INFORME SOBRE: EL ESTADO DE LA CONFIANZA DIGITAL DE 2024

digicert®

INFORME SOBRE EL ESTADO DE LA CONFIANZA DIGITAL DE 2024

DigiCert empezó a realizar su encuesta sobre el estado de la confianza digital en el año 2022. Ahora que todos los sectores se suben al carro de la transformación digital, establecer la confianza digital resulta esencial para garantizar que las personas y los dispositivos con los que nos conectamos sean legítimos y que las transacciones que realizamos estén protegidas.

Jennifer Glenn, directora de investigación de IDC, definió la confianza digital como «la base para proteger el mundo conectado y algo necesario para aquellas organizaciones que quieran garantizar que sus clientes, empleados y socios puedan tener la seguridad de que los procesos e interacciones en línea de su negocio están protegidos».

DigiCert, el principal proveedor global de confianza digital, hace que tanto los usuarios individuales como las empresas pueden utilizar Internet con la tranquilidad de saber que su presencia en el mundo digital está protegida. Para ayudar a nuestros clientes, nos hemos marcado el objetivo de entender cómo perciben la confianza digital las empresas globales y qué iniciativas están poniendo en marcha para establecer, gestionar y ampliar el alcance de la confianza digital.

Confianza digital: claves para avanzar

Con nuestra encuesta inicial, pudimos constatar que el 100 % de las empresas consideraba importante la confianza digital. La práctica totalidad de ellas (el 99 %), veía posible que sus clientes se pasasen a la competencia si dejasen de confiar en la marca. La mayoría de los consumidores (más de dos tercios, concretamente el 68 %) aseguraron que la confianza digital era importante.

En esta última edición, hemos querido realizar un análisis más profundo para ver cómo ha evolucionado la situación desde aquel informe inicial. En su encuesta de 2024 sobre el estado de la confianza digital, DigiCert repasa en más detalle ciertas funciones concretas de la confianza digital y sus flujos de trabajo para hacerse una idea más clara de cómo les está yendo a las empresas y de qué pueden hacer para seguir optimizando sus iniciativas en esta materia.

Metodología

Eleven Research, con sede en Dallas, llevó a cabo la encuesta en la que se basa el Informe sobre el estado de la confianza digital de 2024 durante el cuarto trimestre de 2023. La encuesta, que se realizó por teléfono, estuvo dirigida a 300 directivos sénior de diferentes empresas de todos los tamaños de Norteamérica, EMEA y APJ.

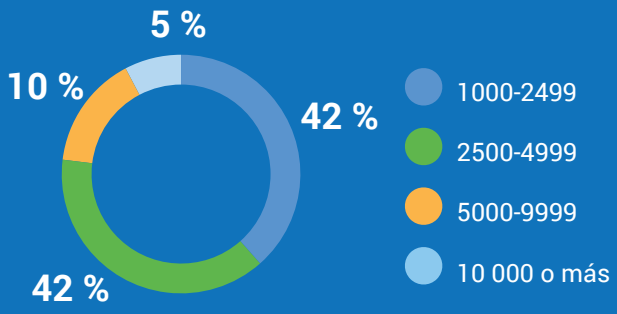
Los encuestados pertenecen a diversos sectores, como el tecnológico, el de la fabricación y el de los servicios financieros. El tamaño de las empresas oscila entre los 1000 y los más de 10 000 empleados.

Con el objetivo de entender mejor las iniciativas concretas de las empresas en materia de confianza digital, Eleven Research se centró en los responsables de cuatro áreas específicas de la confianza digital:

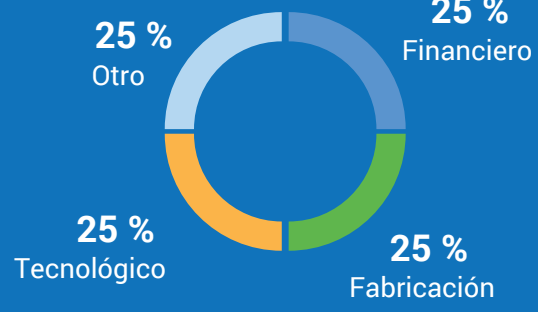
- TI empresarial: proteger las comunicaciones, los datos y los accesos para los empleados, las aplicaciones y las nubes.
- Dispositivos IoT y conectados: proteger los servicios y dispositivos inteligentes (p. ej., monitores de glucosa).
- Software: proteger el software y las aplicaciones de las manipulaciones y los ataques a la cadena de suministro.
- Firma electrónica: garantizar la autenticidad e integridad de los documentos y su contenido.

DISTRIBUCIÓN GEOGRÁFICA

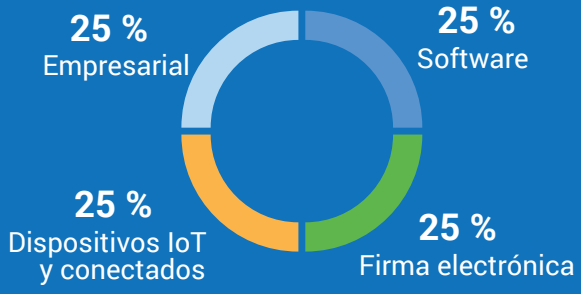
TAMAÑO DE LA EMPRESA



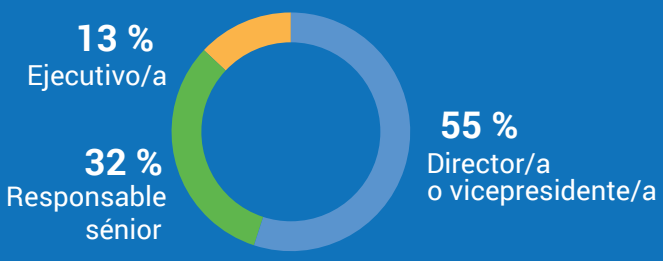
SECTOR



PERFILES



ANTIGÜEDAD



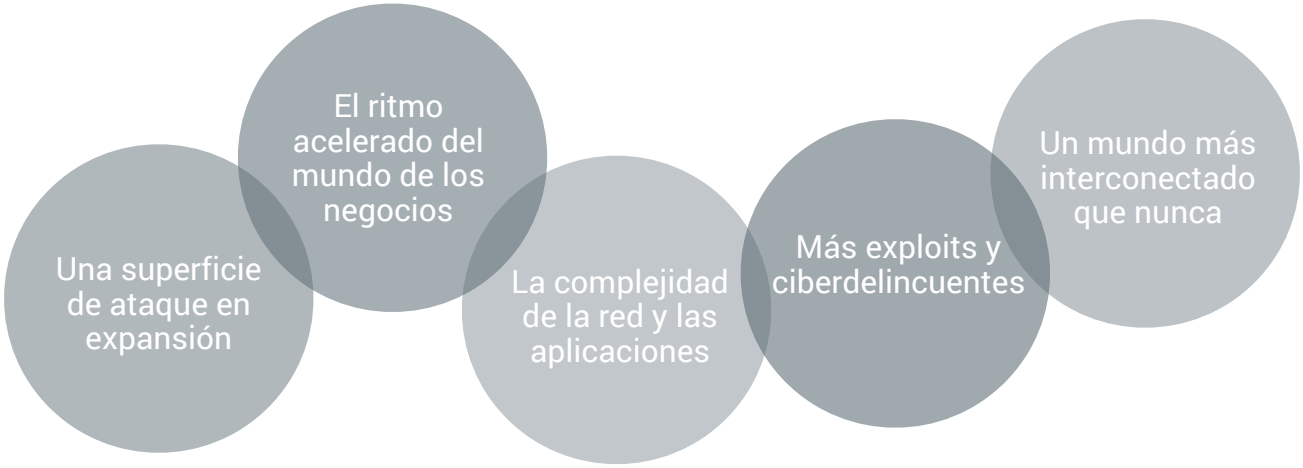
LAS EMPRESAS SIGUEN PRESTANDO MUCHA ATENCIÓN A LA CONFIANZA DIGITAL

En la encuesta del año pasado, quedó claro el gran interés que despierta la confianza digital entre las empresas, por lo que no es ninguna sorpresa que estas sigan muy centradas en este aspecto. Esto se debe a tres motivos principales:

- Actualmente, hay más teletrabajadores que nunca.
- También hay más redes (como las perimetrales o las que se utilizan para conectar a socios y clientes).
- Y, lo más importante, los clientes exigen que las empresas garanticen la confianza digital.

