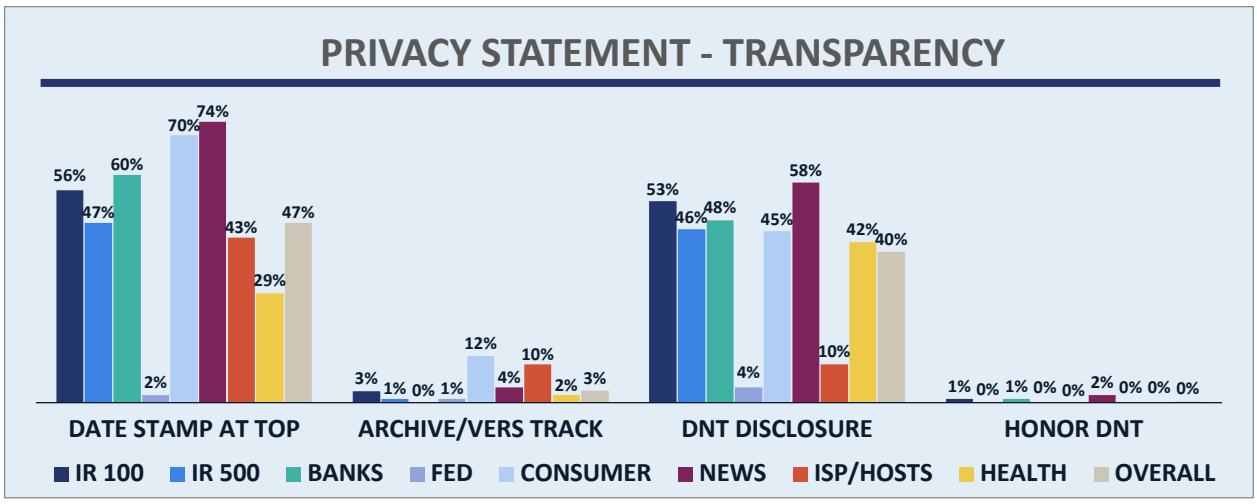


Gráfico 17. Transparencia de la declaración de privacidad por sector.

Dado que la divulgación de la política de "no rastrear" (DNT) de un sitio es actualmente un requisito legal en varias jurisdicciones, es importante que los sitios indiquen cuál es su política DNT y cumplan con la configuración DNT del navegador del usuario que visita el sitio. Como se muestra en el gráfico 17, la divulgación de la política DNT sigue en aumento. Ahora la adopción es del 40 % a comparación de un 37 % en 2017 y un 13 % hace cuatro años. Sin embargo, el cumplimiento de la configuración DNS ha disminuido mucho más, del 2 % en 2017 a menos del 0,5 % este año. En general, parece que el DNT está llegando a su fin. La mayoría de los navegadores ahora incorporan otros mecanismos para bloquear automáticamente rastreadores en línea (p. ej., mediante funciones, extensiones o plugins) o les dan a los usuarios el control directo sobre las listas de bloqueo. Recientemente Apple eliminó el soporte para DNT en la versión 12.1 del navegador Safari. El W3C ha declarado la terminación del proyecto y la nueva Ley de Privacidad del Consumidor de California (CCPA), que entra en vigor el 1 de enero de 2020, ya no lo exige.[5051] Dada esta tendencia, es posible que se retire al DNT como elemento de calificación en auditorías futuras, aunque una porción significativa de la puntuación de privacidad sigue ligada a los rastreadores de los sitios.

Legibilidad y divulgaciones

Diseñar la declaración de privacidad para los lectores previstos en lugar de para una audiencia versada en temas legales ha sido considerado por mucho tiempo como un cambio necesario por los profesionales de la privacidad. No solo es importante que el lenguaje usado sea apropiado para el nivel de lectura de los usuarios, sino que el diseño debe ayudar a maximizar la claridad. El gráfico 18 describe los resultados de los tres elementos de calificación: avisos cortos presentados por capas (base), íconos fáciles de navegar para los usuarios (bonificación) y presentar la declaración de privacidad en varios idiomas (bonificación). El uso de avisos presentados por capas aumentó significativamente del 29 % en 2017 al 47 % este año. El sector de Noticias estuvo a la cabeza con 71 %. El uso de íconos de duplicó del 1 al 2 %, y el sector de Consumidores lideró la lista con 7 %. La presentación de declaraciones de privacidad en varios idiomas realmente disminuyó del 7 al 4 %, lo que se puede atribuir principalmente a los cambios en la lista de organizaciones auditadas. La OTA cree que tener la declaración de privacidad en varios idiomas ayuda a mejorar la transparencia y la claridad. Se observó que, en algunos casos, el lenguaje mostrado en la declaración de privacidad era activado por la configuración del navegador o la ubicación de la dirección IP, por lo que es posible que la auditoría no haya recogido todos los idiomas ofrecidos.

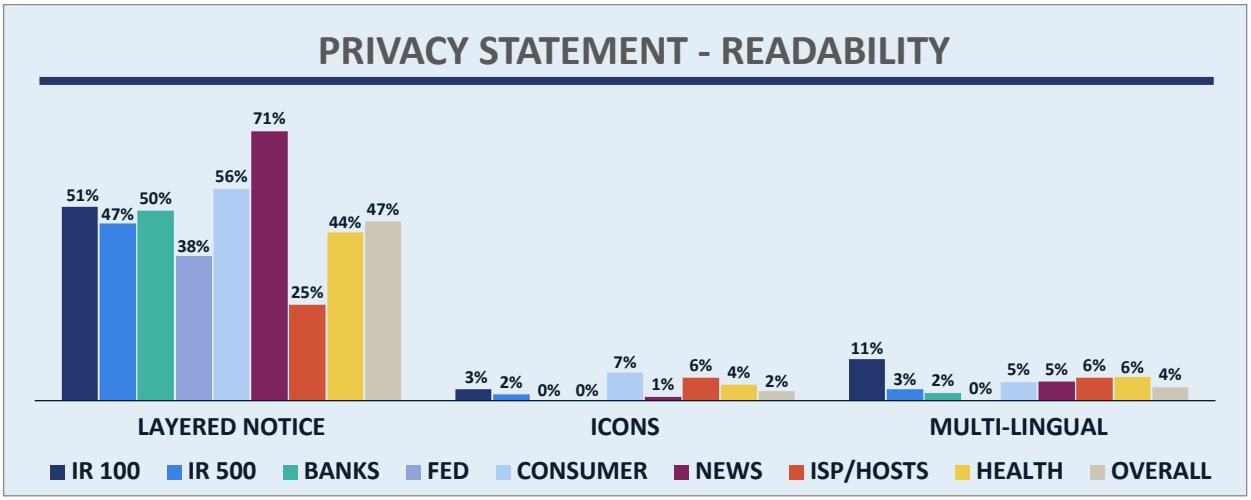


Gráfico 18. Claridad de la declaración de privacidad por sector.

Manejo de datos

Mantener y divulgar las prácticas de intercambio y retención de datos es un componente central de la declaración de privacidad. En la auditoría de 2018, el elemento de intercambio de datos se dividió en dos partes: una para el concepto de que los datos no se comparten excepto con terceros que ayudan a entregar el servicio, y otro para la comunicación de si se comparten datos con afiliados u otras entidades externas. El gráfico 19 presenta los resultados.

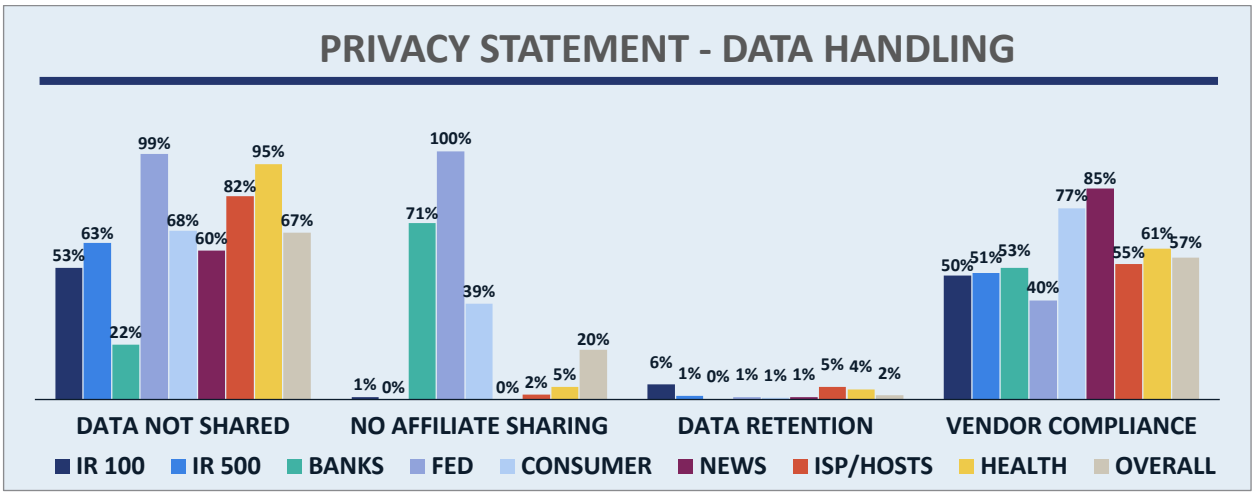


Gráfico 19. Tratamiento de datos de la declaración de privacidad por sector.

El 67 % de las organizaciones comunican si intercambian datos (p. ej., "no vendemos, alquilamos o compartimos datos, salvo a terceros que ayudan a entregar el servicio"), a comparación del 63 % en 2017, pero el lenguaje usado varía ampliamente. El lenguaje usado para comunicar sobre el intercambio de datos con afiliados varía aún más. Los sectores de Minoristas de Internet y Noticias obtuvieron un porcentaje de 0 % (es decir, todos comunican que comparten datos con afiliados) y el sector Federal obtuvo un 100 %. El lenguaje usado para hablar sobre la retención de datos se calificó con más rigurosidad este año para alinearse a los principios del RGPD. En 2017, la adopción fue del 49 % y se otorgaron puntos por casi cualquier referencia a la retención de datos. Este año, el lenguaje usado debía ser más específico e incluso indicar un plazo de tiempo en la medida de lo posible. El uso de lenguaje

que indicara que los proveedores también se sometían a las mismas políticas ("los terceros deben cumplir la declaración de privacidad de la organización") aumentó del 48 % en 2017 al 57 % este año, y el sector de Noticias llevó la delantera con 85 %.Dos sectores tuvieron un notable y marcado aumento en la adopción de este elemento: el sector de Bancos creció del 18 al 53 % y el de Noticias del 51 al 85 %.

