

Un marco de políticas para una Internet abierta y de confianza

Un enfoque para reforzar la confianza en un entorno abierto*



March 2017

Resumen ejecutivo

- La disminución de la confianza es un desafío para Internet. Para proteger las oportunidades de Internet, debemos contrarrestar esta disminución.
- La filtración de datos a gran escala, la incertidumbre acerca de cómo se está utilizando la información, el cibercrimen, la vigilancia y otras amenazas en línea están afectando la confianza que los usuarios tienen en Internet, y cómo la utilizan. También están obstaculizando la adopción de Internet.
- Hoy en día, los creadores de políticas se enfrentan a un importante desafío: incorporar plenamente la revolución digital y al mismo tiempo asegurar la protección y la seguridad de sus ciudadanos.
- La Internet Society cree que, para alcanzar su máximo potencial, Internet necesita estar sólidamente fundada en la confianza. La confianza es un pilar fundamental para cualquier estrategia de conectividad exitosa, tanto en los países desarrollados como en los países en desarrollo. Esto solo se puede lograr a través de la responsabilidad colectiva y la colaboración.
- Una "Internet abierta y de confianza" es una Internet interoperable globalmente que cultiva la innovación y crea oportunidades para todos. Está fundada en la confianza de los usuarios, en tecnologías de confianza, en redes de confianza y en un ecosistema confiable.
- Este marco de políticas define un enfoque para abordar las complejidades que implica la construcción de confianza en un entorno abierto tal como es Internet. Describe **cuatro dimensiones interrelacionadas de confianza que deben considerarse al desarrollar políticas para Internet y proporciona principios para ayudar a construir una Internet de confianza.**

* Este marco no ha sido diseñado para abordar cuestiones de guerra cibernética.

Introducción

Una Internet abierta ofrece oportunidades sociales y económicas para todos. Sin embargo, Internet solo alcanzará su máximo potencial si está sólidamente fundada en la confianza. Una encuesta reciente realizada en Estados Unidos descubrió que el 45% de los usuarios había cambiado su comportamiento en línea debido a sus miedos. Artículos publicados alrededor del mundo expresan preocupaciones similares. Los usuarios de Internet están ansiosos sobre cómo los gobiernos y negocios utilizan su información. Sienten una falta de control y se preocupan por el establecimiento de perfiles de usuarios y la discriminación. También temen convertirse en víctimas de la filtración de datos, el robo de identidad y otras formas de ciberdelito. Para algunos, este escenario ya se ha convertido en una realidad. Además, los usuarios de Internet están preocupados por el impacto que tiene la vigilancia generalizada sobre su privacidad y sus derechos.

Muchos gobiernos están evaluando los efectos de Internet en la sociedad. Hay quienes creen que Internet está habilitando e intensificando las amenazas de parte de criminales, otros estados e incluso de sus propios ciudadanos. Están respondiendo con mayores controles gubernamentales, tales como la restricción del acceso a contenido y la prohibición del uso de las redes sociales. Algunos han impuesto medidas de localización de los datos para mantener el tráfico de Internet dentro de sus propias fronteras. Otros han considerado prohibir tecnologías de confianza claves (por ejemplo, el cifrado) u obligar a los proveedores de tecnología a crear debilidades en sus productos en la creencia de que estas tecnologías afectarán la capacidad de las autoridades de combatir el crimen. Sin embargo, sin el cifrado y otras tecnologías de confianza, no habría actividades bancarias seguras ni confidencialidad en las comunicaciones para *ningún* usuario de Internet. Estas políticas resultan contrarias a lo que realmente se necesita: dañan aun más la confianza del usuario, eliminan oportunidades y reprimen la innovación.

Para alcanzar su máximo potencial, Internet necesita estar sólidamente fundada en la confianza .

Hoy en día, los creadores de políticas tienen que decidir qué camino tomar al desarrollar políticas para Internet. Un camino lleva a una Internet abierta y de confianza con todos los beneficios económicos y sociales que esto implica. El otro camino lleva a una red cada vez más cerrada, en la cual los usuarios no confían y que no logra impulsar el crecimiento. Un camino lleva a las oportunidades, mientras que el otro conduce al estancamiento. Lo esencial es la confianza y cómo mantener la red como un espacio fundamentalmente dinámico que inspire confianza.