LOS TRES MOTIVOS PRINCIPALES

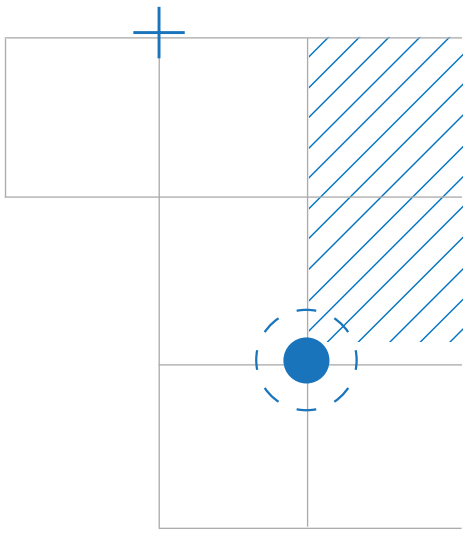
OTROS MOTIVOS



Sin embargo, a las empresas les está costando establecer, supervisar y gestionar la confianza digital por culpa, principalmente, de cinco factores problemáticos:

- **La falta de competencias internas.** La confianza digital es aún una disciplina relativamente nueva, por lo que no todos los profesionales saben cómo implementarla de manera centralizada. Además, muchas PKI privadas se establecieron hace diez años y son frágiles y propensas a fallos, lo que también supone un impedimento para los equipos a la hora de adquirir los conocimientos que tanto necesitan.
- **La complejidad cada vez mayor de las redes y las aplicaciones.** La infraestructura tecnológica de las empresas se ha ido complicando con el tiempo. En lo que respecta a la red, las empresas ya no se limitan a trabajar con centros de datos tradicionales, oficinas remotas y entornos en la nube, sino que, en la actualidad, las redes incluyen redes perimetrales, miles de teletrabajadores y distintas nubes.

  Por otra parte, la arquitectura de las aplicaciones ha pasado de ser monolítica a estar muy distribuida y basada en microservicios, por lo que muchos servicios escapan al control directo de la empresa. Garantizar la confianza digital en un entorno así de complejo resulta verdaderamente difícil.
- **El alcance inabarcable de todo lo que las empresas deben proteger.** A medida que ha ido avanzando la transformación digital, más y más activos digitales se han vuelto imprescindibles para el negocio. De ahí que la superficie que deben proteger las empresas esté creciendo exponencialmente.
- **La falta de apoyo de los responsables.** La pandemia y la inflación han acentuado las dificultades económicas y, en consecuencia, las empresas se han visto obligadas a tomar decisiones difíciles. Por ejemplo, solo en 2023, la ola de despidos en el sector tecnológico se cobró más de 240 000 empleos.[1] Ante tal panorama, no es de extrañar que a veces flaquee el compromiso de los directivos con la confianza digital.
- Por último, **gestionar la rápida expansión de los activos criptográficos requiere mucho tiempo y esfuerzo.** Independientemente de que hablemos de confianza pública o privada, los certificados digitales siguen siendo fundamentales para afianzar las iniciativas relacionadas con la confianza. Sin embargo, gestionar estos certificados ahora que las empresas tienen que lidiar con entornos tan extensos es un reto en sí mismo.



[1] TechCrunch

GARANTIZAR LA CONFIANZA DIGITAL: QUÉ AVANCES SE ESTÁN REALIZANDO

¿Cómo les está yendo a las empresas que están implementando la confianza digital? La respuesta a esta pregunta tiene su intríngulis y está llena de matices, pero la versión corta sería que a las empresas les está yendo bien, pero les podría estar yendo mejor.

El nivel de éxito que alcanzan depende de las áreas específicas en las que se centran. Para entender mejor qué tal lo están haciendo las empresas, hemos examinado cuatro áreas específicas de la confianza digital:

- TI empresarial
- Dispositivos IoT y conectados
- Software
- Firma electrónica

Prácticas de confianza empresarial

En la gran mayoría de los casos, el departamento de TI es el encargado de gestionar la confianza digital empresarial. Los tipos de confianza digital que se gestionan con más frecuencia dentro del ámbito de la confianza digital empresarial incluyen:

- La gestión de certificados
- La gestión de identidades y accesos
- La seguridad del correo electrónico
- La seguridad de los endpoints

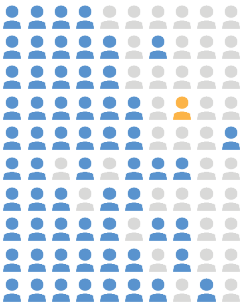
Incluso en el ámbito de la confianza digital empresarial, que sería el que debería estar más maduro, las iniciativas de las empresas en este sentido están aún en ciernes. Muy pocos responsables de la confianza empresarial (apenas 1 de cada 100) se atreven a decir que sus prácticas se encuentran en un estado de «madurez extrema». Además, el 87 % reconoce que sus iniciativas están fragmentadas.

Los certificados digitales sirven para autenticar y proteger las comunicaciones de los usuarios empresariales y las máquinas que utilizan, como servidores o teléfonos inteligentes. A medida que se multiplican y complican las redes corporativas y los casos de uso, las empresas necesitan cada vez más certificados.

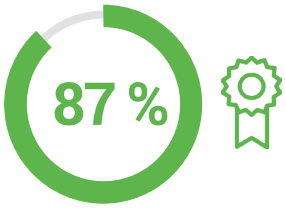
En más o menos la mitad de las empresas que encuestamos (el 52 %), el equipo de TI se encarga de gestionar los certificados; en más de un tercio (el 37 %), los gestionan otros departamentos; y en una de cada nueve (el 11 %), no se gestionan.

Cabe mencionar que, por lo general, en las empresas hay un máximo de cinco departamentos que emiten certificados, pero la mayoría de ellas considera que debería haber más que lo hicieran.

Solo **1 de cada 100** asegura que sus práticas de confianza digital se encuentran en un estado «madurez extrema».



La mayoría se limita a hablar de una madurez «relativa»



Porcentaje de encuestados que reconocen que sus iniciativas de confianza empresarial están fragmentadas.

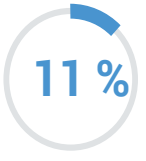
Por lo general, en las empresas hay un máximo de cinco departamentos que emiten certificados.

La mayoria reconoce que debería haber más departamentos que emitiesen certificados.