Cumplimiento del RGPD

Este año, por primera vez, la auditoría incluyó seis variables que pretendían capturar aspectos claves de cumplimiento del RGPD. Es importante tener en cuenta que la mayoría de las organizaciones auditadas tienen sede en EE. UU. y puede que no necesiten cumplir directamente con el RGPD. Sin embargo, la OTA consideró que, dado el alcance del RGPD y su impacto en las leyes de privacidad mundiales, era importante empezar a medir si las organizaciones estaban cumpliendo con los principios clave del RGPD.

En primer lugar, se consideró que el 32 % de las declaraciones de privacidad eran fáciles de leer. El objetivo de este requisito del RGPD es que la mayoría de los usuarios deben poder comprender las declaraciones de privacidad con facilidad, especialmente en lo que se refiere a qué datos están siendo recopilados y compartidos. El sector de Bancos tuvo el porcentaje más alto de declaraciones fáciles de leer (47 %), mientras que el sector de Noticias tuvo el nivel más bajo con 8 %. Es claro que hay más trabajo por hacer en este punto, ya que más de dos tercios de las declaraciones de privacidad no cumplieron este objetivo.

El RGPD no indica exactamente cómo una organización debe transmitir qué datos recopila y por qué, simplemente dice que la empresa debe transmitir esta información a los usuarios de alguna manera. Con este ánimo, la mayoría de las organizaciones (95 %) comunicó de manera suficiente qué datos recopila y por qué motivo. El sector de Bancos lideró el camino con 99 %, mientras que los sectores Federal e ISP/Hosts tuvieron el nivel más bajo con 90 %.

Otros aspectos del RGPD tienen requisitos más específicos. Por ejemplo, el 70 % de las organizaciones auditadas identificó un medio para ponerse en contacto con el responsable de la protección de datos. El sector de Consumidores estuvo a la cabeza con 81 %.El sector Federal se rezagó en esta categoría con 38 %. Otro requisito del RGPD es que las organizaciones deben detallar el proceso para que los usuarios soliciten sus datos o qué datos pueden solicitar. Solo el 50 % de las organizaciones cumplió con este requisito, y el sector de Minoristas de Internet lideró la lista con 71 %.

Por último, hubo dos requisitos del RGPD con tasas de adopción muy bajas. El primero indica que las organizaciones necesitan divulgar si han recibido ciertos tipos de datos confidenciales de terceros (p. ej., datos biométricos, origen étnico o racial, opiniones políticas, creencias religiosas o filosóficas, entre otros). Dado que este requisito solo aplica en casos limitados, la baja adopción no es necesariamente un problema. Solo el 1 % de las organizaciones abordó este tema en su declaración de privacidad, y el sector de Atención médica estuvo a la cabeza con 4 %. El segundo requisito exige que las organizaciones identifiquen con qué categorías de terceros comparten datos; por lo tanto, esto debe aplicar a cualquier organización que comparta datos. Menos del 1 % de las organizaciones cumplió con este requisito.

Seguimiento a través de distintos dispositivos

A partir de la auditoría de 2017, en respuesta al informe de 2017 del FTC acerca del seguimiento a través de diversos dispositivos, se ha recogido la divulgación de este tipo de seguimiento (p. ej., a través de computadora, teléfono, tablet, etc.) y recibe puntos de bonificación. Este año, el 48 % de los sitios

incluía este tipo de divulgación, un incremento en comparación con el 44 % de 2017. Se debe tener en cuenta que el seguimiento a través de diversos dispositivos puede tener beneficios, que incluyen una mejor experiencia para el usuario cuando cambie de dispositivo y beneficios de seguridad para los usuarios que inician sesión desde otros dispositivos o direcciones IP, pero también plantea problemas de privacidad. El sector de Noticias tuvo la mayor adopción (91 %) seguido del sector de Consumidores (80 %), mientras que el sector Federal tuvo la menor adopción (12 %).

Registros WHOIS

Cuando una empresa registra un nombre de dominio, la Corporación de Internet para la Asignación de Nombres y Números (ICANN) exige que envíen su información de contacto. La información se publica en la base de datos de WHOIS, que está a disposición del público, siempre que el registro no sea privado. La llegada del RGPD ha complicado los listados WHOIS porque se ha eliminado la información de contacto personal de muchos registros por razones de privacidad. Muchas organizaciones han ido un paso más allá y ocultado toda su información (incluso a nivel organizacional), lo que hace difícil determinar quién realmente es propietario del dominio.

Como resultado, los registros privados (definidos por la capacidad de determinar qué entidad es propietaria del dominio) se incrementaron este año. En general, el 78 % de los registros eran públicos (en comparación del 87 % en 2017). Un análisis más detallado revela que el 7 % de los registros "privados" estaban vinculados directamente con información eliminada en virtud del RGPD, por lo que el registro público realmente asciende a 85 %.Los sectores que más usaron los registros WHOIS privados fueron ISP/Hosts (32 %), Bancos (29 %) y Atención médica (28 %). Los registros privados limitan la capacidad de los consumidores para descubrir quién es el propietario de un sitio, obstaculiza la transparencia y puede reducir la confianza de los consumidores, por no mencionar que un tercero no podrá contactar al propietario del sitio si detecta una vulnerabilidad. Sin embargo, los registros privados son una práctica válida y legítima cuando se registra un dominio para una empresa o producto nuevos o para un esfuerzo promocional que aún es secreto, pero deberían hacerse público una vez lanzados.

Incidentes de pérdidas de datos y acuerdos normativos

Las violaciones de datos y los acuerdos normativos pueden indicar una deficiencia en la seguridad y privacidad de los datos y las prácticas comerciales. Como tales, pueden tener un gran impacto en la reputación de una organización y la confianza de los consumidores, a la vez que ponen en riesgo la privacidad e identidad de los usuarios. Al mismo tiempo, es importante reconocer que ninguna medida de seguridad es perfecta y que un adversario persistente con tiempo y recursos suficientes puede atacar casi cualquier organización. Según lo expuesto en el Informe de tendencias en incidentes cibernéticos y violaciones de datos de 2018 de la OTA, en 2017 se registraron más de 159.700 incidentes de pérdidas de datos en el mundo.[52]

La auditoría de este año incluye datos adicionales de una variedad de fuentes que brindan un panorama más completo de estos incidentes. El análisis de la OTA reveló que el 15 % de las organizaciones auditadas experimentaron uno o más incidentes, a comparación del 13 % en 2017 y el 5 % en 2016. El número de registros perdidos osciló de entre uno solo hasta más de 150 millones. Dado que los incidentes no son todos iguales, no se penalizó a las organizaciones con una pérdida acumulativa de un máximo de 1000 registros durante el período de auditoría, mientras que la penalización por la pérdida de más de 1000 registros se incrementó proporcionalmente al volumen perdido. Si se tiene en cuenta este ajuste, solo el 12% de las organizaciones fueron penalizadas por una violación de datos. El sector de

Consumidores tuvo el mayor porcentaje de violaciones de datos (34 %), seguido por el de Atención médica (30 %).

En el frente regulatorio, el 2 % de las organizaciones auditadas recibió una penalización por demandas o sanciones iniciadas este año con relación a la protección del consumidor (igual al 2017), y el sector de Consumidores estuvo a la cabeza con 12 %. La evaluación incluyó sanciones del FTC, FCC, CFPB, agencias estatales e internacionales. El enfoque se centró en sanciones relacionadas con acciones de protección al consumidor que involucraran seguridad y privacidad, y no incluyeron sanciones relacionadas con fusiones y adquisiciones o asuntos laborales.

Conclusión

Al igual que en años anteriores, la Auditoría de confianza en línea y cuadro de honor tiene tres objetivos principales:

- Promover buenas prácticas para mejorar la seguridad de los sitios, la protección de los datos y las prácticas de privacidad.
- Reconocer la excelencia en prácticas responsables de seguridad, privacidad y protección al consumidor.
- Proporcionar a los consumidores una mayor transparencia con respecto a las prácticas de seguridad y privacidad de los sitios que visitan.

La auditoría de 2018 registró niveles récord en muchas áreas: el mayor número de organizaciones en el cuadro de honor (del 52 % en 2017 al 70 % en 2018), los más altos niveles de adopción de autenticación de correo electrónico (el 76 % ha configurado SPF y DKIM en el dominio de nivel superior), y los más altos niveles de cifrado de Internet (el 73 % usa cifrado TLS oportunista para correo electrónico y el 93 % cifra todas las sesiones en su sitio web). Se logró todo esto a pesar de que los criterios metodológicos eran más estrictos, de que la puntuación era más ajustada y de que se dio mayor ponderación a prácticas clave de protección al consumidor, seguridad del sitio y privacidad.

Ciertos sectores brillaron este año. Las agencias del gobierno federal se recuperaron luego de obtener malos resultados en la auditoría de 2017, para ir adelante de todos los sectores con un 91 % de ellas en el cuadro de honor. Las organizaciones de Noticias/Medios continuaron su crecimiento casi geométrico en el cuadro de honor, donde el 78 % de ellas se ubicó. El recientemente añadido sector de la Atención médica llegó en último lugar con un 57 % (que en años anteriores se hubiera considerado un resultado sólido), principalmente por su falta de autenticación de correo electrónico.

En muchas áreas se adoptaron las mejores prácticas casi en su totalidad, a un nivel de 90 % o superior. Y aunque esto debería ser motivo de celebración, las organizaciones que aún no han adoptado estas prácticas básicas ampliamente aceptadas deben priorizar su implementación.

En otras áreas hay tendencias preocupantes. A pesar del mayor conocimiento y sensibilidad a las cuestiones de privacidad impulsados por el RGPD, la Ley de Privacidad del Consumidor de California, y las muy publicitadas fallas de privacidad de grandes empresas, las declaraciones de privacidad han mejorado muy poco. La mayoría de las organizaciones han obtenido un puntaje de menos del 50 % en la parte de la auditoría sobre declaraciones de privacidad. Es especialmente preocupante el hecho de que se estén compartiendo datos con terceros afiliados y esto no esté especificado. La comparación inicial con los requisitos exigidos por el RGPD reveló un amplio rango de adopción, del 1 % al 95 %, dependiendo del requisito. Esto deberá ser abordado a medida que el ambiente normativo, ya sea a nivel estatal o mundial, continúe evolucionando.