Internet: confianza en un entorno abierto

Una “Internet abierta y de confianza” es una red de redes globalmente interoperable y distribuida que cultiva la innovación y crea oportunidades para todos. Se fundamenta en la confianza del usuario, en tecnologías de confianza, en redes de confianza y en un ecosistema confiable. Ofrece una gobernanza inclusiva, está construida sobre principios de políticas sólidos y lucha por poner a los intereses de los usuarios de Internet en el centro de sus decisiones.

Una “Internet de confianza” no es una utopía aislada y exenta de las amenazas del mundo. Siempre habrá riesgos y desventajas para un sistema de red abierta. Los actores malintencionados encontrarán formas de explotar las vulnerabilidades. Las tecnologías y habilidades que desarrollamos para mejorar una parte de nuestra vida puede tener un impacto negativo sobre otra. No obstante, las amenazas pueden mitigarse, los riesgos pueden distribuirse y las debilidades pueden compartirse y repararse. La transparencia de Internet también es la forma de protegerla.

Todos las partes interesadas deben desempeñar un papel positivo para fomentar una Internet abierta y de confianza. Debemos trabajar para asegurar los aspectos centrales de la infraestructura de Internet, para proteger la confidencialidad y la integridad de los datos que fluyen sobre la red y para asegurar que existan políticas adecuadas que apoyen las tecnologías, redes y actores que permiten el funcionamiento de Internet. Esto se logra a través de la colaboración y la responsabilidad colectiva.

Se puede encontrar un fundamento útil en los principios descritos en el informe Seguridad colaborativa: cómo fomentar la confianza y proteger las oportunidades – responsabilidad colectiva, valores y propiedades fundamentales, evolución y consenso, y pensar de forma global, actuar de forma local–.

Este marco de políticas de la Internet Society para una Internet abierta y de confianza define un enfoque para abordar las complejidades que implica la construcción de confianza en un entorno abierto tal como es Internet. Se describe a través de cuatro dimensiones de confianza interrelacionadas que es necesario considerar al desarrollar políticas para Internet y proporcionan principios para construir una Internet de confianza.

Este marco para una Internet de confianza recoge las diferencias importantes y valiosas que le otorgan a nuestro mundo su diversidad. No hay una solución única que sirva para todas las decisiones que se toman sobre Internet. Las políticas para Internet pueden tomar muchas formas distintas de acuerdo con las necesidades concretas de cada país. Sin embargo, existe algo que todas comparten: su punto de partida es siempre “*¿Cómo podemos crear confianza en un entorno abierto como lo es Internet?*”



Fig. 1 - Las cuatro dimensiones para una Internet abierta y de confianza

Confianza de los usuarios: Cómo y por qué los usuarios de Internet –incluyendo los gobiernos, el sector privado y los ciudadanos– confían en Internet y cómo construir esa confianza.

Tecnologías para la confianza: Componentes técnicos para establecer y mantener redes, aplicaciones y servicios de confianza.

Redes de confianza: La fuerza de Internet reside en que se trata de una colección de redes interconectadas en constante evolución cuyo control y propiedad están distribuidos. La confianza es el elemento que mantiene a las redes conectadas e intercambiando información.

Ecosistema confiable: Gobernanza de Internet y resolución de sus conflictos.

Esta división tiene su origen en la naturaleza modular y estratificada de Internet. Una red de redes de confianza ofrece un alcance global, mientras que un conjunto de tecnologías para la confianza permite que las aplicaciones que utilizan Internet proporcionen confidencialidad, integridad y capacidad de autenticación. Con todos estos aspectos técnicos en su lugar, un ecosistema confiable permite una confianza sistémica, mientras que la confianza de los usuarios es el motor de toda la creatividad e innovación que vemos en Internet.

La confianza no es solamente una linda idea. Se trata de un conjunto de elecciones, herramientas y capacidades ya programadas en la Internet abierta.

Confianza de los usuarios

Todos los que utilizan Internet son “usuarios de Internet”, ya sean funcionarios de gobierno, anunciantes, maestras, agentes de viaje, estudiantes o artistas. Todos los días decidimos cuánto confiar (o no confiar) en Internet para nuestras interacciones sociales, profesionales o financieras, entre otras.

La confianza de los usuarios es importante para el futuro éxito de Internet, ya que, si sus usuarios no confían en ella, restringirán su uso e incluso podrán dejar de usarla para ciertas actividades. Esto podría tener un fuerte impacto en la evolución de Internet, así como en su uso y crecimiento.