Dónde se gestionan los certificados

Departamento de TI

Departamento distinto del de TI



No se gestionan

Qué resultados da la confianza empresarial

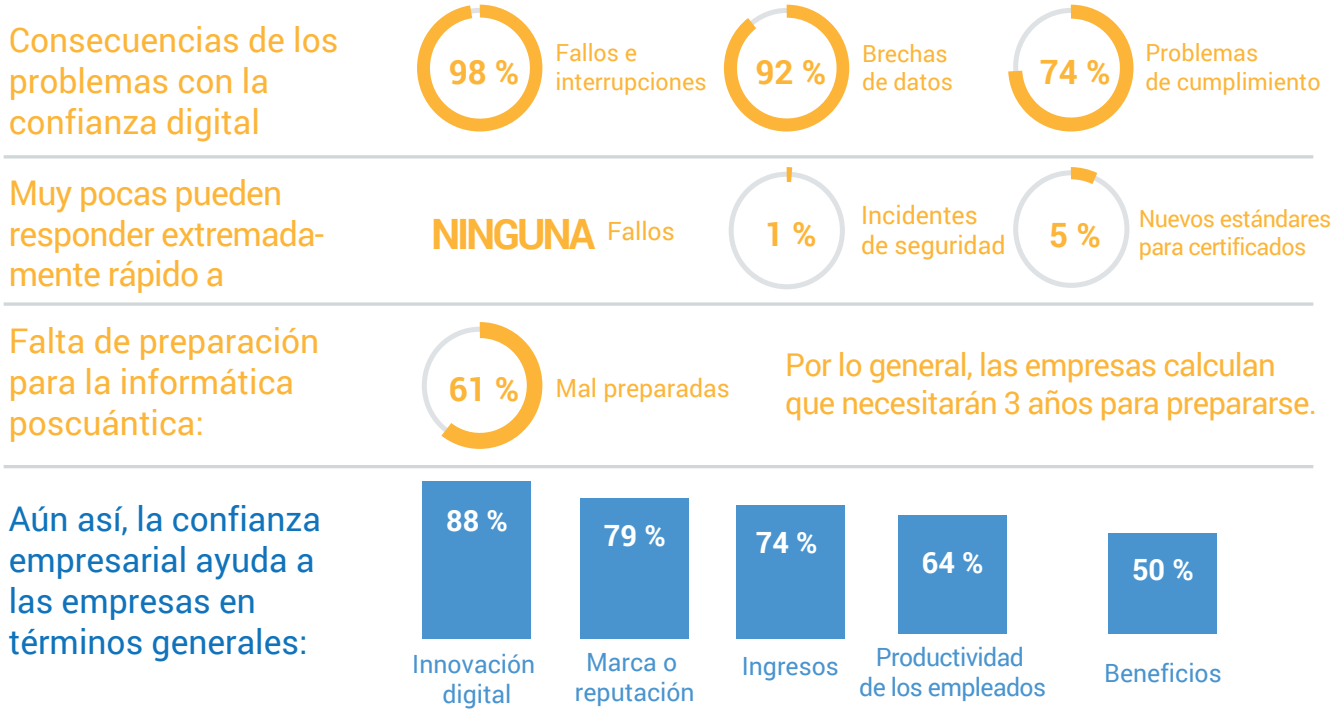
¿Cómo de eficaces están siendo las iniciativas de las empresas en materia de confianza digital? Según parece, no todo lo eficaces que podrían ser. Los encuestados afirmaron haber tenido los siguientes problemas derivados de percances con la confianza digital:

- **Casi todos (el 98 %)** reconocieron haber sufrido al menos algunos fallos e interrupciones.
- **La mayoría (el 92 %)** afirmó haber sufrido brechas de datos.
- Y **una cantidad importante (el 74 %)** tuvo problemas relacionados con el cumplimiento.

Seguimos indagando para evaluar su agilidad en materia de confianza digital:

- **Ninguno** de ellos puede responder a los fallos extremadamente rápido.
- **Casi ninguno** (el 1 %) puede responder a los incidentes de seguridad extremadamente rápido.
- **Muy pocos (el 5 %)** pueden responder extremadamente rápido a los cambios en los estándares aplicables a los certificados.
- **La mayoría (el 61 %)** no están bien preparados para la informática poscuántica y, por norma general, calculan que les llevará tres años llegar a estarlo por completo.

A pesar de estas dificultades, los responsables de la confianza digital empresarial aseguran que sus iniciativas sí están ayudando a la empresa a nivel macro, en ámbitos como la innovación digital, la imagen de la marca o los beneficios que obtienen.



Prácticas de confianza digital para dispositivos IoT y conectados

Aquí nos centramos en empresas que fabrican y venden dispositivos IoT y conectados (como sensores para fábricas, relojes deportivos o termostatos para el hogar). En esta ocasión, hablamos con las personas responsables de tareas como las siguientes:

- Elaborar medidas de autenticación para dispositivos IoT o conectados
- Habilitar el cifrado en dispositivos IoT o conectados
- Firmar actualizaciones de software o firmware para dispositivos IoT o conectados
- Utilizar la criptografía para proteger los dispositivos IoT o conectados

Los responsables de la confianza digital para dispositivos IoT y conectados también mandan el mismo mensaje de «bien, pero podría ir mejor». Solo uno de cada siete asegura que sus prácticas se encuentran en un estado de madurez extrema. La mayoría indicó una madurez «relativa».

Sorprendentemente, **la mayoría (el 87 %)** transmiten la PII procedente de dispositivos IoT o conectados a través de canales sin cifrar.

En **la mayor parte de las empresas (el 88 %)**, existe la figura de «director de seguridad de productos». Todas utilizan certificados digitales para identificar los dispositivos en uso y tienen establecidos rigurosos mecanismos de autenticación de usuarios.

Solo **1 de cada 7** dice que sus prácticas de confianza digital se encuentran en un estado de madurez extrema.

La mayoría se limita a hablar de una madurez «relativa».

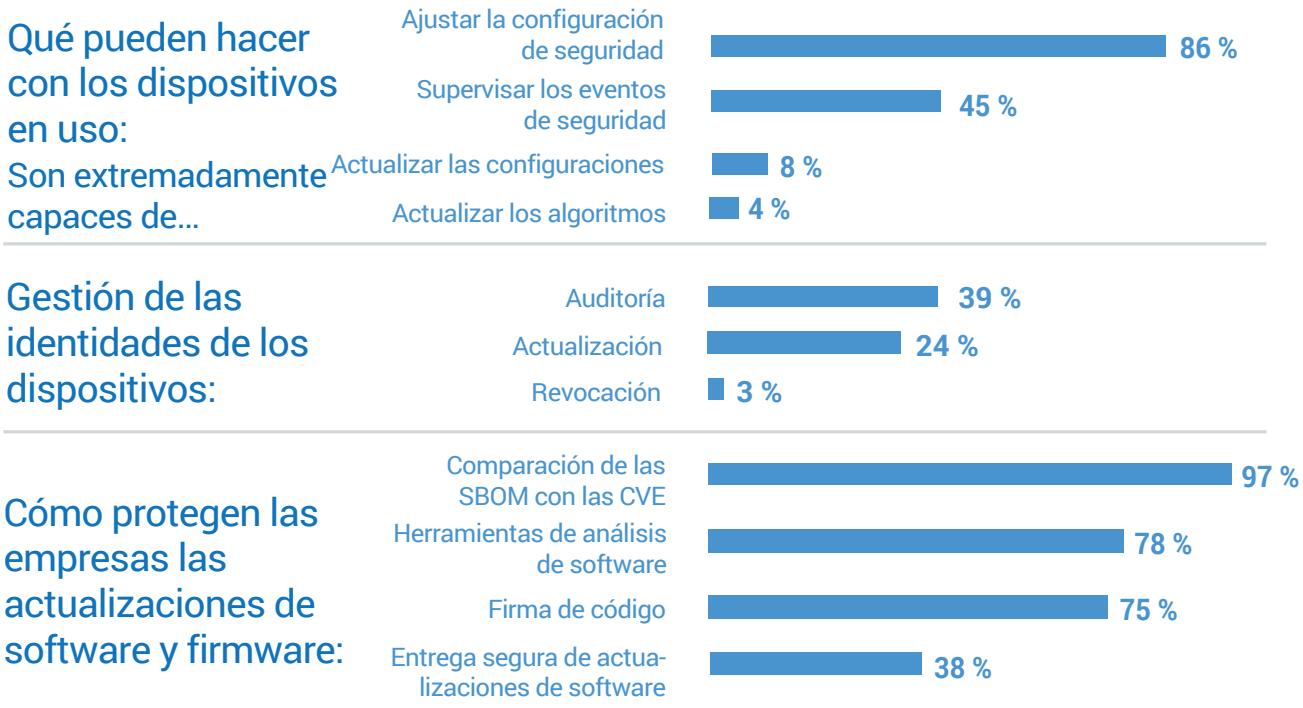
Porcentaje de empresas que transmiten la PII procedente de dispositivos IoT o conectados a través de canales sin cifrar.

Porcentaje de empresas que tienen un/a director/a de seguridad de productos o un equipo de seguridad centralizado que gestiona todos los dispositivos IoT o conectados.

Cómo identifican sus dispositivos y a sus usuarios en activo:

Pedimos a los encuestados que evaluasen sus capacidades en distintos ámbitos relacionados con los dispositivos IoT y conectados. En lo que respecta a la gestión de los dispositivos en uso, hubo un poco de todo: saben gestionar muy bien las configuraciones de seguridad y no se les da mal supervisar los eventos de seguridad, pero la actualización de dispositivos es otro cantar.