De cara al futuro, las organizaciones tienen muchas oportunidades para limitar el impacto de vulneraciones masivas de datos y detener las prácticas cuestionables de recopilación y seguimiento de datos. Muchos propietarios de sitios ahora evitan que los usuarios usen pares de nombre de usuario/contraseña que han sido vulnerados y están implementando la autenticación de múltiples factores para limitar el impacto de las contraseñas vulneradas. También se están incorporando capacidades similares en los navegadores. Además, debido a que muchos usuarios de sitios web no se

están esforzando por limitar la recopilación y el seguimiento de datos, otros han tratado de cubrir este vacío. La mayoría de los navegadores ahora incorporan algún nivel de bloqueo de anuncios y rastreadores.

La mejora de la seguridad y la privacidad es una responsabilidad colectiva de todas las partes interesadas, y cada uno de nosotros debe cumplir con su parte para mantener la confianza en Internet. La OTA colabora con todas las partes interesadas en los sectores público y privado para mejorar el estado de Internet, proporcionando una plataforma de confianza para la innovación. Para obtener información actualizada, visite https://otalliance.org/TrustAudit.

Resultados de la Auditoría de Confianza en Línea y Cuadro de Honor año 2018

La Online Trust Alliance de Internet Society lleva a cabo una Auditoría anual de confianza en línea y cuadro de honor; este es el estándar de hecho para reconocer la excelencia en la protección del consumidor, la seguridad de los datos y las prácticas responsables de privacidad en línea.

El más alto que se haya registrado, impulsado principalmente por mejoras en la autenticación y encriptación de correos electrónicos

CUADRO DE HONOR POR SECTOR

GOBIERNO FEDERAL DE EE. UU.	91%	(el que mejoró más, por encima del 39 % en 2017)
SERVICIOS AL CONSUMIDOR	85%	
NOTICIAS Y MEDIOS DE INFORMACIÓN	78%	(continuó con su rápido crecimiento año tras año: 4 %, 8 %, 23 %, 48 %, 78 %)
BANCOS	73%	(casi triplicó su crecimiento desde 27 % en 2017)
MINORISTAS DE INTERNET	65%	
ISP, OPERADORAS, HOSTERS Y PROVEEDORES DE CORREO ELECTRÓNICO	63%	
ATENCIÓN MÉDICA	57%	(nuevo este año)

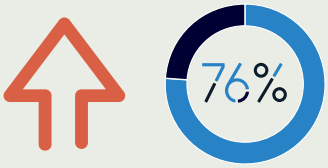
OTA
Online Trust Alliance
an Internet Society initiative

https://otalliance.org/2018HonorRoll

Aspectos Destacados por Categoría año 2018

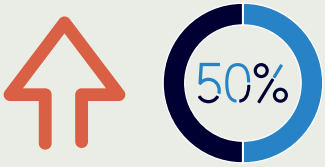
DOMINIO (TLD), MARCA Y PROTECCIÓN DEL CONSUMIDOR

Niveles récord de autenticación de correo electrónico



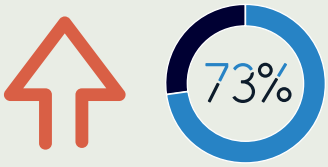
El 76 % utiliza tanto SPF como DKIM en el dominio de primer nivel

SPF y DKIM evitan correos electrónicos falsos/maliciosos.



El 50 % tiene un registro DMARC

DMARC ofrece instrucciones acerca de cómo manejar mensajes que no pasan la autenticación.



El 73 % usa TLS oportunistas

TLS encripta mensajes entre servidores de correo.

SEGURIDAD DE SITIOS, SERVIDORES E INFRAESTRUCTURA

Sesiones web encriptadas

52% → 93%

Salto enorme del 52 % obtenido en 2017
El 93 % usa HSTS/SSL siempre activo/HTTPS en todas partes

6% Solo el 6 % usa la Autorización de la Autoridad de Certificación (CAA)

CAA limita el uso indebido de certificados.

11% Solo el 11 % usa mecanismos de divulgación de vulnerabilidades

Permite informar errores y problemas de seguridad.

PRIVACIDAD, TRANSPARENCIA Y DIVULGACIÓN

70

El puntaje combinado cayó a 70 (el año pasado fue de 73) como resultado de un sistema de calificación más estricto ante las iniciativas GDPR, CCPA y otras iniciativas legislativas.

77%

usan rastreadores web que comparten información con terceros.

15%

El 15 % experimentó una o más pérdidas de datos o incidentes de violaciones de seguridad.

https://otalliance.org/2018HonorRoll

Aspectos Destacados del Sector año 2018

SERVICIOS AL CONSUMIDOR

Este año incorporaron servicios de pago y servicios de streaming de video.

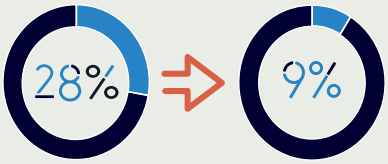
96% Máxima adopción de la autenticación de correo electrónico (96 %).

76 puntaje general máximo de privacidad (76).

43% uso máximo de informes de vulnerabilidad (43 %, el más cercano es de 25 %).

34% Tasa de violaciones más alta (34 %).

MINORISTAS DE INTERNET



Mejora significativa en la autenticación de correos electrónicos (las fallas cayeron de 28 % a 9 %) aunque la adopción de DMARC fue la más baja (34 %).

50% Las fallas de privacidad se incrementaron casi en 50 % (a 23 %) debido a la participación de terceros.

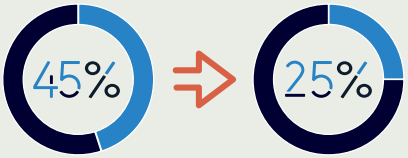
NOTICIAS Y MEDIOS DE INFORMACIÓN

Este año se incorporaron sitios deportivos.

Se continuó con mejoras importantes en todas las áreas, lo que dio lugar a otro salto en el logro en el cuadro de honor (a 78 %).

x4 Casi se cuadriplicó el uso de sesiones siempre encriptadas (de 26 % a 93 %).

ISP, OPERADORAS, HOSTERS Y PROVEEDORES DE CORREO ELECTRÓNICO



Mejora importante en la autenticación de correos electrónicos (las fallas cayeron de 45 % a 25 %).

1.° 11% Mayor adopción de TLS 1.3

2.° 20% Segundo máximo respaldo a IPv6

GOBIERNO FEDERAL

Logro máximo general en el cuadro de honor (91 %) – un cambio importante con respecto al último informe en el que habían caído de 46 % a 39 %.

94 Puntaje máximo de seguridad del sitio (94).

1.° 93% Mayor adopción de DMARC (93 %) y aplicación de políticas DMARC (83 %).

46% Mayor adopción de IPv6 (46 %).

BANCOS

45% → 13% Mejora importante en la autenticación de correos electrónicos (las fallas cayeron de 45 % a 13 %).

2.° 84% Segundo mayor uso tanto de SPF como de DKIM en el dominio de primer nivel (84 %, una mejora frente a apenas 30 % en la última auditoría).

1.° 71% Mayor uso de certificados de validación extendida para sitios web (71 % - más del doble que el siguiente sector más cercano).

ATENCIÓN MÉDICA

NEW

Lo nuevo este año, representa la combinación de importantes farmacias, laboratorios de ensayos, aseguradoras de salud y cadenas de hospitales.

57% El logro general más bajo en el cuadro de honor (57 %), debido principalmente a la falta de autenticación de correos electrónicos (falla del 35 % en esta área).

2.° 73 Segundo puntaje más alto en privacidad (73). Menor adopción de sesiones siempre encriptadas (82 %).

https://otalliance.org/2018HonorRoll

Anexo B: Metodología y calificación

Los criterios y la metodología de la auditoría evolucionan cada año para reflejar los avances en los estándares de seguridad, las normas de privacidad y la implantación en el mundo real. Anualmente, la OTA solicita activamente la opinión de los usuarios de Internet a través de un llamamiento público de 60 días que se hace normalmente los primeros días de septiembre.[53]Además, se consulta a varias agencias gubernamentales de EE. UU. y organizaciones de estándares de la industria. Tras su revisión, el Comité de Planificación de la Auditoría de Confianza de la OTA incorpora algunas de las directivas básica de seguridad y privacidad, incluidos los principios de prácticas honestas de información (Fair Information Practice Principles, FIPP), las normas del NIST y las respaldadas por el programa Deploy360 de Internet Society.[54] Con esta combinación de datos, la ponderación y las puntuaciones se reexaminan anualmente y se reasignan para hacer frente a la evolución del panorama de amenazas, el entorno normativo y la facilidad de implantación. El resultado final se centra en las buenas prácticas aceptadas que reflejan la implantación en el mundo real, cerrando la brecha entre los estándares y las comunidades empresariales. La metodología final para la auditoría de este año se publicó en agosto de 2018 y se comunicó ampliamente para permitir que las organizaciones reevalúen sus prácticas y optimicen sus resultados.[55]

La auditoría de confianza en línea incluye un análisis compuesto que se centra en tres categorías principales:

- Protección al consumidor (protección del DNS, los dominios y la marca)
- Seguridad del sitio, el servidor, la aplicación y la infraestructura
- Privacidad, transparencia y divulgación

Los sitios podían recibir 300 puntos base (un máximo de 100 puntos por categoría) y hasta 60 puntos de bonificación (el 20 % de la puntuación base) por implementar las mejores prácticas emergentes. Además, las organizaciones podrían perder puntos por sanciones, violaciones de datos, vulnerabilidades observadas y otras deficiencias clave.

Para formar parte del cuadro de honor, los sitios debían recibir una puntuación compuesta de al menos el 80 % de los puntos básicos *y* **una puntuación de al menos 60** en cada una de las tres categorías principales. El límite inferior se elevó a 60 en 2017 para reconocer que la "seguridad solo es tan fuerte como el eslabón más débil" y que los sitios se construyen sobre una "cadena de confianza".

La auditoría de 2018 ha sido impulsada por análisis técnicos y datos suministrados por más de una docena de organizaciones. Sin su ayuda y apoyo, esta auditoría y telemetría no serían posibles. El muestreo de datos se completó entre el 10 de diciembre de 2018 y el 31 de enero de 2019. Las organizaciones que proporcionaron datos incluyeron Agari, Disconnect, dmarcian, ImmuniWeb, Infoblox, Internet.nl, Microsoft, Mozilla, SSL Labs, Sucuri, Symantec, Valimail y Verisign. Se obtuvieron datos adicionales de fuentes públicas de datos como BugCrowd, Google, HackerOne, Open Bug Bounty y Twitter, entre otros. Es importante señalar que la configuración o las prácticas de los sitios pueden haber cambiado desde el muestreo y que los datos solo reflejan los hallazgos durante este período de tiempo.