Desde 1996, el Consejo de Arquitectura de Internet, la organización que supervisa el desarrollo de los protocolos técnicos de Internet, reconoció que el crecimiento de Internet dependía de que los usuarios tuvieran confianza en que la red protegería su información y comunicaciones ([RFC 1984](#)).

Sin embargo, construir la confianza de los usuarios no significa simplemente tranquilizar a las personas y esperar que los resultados sean positivos. Construir la confianza de los usuarios significa desplegar la infraestructura adecuada (redes de confianza), motivar a los usuarios para que protejan sus actividades (**tecnologías para la confianza**), establecer **políticas** apropiadas y generar un entorno receptivo que aborde de forma adecuada las preocupaciones justificadas (**ecosistema confiable**).

Los principios de políticas para mejorar la confianza de los usuarios le permiten a los individuos y organizaciones tomar decisiones informadas y racionales sobre cómo utilizar Internet.

Todos nosotros –los gobiernos, el sector privado, la sociedad civil y los ciudadanos– somos usuarios de Internet. Si nos preguntáramos “qué podemos hacer para lograr que Internet sea mejor para nosotros como usuarios?” ya estaríamos a mitad de camino hacia la construcción de una Internet de confianza.

Principios de políticas para apoyar la confianza de los usuarios

Derechos humanos: Las consideraciones sobre los derechos humanos deberían integrarse en las políticas de Internet durante su desarrollo, no añadirse como una idea complementaria. Los derechos de los individuos deben protegerse en Internet.

Confidencialidad en las comunicaciones: Las políticas de Internet deberían apoyar el principio que establece que los usuarios de Internet deben tener la posibilidad de comunicarse en línea de forma confidencial. También deberían incentivar la innovación y el uso de herramientas para facilitar las comunicaciones confidenciales (por ejemplo, el cifrado).

Privacidad: Los derechos y expectativas de privacidad de los individuos se deberían proteger en Internet, independientemente de su nacionalidad o lugar de residencia. No debería haber una vigilancia generalizada de las comunicaciones en Internet. Los individuos deberían tener la posibilidad de comunicarse de forma anónima o seudónima.

Protección del consumidor: Los derechos de los consumidores deberían respetarse en toda la red. Los gobiernos deberían apoyar la confianza del consumidor mediante la promulgación y ejecución de leyes de protección que se apliquen a los negocios realizados en su territorio o que se encuentren bajo su control. También deberían participar en instancias de cooperación internacional transfronterizas para asegurar que los derechos de los consumidores estén protegidos sin importar donde estos vivan.

Control sobre la información: Los usuarios de Internet deberían poder ejercer control sobre su información. Deberían poder trasladar sus datos de un servicio a otro.

Transparencia en la formulación de políticas: Los gobiernos deberían ser abiertos y transparentes con respecto a sus decisiones, políticas, leyes y prácticas. Deberían incluir a las partes interesadas de forma activa en el desarrollo de políticas de Internet.

Certeza legal: Los gobiernos deberían asegurar que las leyes sean claras, fáciles de comprender y accesibles para todos. Deberían abstenerse de ejercer poderes legislativos y ejecutivos en forma caprichosa o arbitraria.

Ejecución y reparaciones: Los gobiernos deberían asegurar que las autoridades regulatorias tengan los recursos y la independencia necesarios para hacer cumplir las leyes y ofrecer reparaciones a los usuarios de Internet que hayan sufrido pérdidas, daños o que hayan sido perjudicados de otra forma.

No discriminación: Los gobiernos también deberían asegurar sus leyes y políticas para evitar que Internet se use como un medio para discriminar a un individuo sobre la base del grupo, clase o categoría al se percibe que dicha persona o cosa pertenece, ni en función de la creación de perfiles de datos.

Controles e informantes: Todas las partes interesadas deberían reconocer y apoyar el valor que las organizaciones de control y los informantes proporcionan a la sociedad.

Tecnologías para la confianza

Las tecnologías para la confianza son los componentes técnicos que permiten establecer y mantener redes, aplicaciones y servicios de confianza. Son el fundamento técnico para una Internet de confianza.