También tienen mucho que mejorar en lo tocante a la gestión de las identidades de los dispositivos, sobre todo en lo que a revocación se refiere. El lado positivo es que, por lo general, protegen bien el software, aunque tienen una asignatura pendiente: la entrega segura de actualizaciones.



Qué resultados da la confianza para dispositivos IoT y conectados

Con estas capacidades (o, en su caso, la falta de ellas), constatamos que los fabricantes de dispositivos IoT y conectados con los que hablamos estaban teniendo dificultades en mayor o menor medida:

- **La mayoría (el 93 %)** sufrió brechas de datos. Muchas de ellas se debieron a que el dispositivo servía de puerta trasera que los ciberdelincuentes utilizaban para acceder a la red con facilidad.
- **La mayoría (el 93 %)** sufrió tanto fallos como interrupciones.
- Y, otro problema relacionado con lo que mencionábamos en el primer punto, el **84 %** sufrió intrusiones en la red.

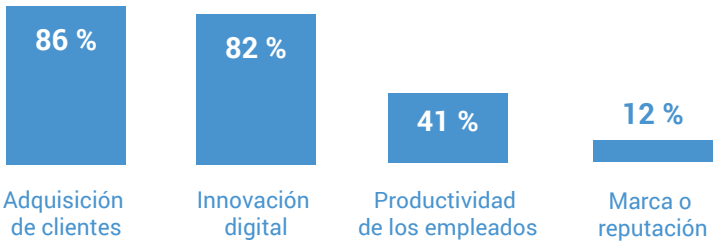
Sin embargo, las prácticas de confianza para dispositivos IoT y conectados sí reportaron alguna ventaja:

- **El 86 %** aseguró que contribuyeron a la adquisición de clientes.
- **El 82 %** afirmó que estas prácticas ayudaron con la innovación digital.

A pesar de ello, está claro que los fabricantes de dispositivos IoT y conectados necesitan mejorar sus iniciativas de confianza digital.

Consecuencias de los problemas con la confianza digital

Así y todo, la confianza digital para dispositivos IoT y conectados ayuda a las empresas en términos generales:



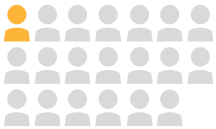
Prácticas de confianza para el software

La confianza para el software garantiza la confianza digital para el software que venden o distribuyen las empresas. También aquí, la encuesta constató que se avanza, pero no todo lo rápido que se podría avanzar. Solo 1 de cada 20 (el 5 %) asegura que sus prácticas de confianza para el software se encuentran en un estado de «madurez extrema». También varía el uso que hacen las empresas de la firma de código:

- **Casi todas (el 99 %)** firman el código fuente del software.
- **El 84 %** dice que firma los binarios del software.
- **El 62 %** firma los scripts de compilación y la configuración de la infraestructura.
- **El 33 %** responde «contenedores y entornos sin servidor».
- **La mayoría (el 67 %)** almacena claves privadas de firma de código en dispositivos conformes con el estándar FIPS 140-2.

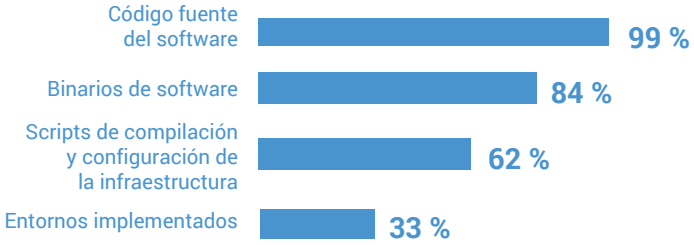
Ninguna de las empresas encuestadas declaró que sería capaz de detectar extremadamente rápido todas las aplicaciones asociadas con una clave privada de firma de código si esta sufriese un ataque.

Solo **1 de cada 20** dice que sus prácticas de confianza digital se encuentran en un estado de madurez extrema.

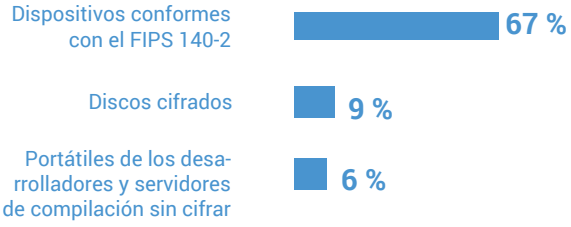


La mayoría se limita a hablar de una madurez «relativa».

Para qué utilizan la firma de código las empresas:



Dónde almacenan las empresas las claves privadas de firma de código:



Si una clave privada de firma de código sufriese un ataque, **NINGUNA** sería capaz de encontrar fácil y rápidamente todas las aplicaciones en las que se utilizó para firmar.

Casi todas elaboran listas de materiales de software (SBOM) por sistema para el software que producen.

Casi todas establecen requisitos para el software de terceros en materia de riesgos, seguridad y

Qué resultados da la confianza para el software

¿Cómo de eficaces están siendo las empresas a la hora de garantizar que el software cumple las normativas pertinentes? Solo 1 de cada 8 son extremadamente eficaces. Además, tienen muchos problemas derivados de percances con la confianza para el software:

- **El 86 %** afirmó haber sufrido brechas de datos.
- **El 80 %** reconoció haber sufrido brechas en la infraestructura de compilación del software.
- **El 79 %** reconoció que el software había dejado de funcionar por culpa de algún certificado de firma de código caducado.
- **El 78 %** entregó software que contenía malware y otras vulnerabilidades.
- **El 75 %** incumplió algún plazo de entrega por problemas con la firma de código o la detección de malware.

Los clientes dependen de la integridad del software de las empresas; pero, a veces, proteger todas las claves necesarias para firmar el código puede antojarse una tarea inabarcable.

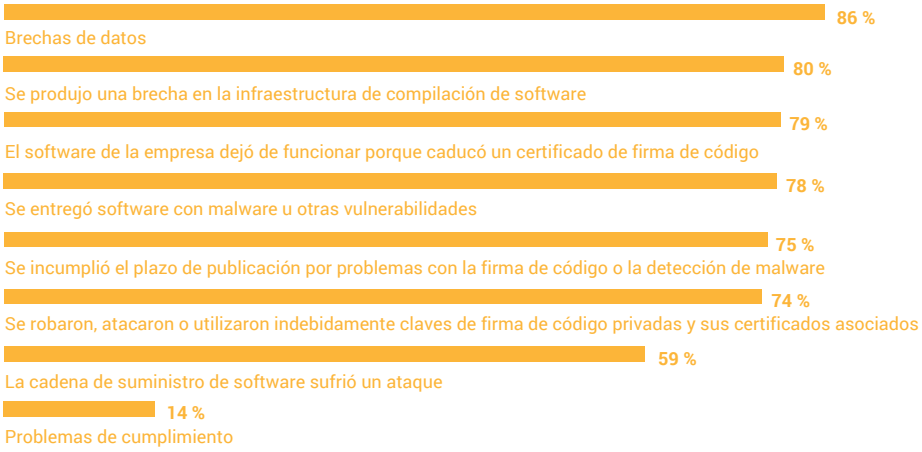
Pocas reconocen que pueden generar fácilmente una lista de los componentes de software utilizados en el software que desarrollan.

Dicho esto, los responsables de la confianza para el software aseguran que sus iniciativas sí están ayudando a la empresa en dos ámbitos generales (la innovación digital y la productividad de los empleados).

Porcentaje de empresas que están obteniendo resultados extremadamente buenos en materia de cumplimiento normativo del software.

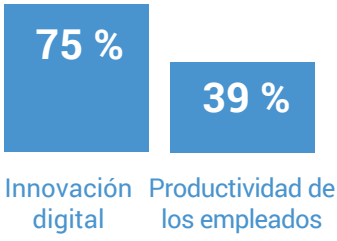
A la mayoría les va relativamente bien.

Consecuencias de los problemas con la confianza digital



Porcentaje de empresas que afirman que es extremadamente sencillo generar una lista de los componentes de software y sus configuraciones en el software que desarrollan.