Protección al consumidor (protección del DNS, los dominios y la marca)

El correo electrónico sigue siendo el vector preferido para ataques de vulneración de correos electrónicos empresariales (BEC, Business Email Compromise), usurpación de identidad y credenciales,

apropiación de cuentas bancaria y distribución de software malicioso.[56] El FBI informa que desde 2013, los fraudes de BEC generaron 12.500 millones de dólares en pérdidas financieras, y la mayoría de esos ataques pudieron haberse evitado.[57] Durante la última década, la OTA ha promovido la autenticación de correo electrónico de un extremo a otro para ayudar a detectar y bloquear correos electrónicos maliciosos y falsificados en todos los dominios y subdominios gestionados por una organización. La adopción ayuda a proteger a los consumidores y destinatarios de correo de la distribución de *malware*, keyloggers (registradores de teclas) y otras amenazas relacionadas como secuestro de datos (*ransomware*), *cryptomining* (usar los recursos informáticos para minar criptomonedas) y apropiaciones de cuentas, a la vez que se protege la reputación de la marca.

- Autenticación de correo electrónico. Marco de directivas de remitente (SPF, Sender Policy Framework) y DomainKeys Identified Mail (DKIM) en los dominios de primer nivel y los subdominios de correo electrónico. La auditoría de 2018 aumenta la ponderación de la autenticación de dominios de primer nivel (los que los usuarios reconocen y que se suelen falsificar) y reduce la puntuación para los subdominios delegados separados. Además, los sitios con registros SPF inválidos recibieron un puntaje parcial o bien ninguno: *parte de la puntuación base* [58]
- Autenticación de mensajes, informes y conformidad basada en dominios (DMARC). No se otorgaron puntos por registros DMARC con política de "moderador" (p=ninguno) y que no emitían informes (RUA o RUF). Estos registros DMARC se llaman "descubiertos" porque no protegen a los consumidores ni a la marca, ya que las redes receptoras no responden a la política y la marcas no reciben la autenticación ni informes de abuso. Se aumentó la ponderación por el uso de la política de "rechazo", *parte de la puntuación base*.[59]
- Implementación de Seguridad de la capa de transporte (TLS, Transport Layer Security) "oportunista" para correo electrónico. Se aumentó la ponderación en 2018: *puntos de bonificación* [60]
- Bloqueo de dominio: *penalización si no está bloqueado*.
- Extensiones de seguridad del sistema de nombres de dominio (DNSSEC): *puntos de bonificación*.[61]
- Implementación del protocolo de Internet versión 6 (IPv6) para el acceso al servidor web: *puntos de bonificación*.[62]
- Autenticación multifactor. Aunque en la auditoría de 2017 se otorgaron puntos por la autenticación multifactor, esto no se repitió en esta auditoría debido a la insuficiencia de fuentes de datos en todos los sectores.

Seguridad de sitios, servidores e infraestructura

Mejores prácticas para proteger los datos en tránsito y los recopilados por los sitios web, y para prevenir ataques maliciosos a los dispositivos de los clientes. Los sitios podían obtener un máximo de 100 puntos base, siempre que no obtuvieran una calificación menor de 60 en cada criterio fundamental de SSL/TLS (cifrados, intercambio de claves o soporte de protocolos). Se analizaron los sitios con varias herramientas para buscar vulnerabilidades conocidas, configuración HSTS y certificados incompatibles.[63, 64] En 2017 se amplió la seguridad de los servidores para incluir la seguridad de las aplicaciones, la gestión de vulnerabilidades y la reputación de IP. Se amplió aún más en 2018 para incluir evaluaciones sólidas de políticas de seguridad de contenido y prevenciones relacionadas con contenidos de terceros en los sitios. En 2018 se incorporó la compatibilidad con Always On SSL en la calificación básica.[65]

Puntos de bonificación/penalización

- Certificados SSL con validación extendida (SSL con EV): *puntos de bonificación*[66]
- Autorización de la Autoridad de Certificación (CAA), nueva en 2018: *puntos de bonificación*
- Cortafuegos de aplicación web: *puntos de bonificación*
- Pruebas para detectar ataques XSS y iFrame, malware, enlaces maliciosos: *penalización si existen estas amenazas*
- Mecanismo de informe de vulnerabilidades y fallas. A partir de 2017, los sitios ganan puntos de bonificación si tienen mecanismos de presentación de informes. Estos pueden incluir formularios en línea y el uso de programas externos de recompensas por informar fallas. Los datos se analizaron mediante búsquedas en línea usando palabras clave, así como buscando programas externos de recompensa por el informe de fallas como HackerOne y Bugcrowd[67][68]: *puntos de bonificación*

Privacidad, transparencia y divulgación

Las mejores prácticas que todas las organizaciones deben seguir incluyen notificar a los usuarios de forma clara y transparente sobre los datos que se recopilan, rastrean y comparten con terceros. La puntuación de privacidad se compone de un máximo de 100 puntos que cubren la inclusión de divulgaciones apropiadas, la estructura de la declaración de privacidad (incluyendo la adopción de los principios generalmente aceptados de prácticas honestas de información [FIPP]) y el seguimiento y la recopilación de datos por parte de terceros.[69] Analistas de la OTA/Internet Society leyeron las declaraciones de privacidad y las calificaron.

Declaración de privacidad: 55 puntos posibles. Los sitios pueden recibir el máximo de puntos si se adhieren a las siguientes pautas:

- Enlace fácil de encontrar en la página de inicio
- Fecha de modificación de la declaración de privacidad en la parte superior de la página
- Divulgación sobre el tratamiento de la configuración "no rastrear" (DNT) del navegador
- Declaración de la política de retención de datos que indique un plazo específico (el plazo fue añadido en 2018)
- Los datos personales no se comparten, salvo con los terceros que prestan el servicio
- Los datos personales no se comparten con afiliados o socios (se separó del criterio básico de intercambio de datos en 2018)
- Cumplimiento de los proveedores. Declaración que establece que los proveedores de servicios deben cumplir con la declaración de privacidad de la organización y tienen prohibido usar o compartir los datos para cualquier fin que no sea la prestación de servicios en nombre de la organización.
- Seguimiento de versiones (o acceso a versiones anteriores), incluye la publicación de los cambios realizados (antes de 2018 otorgaba puntos de bonificación)
- Diseño por capas y/o con poca anticipación

- Cumplimiento de la Ley de Protección de la Privacidad Infantil en Internet (COPPA) o normas relacionadas.[70]

Seguimiento de terceros en el sitio: es posible que los sitios sin rastreadores de terceros (con la excepción de análisis anónimo) obtengan un máximo de 45 puntos. En los casos en que se encontraron rastreadores que comparten datos con terceros, se redujeron puntos.[71]

Puntos de bonificación

- Uso de íconos fáciles de identificar para facilitar la navegación de los usuarios
- Declaración traducida en diferentes idiomas en los casos en que el inglés pueda ser un "segundo idioma"
- Respeto a la configuración "no rastrear" (DNT) del navegador del usuario
- Divulgaciones sobre seguimiento a través de distintos dispositivos (se añadió en 2017)[72]
- Implementación de sistemas de gestión de etiquetas o soluciones de privacidad para gestionar las etiquetas de terceros

Puntos de penalización

- Vulneración de datos: cuando más de 1000 registros fueron vulnerados. En la auditoría de 2018, la penalización se incrementó proporcionalmente según la cantidad de registros vulnerados (*penalización si se produjo un incidente entre el 1 de junio de 2017 y el 31 de diciembre de 2018*).
- Las sanciones de la Comisión Federal de Comercio (FTC), la Comisión Federal de Comunicaciones (FCC), la Oficina de Protección Financiera del Consumidor (CFPB)[73] y otras sanciones estatales o internacionales (*penalización si la sanción se aplicó entre el 1 de junio de 2017 y el 31 de diciembre de 2018*).
- Registro WHOIS público en lugar de privado: *penalización si es privado*

Anexo C: Cuadro de honor con los 50 mejores de 2018

Sector	Organización	Sector	Organización
C	1040.com	C, **R**	**Google Play**
H	**23 and Me**	O	Internet Society
C	Airbnb	C	Lyft
C	Amazon Payments	G	Administración Nacional Oceánica y Atmosférica (NOAA)
R	Apple Inc.	C	Netflix
C	Blogger	C, O	Norton LifeLock
R	Casper	G	Oficina de Administración de Personal (OPM)
H	Costco Pharmacy	**O**	**Online Trust Alliance**
G	Departamento de Agricultura (Servicio de inspección y seguridad alimentaria)	**C**	**PayPal**
G	Departamento de Salud y Servicios Sociales (Medicare)	R	Petco Animal Supplies Inc.
G	Departamento de Salud y Servicios Sociales (Healthcare.gov)	C, N	Reddit
G	Departmento de Hacienda	G	Comisión de Bolsa y Valores (SEC)
C	DocuSign	C	Snapchat
G	Comisión Federal de Comunicaciones (FCC)	G	Administración del Seguro Social (SSA)

G	**Agencia Federal para el Manejo de Emergencias (FEMA)**	C	Square Cash
G	Comisión Federal de Comercio (FTC)	I	Sucuri
B	**First National Bank of Omaha**	B	TD Bank, National Association
R	Fitbit Inc.	B	The Huntington National Bank
C	Flickr	C	Tinder
R, O	Gap Inc.	O	TrustSphere
G	Administración de Servicios Generales (GSA)	C, O	Twitter
I	**Google Cloud**	C	UpWork
C	Google Drive	G	Guardia Costera de los Estados Unidos
N	**Google News** 🔷	R	Walmart Inc.
C	Google Pay	C	YouTube

Códigos de sectores: C – Cosumidores, B – Bancos, G – Gobierno federal de EE. UU., H – Atención médica, I – ISP/Hosts, N – Noticias/Medios, O – Socios de OTA/Internet Society, R – Minoristas de Internet. Como se ha señalado, las organizaciones pueden pertenecer a varios segmentos.

Aquellas que han obtenido las mejores puntuaciones en cada sector están destacadas en negrita. Aquella que obtuvo la puntuación global más alta está marcada con 🔷.