Una tecnología de confianza utilizada comúnmente es el protocolo de seguridad en la capa de transporte (TLS), un protocolo de cifrado que se utiliza para proporcionar confidencialidad e integridad a las comunicaciones, por ejemplo, entre un dispositivo de un usuario y el servidor de una página web. El TLS se desarrolló a través de un proceso abierto en el Grupo de Trabajo en Ingeniería de Internet (IETF). Hoy en día, prácticamente todos los servicios bancarios y gubernamentales en línea utilizan TLS.

Las tecnologías de confianza son importantes para reforzar la confianza en Internet, ya que son las herramientas técnicas que permiten a los usuarios de Internet comunicarse de forma privada (confidencialidad), conocer con quién se están comunicando (autenticación), saber que la información que están mandando o recibiendo no se ha alterado en tránsito (integridad), restringir el acceso a sus datos o comunicaciones (autorización) y conocer si se ha manipulado su dispositivo o tecnología (detección de manipulación y resistencia).

Estas tecnologías se utilizan para asegurar las redes, aplicaciones y servicios que utilizamos todos los días. Sin tecnologías de confianza tales como el TLS y sus antecesores, nunca habríamos visto el auge del comercio electrónico que impulsa el crecimiento del PBI y propaga las oportunidades globalmente. Sin cifrado de las comunicaciones, los gobiernos, las empresas y los individuos no podrían mantener sus comunicaciones confidenciales ni su información segura.

Las tecnologías para la confianza evolucionaron gracias a una característica fundamental de la Internet abierta: la innovación que no requiere permiso previo ni una aprobación especial de una autoridad. La innovación sin pedir permiso construyó la Internet y es esencial para la salud del futuro de la red y de las economías que de ella dependen.

A medida que las amenazas continúen apareciendo y creciendo, debemos asegurarnos de tener todas las herramientas necesarias para mantener la privacidad, la seguridad y, en última instancia, las oportunidades sociales y económicas.

Necesitamos políticas que apoyen el desarrollo, la disponibilidad y el uso de tecnologías de confianza, no que lo dificulten.

Dependemos de las tecnologías para la confianza todos los días, para asegurar nuestras redes, nuestras transacciones e incluso nuestras vidas. Por esta razón, deben ser tan sólidas y ubicuas como sea posible.

Principios de políticas para apoyar el uso de tecnologías de confianza

Los gobiernos deberían:

- motivar a los usuarios para que adopten sus propias medidas técnicas para proteger sus datos y sus comunicaciones en Internet;
- incentivar el desarrollo y el acceso abierto a herramientas "fáciles de usar" que permitan a los usuarios comunicarse de forma confidencial;
- estimular a los proveedores de servicios en línea para que ofrezcan a sus clientes soluciones integrales de cifrado.

Con respecto al cifrado:

(Estas recomendaciones resumen los principios de la iniciativa www.securetheinternet.org apoyada por muchas empresas, individuos y organizaciones, incluida la Internet Society.)

Los usuarios de Internet tienen la opción de utilizar, y las empresas deberían tener la libertad de proporcionar, el cifrado más potente disponible, incluido el cifrado de extremo a extremo, sin temor de que los gobiernos obliguen a permitir el acceso al contenido, a los metadatos o a las claves de cifrado sin el debido proceso y respeto por los derechos humanos.

Los gobiernos no deberían prohibir o limitar el acceso de los usuarios al cifrado de ninguna forma, ni prohibir la implementación o el uso del cifrado por grado o por tipo.

Los gobiernos no deberían exigir el diseño o la implementación de "puertas traseras" o vulnerabilidades en las herramientas, tecnologías o servicios.

Los gobiernos no deberían exigir que las herramientas, tecnologías o servicios estén diseñados o desarrollados para permitir que terceros accedan a los datos no cifrados o a las claves de cifrado.

Los gobiernos no deberían buscar debilitar o socavar los estándares de cifrado o influenciar de forma intencional el establecimiento de estándares de cifrado salvo para promover un alto nivel de seguridad de la información. Ningún gobierno debería exigir tecnologías, herramientas, estándares o algoritmos de cifrado no seguros.

Los gobiernos no deberían obligar o presionar a ninguna entidad, ya sea mediante un acuerdo público o privado, a participar en actividades que no sean consistentes con sus principios.

Redes de confianza

La Internet es un conjunto de redes interconectadas en continua evolución, sin propietario común ni control centralizado. La confianza es el elemento que mantiene a las redes conectadas e intercambiando información.