Aún así, la confianza digital para el software ayuda a las empresas en términos generales:



Prácticas de confianza para la firma electrónica

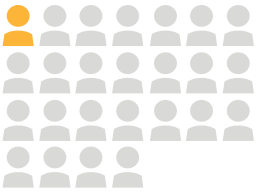
Los certificados de firma de documentos permiten a particulares, equipos y empresas añadir una firma electrónica digital a un documento en diversos formatos de archivo para demostrar la titularidad, garantizar que no se puede modificar y proteger la información confidencial.

Pedimos a los encuestados que evaluasen el nivel de madurez de sus prácticas de confianza para la firma electrónica, y 1 de cada 25 empresas (el 4 %) dice que se encuentran en un estado de madurez extrema, el porcentaje más bajo de los cuatro ámbitos objeto de la encuesta.

Una particularidad de este segmento es que las firmas electrónicas las gestionan departamentos distintos del de TI (el jurídico, el de RR. HH., el de contratación, etc.), y solo 1 de cada 8 entiende la diferencia entre las firmas electrónicas básicas y las basadas en certificados.

- **En torno a la mitad (el 48 %)** utiliza sellos electrónicos en sus documentos (en el ámbito jurídico, de ventas, de la contratación, etc.).
- **La mayoría (el 86 %)** utiliza firmas digitales con certificados emitidos por terceros de confianza para verificar la identidad de los firmantes.

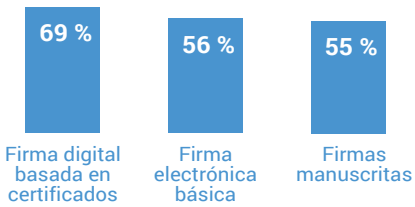
Solo **1 de cada 25** dice que sus prácticas de confianza digital se encuentran en un estado de madurez extrema.



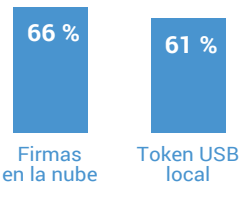
La mayoría se limita a hablar de una madurez «relativa».

Tienen clara la diferencia entre las firmas electrónicas básicas y las firmas digitales basadas en certificados.

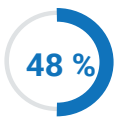
Tipos de firmas utilizadas:



Tipos de firmas que utilizan las que recurren a la firma electrónica:

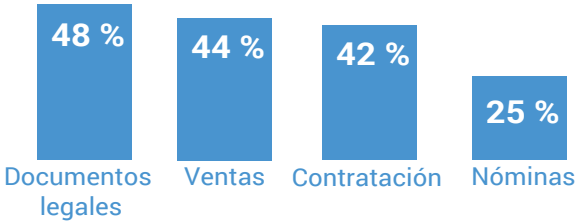


Utilizan firmas digitales con certificados emitidos por terceros de confianza para verificar la identidad de los firmantes.



La mitad utiliza sellos electrónicos en los documentos.

Casos de uso más habituales:



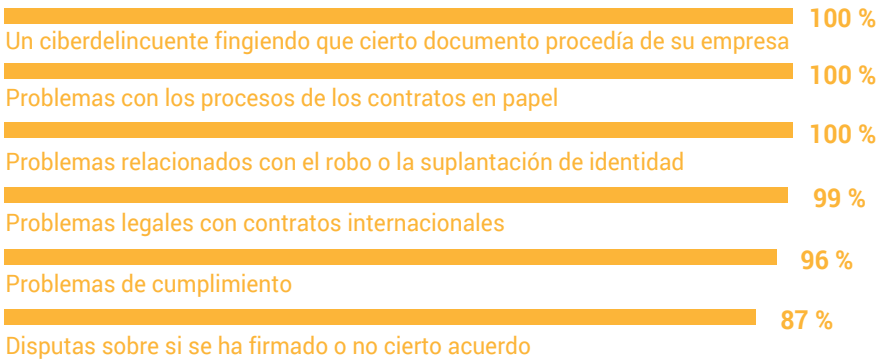
Qué resultados da la confianza para la firma electrónica

Este grupo resultó ser el que más incidentes sufre debido a percances con la confianza:

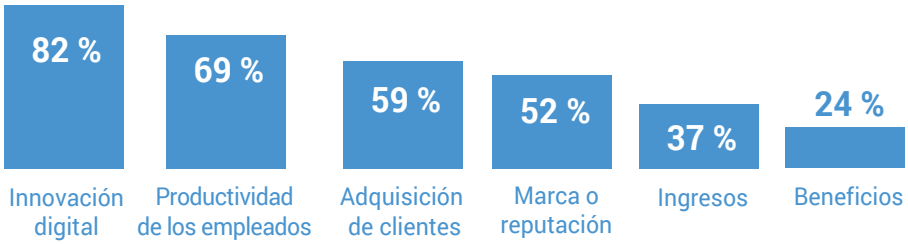
- **El 100 %** reconoció que un ciberdelincuente había fingido que cierto documento procedía de su empresa.
- **El 100 %** tuvo problemas con los procesos de los contratos en papel.
- **El 100 %** tuvo problemas relacionados con el robo o la suplantación de identidad.
- Casi todas **(el 99 %)** tuvieron problemas legales con contratos internacionales.
- **El 96 %** tuvo problemas relacionados con el cumplimiento.
- **El 87 %** se vieron envueltas en disputas sobre si se había firmado o no cierto acuerdo.

A pesar de estos problemas, aseguran que sus iniciativas las benefician en términos generales, por ejemplo, en aspectos como la innovación digital, la productividad, la adquisición de clientes, etc.

Consecuencias de los problemas con la confianza digital



Aún así, la confianza empresarial ayuda a las empresas en términos generales:



QUÉ HEMOS APRENDIDO DE LOS EXPERTOS EN CONFIANZA DIGITAL

Hasta ahora, hemos hablado de los resultados de todas las empresas combinadas. Sin embargo, constatamos que, dentro de ese grupo, algunas obtuvieron mejores o peores resultados que la media.

Nos llamaron la atención estas diferencias, por lo que decidimos desglosar y comparar esos resultados. Para ello, puntuamos las respuestas a todas las preguntas destinadas a medir resultados (por ejemplo, «¿Han sufrido brechas?» o «¿Con qué rapidez pueden responder a los incidentes?»). Otorgamos puntos positivos para los resultados satisfactorios y puntos negativos para los resultados mejorables y calculamos el total para atribuir a cada encuestado una puntuación global.

A las empresas cuya puntuación las situó en el 33 % superior en todas las categorías las llamamos «líderes en confianza digital». Aquellas cuyos resultados las sitúan en el 33 % inferior son los «rezagados en confianza digital».

Realizamos un análisis para entender las diferencias entre los resultados y las prácticas de estos dos grupos para cada uno de los cuatro ámbitos de la confianza digital.

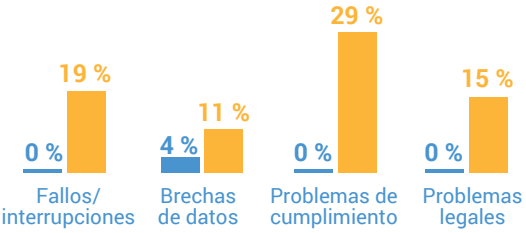
Confianza para TI empresarial

En este primer ámbito, los líderes obtienen resultados considerablemente mejores. Experimentan muchos menos problemas relacionados con la confianza empresarial (apenas sufren fallos, se producen pocas brechas de datos y no tienen problemas legales ni de cumplimiento).

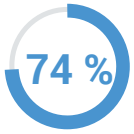
En torno a tres cuartos de los líderes (el 74 %) dicen que pueden responder a los fallos extremadamente rápido, cifra que se queda en el 59 % en el caso de los rezagados.

Los líderes son casi seis veces más propensos a decir que están preparados para la informática poscuántica **(el 59 %, en comparación con el 11 % de los rezagados)**.