Anexo D: Miembros del cuadro de honor 2018

500 Minoristas de Internet de 2018 – Cuadro de honor

65 % en el cuadro de honor – 31 % reprobado – 14 % en los "Mejores"

- ❷ 1-800 Contacts Inc.
- 1-800-Flowers.com Inc.
- 1Sale
- ❷ Abercrombie & Fitch Co.
- ❷ AC Lens
- adidas AG
- Adorama Camera Inc.
- ❷ Adore Me Inc.
- Aéropostale Inc.
- AJ Madison Inc.
- ❷ Albertsons Inc.
- Aleph Objects Inc.
- ❸ Alex and Ani LLC
- ❼ Alibris Inc.
- Allied Electronics
- ❼ Amazon.com Inc.
- ❼ American Greetings Corp.
- American Standard Brands
- AmeriMark Direct LLC
- ❹ APMEX Inc.
- ❸ **Apple Inc.**
- Aquasana Inc.
- Art.com Inc.
- Ascena Retail Group
- ❷ Ashley Stewart Inc.
- ASOS Plc Holdings
- ❷ AutoZone Inc.
- ❷ B&H Foto & Electronics Corp.
- ❷ Backcountry.com
- Balsam Brands
- Barcodes Inc.
- Bare Necessities
- ❷ Barnes & Noble Booksellers Inc.
- Barneys New York Inc.
- ❼ Bass Pro Shops
- ❷ BaubleBar Inc.
- BeachCamera.com
- bebe stores Inc.
- Belk Inc.
- ❻ Best Buy Co. Inc.
- ❷ Better World Books
- Big 5 Corp.
- Birchbox Inc.
- Bissell
- ❹ BJ's Wholesale Club
- Black & Decker Inc.
- Black Diamond Equipment Ltd.
- Blain Supply Inc.
- ❷ Blue Nile Inc.
- ❸ Bluefly Inc.
- Bob's Discount Furniture LLC
- Boohoo.com plc
- ❸ Bookbyte
- Boot Barn Inc.
- ❷ Boscov's Department Store LLC
- Boston Proper LLC
- ❸ Boxed Wholesale
- Brilliant Earth LLC
- Brooklinen
- Brooks Brothers
- ❻ BuildASign.com
- ❹ BuildDirect Technologies Inc.
- ❹ Burberry Ltd.
- CafePress Inc.
- Camping World Inc.
- ❷ Carter's Inc.
- ❷ **Casper**
- Chanel S.A.
- ❸ Chico's FAS Inc.
- ❷ Christopher & Banks Corp.
- Classic Firearms
- ❸ Code42 Software Inc.
- Columbia Sportswear Co.
- Concept2 Inc.
- Cool Stuff Inc.
- ❹ Costco Wholesale Corp.
- Crocs Inc.
- Crucial Technology
- ❹ Crutchfield Corp.
- ❷ CustomInk
- Cutlery and More LLC
- ❷ CVS Caremark Corp.
- ❸ Cymax Stores Inc.
- Databazaar.com
- dbrand
- Deckers Brands
- ❷ DeepDiscount.com
- ❷ Dell Inc.
- Destination XL Group Inc.
- Dick Blick Holdings Inc.
- ❷ Diesel
- Digi-Key Electronics
- ❹ Dollar Shave Club
- Dollar Tree Inc.
- ❷ Dolls Kill
- ❷ Dover Saddlery Inc.
- DrJays.com
- Duluth Trading Company
- Dyson Ltd.
- eCampus.com
- ❹ Eddie Bauer LLC
- ❹ Entertainment Earth Inc.
- ❻ Etsy Inc.
- Everlane Inc.
- Evine Live Inc.
- ❷ Fanatics Inc.
- Fashion Nova
- ❸ **Fitbit Inc.**
- Flight Club
- Floor & Décor Outlets of America Inc.
- Focus Camera Inc.
- ❸ Follett Higher Education
- ❷ Foot Locker Inc.
- ❹ Forever 21
- ❹ Fossil Inc.
- FragranceNet.com Inc.
- FreshDirect LLC

Negrita: 50 Mejores ◆Mayor puntuación en el sector ❷❸❹❺❻❼Años consecutivos en el cuadro de honor

500 minoristas de Internet de 2018 – Cuadro de honor, continuación

Full Compass Systems Ltd.
Furniture.com Inc.
6 GameFly Inc.
Gander Mountain
4 **Gap Inc.**
Gardeners Supply Company
Gear Patrol LLC
GlassesUSA LLC
Global Equipment Company Inc.
Glossier Inc.
GNC Holdings Inc.
2 Godiva Chocolatier Inc.
3 **Google Play** ◆
3 GoPro Inc.
GrabAGun.com
Grizzly Industrial Inc.
Groupon Goods
Guess Inc.
Hallmark Cards Inc.
HanesBrands Inc.
Hanover Company Store LLC
3 Harry's Inc.
Helix Sleep
Herman Miller Inc.
3 hhgregg Appliances Inc.
Hobbico
2 Home Chef
2 Hot Topic Inc.
HP Home & Home Office Store
4 iHerb Inc.
4 IKEA
2 Indigo Books & Music Inc.
Inditex Group
J. Crew Group Inc.
J. Jill
2 J.C. Penney Co. Inc.
2 J.Hilburn Inc.
Jabra
6 JackThreads Inc.
JEGS High Performance Inc.
JetPens.com
JM Bullion Inc.
4 Joann.com
KEH Inc.
2 Keurig Green Mountain Inc.
Klipsch Group Inc.
2 Lakeshore Learning
3 Lands' End
LD Products Inc.
2 Leesa Sleep LLC
2 Lenovo Group Ltd.
Leslies Poolmart Inc.
Levi Strauss & Co.
4 LifeWay Christian Resources
2 LightIntheBox Ltd.
2 Living Spaces
6 LivingSocial Inc.
Loot Crate Inc.
3 Lowe's Cos. Inc.
LuckyGunner LLC
LuLuLemon Athletica Inc.
2 LuLu's Fashion Lounge Inc.
Lumber Liquidators Inc.
LVMH
M. Gemi
2 Macy's Inc.
Mattel
2 Mattress Firm Inc.
Meijer Inc.
2 Michael Kors Holdings Ltd.
Micro Electronics Inc.
2 MidwayUSA Inc.
MLB Advanced Media
Moda Operandi Inc.
4 Monoprice Inc.
Monrovia
2 MotoSport LLC
Mouser Electronics Inc.
MSC Industrial Supply Co. Inc.
2 MVMT Watches
NakedWines.com Inc.
4 Liga Nacional de Hockey (NHL)
3 NatureBox Inc.
2 Nebraska Furniture Mart
4 New Avon LLC
2 New Balance Athletics Inc.
New York & Co. Inc.
5 Newegg Inc.
5 Nike Inc.
2 Nine West Holdings Inc.
5 Nordstrom Inc.
2 Office Depot Inc.
4 OmahaSteaks.com Inc.
OMEGA Engineering Inc.
OpticsPlanet Inc.
3 O'Reilly Auto Parts
2 Otto Group
OvernightPrints.com
7 Overstock.com Inc.
Painful Pleasures Inc.
Palmetto State Armory
2 Panasonic Corp.
2 Patagonia
7 Payless ShoeSource Inc.
PC Connection Inc.
Performance Bicycle
4 **Petco Animal Supplies Inc.**
3 PetFlow
2 PetSmart Inc.
4 Pier 1 Imports Inc.
3 Power Equipment Direct Inc.
Primary Arms LLC
Pro:Direct
3 PropertyRoom.com Inc.
Provo Craft & Novelty Inc.
2 Purple
2 Qurate
4 REI
2 Reitmans (Canada) Ltd.
Rent the Runway Inc.
2 Replacements Ltd.
3 Restoration Hardware
RevZilla Motorsports LLC
2 Richline Group
RobotShop Inc.
6 RockAuto LLC
Rockler Companies Inc.
Rooms To Go Inc.
2 rue21 Inc.

Negrita: 50 Mejores ◆Mayor puntuación en el sector ❷❸❹❺❻❼Años consecutivos en el cuadro de honor

500 Minoristas de Internet de 2018 – Cuadro de honor, continuación

Rural King
3 Saatva Inc.
Samsonite International S.A
Scholastic Inc.
School Specialty Inc.
2 Sears Holdings Corp.
Sears Hometown and Outlets Stores
Sennheiser Electronic GMBH & Co.
4 Shindigz
Shoe Carnival Inc.
Shoes of Prey Inc.
ShoppersChoice.com LLC
Shutterfly Inc.
Signet Jewelers Ltd.
Silver Star Brands
Skinit Acquisition LLC
Sonos Inc.
6 Spiraledge
ssense.com
2 Staples Inc.
SteelSeries ApS
Stitch Fix
3 Summit Racing Equipment
Sun Basket
2 Sur La Table Inc.
5 Sweetwater
Tackle Warehouse LLC
Tapestry
2 Target Corp.
Tarte Inc.
Teespring Inc.
2 Tennis Warehouse
4 The Clymb
The Container Store Inc.
The Estee Lauder Cos. Inc.
The Finish Line Inc.
2 The Great Courses
3 The Home Depot Inc.
4 The Honest Company Inc.
2 The Kroger Co.
2 The Lakeside Collection
The Men's Wearhouse Inc.
4 The Nature’s Bounty Co.
4 The Orvis Co. Inc.
3 The RealReal Inc.
The Walt Disney Company Ltd.
2 ThriftBooks Global LLC
2 Thrive Market
2 Tiffany & Co.
4 Tilly's Inc.
4 TJX Cos. Inc.
4 TOMS Shoes LLC
Tory Burch LLC
Traeger Grills
Trans World Entertainment
TSC
2 Tuft & Needle
Uniqlo
United States Mint
Value City Furniture
Vera Bradley Retail Stores LLC
VIPOutlet
Vitamin Shoppe Industries Inc.
Vizio Inc.
W.W. Grainger Inc.
2 **Walmart Inc.**
4 Warby Parker
6 Wayfair Inc.
Weber Grills
Whirlpool
2 Wolverine Worldwide Inc.
Xerox Corp.
YDesign Group LLC
4 Zazzle Inc.
Zenni Optical Inc.
4 Zumiez Inc.