La construcción y mantenimiento de una Internet de confianza implica que diferentes actores –con diferentes papeles y responsabilidades– deben tomar medidas, lo más cerca posible del lugar donde ocurren los conflictos.

No existe tal cosa como una única red global, sino que Internet es una red de redes. Los caminos que siguen las comunicaciones no se deciden por adelantado y no respetan las fronteras nacionales. Los usuarios de Internet no deciden cómo se envían sus comunicaciones, sino que simplemente “confían” que los operadores de red entregarán los datos al lugar debido. Esta estrategia de transporte puede parecer caótica, pero proporciona resiliencia y velocidad en una escala que la humanidad nunca había logrado antes.

En este contexto, la confianza no es una esperanza o un sentimiento, sino que es una forma recíproca y práctica de realizar negocios. Los operadores de red confían que sus pares llevarán a cabo las operaciones necesarias para proporcionar comunicación de extremo a extremo. Si un operador no logra mantener esta confianza, sus pares encontrarán otras maneras de enviar su tráfico y simplemente dejarán de tener trato con el mismo. Este enfoque es importante porque proporciona opciones viables y no permite que el sistema se rompa.

La clave de las redes de confianza es **la responsabilidad colectiva y la colaboración**. Esta es la noción de que todas las partes interesadas deben colaborar y compartir la responsabilidad para abordar las cuestiones de Internet.

Los elementos centrales de las redes de una Internet de confianza son los Invariantes de Internet de la Internet Society y los principios de Seguridad colaborativa.

La adopción de estos elementos centrales como fundamento para la toma de decisiones crea un entorno en el que las redes de confianza podrán continuar evolucionando y creciendo.

Principios de políticas para apoyar las redes de confianza

Seguridad:

Las estrategias y políticas nacionales de ciberseguridad deberían promover la prosperidad económica y social y no deberían impedir el crecimiento, la innovación o el desarrollo.

Al desarrollar las estrategias y políticas de ciberseguridad, los gobiernos deberían recoger la experiencia de todas las partes interesadas y trabajar junto con ellas para desarrollar soluciones de forma colaborativa.

Las políticas de ciberseguridad deberían integrar los derechos humanos; su objetivo debería ser ofrecer protección y seguridad y a la vez preservar los derechos de los individuos.

Los gobiernos deberían liderar dando el ejemplo, pero también reconocer que algunas de las partes interesadas podrían ser líderes en sus áreas. Algunas veces, las mejores soluciones son aquellas que surgen de forma orgánica sin ninguna dirección gubernamental. Se deberían definir e implementar soluciones en aquellas áreas donde puedan tener mayor impacto.

La colaboración transfronteriza será esencial para mantener la seguridad y la resiliencia de Internet.

Conexión de redes y envío de tráfico:

Los gobiernos no deberían exigir la localización de los datos ni prescribir rutas para el tráfico de Internet.

Los gobiernos deberían alentar a las empresas regionales e internacionales para que participen en un entorno de peering e interconexión local (por ejemplo, reduciendo las barreras y/o proporcionando incentivos económicos).

Los gobiernos deberían promover la inversión en más infraestructura de Internet (por ejemplo, cables submarinos, IXPs e infraestructuras nacionales) para lograr una mayor resiliencia que beneficie al ecosistema de Internet en su conjunto.

Los gobiernos deberían proporcionar un entorno legal que apoye los mercados competitivos en los servicios en línea.

Estándares técnicos abiertos:

Las políticas deberían apoyar una Internet construida sobre estándares técnicos abiertos. Las partes interesadas pueden mostrar su apoyo respaldando y promoviendo los Principios OpenStand.

Ecosistema confiable

Cuando los gobiernos elaboran políticas para Internet, no solo piensan en responder a la pregunta “¿confiamos en Internet para nuestro propio uso?”. También consideran el impacto que Internet puede tener en la seguridad y bienestar de sus ciudadanos, su economía, su soberanía, así como en “quién tiene el control”. Al equilibrar todos estos intereses, surge una ecuación de confianza mucho más compleja que la confianza de los usuarios. Sin embargo, es fundamental abordarla, dado que esta es la razón por la cual los gobiernos se enfocan tan intensamente en la confiabilidad del ecosistema de Internet y su gobernanza.

La confiabilidad del ecosistema de Internet surge a partir de la forma en que se desarrolló la red de redes y de sus procesos de gobernanza de múltiples partes interesadas, donde quienes se ven afectados por las decisiones tienen la oportunidad de ser parte de las mismas.