Tuvieron menos problemas relacionados con sus iniciativas de confianza empresarial:



Respuesta más rápida ante los fallos



Porcentaje de líderes que responden extremadamente rápido

Porcentaje de rezagados que responden extremadamente rápido

Más preparados para la informática poscuántica

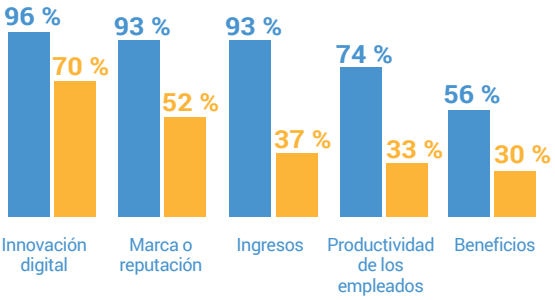
Porcentaje de líderes que están preparados

Porcentaje de rezagados que están preparados

Más rapidez a la hora de prepararse para la informática poscuántica

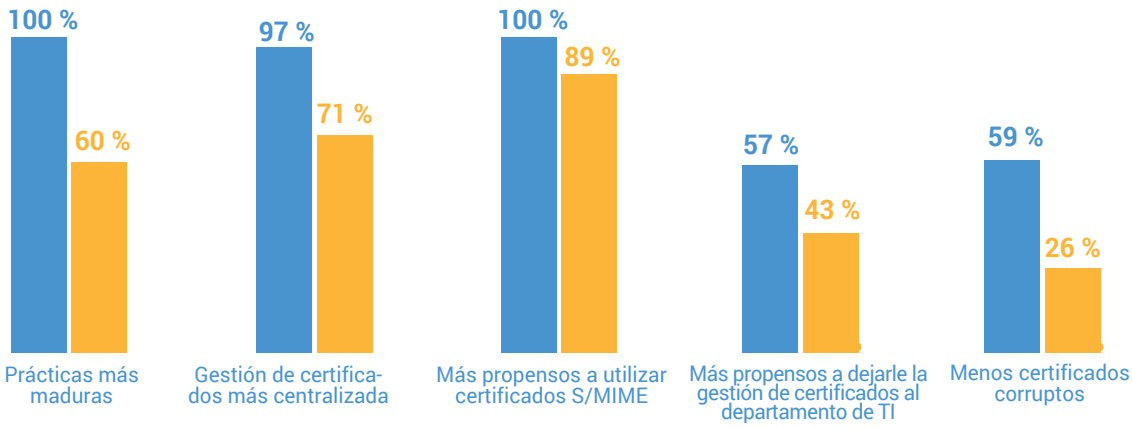
Los líderes tardarán dos años en prepararse y los rezagados, tres.

La confianza empresarial ha ayudado considerablemente a las empresas en estos ámbitos:



¿Qué hacen los líderes que no hacen los rezagados?

Para empezar, el 100 % de los líderes en confianza para TI empresarial aseguran que sus prácticas se encuentran en un estado de madurez extrema. Sus procesos están más centralizados, utilizan certificados S/MIME para proteger las comunicaciones por correo electrónico y gestionan los certificados en el departamento de TI. También afirman tener menos certificados corruptos.

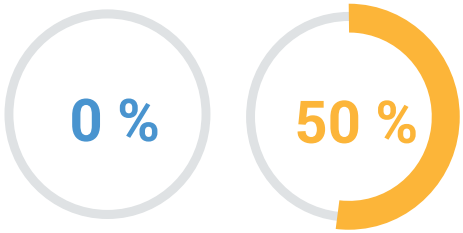


Confianza digital para dispositivos IoT y conectados

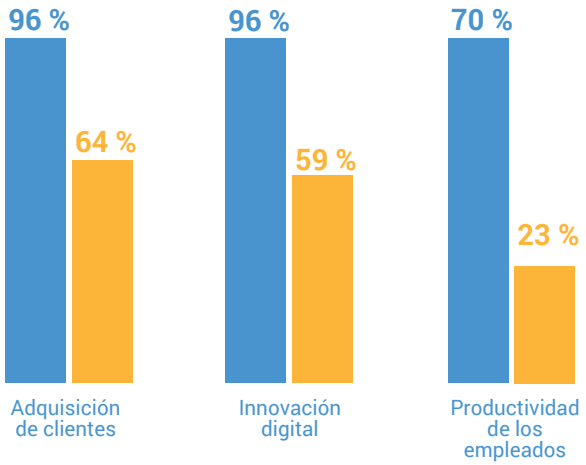
A continuación, nos centramos en los profesionales de la confianza digital para dispositivos IoT y conectados. También en este frente, los líderes obtienen resultados considerablemente mejores que los rezagados. Los primeros no tuvieron ningún problema de cumplimiento relacionado con la confianza para dispositivos IoT y conectados, mientras que la mitad de los rezagados **(el 50 %)** sí tuvieron problemas de este tipo.

Las empresas líderes también tenían la sensación de que se beneficiaban más de sus iniciativas de confianza en este ámbito. Tanto es así que casi todas ellas (el 96 %) dijeron que las ayudaban con la adquisición de clientes y con la innovación digital, y la mayoría de ellas (el 70 %) aseguraron que contribuyen a mejorar la productividad de los empleados. Esto contrasta con el 64 %, el 59 % y el 23 %, respectivamente, en el caso de las empresas rezagadas.

Tuvieron menos problemas de cumplimiento



La confianza para IoT ha ayudado considerablemente a las empresas en estos ámbitos:

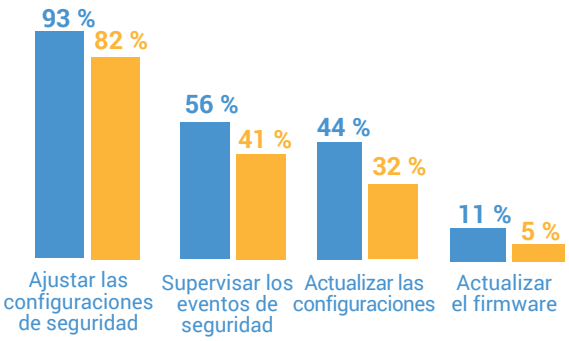


¿En qué se diferencian las prácticas de unos y otros?

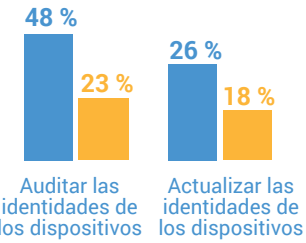
En primer lugar, los líderes están mejor preparados para supervisar los dispositivos en uso y hacer cambios en ellos, así como para auditar y actualizar las identidades de los dispositivos.

Por último, NINGUNA de las empresas rezagadas siente que está extremadamente preparada para afrontar problemas con el IoT, mientras que el 19 % de los líderes aseguran estarlo.

Mayor facilidad para hacer cambios en los dispositivos en uso:

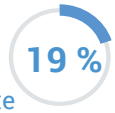


Mayor capacidad para:



Más preparados para hacer frente a los problemas con la confianza para IoT

Porcentaje de rezagados que están extremadamente preparados.



Porcentaje de líderes que están extremadamente preparados.

Confianza para el software

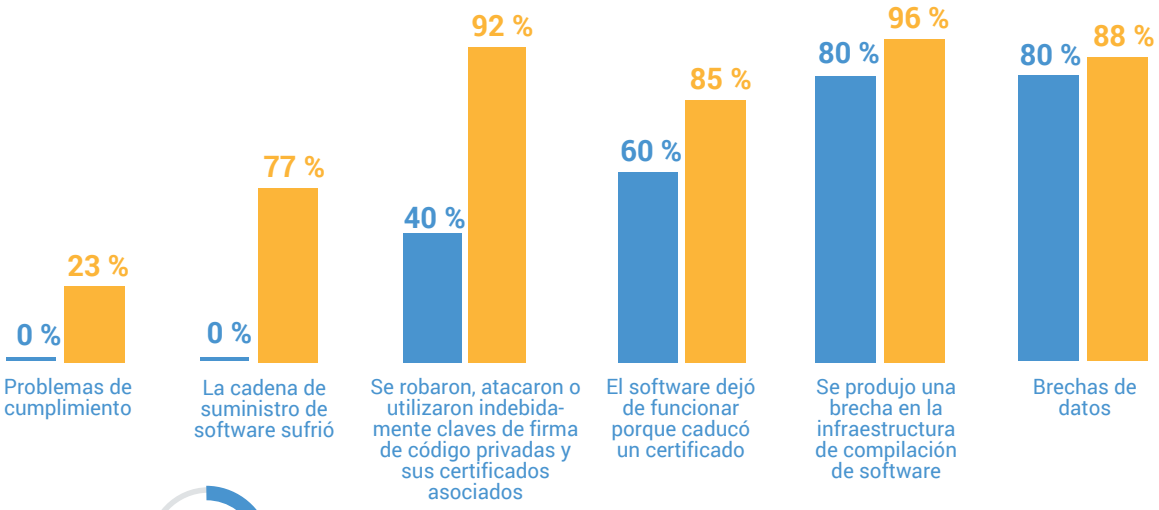
A continuación, pasamos a los profesionales de la confianza para el software. En ese ámbito, los líderes siguen obteniendo resultados mejores que los rezagados y sufren muchos menos problemas derivados de percances con la confianza para el software. Por ejemplo, ninguno de los líderes tuvo problemas de cumplimiento ni sufrió ataques a la cadena de suministro de software, cosas que sucedieron al 23 % y el 77 % de los rezagados, respectivamente.