Negrita: 50 Mejores ◆Mayor puntuación en el sector 2 3 4 5 6 7 Años consecutivos en el cuadro de honor

Bancos 100 de 2018 – Cuadro de honor

73 % en el cuadro de honor – 27 % reprobados – 6 % entre los "Mejores"

American Express National Bank
5 Arvest Bank
Associated Bank, National Association
BancorpSouth Bank
7 Bank of America, National Association
3 Bank of Hawaii
Bank of Hope
3 Bank of the West
Bank OZK
Barclays Bank Delaware
5 Branch Banking and Trust Company
4 Capital One, National Association
Cathay Bank
Centennial Bank
Charles Schwab Bank
2 Chemical Bank
CIBC Bank USA
5 Citibank, National Association
2 Citizens Bank, National Association
5 City National Bank
3 Comerica Bank
3 Commerce Bank
3 Compass Bank
3 Deutsche Bank Trust Co, Americas
4 Discover Bank
E*TRADE Bank
4 Fifth Third Bank
First Hawaiian Bank
First Midwest Bank
2 **First National Bank of Omaha** ◆
4 First Republic Bank
7 Frost Bank
Goldman Sachs Bank USA
3 Hancock Whitney Bank
HSBC Bank USA, National Association
4 Iberiabank
Investors Bank
3 JPMorgan Chase Bank, National Assoc.
3 KeyBank National Association
Manufacturers & Traders Trust Co.
MB Financial Bank, National Assoc.
MidFirst Bank
6 Morgan Stanley Bank, National Assoc.
4 MUFG Union Bank, National Assoc.
New York Community Bank
Old National Bank
Pacific Western Bank
Pinnacle Bank
PNC Bank, National Association
Prosperity Bank
5 Regions Bank
Sallie Mae Bank
2 Signature Bank
2 Silicon Valley Bank
South State Bank
Stifel Bank and Trust
3 SunTrust Bank
2 Synovus Bank
3 TCF National Bank
3 **TD Bank, National Association**
2 The Bank of New York Mellon
4 **The Huntington National Bank**
The Northern Trust Company
TIAA, FSB
7 U.S. Bank National Association
UBS Bank USA
UMB Bank, National Association
3 Umpqua Bank
United Bank
USAA Federal Savings Bank
Washington Federal, National Assoc.
Western Alliance Bank
Zions Bancorporation, N.A.

Negrita: 50 Mejores ◆Mayor puntuación en el sector ❷❸❹❺❻❼Años consecutivos en el cuadro de honor

Gobierno federal de EE. UU. 100 de 2018 – Cuadro de honor

91 % en el cuadro de honor – 8 % reprobados – 26 % entre los "Mejores"

Oficina Administrativa de los Tribunales de los Estados Unidos (Poder Judicial)
Oficina de Estadísticas Laborales (BLS)

4 Oficina del Censo

Centros para el Control y la Prevención de Enfermedades (CDC)

Oficina de Protección Financiera del Consumidor

2 Departamento de Agricultura

Departamento de Agricultura (ChooseMyPlate.gov)

Servicio de Inspección y Seguridad Alimentaria del Departamento de Agricultura (FSIS)
Departamento de Comercio

Departamento de Comercio - Servicio Meteorológico Nacional/NOAA
Departamento de Comercio (Exportaciones)

2 Departamento de Comercio (NIST)

2 Departamento de Comercio (NTIA)

Departamento de Comercio (Patentes y Marcas)

Departamento de Comercio (Privacy Shield)

Departamento de Defensa

4 Departamento de Educación

2 Departamento de Educación (Subsidios y Asistencia)

Departamento de Educación (Centro Nacional de Estadísticas de Educación)
Departamento de Educación (Préstamos Estudiantiles)

4 Departamento de Energía

2 Departamento de Energía (Energy Star)

Departamento de Salud y Servicios Sociales (Medicare)

Departamento de Salud y Servicios Sociales (Medicare/Medicaid)

Departamento de Salud y Servicios Sociales (Oficina para la Salud de la Mujer)

3 **Departamento de Salud y Servicios Sociales (Healthcare.gov)**

2 Departamento de Salud y Servicios Sociales (HHS)

Departamento de Seguridad Nacional (Servicio de Inmigración y Control de Aduanas de EE. UU.)
Departamento de Seguridad Nacional (Oficina de Aduanas y Protección Fronteriza)

2 Departamento de Seguridad Nacional (DHS)

Departamento de Seguridad Nacional (DHS)

Departamento de Seguridad Nacional (ICE)

Departamento de Seguridad Nacional (Casos de Inmigración y Control de Aduanas de EE. UU.)
Departamento de Vivienda y Desarrollo Urbano (HUD)

4 Departamento del Interior

Departamento del Interior (Servicio Geológico de EE. UU.)

2 Departamento del Interior (Servicio Geológico de EE. UU.)

Departamento de Justicia (Agencia Federal de Prisiones)

3 Departamento de Justicia (DOJ)

2 Departamento de Trabajo

Departamento de Trabajo (OSHA)

Departamento de Estado

Departamento de Estado (Office of the Historian)

Departamento de Estado (Solicitudes de visa en línea)

Departamento de Estado (Viajes)

Departamento de Transporte

Departamento de Hacienda

Departamento del Tesoro (TreasuryDirect)

Agencia de Protección Ambiental

Administración Federal de Aviación (FAA)

4 Oficina Federal de Investigación (FBI)

2 **Comisión Federal de Comunicaciones (FCC)**

2 Corporación Federal de Seguro de Depósitos (FDIC)

2 **Agencia Federal para el Manejo de Emergencias (FEMA)**◆

Sistema de la Reserva Federal

2 Comisión Federal del Comercio (Información al consumidor)

2 Comisión Federal del Comercio (Registro Nacional No Llame)

4 **Comisión Federal de Comercio (FTC)**

4 First Gov (USA.gov)

Administración de Alimentos y Medicamentos (FDA)

Administración de Servicios Generales (GSA)

2 Servicio de Impuestos Internos (IRS)

4 Administración Nacional de la Aeronáutica y del Espacio (NASA)

Administración Nacional de Seguridad del Tráfico en las Carreteras (NHTSA)
Institutos Nacionales de la Salud (Cancer.gov)

Institutos Nacionales de la Salud (MedlinePlus)

4 Institutos Nacionales de la Salud (NIH)

2 **Administración Nacional Oceánica y Atmosférica (NOAA)**

4 Servicio de Parques Nacionales (NPS)

2 Fundación Nacional para la Ciencia (NSF)

Oficina de Administración de Personal (OPM)

Oficina del Registro Federal

Cuerpo de Paz

Comisión de Bolsa y Valores (SEC)

2 Administración de Pequeños Negocios (SBA)

4 Administración del Seguro Social (SSA)

Guardia Costera de los Estados Unidos

Fuerzas Armadas de los EE. UU. (Fuerza Aérea)

Negrita: 50 Mejores ◆Mayor puntuación en el sector ❷❸❹❺❻❼Años consecutivos en el cuadro de honor

Consumidores 100 de 2018 – Cuadro de honor

85 % en el cuadro de honor – 9 % reprobados – 40 % entre los "Mejores"

- 3 **1040.com**
- 3 1040NOW
- Addicting Games
- 3 **Airbnb**
- **Amazon Payments**
- 3 Ancestry
- Answers.com
- AOL
- Ask.fm
- 7 Badoo.com
- BigFishGames
- Bing
- **Blogger**
- 3 Booking.com
- 5 Box
- 3 CareerBuilder
- 2 Classmates
- Craigslist
- Dailymotion
- DeviantArt
- 3 **DocuSign**
- 5 Dropbox
- eBay
- eHow
- 4 eSmart (Liberty Tax)
- 3 Expedia
- 4 ezTaxReturn.com
- 3 FileYourTaxes
- 6 Fiverr
- 4 **Flickr**
- 3 Free Tax Return.com
- 4 FreeTaxUSA
- 3 Glassdoor
- 4 **Google Drive**
- **Google Pay**
- **Google Play**
- 3 H&R Block
- HBO Now
- Hotels.com
- Hotwire
- Hulu
- 5 iCloud
- ID Watchdog
- 3 Identity Guard
- IdentityForce
- IMDb
- 3 Imgur
- 3 Indeed
- 6 Instagram
- JobDiagnosis.com
- 3 KAYAK
- 7 LinkedIn
- 3 **Lyft**
- 4 Match.com
- 3 MediaFire
- 3 Meetup
- 3 Miniclip
- 3 Monster
- MSN
- MySpace
- **Netflix**
- 4 **Norton LifeLock**
- 3 OkCupid
- OLT Online Taxes
- OneDrive
- 3 Orbitz
- 3 Pandora
- **PayPal** ◆
- 6 Pinterest
- Pogo
- 3 Priceline
- 7 Publishers Clearing House
- 3 **Reddit**
- Shutterfly
- Simply Hired
- 3 **Snapchat**
- 3 SoundCloud
- 3 Spotify
- **Square Cash**
- 4 TaxACT
- 4 TaxSlayer
- **Tinder**
- Travelocity
- TripAdvisor
- 7 Tumblr
- 3 TurboTax
- 7 **Twitter**
- **UpWork**
- Venmo
- Vimeo
- VRBO
- Western Union
- Wikia
- wikiHow
- Wikipedia
- 6 Wordpress
- Xoom
- Y8
- 5 Yahoo!
- Yelp
- 6 **YouTube**
- Zelle
- 3 Zoosk
- 7 Zynga

Negrita: 50 Mejores ◆Mayor puntuación en el sector 2 3 4 5 6 7 Años consecutivos en el cuadro de honor

Noticias/Medios 100 de 2018 – Cuadro de honor

78 % en el cuadro de honor – 19 % reprobados – 2 % entre los "Mejores"

- ❸ American City Business Journals
- ❷ AOL News
- AP
- Axios
- Bankrate
- BBC.com
- Bleacher Report
- Bloomberg News
- ❷ Boston.com
- Breitbart
- ❸ Business Insider
- ❸ BuzzFeed
- Cars.com
- CBS News
- CBS Sports
- Chicago Tribune
- Chron
- CNBC
- ❷ CNET
- CNN
- Consumer Reports
- Daily Caller
- Deadspin
- Digital Trends
- ❸ Engadget
- ESPN
- ❷ Everyday Health
- ❷ Fox News
- Fox Sports
- ❸ Gizmodo
- ❺ **Google News** ◆
- ❷ Huffington Post
- ❷ Independent
- ❷ Kotaku
- Lifewire
- Live Science
- Los Angeles Times
- ❷ Mashable
- ❸ MSN News
- ❷ National Geographic
- NBC Sports
- New York Magazine
- ❺ New York Times
- Newsweek
- NJ.com
- ❷ NPR
- NY Daily News
- Patch
- PBS
- ❷ Politico
- Polygon
- ❸ **Reddit**
- Reuters
- SB Nation
- SFGate
- ❷ Slate
- ❷ TechCrunch
- ❸ The Atlantic
- ❷ The Daily Beast
- ❸ The Guardian
- The Motley Fool
- The National Weather Service
- The New York Post
- The Sun
- The Telegraph
- ❷ TMZ
- US News
- USA Today
- ❸ Vice
- ❷ Vox
- Wall Street Journal
- Washington Post
- Washington Times
- Weather Channel
- Weather Underground
- ❸ WebMD
- ❷ Wired
- ❸ Yahoo News