Internet se ha convertido en una plataforma global para la innovación y el crecimiento económico a través de procesos participativos de abajo hacia arriba, priorizando la estabilidad e integridad de los sistemas y manteniendo la naturaleza abierta de las tecnologías subyacentes. Estos principios son parte del “ADN” de Internet.

En esencia, la gobernanza de múltiples partes interesadas personifica la transparencia, la inclusión, la responsabilidad compartida, incorpora la rendición de cuentas (*accountability*) y es eficaz en la resolución de cuestiones comunes de Internet.

A su vez, los miembros de la comunidad técnica compartimos un sentido de supervisión colectiva con respecto al núcleo público de Internet y los estándares abiertos en los que se basan sus tecnologías y redes.

Estas características fortalecen la confianza de las partes interesadas en la forma en que se opera y gobierna el ecosistema de Internet.

Internet no presenta un problema de
“control y comando”, sino que se trata de un
desafío de coordinación. ¿Cómo podemos
trabajar de forma eficaz con quienes son
responsables de sus diferentes partes, siendo
que muchos se encuentran más allá de
nuestras fronteras?

Ecosistema confiable: Atributos de una gobernanza de múltiples partes interesadas exitosa

Inclusión y transparencia: La inclusión es la base de la legitimidad en la toma de decisiones en forma colaborativa. Quienes se ven significativamente afectados por una decisión deberían tener la oportunidad de participar en la toma de la misma. La inclusión no es solamente un objetivo admirable, sino que es una parte esencial de cualquier proceso eficaz. Cuanto menos inclusivo sea un proceso, menos probable será que genere confianza y apoyo entre quienes se encuentran por fuera del mismo. La transparencia es una condición esencial para la inclusión, ya que reúne en el proceso tanto a expertos como a los grupos afectados. La transparencia de las contribuciones, los procesos y la toma de decisiones es fundamental para Internet.

Responsabilidad compartida: Todas las partes interesadas comparten la responsabilidad colectiva por la vitalidad continua de Internet y los beneficios que aporta a nuestra sociedad y a la economía mundial. En la comunidad técnica, compartimos el sentido de supervisión colectiva de Internet y de los estándares abiertos en los que se basan sus tecnologías.

Toma de decisiones e implementación eficaz de las mismas: Las decisiones más eficaces son aquellas que se basan en un proceso abierto y deliberativo que considera una amplia variedad de fuentes de información y perspectivas. Esto es importante tanto para la calidad como para la implementación de la decisión.

Dado que Internet es operada por una variedad de partes interesadas de los sectores público y privado y la sociedad civil, para que las soluciones se puedan implementar de forma exitosa es necesario que sean imaginativas y colaborativas. No es tan sencillo como aprobar una ley nacional. Las partes interesadas que han formado parte de un proceso trabajan más para lograr que su implementación tenga éxito.

Colaboración mediante una gobernanza distribuida e interoperable: Para aprovechar con eficacia los esfuerzos de múltiples actores, la comunidad técnica ha desarrollado sistemas de gobernanza autónomos basados en la colaboración y el respeto mutuo. Las numerosas organizaciones que participan en la gobernanza de Internet desempeñan funciones complementarias. Debemos reconocer esta autonomía y mantener el diálogo y la participación mutua en las áreas en que diferentes organizaciones se solapan.

El siguiente es un resumen de las características de los enfoques para una gobernanza de Internet exitosa incluidas en el documento de la Internet Society titulado *Gobernanza de Internet: ¿Por qué funciona el enfoque de múltiples partes interesadas?*

Conclusión

Para asegurar que los beneficios de la economía digital alcancen a todos los individuos alrededor del mundo y que florezca la innovación, juntos debemos construir una Internet abierta y de confianza. Creemos que este marco de políticas proporciona un enfoque para abordar las complejidades que implica la construcción de confianza en un entorno abierto como es Internet.

A la hora de considerar políticas relacionadas con Internet, les pedimos que tengan en cuenta estas diferentes dimensiones de confianza y cómo se interrelacionan. Cualquier comentario sobre este marco de políticas para una Internet abierta y de confianza será bienvenido. Envíe sus comentarios a trust@isoc.org

Una Internet abierta y de confianza es fundamental para el éxito de la economía digital. Debemos trabajar en forma colaborativa para convertirla en realidad.