Además, uno de cada cinco líderes **(el 20 %)** asegura que sus prácticas de confianza se encuentran en un estado de madurez extrema, algo que no se atreve a decir ninguno de los rezagados.

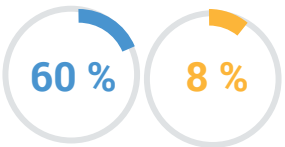
Los líderes también obtienen resultados mucho mejores en lo que a cumplimiento se refiere (el 60 %, en comparación con solo el 8 % de los regazados).

Por último, los líderes aseguran que sus iniciativas de confianza para el software han tenido consecuencias más positivas para la empresa en su conjunto que en el caso de los rezagados, y que les ayudan en ámbitos como la innovación digital, la adquisición de clientes y la productividad de los empleados.

Los líderes tienen menos problemas derivados de percances con la confianza

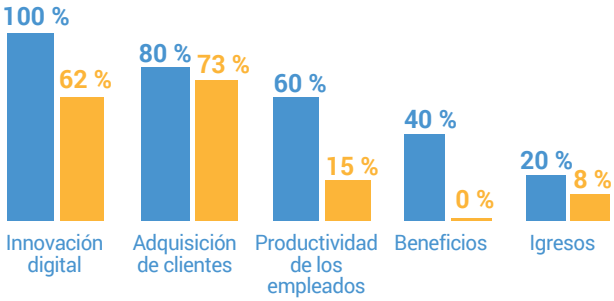


Porcentaje de líderes con prácticas de confianza extremadamente maduras para el software, en comparación con el **CERO POR CIENTO** de los rezagados.



Los líderes están obteniendo resultados extremadamente buenos en materia de cumplimiento normativo.

La confianza para el software ha ayudado considerablemente a las empresas en estos ámbitos:



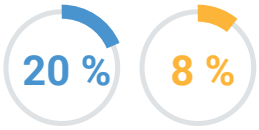
¿Qué hace destacar a los líderes?

El número de líderes que tienen establecido un proceso de aprobación oficial para acceder a las claves criptográficas es el doble que el de los rezagados (el 80 % en el primer caso y el 38 % en el segundo).

Además, hay muchos más líderes que aseguran que les resulta extremadamente sencillo elaborar una lista de todos los componentes de software y de sus configuraciones para el software que desarrollan (el 20 %, y solo un 8 % en el caso de los rezagados).

Más propensos a tener un proceso de aprobación para acceder a cualquier clave.

A los líderes les resulta extremadamente sencillo elaborar una lista de todos los componentes de software y de sus configuraciones para el software que desarrollan.



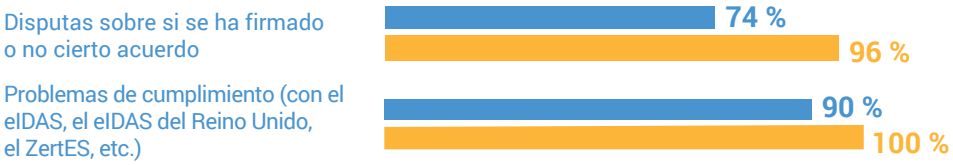
Confianza para la firma electrónica

El último grupo al que encuestamos estaba formado por profesionales de la confianza para la firma electrónica, un ámbito que suele gestionar personal sin conocimientos técnicos especializados (responsables del departamento jurídico, de RR. HH. o de ventas, por ejemplo). Sin la participación del equipo de TI, se desperdician las capacidades técnicas que ayudarían a gestionar todos los aspectos de las iniciativas de confianza para la firma electrónica, y eso queda patente en los resultados.

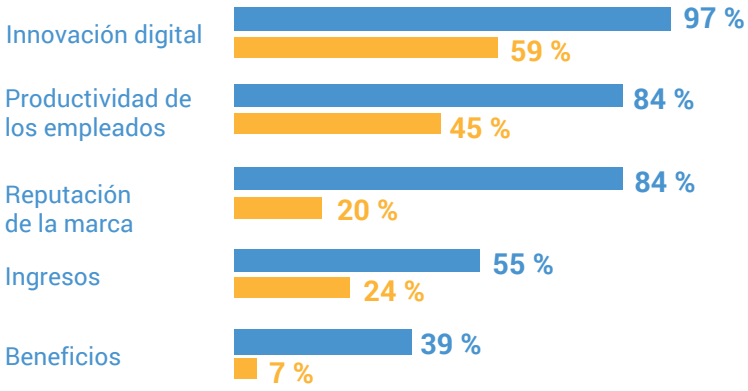
Por ejemplo, aunque hay más líderes que rezagados que sostienen que sus prácticas de confianza para la firma electrónica se encuentran en un estado de madurez extrema, la cifra sigue siendo baja (el 10 %). Por otra parte, gracias a sus iniciativas en este ámbito, los líderes tienen menos problemas y más ventajas empresariales que los rezagados.

Porcentaje de líderes con prácticas de confianza extremadamente maduras para la firma electrónica, en comparación con el CERO POR CIENTO de las empresas del tercio inferior.

Los líderes tienen menos problemas relacionados con la confianza para firmas electrónicas:

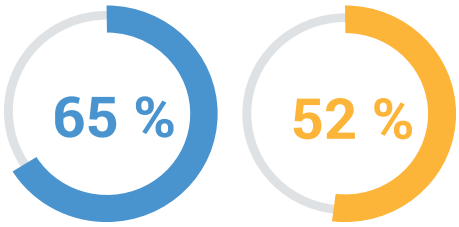


La confianza para firmas electrónicas ha ayudado considerablemente a las empresas en estos ámbitos:



¿Qué caracteriza a los líderes?

En esencia, estas diferencias se deben a una cualidad fundamental: los líderes están más maduros con respecto a la comprensión, implementación y gestión de políticas y controles para los sellos y firmas electrónicos.



Los líderes están más maduros con respecto a la comprensión, implementación y gestión de políticas y controles para los sellos y firmas

CONCLUSIONES A LAS QUE HA LLEGADO DIGICERT

A medida que se multiplican las amenazas, crece también la brecha entre las empresas a la vanguardia de la confianza digital y aquellas que se están quedando a la zaga. Los líderes y los rezagados son conscientes de sus carencias, por lo que el verdadero riesgo reside en las empresas que ocupan el tercio intermedio de la clasificación, que muchas veces tienen la falsa sensación de estar bien protegidas. Si se sigue abusando de este exceso de confianza, la brecha seguirá ensanchándose y las consecuencias podrían llegar a ser muy graves.

¿Qué deberían hacer las empresas para optimizar sus iniciativas de confianza digital en general y, en concreto, las relativas a ámbitos específicos como el de la confianza para la TI empresarial, el software, los dispositivos y los documentos?