Negrita: 50 Mejores ◆Mayor puntuación en el sector ❷❸❹❺❻❼Años consecutivos en el cuadro de honor

Operadores, proveedores de servicios de Internet y hosts 100 de 2018 – Cuadro de honor

63 % en el cuadro de honor – 35 % reprobados – 4 % entre los "Mejores"

- 2 1&1
- A2 Hosting
- Akamai Technologies
- Amazon Web Services (AWS)
- 2 AOL Mail
- AT&T
- AT&T Wireless
- 2 Automattic
- 2 BlueHost
- 2 C Spire Wireless
- Cable ONE
- Comcast
- Consolidated Communications
- 2 Cox Communications
- Cricket Wireless
- CyrusOne
- 2 Digital Ocean
- e-vergent
- Etheric Networks
- Everywhere Wireless
- 2 Frontier Communications
- GoDaddy
- 2 **Google Cloud** ◆
- 2 Google Gmail
- 2 HostGator
- HostMonster
- 2 iCloud Mail
- 2 Incapsula Inc
- iPage
- KnownHost
- 2 Linode
- 2 LiquidWeb
- 2 Mail.com
- 2 MetroPCS
- 2 Microsoft Azure
- 2 Microsoft Outlook.com
- 2 New Dream Network, LLC
- Optimum by Altice
- Peer 1 Network (USA) Inc
- 2 ProtonMail
- Psychz Networks
- Rackspace
- RCN
- Rise Broadband
- Shopify
- 2 SingleHop
- 2 SoftLayer
- 2 Squarespace
- **Sucuri**
- Suddenlink Communications
- TDS Telecom
- TierPoint
- Tutanota
- 2 Verizon
- 2 Verizon Wireless
- WATCH Communications
- 2 Weebly
- Winters Broadband
- WOW!
- 2 Yahoo Mail
- Yandex Mail
- 2 Zoho Mail

Negrita: 50 Mejores ◆Mayor puntuación en el sector 2 3 4 5 6 7 Años consecutivos en el cuadro de honor

Atención médica 100 de 2018 – Cuadro de honor

57 % en el cuadro de honor – 43 % reprobados – 4 % entre los "Mejores"

23andMe ◆
Adventist Health System
Aetna Group
Ahoid Delhaize (Food Lion Pharmacy)
Albertsons Pharmacy
Alere, Inc.
Anthem
Any Lab Test Now
Ascension Health
Baylor Scott & White Health
BCBS of MN
BCBS of NJ GRP
CA Physician's Service (d/b/a BS of CA)
Cambria Health Solutions
Carefirst Inc. Group
Caresource Group
Cigna Health Group
Cigna Pharmacy
Costco Pharmacy
Counsyl
CVS Pharmacy
DaVita Healthcare Partners, Inc.
Dignity Health
Diplomat Pharmacy
Express Scripts
Florida Blue
Gene by Gene
HCSC Group
Health Net of California, Inc.
Highmark Group
Hospital Corporation of America (HCA)
Independence Health Group Inc. Group
Kroger Pharmacy
Laboratory Corporation of America
Mercy Health
Myriad Genetics, Inc.
Northwell Health
Pathway Genomics
PharMerica
Prime Healthcare Services
Providence Health and Services
Publix Pharmacy
Quest Diagnostics, Inc.
Rite Aid Pharmacy
SSM Health Care
Tenet Healthcare
United Health
UnitedHealth (Optum Rx)
Univera Healthcare Advantage
Universal Health Services
Unum Group
UPMC (hospitales)
UPMC Health System Group (seguros)
Walgreens Boots Pharmacy
Walmart Pharmacy

Socios de OTA/Internet Society de 2018 – Cuadro de honor

98 % en el cuadro de honor – 2 % reprobados – 12 % entre los "Mejores"

❻ ACT | The App Association
❹ ADT
❼ Agari
❷ Classmates
❼ Constant Contact
❼ DigiCert
❺ Distil Networks
❸ Dmarcian Inc.
❼ Ensighten
❹ **Gap Inc.**
❼ GetResponse
❷ Global Cyber Alliance
❷ Guardian Life
❼ High-Tech Bridge (now ImmuniWeb)
❼ Iconix
❼ Identity Guard
❸ Infoblox
❷ Intelius
❷ **Internet Society**
❼ Intersections
❹ Kromtech Alliance Corp.
❺ LashBack
❹ MacKeeper
❹ Malwarebytes
❼ Marketo
❼ Microsoft
❸ National Association of REALTORS
❹ **Norton LifeLock**
❼ **Online Trust Alliance** ◆
❺ OPTIZMO
❷ PeopleConnect
❹ PhishLabs (antes Brand Protect)
❷ Security Scorecard
❹ SimpliFi
❼ Symantec
❺ The Media Trust
❼ **TrustSphere**
❼ **Twitter**
❹ UnsubCentral
❸ Valimail
❻ Verisign
❸ Yes Marketing
❸ Zeta Interactive

* Organizaciones socias de Internet Society que antes estaban afiliadas a OTA.

Negrita: 50 Mejores ◆Mayor puntuación en el sector ❷❸❹❺❻❼Años consecutivos en el cuadro de honor

Anexo E: Lista de verificación de las mejores prácticas

Protección de DNS, el dominio, la marca y los consumidores		
❑	Registros SPF válidos y DKIN en el dominio corporativo y los subdominios	Puntuación base
❑	Registros DMARC con política de rechazo/cuarentena	Puntuación base
❑	Registros DMARC "descubiertos" (p=ninguno y sin RUA o RUF)	Inválido
❑	Cifrado TLS oportunista para correo electrónico	Puntos de bonificación
❑	Implementación de DNSSEC	Puntos de bonificación
❑	Adopción de IPv6	Puntos de bonificación
❑	Autenticación multifactor	Puntos de bonificación
❑	Dominio bloqueado	Penalización por no bloquearlo
❑	Autenticación de correo entrante y comprobación DMARC	Sin puntaje; recomendado
Seguridad de sitios, servidores e infraestructura		
❑	Seguridad y configuración del servidor	Puntuación base, agregado, múltiples pruebas
❑	Certificado SSL/TLS, protocolo, intercambio de claves, cifrados	Puntuación base, agregado, múltiples pruebas
❑	Always on SSL (https por defecto)	Puntuación base
❑	Gestión de vulnerabilidades en el servidor	Puntuación base
❑	Autorización de la Autoridad de Certificación (CAA)	Puntos de bonificación
❑	Tipo de certificado (SSL con EV)	Puntos de bonificación
❑	Cortafuegos de aplicación web	Puntos de bonificación
❑	Malware, enlaces maliciosos	Penalización
❑	Vulnerabilidad de XSS/iFrame	Penalización
❑	Mecanismo de informes de vulnerabilidades/fallas	Puntos de bonificación
❑	Protección contra bots	Sin puntaje; recomendado
❑	Mecanismos de mitigación de DDoS	Sin puntaje; recomendado
Declaración de privacidad, seguimiento, transparencia y divulgaciones		
❑	Enlace a la declaración de privacidad en la página de inicio	Puntuación base
❑	Fecha de modificación de la declaración de privacidad en la parte superior de la página	Puntuación base
❑	Diseño de avisos cortos por capas (enlaces/expansión de secciones)	Puntuación base
❑	Ley de protección de la privacidad infantil en Internet (COPPA) o reglamentos relacionados	Puntuación base
❑	Divulgación de "no rastreo" (DNT)	Puntuación base
❑	Declaración de retención de datos	Puntuación base
❑	Datos personales que no se comparten, salvo a terceros para prestar un servicio	Puntuación base
❑	Los datos personales no se comparten con afiliados/socios	Puntuación base
❑	Los proveedores se someten a la declaración de privacidad	Puntuación base
❑	Versiones archivadas/anteriores de la declaración de privacidad están disponibles	Puntuación base
❑	Se usan íconos para identificar claramente las secciones	Puntos de bonificación
❑	Opción de declaración en otros idiomas con un enlace claro	Puntos de bonificación
❑	Acata la configuración DNT del navegador	Puntos de bonificación
❑	Divulgación de seguimiento a través de diversos dispositivos	Puntos de bonificación
❑	Divulgación sobre si los datos se comparten con fines legales	Puntos de bonificación
❑	Se notifica al usuario si un tercero solicita sus datos personales	Puntos de bonificación
❑	Sistema de gestión de etiquetas (TMS) existente	Puntos de bonificación
❑	Presencia de rastreadores de terceros que comparten datos	Penalización, número de rastreadores
❑	Vulneración de datos reportada	Penalización, número de incidentes, tamaño de la vulneración
❑	Medida coercitiva de FTC/FCC/CFPB/el estado/internacional	Penalización, número de sanciones
❑	¿El registro WHOIS es privado?	Penalización
❑	Cumplimiento de la normativa en las jurisdicciones apropiadas (p. ej., RGPD)	Recomendado

Anexo F: Recursos de implementación

Auditoría de confianza en línea 2018 https://otalliance.org/2018HonorRoll

Metodología de la auditoría 2018 https://otalliance.org/2018-online-trust-audit-methodology

Mejores prácticas

Always on SSL https://otalliance.org/AOSSL

Autorización de la Autoridad de Certificación (CAA) https://cabforum.org/

DMARC https://otalliance.org/DMARC

DNSSEC https://www.internetsociety.org/deploy360/dnssec/

Validación DNSSEC https://dnssec-debugger.verisignlabs.com/

Mejores prácticas en el uso del certificado SSL https://otalliance.org/SSL

Autenticación de correo electrónico https://otalliance.org/Eauth

Beneficios de los certificados de validación extendida https://otalliance.org/EVSSL

Análisis de estándares de Internet admitidos https://internet.nl/

IPv6 https://www.internetsociety.org/deploy360/ipv6/

Publicidad malintencionada https://otalliance.org/Malvertising

Verificación de registros SPF/DMARC https://otalliance.org/EauthTool

Comprobación de certificado SSL para servidores web https://ota.ssllabs.com/

Comprobación de certificados SSL/TLS para servidores web https://www.immuniweb.com/ssl/

Comprobación de seguridad para servidores web https://www.immuniweb.com/websec/

Análisis de seguridad/software malicioso para sitios web https://sitecheck.sucuri.net/

Análisis de seguridad para sitios web https://observatory.mozilla.org/

Seguridad de la capa de transporte (TLS) para correo electrónico https://otalliance.org/TLS

Formulario de informe de vulnerabilidades/fallas https://otalliance.org/VulnerabilityReports

Recursos relacionados

Informe de tendencias de incidentes cibernéticos y vulneración de datos https://otalliance.org/Incident

Marco de confianza de IoT https://www.internetsociety.org/iot/trust-framework

Recursos para casas inteligentes https://otalliance.org/SmartHome

Prácticas para dar de baja el marketing por correo electrónico https://otalliance.org/unsub

Auditoría de transparencia de la publicidad nativa https://otalliance.org/Native

Documentos informativos sobre la visión de la confianza https://otalliance.org/vision-trust

Internet Society – Programa Deploy360 https://www.internetsociety.org/deploy360/

Internet Society – Informe global sobre Internet http://www.internetsociety.org/globalinternetreport/

Agradecimientos

Hemos recibido asistencia para el análisis de los datos por parte de Agari, Disconnect, dmarcian, Google, High-Tech Bridge (ahora ImmuniWeb), Infoblox, Internet.nl, Microsoft, Mozilla, Open Bug Bounty, SSL Labs, Sucuri, Symantec, Twitter, Valimail y Verisign.

Acerca de Online Trust Alliance (OTA) de Internet Society

La Online Trust Alliance (OTA) de Internet Society identifica y promueve las mejores prácticas de seguridad y privacidad que fomentan la confianza del consumidor en Internet. Las principales organizaciones públicas y privadas, proveedores, investigadores y legisladores contribuyen a las directrices de la OTA y las siguen para ayudar a que las transacciones en línea sean más seguras y protejan mejor los datos de los usuarios. Internet Society es una organización mundial sin fines de lucro dedicada a garantizar una Internet abierta, globalmente conectada, fiable y segura para todos.

1604-2

Patrocinada en parte por

Notas finales

[1]Hombre que estafó a Google y Facebook se declara culpable de robar 123 millones de dólares con ataques BEC https://www.scmagazine.com/home/security-news/cybercrime/google-facebook-fraudster-pleads-guilty-to-stealing-123-million-in-bec-scams/

[2]Marriott dice que menos clientes se vieron afectados por la violación masiva de datos https://www.usatoday.com/story/travel/news/2019/01/04/marriott-says-fewer-customers-affected-massive-data-hacking/2481601002/

[3]Los problemas de privacidad de Facebook: un resumen https://www.theguardian.com/technology/2018/dec/14/facebook-privacy-problems-roundup

[4]Reglamento General de Protección de Datos de la UE (RGPD) https://eugdpr.org/

[5]Encuesta Global sobre Seguridad y Confianza en Internet 2018 de CIGI-Ipsoshttps://www.cigionline.org/internet-survey-2018

[6]Marco de confianza de IoT de la OTA https://www.internetsociety.org/iot/trust-framework/

[7]Auditoría de confianza en línea y cuadro de honor https://otalliance.org/HonorRoll

[8]Lista de fuentes de Internet Retailer® https://www.digitalcommerce360.com/product/top-500-database/.En algunos gráficos y tablas, en aras de la brevedad, los 100 y los 500 Mejores Minoristas de Internet se han abreviado como "IR 100" e "IR 500" respectivamente.

[9]Bancos mejor clasificados por la Federal Deposit Insurance Corporation (FDIC) según sus activos https://www.fdic.gov/bank/statistical/

[10]Sitios de proveedores de servicios al consumidor de alto nivel basados en el tráfico del sitio donde el usuario se tiene que registrar o crear una cuenta para poder usar el servicio, y que no ofrecen servicios financieros ni de comercio electrónico.

[11]Organizaciones afiliadas a Internet Society que eran socias de la OTA antes de que OTA se integrara a Internet Society.

[12]Los datos no incluyen los resultados del sector de Socios de la OTA porque su alto nivel de cumplimiento distorsionaría los resultados en los gráficos.

[13]El protocolo de seguridad de la capa de transporte (TLS) versión 1.3 https://tools.ietf.org/html/rfc8446

[14]Incluye incidentes de pérdida de datos tanto físicos como electrónicos

[15]Por qué necesita IPv6 https://www.infoblox.com/solutions/ipv6-readiness

[16]Seguridad IPv6 https://www.internetsociety.org/deploy360/ipv6/security/

[17]Directiva operativa vinculante 18-01 del DHS https://cyber.dhs.gov/bod/18-01/

[18]IETF RFC 4408 https://www.ietf.org/rfc/rfc4408.txt

[19]TLS de Gmail para la advertencia de correo electrónico https://arstechnica.com/information-technology/2016/02/gmail-to-warn-you-if-your-friends-arent-using-secure-email/

[20]Informe sobre DNSSEC de la ICANN http://stats.research.icann.org/dns/tld_report/

[21]M-08-23, Protección de la infraestructura del sistema de nombres de dominio del gobierno federal, agosto de 2008 https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2008/m08-23.pdf

[22]Adopción de IPv6 http://www.worldipv6launch.org/measurements/

[23]¿Qué es el "relleno de credenciales"?https://www.wired.com/story/what-is-credential-stuffing/

[24]Los hackers se están pasando más de 2200 millones de registros filtrados https://www.wired.com/story/collection-leak-usernames-passwords-billions/

[25]Prueba de SSL de ImmuniWeb https://www.immuniweb.com/ssl/

[26]Qualys SSL Labs https://www.ssllabs.com/projects/documentation/

[27]Ataque DROWN (desencriptado de RSA con encriptado débil obsoleto) https://drownattack.com/

[28]Comprobación de seguridad de sitios web de ImmuniwWeb https://www.immuniweb.com/websec/

[29]Observatory by Mozilla https://observatory.mozilla.org/

[30]Sucuri SiteCheck https://sitecheck.sucuri.net/

[31]Resumen de CAA https://blog.qualys.com/ssllabs/2017/03/13/caa-mandated-by-cabrowser-forum

[32]Integridad de la publicidad y los contenidos de la OTA https://otalliance.org/resources/advertising-integrity-fraud

[33]Informe de SSL Pulse sobre Qualys SSL Labs https://www.ssllabs.com/ssl-pulse/

[34]Desaprobación de versiones anteriores de TLS https://www.ssl.com/article/deprecating-early-tls/

[35]Open Bug Bounty https://www.openbugbounty.org/report/

[36]Let's Encrypt https://letsencrypt.org/

[37]Predicciones 2019 del CA Security Council http://vmblog.com/archive/2019/01/10/ca-security-council-2019-predictions-the-good-the-bad-and-the-ugly.aspx

[38]La mitad de todos los sitios de suplantación de identidad (phishing) ahora tienen el candado https://krebsonsecurity.com/2018/11/half-of-all-phishing-sites-now-have-the-padlock/

[39]Mandato de normas de seguridad y privacidad para la declaración electrónica (eFile) del IRS, publicada el 1 de enero de 2010 https://www.irs.gov/uac/irs-e-file-security-privacy-and-business-standards-mandated-as-of-january-1-2010

[40]Los certificados de validación extendida están muertos https://www.troyhunt.com/extended-validation-certificates-are-dead/

[41] Nótese que aproximadamente el 30 % de los sitios auditados en 2018 son nuevos, por lo que es difícil hacer una comparación precisa con el año anterior.

[42]Kaspersky Labs: ataques DDoS en el cuarto trimestre de 2018 https://securelist.com/ddos-attacks-in-q4-2018/89565/

[43]Formulario de informes de vulnerabilidades de la OTA https://otalliance.org/VulnerabilityReports

[44]Código malicioso oculto en imágenes de anuncios les cuesta a las redes publicitarias 1130 millones de dólares https://www.zdnet.com/article/malicious-code-hidden-in-advert-images-cost-ad-networks-1-13bn-last-year/

[45]Amazon hace una demanda por anuncios maliciosos https://www.geekwire.com/2018/amazon-files-suit-malvertising-campaign-alleging-sophisticated-widespread-scheme-deceive-consumers/

[46]Reglas de Privacidad Transfronterizas de APEC http://www.cbprs.org/

[47]Ley de Privacidad del Consumidor de California https://en.wikipedia.org/wiki/California_Consumer_Privacy_Act

[48]COPPA https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

[49]Nótese que si bien se verificó la presencia de dichas soluciones, es posible que los sitios no usen las soluciones o los datos.

[50]Apple elimina "no rastrear" de Safari https://gizmodo.com/apple-is-removing-do-not-track-from-safari-1832400768

[51]Extensión de preferencias de rastreo (DNT) https://www.w3.org/TR/tracking-dnt/

[52]Informe de Incidentes Cibernéticos y Tendencias de Vulneración de Datos de 2018 de la OTA https://otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf

[53]Comunicado de prensa sobre el llamamiento a comentarios https://otalliance.org/news-events/press-releases/ota-requests-public-comments-2018-online-trust-audit-methodology

[54]Programa Deploy360 de Internet Society https://www.internetsociety.org/deploy360/

[55]Comunicado de prensa sobre la metodología, 23 de agosto de 2018https://otalliance.org/news-events/press-releases/internet-society%E2%80%99s-online-trust-alliance-announces-methodology-tenth

[56] Verizon: Informe de investigaciones sobre vulneración de datos, página 11 https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

[57] Vulneración de correos electrónicos, la estafa de 12.000 millones de dólares https://www.ic3.gov/media/2018/180712.aspx

[58]Información general, recursos y herramientas para la autenticación de correo electrónico de la OTA https://otalliance.org/eauth

[59]Información general sobre DMARC y recursos de la OTA https://otalliance.org/DMARC

[60]Buenas prácticas de seguridad e implementación de SSL/TLS https://otalliance.org/resources/ssl-best-practices

[61]Fundamentos de DNSSEC https://www.internetsociety.org/deploy360/dnssec/basics/

[62]IPv6 https://www.internetsociety.org/deploy360/ipv6/

[63]Qualys SSL Labshttps://ota.ssllabs.com/

[64]ImmuniWeb https://www.immuniweb.com/ssl/

[65]AOSSL https://otalliance.org/AOSSL

[66]SSL con EV https://otalliance.org/resources/extended-validation-certificates-evssl

[67]Prácticas y directrices de reporte de vulnerabilidades de la NTIA https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities

[68]Formulario de informes de vulnerabilidades de la OTA https://otalliance.org/VulnerabilityReports

[69]FIPP https://cryptome.org/2014/11/nstic-fipps.pdf

[70]COPPA https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children's-privacy

[71]Datos de seguimiento de terceros. La fuente principal incluye datos de https://disconnect.me/trackerprotection/blocked que compensan https://disconnect.me/trackerprotection/unblocked

[72]Recomendaciones de la FTC sobre seguimiento a través de distintos dispositivos https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf

[73]CFPB https://www.consumerfinance.gov/