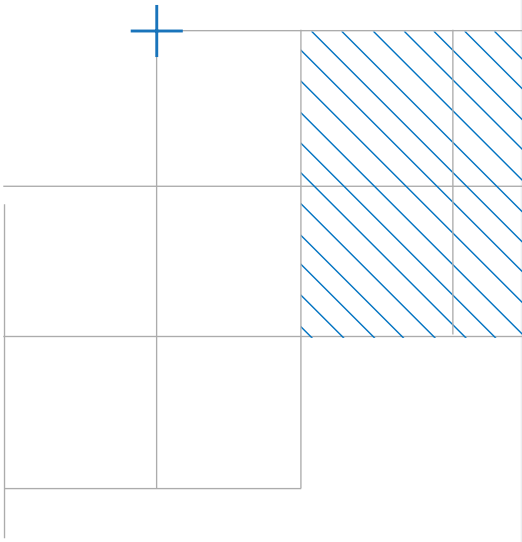
DigiCert es el principal proveedor global de confianza digital. Gracias a él, tanto los usuarios individuales como las empresas pueden utilizar Internet con la tranquilidad de saber que su presencia en el mundo digital está protegida. Llevamos más de dos décadas trabajando en el ámbito de la confianza digital, y nuestro consejo para las empresas que quieran cosechar el mismo éxito que los líderes es que se aseguren de seguir estas pautas:

Hacer inventario

Eso que se suele decir de que no se puede gestionar lo que no se ve no es menos cierto en el caso de la confianza digital. Por eso es importante tener una visión completa de cómo se crean, protegen y utilizan las identidades digitales y claves criptográficas dentro de la empresa. Para lograrlo, tiene dos opciones: examinar a mano los procesos empresariales o utilizar la tecnología para analizar el entorno constantemente y procesar datos de otras fuentes como los sistemas de gestión de activos de TI.

Definir políticas

Existen multitud de opciones de políticas que le ayudarán en su misión de alcanzar la confianza digital. Las empresas deberían definir políticas que permitan autenticar los dispositivos y a los usuarios de forma segura, tanto en el caso de plantillas remotas como tradicionales. Determine qué políticas hacen falta para garantizar el cumplimiento de las normativas, sobre todo para los fabricantes de dispositivos médicos y otros sectores muy regulados. Si su empresa publica software crítico para el negocio, defina políticas que garanticen la seguridad de la cadena de suministro de software. Establezca iniciativas «zero trust» o perfecciónelas si ya las tiene, especialmente para las cargas de trabajo en la nube que procesan datos regulados y confidenciales. Estos ejemplos de políticas serían complementarios a las políticas básicas que rigen el uso de la criptografía y la infraestructura de clave pública en el seno de la empresa.



Centralizar la gestión de la PKI

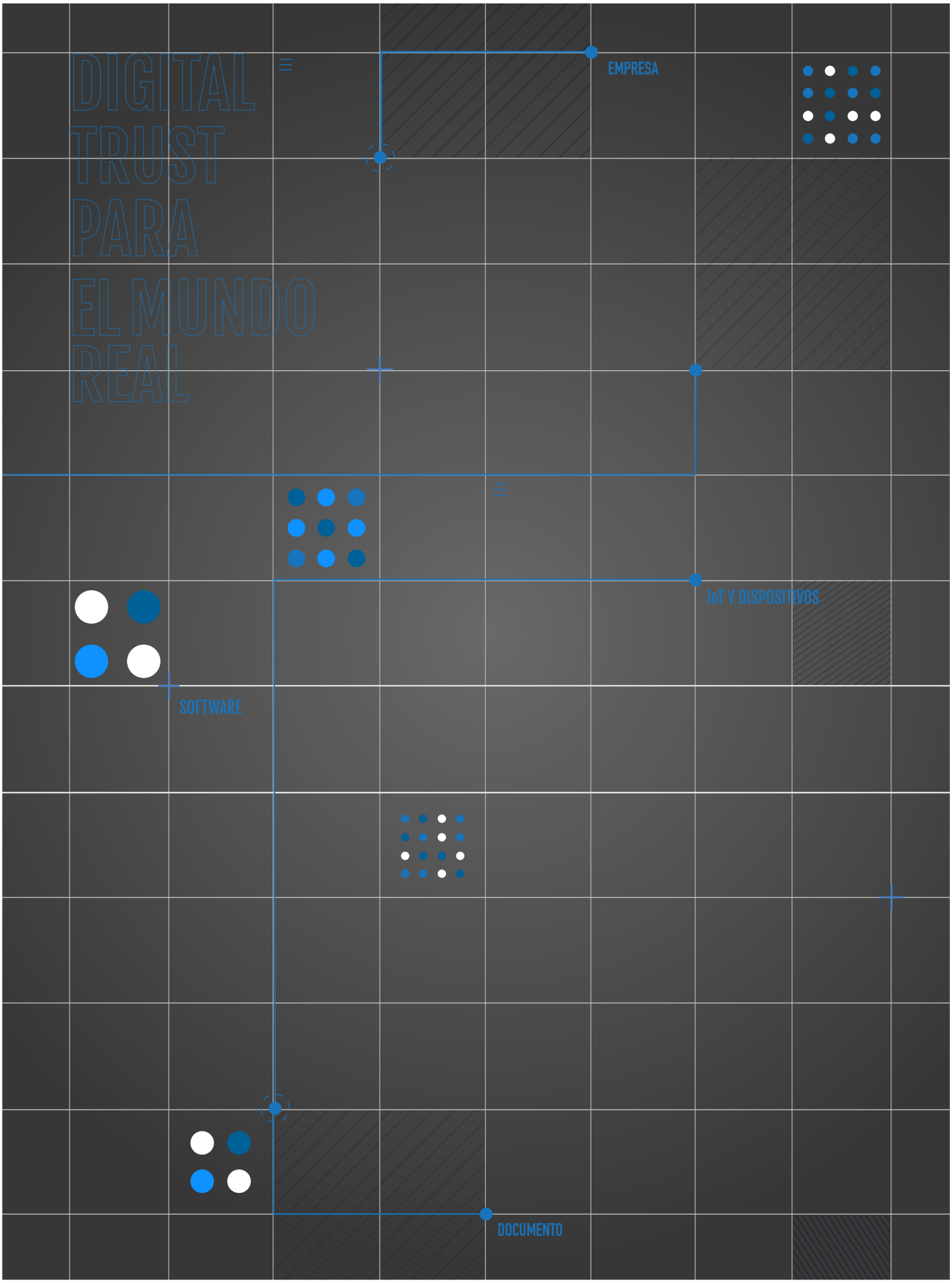
Las empresas necesitan cierto nivel de «agilidad criptográfica», esto es, la capacidad de actualizar y corregir los activos criptográficos con rapidez. Para evitar interrupciones en el futuro y minimizar el riesgo, le recomendamos implementar herramientas que le permitan centralizar y automatizar la gestión de los certificados digitales y la PKI. Hacerlo le reportará varias ventajas, como una seguridad reforzada, una mayor eficiencia y una administración más sencilla.

Priorizar lo más importante para el negocio

Repase el inventario para identificar aquellos activos relacionados con los procesos y aplicaciones críticos para el negocio. Estos son los aspectos en los que debería centrarse primero. Corrija las posibles vulnerabilidades de seguridad antes de pasar a implementar soluciones para optimizar las tareas que contribuyen a garantizar la confianza digital. Por ejemplo, haga lo necesario para que los usuarios puedan incorporar en sus dispositivos el acceso remoto seguro de manera automática y sencilla, sin necesidad de que intervenga el equipo de TI. Agilice y proteja la emisión e instalación de certificados de servidor para blindar los datos y las comunicaciones. Al hacerlo, estará reforzando la seguridad en la nube.

Conclusión

Las empresas que hacen de la confianza digital una prioridad disfrutan de una imagen de marca más sólida, se exponen a menos riesgos de ciberseguridad y consiguen operaciones más eficientes. Los clientes, socios y demás partes interesadas confían en ellas por su transparencia y las medidas de seguridad que siguen. Establecer la confianza digital permite sortear las dificultades derivadas de las normativas, lo que garantiza su cumplimiento y reduce el riesgo de enfrentarse a problemas legales y financieros. De esta forma, los datos están blindados y la resiliencia, garantizada. Es la manera de afrontar las amenazas que van surgiendo en el entorno digital de hoy en día.


DIGITAL
TRUST
PARA
EL MUNDO
REAL
EMPRESA
IoT Y DISPOSITIVOS
SOFTWARE
DOCUMENTO